В. Б. Дудикевич, В. О. Хорошко, Ю. Є. Яремчук

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В. Б. Дудикевич, В. О. Хорошко, Ю. Є. Яремчук

Міністерство освіти і науки України
Вінницький національний технічний університет

Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є.

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Вінниця
ВНТУ
2018

УДК 004.056(075.8)
Д81

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 10 від 23.02.2017 р.)

Рецензенти:
Л. М. Щербак, доктор технічних наук, професор
В. В. Козловський, доктор технічних наук, професор
О. Н. Романюк, доктор технічних наук, професор

Дудикевич, В. Б.

Д81 Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.

У посібнику наводяться суть, підходи забезпечення та основні особливості інформаційної безпеки. Розглядаються основні поняття та положення інформаційної безпеки, концепції та моделі інформаційної безпеки, найпоширеніші загрози та методологія формування множини загроз інформації, критерії оцінювання безпеки інформації, політика інформаційної безпеки, основні поняття та етапи керування ризиками інформації, керування доступом до інформації та безпекою інформаційних технологій, основні програмні та технічні заходи забезпечення інформаційної безпеки.

Посібник призначено для студентів вищих навчальних закладів, що вивчають та займаються інформаційною безпекою.

УДК 004.056(075.8)

Зміст

ВСТУП

З тих пір, як людина навчилася говорити і записувати мову, вона одержує і береже, викрадає і захищає інформацію. Бурхливий розвиток техніки, технології, інформатики в останнє десятиріччя викликав ще більш бурхливий розвиток технологічних пристроїв і систем розвідки. У створенні пристроїв і систем ведення розвідки вкладалися і вкладаються величезні кошти в усіх розвинених країнах.

Сьогоденність висуває вимоги не тільки щодо потреби інформації, але й її аналізу, збирання та захисту.

Багатосторонній аналіз теоретичних і практичних робіт показує, що в даний час виникла необхідність реалізації концепції захисту інформації. Реалізація даної концепції дозволяє забезпечити необхідний рівень захищеності інформації.

Мета заходів у сфері інформаційної безпеки (ІБ) – захист інтересів суб'єктів інформаційних відносин. Інтереси ці різноманітні, але всі вони концентруються навколо трьох основних аспектів:

- доступність;
- цілісність;
- конфіденційність.

Перший крок при побудові системи ІБ – ранжування й деталізація цих аспектів.

Важливість проблематики ІБ пояснюється двома основними причинами:

а) цінністю накопичених інформаційних ресурсів;

б) критичною залежністю від інформаційних технологій.

Руйнування важливої інформації, крадіжка конфіденційних даних, перерва у роботі внаслідок відмови – все це виливається у великі матеріальні втрати, завдає шкоди репутації організації. Проблеми з системами керування або медичними системами загрожують здоров'ю й життю людей.

Сучасні інформаційні системи складні й, виходить, небезпечні вже самі по собі, навіть без урахування активності зловмисників. Постійно виявляються нові вразливі місця в програмному забезпеченні. Доводиться брати до уваги надзвичайно широкий спектр апаратного й програмного забезпечення, численні зв'язки між компонентами.

Змінюються принципи побудови корпоративних ІС. Використовуються численні зовнішні інформаційні сервіси. Отримало широке поширення явище, позначене англійським словом «аутсорсинг», коли частина функцій корпоративної ІС передається зовнішнім організаціям. Розвивається програмування з активними агентами.

Підтвердженням складності проблематики ІБ є паралельний (і досить швидкий) ріст витрат на захисні заходи й кількості порушень ІБ у

поєднанні з ростом середнього збитку від кожного порушення. (Остання обставина – ще один доказ на користь важливості ІБ).

Успіх у сфері інформаційної безпеки може принести тільки комплексний підхід, що уособлює в собі заходи чотирьох рівнів:

- законодавчого;
- адміністративного;
- процедурного;
- програмно-технічного.

Проблема ІБ – не тільки (і не стільки) технічна; без законодавчої бази, без постійної уваги керівництва організації й виділення необхідних ресурсів, без заходів керування персоналом і фізичного захисту вирішити її неможливо. Комплексність також ускладнює проблематику ІБ; необхідна взаємодія фахівців з різних галузей.

Як основний інструмент боротьби зі складністю пропонується об'єктно-орієнтований підхід. Інкапсуляція, успадкування, поліморфізм, виділення граней об'єктів, варіювання рівня деталізації – все це універсальні поняття, знання яких необхідно всім фахівцям з інформаційної безпеки.

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Необхідно всіляко підкреслювати важливість проблеми ІБ; сконцентрувати ресурси на найважливіших напрямках досліджень; скоординувати освітню діяльність; створити й підтримувати негативне ставлення до порушників ІБ – все це функції законодавчого рівня.

На законодавчому рівні особливої уваги заслуговують правові акти й стандарти.

Головне завдання засобів адміністративного рівня – сформувати програму робіт у сфері інформаційної безпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ.

Основою програми є політика безпеки, що уособлює підхід організації до захисту своїх інформаційних активів.

Розробка політики й програми безпеки починається з аналізу ризиків, першим етапом якого, у свою чергу, є ознайомлення з найпоширенішими загрозами.

Головні загрози – внутрішня складність ІС, ненавмисні помилки штатних користувачів, операторів, системних адміністраторів й інших осіб, що обслуговують інформаційні системи.

На другому місці за розміром збитку стоять крадіжки й підробки.

Реальною небезпекою є: пожежі й інші аварії підтримувальної інфраструктури.

У загальному числі порушень зростає частка зовнішніх атак, але основний збиток, як і раніше, наносять «свої».

Для переважної більшості організацій досить загального знайомства з ризиками; орієнтація на типові, апробовані рішення дозволить забезпечити

базовий рівень безпеки при мінімальних інтелектуальних і поміркованих матеріальних витратах.

Розробка програми й політики безпеки може бути прикладом використання поняття рівня деталізації. Все це повинно підрозділятися на кілька рівнів, що трактують питання різного ступеня специфічності. Важливим елементом програми є розробка й підтримка в актуальному стані карти ІС.

Безпеку неможливо додати до системи; її потрібно закладати з самого початку й підтримувати до кінця.

Заходи процедурного рівня орієнтовані на людей (а не на технічні засоби) і підрозділяються на такі види:

- керування персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

На цьому рівні застосовуються важливі принципи безпеки:

- безперервність захисту в просторі й часі;
- поділ обов'язків;
- мінімізація привілеїв.

Тут також застосовується об'єктний підхід і поняття життєвого циклу. Перший дозволяє розділити контрольовані сутності (територію, апаратуру й т. д.) на відносно незалежні підоб'єкти, розглядаючи їх з різним ступенем деталізації й контролюючи зв'язок між ними.

Поняття життєвого циклу корисно застосовувати не тільки до інформаційних систем, але й до співробітників. На етапі ініціації повинен бути розроблений опис посади з вимогами до кваліфікації й виділених комп'ютерних привілеїв; на етапі встановлення необхідно провести навчання, у тому числі з питань безпеки; на етапі виведення з експлуатації потрібно діяти акуратно, не допускаючи завдання збитків скривдженими співробітниками.

Інформаційна безпека багато в чому залежить від акуратного ведення поточної роботи, що охоплює:

- підтримку користувачів;
- підтримку програмного забезпечення;
- конфігураційне керування;
- резервне копіювання;
- керування носіями;
- документування;
- регламентні роботи.

Елементом повсякденної діяльності є відстеження інформації у сфері ІБ; як мінімум, адміністратор безпеки повинен підписатися на список розсилань з нових прогалин у захисті (і вчасно ознайомлюватися з вхідними повідомленнями).

Потрібно, однак, заздалегідь готуватися до неординарних подій, тобто до порушень ІБ. Заздалегідь продумана реакція на порушення режиму безпеки переслідує три головні цілі:

- локалізація інциденту й зменшення нанесеної шкоди;
- виявлення порушника;
- попередження повторних порушень.

Виявлення порушника – процес складний, але перший і третій пункти можна й потрібно ретельно продумати й відпрацювати.

У випадку серйозних аварій необхідне проведення відбудовних робіт. Процес планування таких робіт можна розділити на такі етапи:

- виявлення критично важливих функцій організації, встановлення пріоритетів;
- ідентифікація ресурсів, необхідних для виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відбудовних робіт;
- підготовка до реалізації обраної стратегії;
- перевірка стратегії.

Програмно-технічні заходи, тобто заходи, спрямовані на контроль комп'ютерних сутностей – устаткування, програм й/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки.

На цьому рубежі стають очевидними не тільки позитивні, але й негативні наслідки швидкого прогресу інформаційних технологій. По-перше, додаткові можливості з'являються не тільки у фахівців з ІБ, але й у зловмисників. По-друге, інформаційні системи весь час модернізуються, перебудовуються, до них додаються недостатньо перевірені компоненти (у першу чергу програмні), що утрудняє дотримання режиму безпеки.

Заходи безпеки доцільно розділити на види:

- превентивні, такі, що перешкоджають порушенням ІБ;
- заходи виявлення порушень;
- локалізовальні, такі, що звужують зону впливу порушень;
- заходи щодо виявлення порушника;
- заходи відновлення режиму безпеки.

У продуманій архітектурі безпеки всі вони повинні мати місце.

З практичної точки зору важливими також є такі принципи архітектурної безпеки:

- безперервність захисту в просторі й часі, неможливість оминути захисні засоби;
- наслідування визнаним стандартам, використання апробованих рішень;
- ієрархічна організація ІС з невеликою кількістю сутностей на кожному рівні;
- посилення найслабшої ланки;
- неможливість переходу в небезпечний стан;

- мінімізація привілеїв;
- поділ обов’язків;
- ешелонованість оборони;
- розмаїтість захисних засобів;
- простота й керованість інформаційної системи.

Центральним для програмно-технічного рівня є поняття сервісу безпеки. До числа таких сервісів входять:

- ідентифікація й аутентифікація;
- керування доступом;
- протоколювання й аудит;
- шифрування;
- контроль цілісності;
- екранування;
- аналіз захищеності;
- забезпечення відмовостійкості;
- забезпечення безпечного відновлення;
- тунелювання;
- керування.

Ці сервіси повинні функціонувати у відкритому мережевому середовищі з різнорідними компонентами, тобто бути стійкими до відповідних загроз, а їхнє застосування повинне бути зручним для користувачів й адміністраторів. Наприклад, сучасні засоби ідентифікації/аутентифікації повинні бути стійкими до пасивного й активного прослуховування мережі й підтримувати концепцію єдиного входу в мережу.

Виділимо найважливіші моменти для кожного з перерахованих сервісів безпеки.

1. Кращими є криптографічні методи аутентифікації, реалізовані програмним або апаратно-програмним способом. Парольний захист став анахронізмом, біометричні методи мають потребу в подальшій перевірці в мережевому середовищі.
2. При розмежуванні доступу повинна враховуватися семантика операцій, але поки для цього є тільки теоретична база. Ще один важливий момент – простота адміністрування в умовах великої кількості користувачів і ресурсів, а також безперервних змін конфігурації. Протоколювання й аудит повинні бути багаторівневими та такими, що проникають всюди, з фільтрацією даних при переході на більш високий рівень. Це необхідна умова керованості. Бажане застосування засобів активного аудиту, однак потрібно усвідомлювати обмеженість їхніх можливостей і розглядати ці засоби як один з рубежів ешелонованої оборони, причому не найнадійніший. Варто конфігурувати їх таким чином, щоб мінімізувати кількість фіктивних тривог і не робити небезпечних дій при автоматичному реагуванні.

Усе, що пов’язано з криптографією, складно не стільки з технічної, скільки з юридичної точки зору; для шифрування це складніше у декілька разів. Даний сервіс є інфраструктурним, його реалізація повинна мати місце на всіх апаратно-програмних платформах і задовольняти жорсткі вимоги, які стосуються не тільки безпеки, але й продуктивності. Поки ж єдиним доступним виходом є застосування вільно розповсюджуваного програмного забезпечення (ПЗ).

Надійний контроль цілісності також базується на криптографічних методах з аналогічними проблемами й методами їхнього вирішення. Можливо, прийняття Закону про електронний цифровий підпис змінить ситуацію на краще, буде розширений спектр реалізацій. На щастя для статичної цілісності, є й некриптографічні підходи, засновані на використанні запам’ятовувальних пристроїв, дані на яких доступні тільки для читання. Якщо в системі розділити статичну й динамічну складові й помістити першу в постійний запам’ятовувальний пристрій (ПЗП) або на компакт-диск, можна в зародку придушити загрози порушення цілісності. Розумно, наприклад, записувати реєстраційну інформацію на пристрої з одноразовим записом; тоді зловмисник не зможе «приховати сліди».

Аналіз захищеності – це інструмент підтримки безпеки життєвого циклу. Схожість його з активним аудитом – евристичність, необхідність практично безперервного відновлення бази знань і роль не найнадійнішого, але необхідного захисного рубежу, на якому можна розташувати вільно розповсюджуваний продукт.

Місія забезпечення інформаційної безпеки складна, у багатьох випадках нездійсненна, проте завжди шляхетна.

Абсолютний характер вимог повноти всіх загроз інформації, потенційно можливих у сучасних умовах, і методика формування цієї повної множини загроз, а також можливість застосування експертних методів оцінювання – все це необхідно для забезпечення організації інформаційної безпеки.

Знання причин порушення цілісності інформації і каналів несанкціонованого доступу до неї, зокрема природних і штучних завад, комп’ютерних вірусів, дозволяє зрозуміти механізми захисту інформації.

Вивчення матеріалу, викладеного у навчальному посібнику, дозволяє студентам засвоїти підходи до розуміння проблем інформаційної безпеки.

Автори врахували всі зауваження, які вони отримали після виходу першого видання.

Автори також висловлюють щиру подяку доктору юридичних наук, професору Хахановському Валерію Георгійовичу (Київський національний університет внутрішніх справ), доктору політичних наук, професору Сосніну Олександру Васильовичу (дипломатична академія України при Міністерстві закордонних справ України) та доктору технічних наук, професору Козловському Валерію Вікторовичу (Інститут спеціального зв’язку та захисту інформації Національного технічного університету «КПІ») за уважне та

доброзичливе рецензування й зауваження, що сприяло значному поглибленню та покращенню другого видання навчального посібника.

Крім того, автори висловлюють подяку за співробітництво та слушні зауваження співробітникам Служби безпеки України та Державної служби спеціального зв’язку та захисту інформації.

ГЛАВА 1
ІНФОРМАЦІЯ ТА ЇЇ ЗВ'ЯЗОК З ГАЛУЗЗЮ ДІЯЛЬНОСТІ СУСПІЛЬСТВА

Інформація безпосередньо пов'язана з галуззю діяльності суспільства. Ізольована інформація не дозволяє скласти повне уявлення про подію так само, як окремий елемент загадкової картинки не дозволить судити про її повний зміст, хоч би як ви його не крутили в себе перед очима. Шляхом додавання інформації можна прискорити відновлення загадкової картинки. Вважається, що інформація – це об'єкт, що існує в абсолюті, ідентичний для всіх, а виходити потрібно з того, що мова йде про конструкцію, що кожний будує сам для себе відповідно до своїх потреб. Справжня інформація існує лише в тому випадку, якщо попередньо є намір (задум), мета, проект. Намір обумовлює ставлення, більш-менш усвідомлене, до аналізу навколишньої діяльності, що, у свою чергу, виражається в пробудженні уваги, у результаті чого єдине слово, об'єкт або подія, що його стосується, виловлюється з неупорядкованої множини сигналів. Отже, істинна інформація є результатом взаємної пари намір-увага, а все інше є тільки шумовим фоном.

1.1 Види інформації

Розрізняють два основних види інформації:

1. Біологічна інформація;
2. Соціальна інформація.

Соціальна інформація викликає найбільший інтерес при дослідженні в галузі життєдіяльності суспільства.

Соціальна інформація тісно пов'язана з практичною діяльністю людини, тому тут можна виділити стільки типів і різновидів, скільки є видів діяльності людини.

Прикладами можуть слугувати політична, військова, естетична, етична, економічна, технологічна (ноу-хау), вимірювальна, науково-технічна інформації. При цьому можливі різноманітні класифікації за різноманітними ознаками. Зокрема соціальна інформація ділиться на два класи:

- масова інформація;
- спеціальна інформація.

Масова інформація адресована всім членам суспільства незалежно від їхнього становища і роду діяльності. Спеціальна інформація адресована не всім членам суспільства, а певним соціальним групам (вченим даної спеціальності, економістам, військовим і т. д.). Для сприйняття цілей інформації необхідний початковий запис спеціальних знань і володіння

професійною мовою. Ось найбільш важливі різновиди спеціальної соціальної інформації.

НАУКОВА ІНФОРМАЦІЯ утворюється в результаті науково-технічної діяльності. Наукову інформацію можна визначити як передане в інформаційному процесі наукове знання. Наукова інформація, як і наукове знання, є результатом абстрактно-логічного мислення й адекватно уособлює об'єктивні закономірності, явища і процеси реального світу, суспільства і духовної діяльності людини, вона повинна бути природно отримана науковими методами, що забезпечують істинність знання.

ТЕХНІЧНА ІНФОРМАЦІЯ створюється в сфері техніки і призначена для вирішення технічних задач (розробка нових технічних виробів, матеріалів, технологій). Структура та властивості наукової і технічної інформації досить близькі, тому ці два види часто об'єднують терміном «науково-технічна інформація». Проте, розрізняючи науку і техніку як сфери суспільного виробництва, розрізняють й інформаційні процеси, характерні для цих сфер, зокрема документи, призначені для техніки (патенти, стандарти, комп'ютерні програми, конструкторська документація), або переважно для науки (звіти про науково-дослідні роботи, монографії, теоретичні журнали, збірники наукових праць).

ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ безпосередньо використовується для створення матеріальних благ. Нові високоефективні технології створюють певний імідж суспільства, держави.

ПЛАНОВО-ЕКОНОМІЧНА ІНФОРМАЦІЯ про стан і перспективи розвитку народного господарства використовується для організації планування і впливу на управління суспільним виробництвом, у тому числі й в умовах ринкових відносин.

Інформація має деякі загальні для всіх її видів властивості. Основною властивістю інформації варто вважати її нерозривний зв'язок з певною самостійно організовувальною системою. Іншими важливими властивостями інформації є структурованість, значення і цінність.

Структурування інформації відбувається паралельно з формуванням моделі зовнішнього світу, а найчастіше є першим етапом у наукових дослідженнях.

Для системи, що самостійно організовується, характерно прямування-прагнення до мети, до більш сприятливого становища стосовно власних критеріїв або стабілізації та зберігання зайнятого становища. Усе, що забезпечує цей рух, є цінним для системи. Звідси випливає, що цінними є і речовина, і енергія, і інформація. Цінність інформації виражається в таких поняттях, як змістовність, своєчасність, повнота, достовірність, оперативність.

1.2 Інформація для ухвалення рішення

Фундаментом для побудови інформації слугує 3В /buns – besoins – bases / [1] цілі – потреби – бази. Цілі пов'язані одна з одною в ієрархічну структуру. Кожна мета обумовлюється метою вищого порядку, залишаючись при цьому автономною за характером своїх потреб і баз для спостереження. Кожній з цих цілей відповідають різноманітні потреби в інформації й, отже, різні бази для спостереження. Це є справедливим для будь-якої організації і, зокрема, для підприємств, де варто розрізняти стратегічний (будівництво фабрики, впровадження нової технології і т. п.) і тактичний (вибір майданчика для будівництва фабрики, розробка нової технології власними силами і т. п.) рівні. Правильне визначення цілей на кожному рівні дозволяє правильно визначити потреби в інформації і, одночасно, бази для спостереження.

1.2.1 Інформація для стратегічних рішень

Стратегічні рішення прямо впливають на долю підприємства, на його розвиток і життєздатність. Навколишній світ постійно змінюється, і швидкість цих змін постійно збільшується. Тому кількість стратегічних рішень постійно зростає, їхні наслідки усе складніше і складніше прогнозувати, а ціна помилки постійно підвищується. Цим і визначається значення стратегічної інформації, без якої неможливо прийняти правильне рішення. Рішення полягає в поетапному підході відповідно до методу «3В»: робота, а потім і бази для спостереження, повинна починатися з визначення цілей, що обумовлюють потреби в інформації.

Таким чином, перше, що необхідно зробити, це визначити стратегічні цілі, які повинні визначити подальший розвиток підприємства. Наступний етап – це визначення стратегічних потреб, що містять у собі все, що може чинити довгостроковий вплив на діяльність підприємства. На підставі виявлених потреб визначають стратегічні бази. Для цього складають картотеку напрямків для спостереження. Для полегшення цієї роботи розділяють сферу на три галузі:

- безпосередня сфера дій містить у собі все, що знаходиться в прямому зв'язку з діяльністю підприємства;
- сфера впливу містить у собі все, що може вплинути на дії, здійснювані в рамках попередньої сфери;
- сфера інтересів містить у собі галузі діяльності, якими підприємство поки не займається, але може зайнятися в майбутньому, а також ті галузі діяльності, що можуть вторгнутись в основну сферу діяльності підприємства.

Користь такого розподілу полягає в тому, що він змушує звернути увагу на межі звичайної сфери діяльності, тобто туди, звідки, зазвичай виходять найбільш значні сприятливі можливості і найбільші небезпеки.

Чим більше поставлені цілі віддалені в часі, тим ширшим повинно бути поле зору, тим більшою повинна бути сфера інтересів. Особливе значення це має на стратегічному рівні. На тактичному й оперативному рівнях можна обмежитися двома першими сферами.

1.2.2 Інформація для тактичних рішень

Інформація для тактичних рішень складається з вибору:

- тактичних цілей;
- тактичних потреб першого і другого типів;
- тактичних баз першого і другого типів.

Тактична мета полягає у виборі найкращого способу досягнення стратегічної мети й у контролі незмінності умов, що зумовили цей вибір.

Тактичні потреби полягають у необхідності розрізнення постійних і змінних величин, пов'язаних з тимчасовою шкалою дій. Зокрема, це полягає в правильному виборі напрямків. Для правильного вибору необхідно знати загальні характеристики кожного з напрямків, що належить до *потреб першого типу*. Необхідність постійного спостереження за станом навколишнього середовища для своєчасного виявлення всіх завад, що можуть стати причиною значних відхилень від наміченого шляху, відносять до *потреб другого типу*.

Ці два види потреб настільки різні, що відповідні їм бази практично не мають нічого спільного одна з одною. У першому випадку створюються і знищуються бази для інформації, що збирається «за запитом»: щораз, коли з'являється новий напрямок, починається спроба максимально повного ознайомлення з характеристиками для ухвалення рішення про те, чи варто йти в цьому напрямку. В другому випадку ведеться всеосяжне спостереження навколишнього середовища, тому що невідомо, звідки може прийти небезпека.

До *тактичних баз першого типу* відносять бази інформації, що збираються «за запитом», які потребують ретельного дослідження нових напрямків з урахуванням політичної, соціально-культурної й економічної інформації.

Тактичні бази другого типу з девізом «всеосяжне спостереження навколишнього середовища» містять у собі всі чинники навколишнього середовища, зміна яких може мати середньостроковий вплив на діяльність підприємства. Перелік критеріїв, що враховуються на стратегічному рівні, продовжується на тактичному і містить у собі:

- основної галузі діяльності і види продукції (теперішні і майбутні), зони і території діяльності;
- виробничі потужності і засіб виробництва;
- патентна і ліцензійна активність.

Природно, тактичні бази і параметри, що враховуються, змінюються залежно від політичної лінії, наміченої керівництвом.

1.2.3 Інформація для вирішення оперативних питань

ОПЕРАТИВНІ ЦІЛІ. На цьому рівні стратегічна мета уже визначена, шлях її досягнення обраний, і тепер необхідно забезпечити просування вперед у найкращих умовах, уникаючи дрібних останніх завад і, по можливості, скорочуючи шлях.

ОПЕРАТИВНІ ПОТРЕБИ. Мова йде про сприятливі можливості або про загрози. В усіх випадках потрібна свіжа, точна, надійна і цілеспрямована інформація, тому що мова йде про максимально швидке реагування, тобто про реагування без найменших зволікань і без імпровізації: сприятливі можливості не повторюються двічі, і загрози, якщо їм вчасно не запобігти, можуть виявитися згубними.

ОПЕРАТИВНІ БАЗИ. Мова йде про найближче оточення підприємства, за котрим необхідно стежити з підвищеною увагою. Сюди входять конкуренти та їхня комерційна політика. Не варто забувати про інші не менш важливі напрямки спостереження: постачальники, система торгівлі і численні інші об'єкти спостереження, вибрані з урахуванням специфічних потреб кожного конкретного випадку.

Для того, щоб інформація, яка збирається, принесла користь, необхідно навчитися правильно збирати її. Цілком природно, що спочатку ви будете робити помилки, приймаючи необґрунтовані чутки за справжню інформацію. Лише в процесі пошуку інформації можна навчитися збирати її. Використання методу «ЗВ» допоможе вам розпізнати корисну інформацію з першого погляду.

КАРТОТЕКА СПОСТЕРЕЖЕНЬ. Вважається раціональним об'єднання всіх баз у рамках однієї картотеки. Основними базами є:

- конкуренція (вся інформація про діючих і потенційних конкурентів);
- ринок (уся ринкова інформація, смаки і запити споживачів, канали збуту і т. п.);
- технологія виробництва і використання продукції;
- законодавство (вся інформація з законодавства, що стосується діяльності підприємства, а також інформація з діяльності органів, що розробляють і приймають нові законодавчі положення);
- ресурси (вся інформація з матеріально-технічних ресурсів, необхідних для нормальної діяльності підприємства, щодо сировини, постачання, робочої сили і фінансів);
- загальні тенденції (політична, економічна, соціальна, демографічна і т. п. інформація);
- інші чинники, що впливають на діяльність підприємства (чинники, не враховані в попередніх базах).

Метод «ЗВ» дозволяє вам забезпечити спостереження за потрібними базами. Проте при розвитку підприємства можуть з'явитися нові цілі, ринок і навколишнє середовище постійно змінюватимуться. Тому ви повинні передбачити можливість періодичного перегляду ваших баз на основі повторного аналізу цілей і потреб вашого підприємства.

Інформація є цінною тільки тоді, коли вона може використовуватися. Якщо інформація не слугує для ухвалення рішення, то вона є безпредметною, а, отже – неіснуючою.

Таким чином, для одержання якісної інформації необхідно сформулювати цілі, визначити потреби і побудувати бази для спостереження. Для діяльності підприємства звичайно достатньо шести баз для спостереження: конкуренція, ринки, технологія, законодавство, ресурси, спільні тенденції.

1.3 Як збирати і обробляти інформацію

1.3.1 Шлях інформації

Намітимо загальну методику одержання інформації на прикладі запуску нової продукції.

1. При запуску нової продукції більша частина інформації вже пройшла через ті етапи, де виток імовірний, навіть можливий: рішення фінансистів, що повинні встановити ціни, вивчити ринок і дати кредит з бюджету на дослідження; заявлені патенти або такі, що купуються. В усі ці операції залучено багато людей, не рахуючи сторонніх учасників (банки, професійні організації і т. п.), що робить цілком неможливим повне дотримання таємності.

2. Для збуту продукції створюється команда, про існування якої добре відомо всім співробітникам підприємства. Нові дії команди розширюють коло посвячених (створення нового цеху або заводу і т. п.). Ці посвячені більш-менш відірвані один від одного у своїй професійній діяльності або особистому житті настільки, що інформація випаровується. Нарешті з’являються чутки. Тоді інформація виявляється на межі приватного і громадського життя. Іноді такий етап виявляється досить пікантним, оскільки конкурент насторожується і може почати вживати контрзаходів раніше, ніж становище стабілізується.

3. Робиться повідомлення. Публікується інформація. Слово «публікується» не означає «широко поширюється». Деякі виробництва користуються потоком статей та інформації. У інших випадках інформація не потрапляє в поле зору спеціалізованих видань і конфіденційних збірників, хоча найчастіше саме вони містять важливі нові технології. На такій стадії реальні характеристики продукції ще невідомі.

4. Випускається продукція. Усі можуть її купити, споживачі її досліджують і порівнюють з іншою. Конкуренти її розбирають і розгвинчують, а всі характеристики продукції стають надбанням громадськості і тим або іншим чином публікуються.

5. Продукція фіксується, класифікується і, можливо, стає статистичним об’єктом. При нагоді її характеристики займають своє місце в банку даних, що являє собою електронну бібліотеку, де накопичуються, часто з запізненням, резюме статей журналів і збірників.

6. Продукція зникає, її місце займає нова. Стирається інформація про стару, про неї не залишається нічого, крім інформації в архіві.

7. Досвід показує, що зміни і накопичення інформації відбуваються в невеликому переліку привілейованих місць, що називаються «Сімейство джерел».

8. Ось перелік основних сімейств джерел для будь-якого підприємства:

КЛІЄНТИ – покупці клієнтів; їхні інженери і кадри;

ПОСТАЧАЛЬНИКИ – відповідно до їхньої діяльності;

БАНКІРИ – розділені на банківські, фінансові, біржові і кредитні установи;

СУСПІЛЬНІ СЛУЖБИ – рекламні агенції, фірми суспільних зв'язків, мисливці за інтелектами та ін.;

РОЗПОДІЛЬНИКИ і АГЕНТИ – поза залежністю від особливостей, варто брати до уваги як торговців, так і покупців;

КОНСУЛЬТАНТИ і ЕКСПЕРТИ – незалежні фахівці, або такі, що працюють на підприємстві, які продають свої знання у формі порад або спеціальних розробок;

ШИРОКА ПУБЛІКА – місцева, національна або міжнародна преса;

СПЕЦІАЛЬНІ ВИДАННЯ і БАНКИ ДАНИХ – їхня галузь діяльності припускає щомісячне опрацювання матеріалів конфіденційних видань, що потрапляють у наукові, технічні і фахові збірники. Разом з банком даних вони складають ресурси бази даних;

ЯРМАРКИ, САЛОНИ і КОНФЕРЕНЦІЇ – ці демонстрації дозволяють обновити контакти з клієнтами, конкурентами і т. д., а також побачити різноманітну продукцію, презентовану на ринку. Наукові і технічні виставки дозволяють визначити країну, що йде попереду у своїх дослідженнях;

АДМІНІСТРАЦІЯ – усі нормативні зобов'язання і вимоги керівництва для майже всіх видів промисловості, комерційної і фінансової діяльності підприємства. Вони зібрані в архівах і здебільшого є опублікованою інформацією. Виділення необхідної кількості джерел з усього сімейства в більшості випадків дозволяє добратися прямо до інформації без того, щоб проходити всі шляхи її просування.

Назвемо шляхи пошуку інформації – **шляхом інформації.**

1.3.2 Канали інформації

Аналізуючи бази і джерела інформації, можна визначити канали інформації, перегрупувавши сімейство джерел таким чином:

- **канал тексту** – загальні публікації + спеціальні публікації і банки даних. Цим каналом підприємство одержує 30–40% всієї інформації;
- **канал фірма** – клієнти + постачальники + банкіри + розподільники й агенти. Через цей канал проходить від 30 до 40% інформації. Разом із персоналом, який більш-менш контактує зі сторонніми організаціями, це складає внутрішню мережу підприємств;

- **канал консультант** – суспільні служби + консультанти + адміністрація. Цим каналом проходить 10–15% інформації;
- **канал розмова** – ярмарки + салони і конференції. Через цей канал проходить 5–6% інформації;
- **канал джокер** – додатковий канал.

Методика пошуку інформації, що враховує всі п'ять каналів, називається **4К+1** (1 – частина, що відповідає джокерові).

Розглянемо варіанти пошуку джерел інформації.

1. Методика 4К+1 у формі «дощ, що мрячить». У цьому випадку бази спостереження підживлюються регулярно чотирма каналами.

2. Методика 4К+1 за методом «гроза». Цей метод полягає в постійному поповненні інформації й одержанні своєчасної відповіді або виявленні небезпеки шляхом спостереження за каналом джокер.

Перед тим, як займатися пошуком інформації в незручних місцях, варто переконатися, що вона не отримана і тому потрібно починати свої дії, особливо активізуючи основні два канали: текст і фірму.

3. Методика багатоджерельного пошуку. Якщо попередні пошуки довго не завершуються або ви дійшли висновку, що небагато шансів швидко завершити пошук у силу екстраординарності проблеми, – звертайтеся до кількох джерел. Щоб це зробити, необхідно встановити, які із сімейства джерел вже опрацьовані, проробивши попередню роботу з самим джерелом, і з'ясувати чи містить воно пошукову інформацію. Все це необхідно для того, щоб визначитися у формі подання і доступу до інформації.

Така методика, так само як і наступні, набагато складніша і дорожча, ніж попередня.

4. Стежина інформації. Якщо проблема за своєю природою не може бути відзначена серед сімейств, тоді необхідно відновити стежину просування інформації.

5. Методика 3В. Для досягнення певної мети необхідно користуватися всіма базами і джерелами інформації.

Таємність інформації. Більша частина корисної інформації не є таємницею. Таємницею можна назвати те, що тримається осторонь, удалині від сторонніх очей. Мова йде про таку інформацію, що з політичних або комерційних міркувань вважається ключовим моментом певної ситуації. Промислові таємниці стосуються, в основному, виробництва, особливо технології. Вони повинні охоронятися. Звідси і поняття «захист інформації» і «дотримання таємності».

1.3.3 Обробка інформації

Обробка інформації складається з трьох основних операцій – це аналіз, синтез і циркуляція.

Першою і найважливішою операцією є аналіз, що слугує додатковим фільтром, який відкидає непотрібне і є захистом від шуму без підстави. Ця

операція складається, насамперед, у визначенні важливості, точності і значущості інформації.

Важливість інформації. Побудова баз спостереження, згідно з процедурою ЗВ, гарантує зв'язок з інформацією, що спостерігається. Але інформація, пов'язана тематично, може не мати особливого значення. Інформація є важливою, якщо вона пов'язана, тобто має зв'язок з елементами бази і якщо вона спроможна внести вклад в організацію. Коли внесок значний і безпосередній, інформація потребує термінових дій. Інформація, що не має значення, повинна бути вилучена, щоб уникнути втрати часу і енергії.

Точність інформації. Не завжди легко встановити є інформація достовірною чи помилковою, особливо якщо вона містить відомості про події, що ще не відбулися. Допускається два критерії, за якими можна судити про точність інформації: надійність джерела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження в інших джерелах, якщо можливо, – незалежних. Рішення полягає в пошуку пов'язаних подій у різноманітних інформаціях. При відсутності надійності джерела інформації не варто її відкидати, особливо якщо вона справляє враження важливої. Необхідно просто відкласти про запас та чекати нових елементів, що дозволять її або підтвердити, або ні.

Значущість інформації. Інформація може бути важливою та точною й у той же час даремною, оскільки вона недостатня для розуміння і дії. Два тлумачення, наведені окремо або паралельно, дозволяють судити про значимість інформації. Перше називається «циркуляція». Воно складається у швидкій циркуляції інформації серед осіб, яких вона стосується, у надії на можливість встановлення зв'язку з іншою інформацією. Друге тлумачення називається «синтез». Воно полягає в об'єднанні всіх частин інформації, що схоже на складання головоломки для створення повного уявлення. Це не завжди легко, тому що часто не вистачає частин або вони непідходящої форми. Іноді навпаки, частини ідеально підходять, даючи зрозуміле уявлення про ситуацію. Частіше доводиться робити певний шлях при формуванні гіпотези: спробу синтезу, циркуляцію, пов'язати це з дослідженням допоміжної інформації для того, щоб отримати зрозуміле та повне уявлення.

Для визначення значимості інформації використовують два допоміжних підходи. Перший називається «розширення», а другий – «намір».

Підхід до методу розширення полягає в тому, що для даних, наявних у розпорядженні, шукається найбільш відповідне пояснення. Часто при завершенні різноманітних гіпотез виявляються протиріччя. У такому випадку важливо знайти всю інформацію, здатну підтвердити одну гіпотезу і відкинути інші.

Підхід до методу «намір» полягає у виявленні такої діючої особи, у наміри якої входять останні факти. Поставте себе на її місце, щоб

зрозуміти, яку гру вона веде, щоб зробити висновок про її можливі дії. Виходячи з цього, будується безліч гіпотез щодо її намірів і, досліджується, як вони повинні були б пояснити факти. Нарешті, порівнявши імовірні факти з наявними даними, вибирається гіпотеза, що охоплює найбільший діапазон спостережень.

1.3.4 Цикл інформації

Щоб переконатися в корисності джерела інформації, необхідно здійснювати постійну перевірку джерел за двома простими критеріями: забезпечення і ефективність.

Перевірка забезпечення джерел полягає у визначенні цінності, корисності, своєчасної подачі інформації.

Ефективність джерел полягає в одержанні свіжої і конфіденційної інформації.

Таким чином, обробка інформації здійснюється за «малим» (рис. 1.1) і «великим» (рис. 1.2) циклами інформації.

«Малий» цикл інформації охоплює: джерела, збирання, обробку.

«Великий» цикл інформації містить у собі: мету, необхідність, обробку, дію.

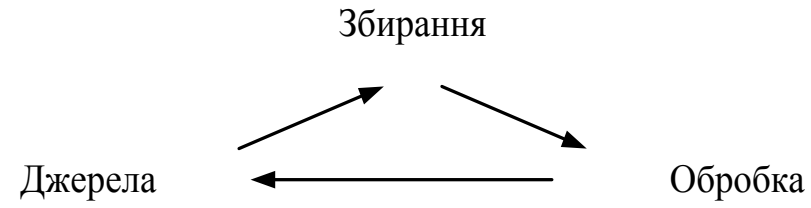


Рисунок 1.1 – «Малий» цикл інформації

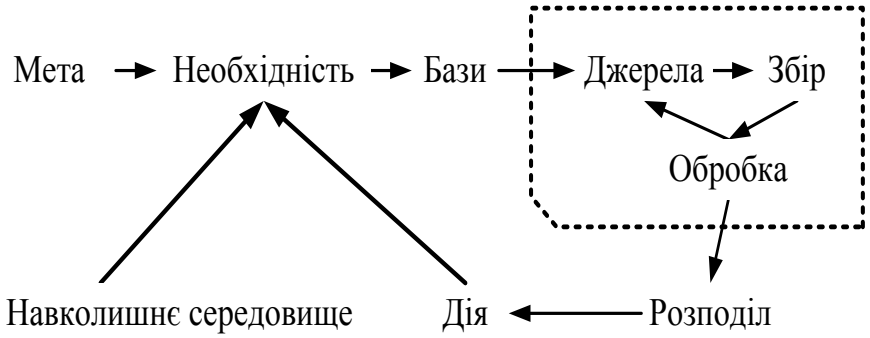


Рисунок 1.2 – «Великий» цикл інформації

1.3.5 Помилкова інформація

Помилкова інформація або дезінформація містить неправду про саму природу об’єкта, про ті чи інші його якості. Дезінформація залежить від

точки зору адресата. Для нього це повідомлення повинно бути отримано як правдива інформація, у протилежному випадку маневр зазнає невдачі. Отже, адресат повинен апріорі бути налаштований позитивно до помилкової інформації. У помилковій інформації є дві складові: сюжет, що підживлюється певною увагою, і сюжет помилковий, що відповідає на цю увагу, пропагандуючи помилкову інформацію. На рисунку 1.3 наведено шлях помилкової інформації.

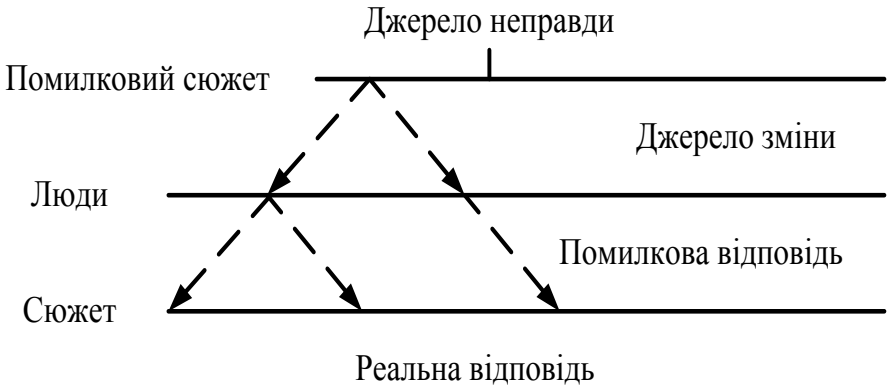


Рисунок 1.3 – Шлях помилкової інформації

Все мистецтво помилок складається з одержання відповіді, яка повинна бути близькою до реальної ймовірності й у той же самий час повинна містити щось віддалене, щоб ввести адресата в оману. Для того, щоб неправда була сприйнята, необхідно, насамперед, знати адресата і, особливо, привілейовані джерела інформації. Потім відправити повідомлення через визнані джерела.

При цьому дезінформація може потрапити до вас з джерела, яке ви вважаєте достовірнішим.

Існують два види дезінформаторів: дезінформатори випадкові й ті, що цим займаються професійно.

Дуже важко відстежити випадкову дезінформацію. Як чиста правда вона надходить занадто пізно, коли мета дезінформації вже досягнута. З професіоналами дезінформації справа набагато простіша. Спочатку через створення зіпсованих ефектів для маніпуляторів «дезінформація є такою досконалою, що її автори не можуть відрізнити правду від вигадки». Неможливо довго приховувати що-небудь. Коли зустрічаєшся з такими дезінформаторами, потрібно прив’язуватися до змісту інформації, щоб виявити мотиви, якими вони керуються. Скрізь зустрічаються факти з використанням техніки, яка має назву «білий шум». Ця техніка полягає у подачі такої кількості новин, що неможливо зробити сортування. Володіння циклами інформації в більшості випадків охороняє від маневрів помилки.

1.3.6 Витік інформації

Більша частина витоку інформації відбувається через недбалість. Тому захист інформації, насамперед, справа навчання. Необхідно знову і знову нагадувати всім (від простого службовця до керівного складу) про елементарні заходи безпеки. Уважність повинна починатися з голови і поширюватися по всьому організму доти, поки не стане рефлексом, що є природною дією, про яку ніхто не думає. Такий результат не досягається без зусиль, але, зрештою, вигода бере верх над невеликими незручностями на самому початку.

Ризиковані точки витоку інформації багаточисельні і важко піддаються контролю. Як приклад розглянемо невеликий перелік простих заходів витоку інформації.

1. Встановіть у бюро ріжучий апарат поблизу копіювального і виробіть у собі рефлекс знищувати всі непотрібні документи.

2. Керуючись конфіденційністю даних у пам'яті комп'ютера, прийміть якийсь код.

3. Контролюйте доступ до комп'ютера ззовні. Найпростіша процедура полягає в забороні користування протягом певного часу і оголошенні сигналу тривоги, якщо три введені слова помилкові. Це сприяє запобіганню крадіжки даних і захищає всю систему від руйнування.

4. Періодично робіть копії інформації, що охороняється, і зберігайте їх у надійному місці.

5. Обмежте вихід інформації до мінімуму.

6. Для того, щоб вводити помилку, інформацію можна піддати деякому упакуванню: підінформація – інформація подається правдива, але розрізнена або неповна, або занадто загальна; інформація помилкова; надінформація – подається велика кількість інформації, але частина її є даремною або помилковою, але все це подається так, щоб неможливо було виявити.

7. Обмежте місця прийому відвідувачів і не залишати їх самих.

8. Не зловживайте набором стажистів і тимчасових співробітників, що часто мають доступ до великої кількості інформації. Бійтеся особливо тих «студентів», яким під сорок.

9. Закривайте на ключ усі важливі документи наприкінці робочого дня. Це правило повинно застосовуватися з усією суворістю в усіх дослідницьких бюро, нічого ніде не повинно просто так лежати.

10. Телефони, телекси, телефакси повинні розглядатися з погляду безпеки передачі інформації особливо в певні країни, з якими необхідно звести контакти до мінімуму і застосувати код для повідомлення надважливої інформації.

Ці заходи ефективні, але не можна забувати, що берегти таємницю повинні самі люди.

Щоб уникнути витоку інформації, потрібно, насамперед, стежити за резервуарами її накопичення; за кранами, що управляють інформаційними потоками; за центрами розподілу інформації.

Запитання для самоконтролю

1. Що являє собою інформація? В якому випадку існує справжня інформація?
2. Які основні властивості інформації?
3. На які два класи поділяють інформацію і що вони собою являють?
4. Що є фундаментом для побудови інформації?
5. Що містять у собі стратегічні потреби?
6. Що необхідно для визначення стратегічних баз?
7. З якою метою роблять поділ сфери дії на галузі? Яка користь такого розподілу?
8. У чому полягає тактична мета?
9. Яку інформацію містять у собі тактичні бази першого і другого типу?
10. Що являють собою тактичні цілі, тактичні потреби і тактичні бази?
11. Що необхідно для одержання якісної інформації?
12. Простежте самостійно стежину інформації від запуску нової продукції до її зникнення.
13. Перерахуйте основні джерела отримання інформації.
14. Які канали інформації існують?
15. Перерахуйте методики пошуку джерел інформації.
16. Яка інформація є таємною?
17. У чому полягає операція синтезу?
18. У чому полягає важливість, точність і значущість інформації?
19. Які підходи використовують для визначення значущості інформації та у чому вони полягають?

ГЛАВА 2
НЕОБХІДНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

Сучасний багатосторонній аналіз результатів творчих і практичних робіт дає вагомі підстави стверджувати, що в даний час дозріли як об'єктивна необхідність, так і об'єктивні передумови реалізації концепції захисту інформації (ЗІ). Раціональна її реалізація дозволить забезпечити необхідний рівень захищеності інформації, без чого не можуть бути вирішені актуальні проблеми інформатизації суспільства.

Тому під ЗІ розуміється сукупність організаційно-технічних заходів і методів відповідно до обраного критерію оптимізації й обмежень, спрямованих на захист інформації в процесі її формування, передачі, прийому, обробки, накопичення і використання з метою забезпечення необхідної надійності.

Під надійністю інформації розуміється інтегральний показник, що характеризує якість інформації з таких позицій:

1. З погляду фізичної цілісності, тобто наявності або відсутності перекручування або знищення елементів цієї інформації.
2. З погляду довіри до інформації, тобто наявності або відсутності в ній підміни (несанкціонованої модифікації) її елементів при зберіганні цілісності.
3. З погляду безпеки інформації, тобто наявності або відсутності несанкціонованого одержання її особами, що не мають на це спеціальних повноважень.

2.1 Класифікація цілей захисту

Загальна класифікація цілей захисту інформації наведена на рис. 2.1. Аналіз класифікації показує, що друга мета захисту – попередження несанкціонованої модифікації інформації – в значній мірі є деякою комбінацією першої і третьої цілей. Дійсно, несанкціонована модифікація може бути випадковою або злочинною. Випадкова модифікація може бути наслідком перекручування деякої інформації. Злочинна ж модифікація є результатом злочинних дій.

Під системою ЗІ розуміється її захист:

- по-перше, в усіх структурних елементах;
- по-друге, на всіх ділянках і технологічних маршрутах обробки інформації;
- по-третє, на всіх етапах життєвого циклу інформації;
- по-четверте, з урахуванням взаємодії з зовнішнім середовищем.

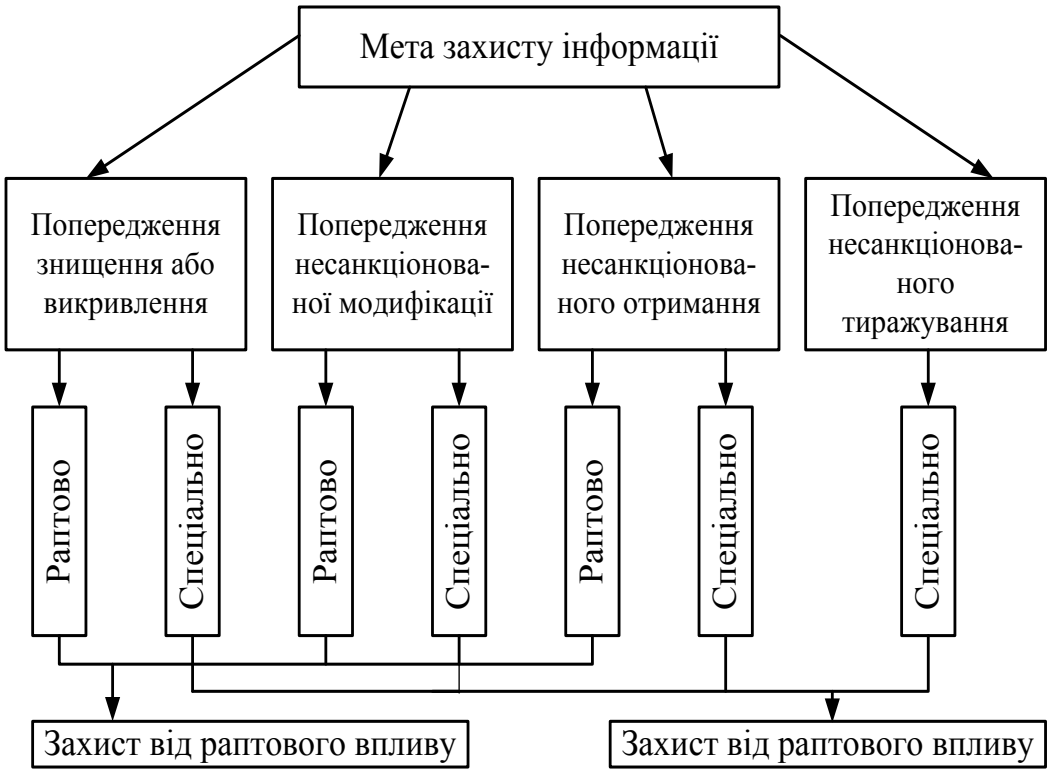


Рисунок 2.1 – Загальна класифікація цілей захисту інформації

Об'єктами захисту є:

1. Вихідні дані, тобто дані, що надійшли від користувачів або абонентів.
2. Довільні дані, тобто дані, отримані в процесі обробки вихідних даних.
3. Нормативно-довідкові, службові і допоміжні дані, також дані системи захисту.
4. Постановка завдань та методів. Моделі, алгоритми і програми, які використовуються при обробці даних.
5. Технічна, технологічна, політична, військова й економічна документації.

Захист інформації повинен здійснюватися в таких зонах:

- зона ресурсів, тобто зона функціонуючих технічних засобів;
- зона помешкань, тобто сукупність помешкань, у яких розташовані технічні засоби і розміщуються люди, що мають відношення до них;
- зона території, що охороняється, тобто та частина території, на якій розташовані будинки з зоною помешкань і на якій може повністю регулюватися доступ людей, а також можуть регулюватися і контролюватися всі дії і заходи, здійснювані на ній;
- зона, що не охороняється, але контрольована територія, тобто та частина зовнішньої території, в якій може здійснюватися регулярний контроль її стану і зроблених на ній дій;
- зовнішня зона, тобто та частина території, на якій можуть

здійснюватися дії і відбуватися події, що впливають на надійність інформації, тобто інформація, яка не може бути під постійним контролем.

Об'єктивна необхідність ЗІ на сучасному етапі і при тій комплексно-системній постановці, як це сформульовано, обумовлена тими застосуваннями принципової значимості, що сталися в нижченаведених напрямках.

1. У концепціях застосування обчислювальної техніки в різноманітних сферах діяльності.

2. У розвитку самої обчислювальної техніки і її програмного забезпечення, а також у концепціях організації і використання ресурсів обчислювальної техніки.

3. У розвитку радіоелектроніки і елементної бази, що дозволило створити високоефективні засоби радіоелектронної розвідки.

Основні зміни в розвитку обчислювальної техніки і її програмне забезпечення можуть бути охарактеризовані таким чином:

1. Розширення типів ЕОМ, що випускаються.
2. Масовий випуск персональних ЕОМ.
3. Розширення номенклатури зовнішніх пристроїв.
4. Різке розширення об'єктів ЗП прямого доступу.
5. Масовий випуск машинних носіїв інформації великого обсягу персонального і групового використання – магнітних дисків.
6. Різке зниження об'ємів апаратури обчислювальної техніки за рахунок мікромініатюризації електронних пристроїв.
7. Різкий розвиток єдиного програмного забезпечення, призначеного для забезпечення програмування, забезпечення функціонування технічних засобів і виконання інших функцій.
8. Інтенсивний розвиток системного програмного забезпечення, призначеного для організації і забезпечення функціонування інформаційно-обчислювальних систем і мереж, також й автоматизованої передачі даних по мережах.
9. Інтенсивний розвиток і повсюдне впровадження систем управління базами даних, призначених для централізованого накопичення і збереження великих масивів даних, пошуку і видачі їх користувачам та іншим, розв'язуваним у системі завданням.
10. Інтенсивний розвиток пакетів прикладних програм, що істотно полегшує розробку завдань функціональної обробки інформації.
11. Інтенсивний розвиток і удосконалювання засобів візуалізації, що розширює можливості і полегшує умови використання обчислювальної техніки.

Для сучасних концепцій організації і використання ресурсів обчислювальної техніки характерними є такі особливості:

- створення потужних обчислювальних центрів колективного користування (ОЦКК), призначених для промислової переробки інформації;

- тенденції об’єднання ОЦКК мережею передачі даних у мережу ОЦКК є прологом створення в державі організованої індустрії переробки інформації;

- масове застосування автоматизованих робочих місць (АРМ), створюваних шляхом безпосереднього оснащення робочих місць засобами обчислювальної техніки;

- значне поширення абонентських пунктів різноманітного призначення й інформаційно-обчислювальних пунктів групового використання оснащених малими і середніми ЕОМ;

- об’єднання АРМ у локальні інформаційно-обчислювальні мережі;

- поєднання АРМ, абонентських пунктів, групових інформаційно-обчислювальних пунктів і локальних мереж із ОЦКК і мережами ОЦКК.

Серйозні зміни, що мають принципове значення, відбуваються в концепціях застосування обчислювальної техніки в сфері управління. Причому, упровадження систем комплексної автоматизації породжує ряд проблем, пов’язаних із забезпеченням високої якості інформації, і, насамперед, її надійності в тій інтерпретації поняття надійності, як це було вже сформульовано. Неважко помітити, що при реалізації комплексних АСУ характерними і типовими стають нижченаведені особливості.

1. Все більша питома вага автоматизованих процедур у загальному обсязі процесів обробки інформації.
2. Всезростаюча важливість і відповідальність рішень, прийнятих в автоматизованому режимі і на основі автоматизованої обробки інформації.
3. Велика і всезростаюча концентрація в автоматизованих системах обробки даних (АСОД) інформаційно-обчислювальних ресурсів.
4. Велика територіальна поширеність компонентів АСОД і АСУ.
5. Складні режими функціонування технічних засобів АСОД.
6. Накопичення на технічних носіях величезних обсягів інформації, причому для багатьох видів цієї інформації усе більш важким стає виготовлення немашинних аналогів.
7. Інтенсивна циркуляція інформації між компонентами АСУ, у тому числі і розташованих на великих відстанях один від одного.
8. Інтеграція в єдиних базах даних інформації різноманітного призначення і різноманітної належності.
9. Довгострокове збереження великих масивів інформації на машинних носіях.
10. Безпосередній і одночасний доступ до ресурсів (у тому числі і до інформації) великої кількості користувачів різноманітних категорій і різноманітної належності.
11. Всезростаюча вартість ресурсів АСОД і АСУ.

У цих умовах різко зростає уразливість інформації, тобто її схильність до впливу різноманітних дестабілізувальних факторів, що може виявлятися в зниженні якості інформації. Результатом же зниження якості інформації

буде висока ймовірність великомасштабних наслідків негативного характеру.

Оскільки інформаційні технології в основних сферах діяльності суспільства усе більше і більше стають автоматизованими, то зниження якості інформації в сучасних АСОД неминуче призведе до зниження ефективності відповідних сфер діяльності. Іншими словами, якість інформації в АСОД прямо і безпосередньо переноситься на якість функціонування тих сфер діяльності, в інтересах яких обробляється інформація.

Через те, що на машинних носіях накопичуються величезні масиви інформації, то порушення фізичної цілісності може призвести до великих втрат, а оскільки для дуже великих обсягів інформації усе меншими стають можливості створення і підтримки немашинних її аналогів, то й відновити порушену цілісність буде усе більш важкою і дорогою справою. Крім того, оскільки сучасні АСОД стають усе більш територіально розподіленими, обслуговують велику кількість різноманітних користувачів, функціонують у складних режимах, що різко збільшує можливості несанкціонованої модифікації і несанкціонованого одержання інформації, у тому числі й у злочинних цілях.

Отже, для забезпечення необхідної якості інформації повинні застосовуватися спеціальні заходи. Тобто, захист інформації об’єктивно набуває характеру завдання підвищеної актуальності.

Об’єктивні передумови вирішення проблеми ЗІ створюються нижчевказаними обставинами.

По-перше, до теперішнього часу практично повсюдно усвідомлена необхідність захисту.

По-друге, зараз вже розроблено достатньо розвинений арсенал засобів захисту.

По-третє, вже зараз накопичено деякий досвід з організації захисту.

На підставі глибокого аналізу всі потенційно можливі шляхи несанкціонованого одержання інформації можуть бути розділені на три класи.

1. Непрямі шляхи, куди віднесені такі шляхи, що дозволяють здійснювати несанкціоноване одержання інформації без фізичного доступу до неї.

2. Прямі шляхи, по яких несанкціоноване одержання інформації можливо тільки при фізичному доступі до неї, але при цьому не потрібно здійснювати будь-яку технічну дію.

3. Прямі шляхи, по яких несанкціоноване одержання інформації можливе тільки при фізичному доступі до неї, і при цьому необхідно здійснити технічні дії.

Систематизований перелік груп потенційно можливих шляхів несанкціонованого одержання інформації:

- застосування пристроїв для прослуховування;

- дистанційне фотографування;
- перехоплення електромагнітних випромінювань;
- розкрадання носіїв інформації;
- розкрадання виробничих відходів;
- зчитування даних у масивах інших користувачів;
- читання залишкової інформації в ЗУ системи після виконання санкціонованих запитів;
- копіювання носіїв інформації;
- несанкціоноване використання терміналів зареєстрованих користувачів;
- маскування під зареєстрованого користувача за допомогою розкрадання паролів і реквізитів розмежування доступу;
- маскування несанкціонованих запитів під запити операційної системи (містифікація);
- використання програмних пасток;
- одержання захищених даних за допомогою серії дозвільних запитів;
- використання недоліків мов програмування й операційних систем;
- навмисне внесення в бібліотеку програм спеціальних блоків типу «троянських коней»;
- незаконне підключення до апаратури, ліній зв'язку, живлення і заземлення;
- злочинне виведення з ладу механізмів захисту.

2.2 Основні положення концепції захисту інформації

У поняття системного підходу до ЗІ входять такі положення.

1. Дослідження і розробка з єдиних методологічних понять усієї сукупності питань, пов'язаних із ЗІ.

2. Розгляд у єдиному комплексі усіх видів захисту інформації; забезпечення фізичної цілісності; попередження несанкціонованої модифікації, попередження несанкціонованого одержання.

3. Системне врахування всіх факторів, які впливають на захищеність інформації.

4. Комплексне використання всіх наявних засобів ЗІ.

Концептуальність підходу означає, що вирішення всіх питань ЗІ здійснюється в рамках єдиної концепції, що об'єднує найбільш раціональним способом всі системні рішення захисту.

Центральним результатом, отриманим у рамках системно-концептуального підходу до проблеми захисту інформації, є висновок, що ефективний ЗІ не може бути забезпечений простим застосуванням деяких механізмів роботи. ЗІ необхідно управляти.

Управління ЗІ являє собою складну сукупність взаємозалежних процесів безперервного створення й удосконалення механізмів ЗІ. При цьому істотно важливою є та обставина, що зазначені питання повинні

бути регулярними, тобто постійно керованими, причому управління повинне здійснюватися з метою досягнення необхідного рівня захисту при мінімальних затратах сил або з метою досягнення максимального рівня захисту при заданих затратах сил і засобів.

На підставі методології системно-концептуального підходу розглянемо узагальнену структуру уніфікованої концепції ЗІ.

Конструктивними елементами концепції є функції, завдання, засоби і системи захисту.

Функція захисту – сукупність однорідних у функціональному відношенні заходів, регулярно здійснюваних з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного ЗІ.

Засоби захисту – пристрої, програми та заходи, спеціально призначені для вирішення завдань захисту інформації.

Завдання захисту – організовані можливості засобів, методів і заходів з метою реалізації функцій захисту.

Система ЗІ – організована сукупність усіх засобів, методів і заходів, що передбачаються з метою ЗІ.

Перераховані елементи концепції складають логічну і повну послідовність рішень, реалізація яких і створює об'єктивні передумови для надійного ЗІ.

У суворій відповідності з основною передумовою про необхідність регулярного управління процесами ЗІ, всі елементи зазначеної послідовності розділені на дві частини: створення механізмів захисту й управління механізмами захисту.

Важливим результатом системно-концептуального підходу до розглянутої проблеми є висновок про неможливість надійного ЗІ без дотримання при побудові цілого ряду достатньо специфічних умов. Ці умови повинні дотримуватися в процесі створення і функціонування інформації, в силу чого в концепції вони виступають як зворотний зв'язок від конструктивних елементів концепції захисту до концепцій побудови й організації функціонування інформації.

Дослідження в рамках системно-концептуального підходу до ЗІ показують, що концепція є уніфікованою в тому, що на її основі може бути реалізована раціональна система управління ЗІ практично будь-якої інформації. Для цього необхідно:

1. Уніфікувати основні положення концепції ЗІ.

2. Вирішити організаційно-правові питання організації робіт зі створення систем захисту, організації і забезпечення їх функціонування.

3. Розробити робочий інструмент для створення організації і забезпечення систем ЗІ.

2.3 Визначення і аналіз поняття загрози інформації

Під загрозою **інформації** будемо розуміти засіб виникнення на якому-небудь етапі життєдіяльності інформації такого явища або події, наслідком якого можуть бути небажані впливи на неї: порушення (або небезпека порушення) фізичної цілісності, несанкціонована модифікація (або загрози такої модифікації), несанкціоноване одержання (або загрози такого одержання) інформації. Ті чинники, наслідком яких можуть бути зазначені впливи на інформацію, назовемо дестабілізувальними.

Відповідно до технології і функціонування інформації, фактори або типи дестабілізувальних чинників такі:

1. Кількісна недостатність;
2. Якісна недостатність;
3. Відмова;
4. Збої;
5. Помилки;
6. Стихійні лиха;
7. Побічні явища.

Названі типи дестабілізувальних чинників визначаються так.

1. **Кількісна недостатність** – фізична недостача одного або декількох технічних компонентів для забезпечення необхідної захищеності інформації з розглянутих показників.

2. **Якісна недостатність** – недосконалість конструкції або організації одного або декількох компонентів, у силу чого не забезпечується необхідний ЗІ.

3. **Відмова** – порушення працездатності елемента, що призводить до неможливості виконання ним своїх функцій.

4. **Збій** – тимчасове порушення працездатності якогось елемента, наслідком чого може бути неправильне виконання ним у цей момент своїх функцій.

5. **Стихійне лихо** – спонтанно виникаюче неконтрольоване явище.

6. **Злочинна дія** – дія людей, спеціально спрямована на порушення захищеності інформації.

7. **Помилка** – неправильне (одноразове або систематичне) виконання однієї або декількох функцій, що відбуваються внаслідок специфічного (постійного або тимчасового) його стану.

8. **Побічне явище** – явище, що супроводжує виконання елементом своїх основних функцій, але наслідком якого може бути порушення захищеності інформації.

Джерелами дестабілізувальних чинників, тобто середовищем їхньої появи, можуть бути як компоненти технічних засобів, так і зовнішнє середовище. До повної множини джерел належать:

1. Люди, окремі особи або групи осіб, дії яких можуть бути причиною порушення ЗІ.

2. Технічні пристрої – технічні засоби.

3. Моделі, алгоритми і програми.

4. Технологія функціонування – сукупність засобів, прийомів, правил, заходів і угод, які використовуються у процесі опрацювання і передачі інформації.

5. Зовнішнє середовище – сукупність елементів, що можуть впливати на ЗІ.

Оскільки в загальному вигляді кожний із типів може виявлятися в кожному з перерахованих джерел, то на підставі цього можна описати механізм формування причин порушення ЗІ (рис. 2.2).

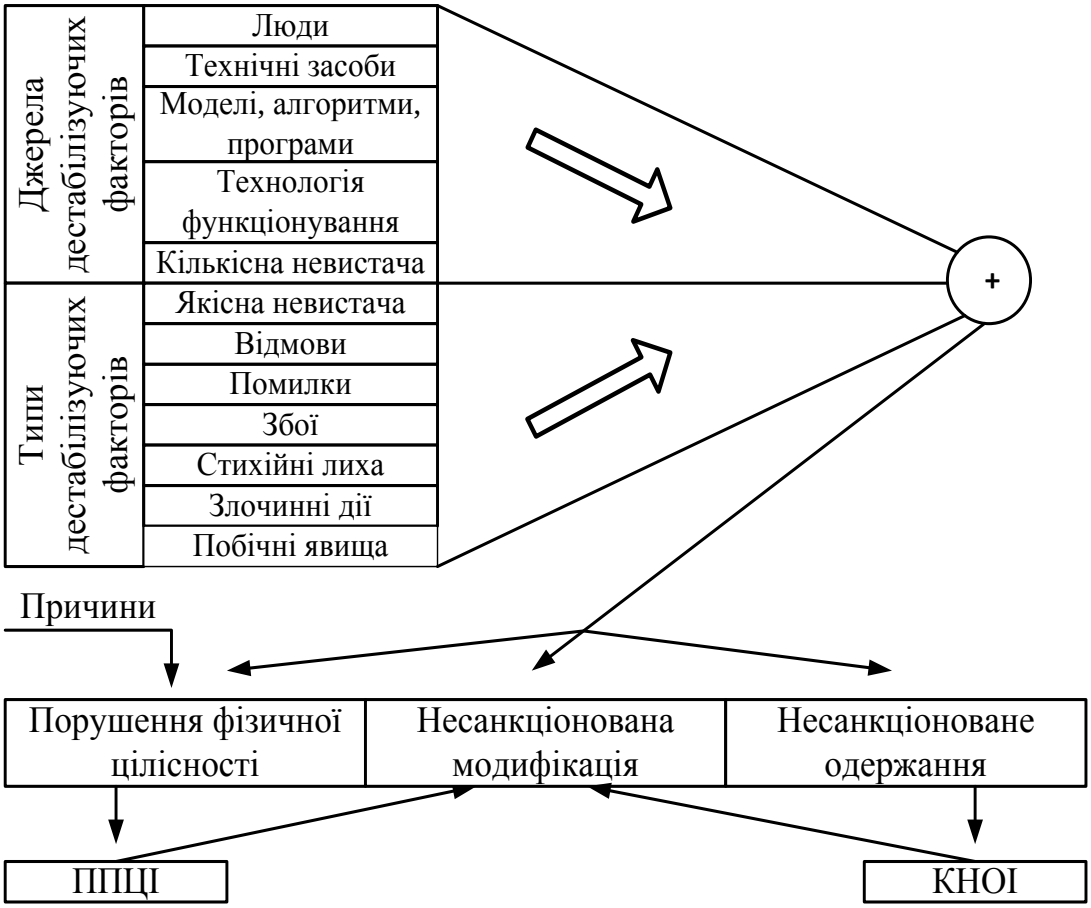


Рисунок 2.2 – Механізм формування причин порушення ЗІ

Аналіз показує, що деякі типи чинників у певних джерелах не можуть з’являтися за своєю природою.

Таким чином, усі чинники, наслідком яких може бути порушення захищеності інформації, можна розділити на групи, кожна з якої містить деяку кількість однорідних чинників.

Як уже відзначалося раніше, розрізняються три види уразливості: порушення фізичної цілісності, несанкціонована модифікація і несанкціоноване одержання; причому, різноманітні дестабілізувальні чинники в загальному випадку по-різному можуть впливати на різноманітні

види уразливості, то для конкретних і цілеспрямованих оцінок введемо поняття причин порушення захищеності для кожного виду уразливості. При цьому під причиною порушення захищеності будемо розуміти той конкретний прояв дестабілізувального чинника, що безпосередньо впливає на ЗІ.

Тоді, при системному розгляді проблем ЗІ, повинні самостійно розглядатися причини порушення ЗІ для кожного виду захисту. Причини порушення захищеності щодо фізичної цілісності інформації (ППЦІ) та несанкціонованого одержання інформації – канали несанкціонованого одержання інформації (КНОІ). Що стосується несанкціонованої модифікації, то вона може мати місце або внаслідок порушень цілісності (викривлень) інформації з якої-небудь причини, або внаслідок злочинних дій людей.

2.4 Система показників уразливості інформації і вимоги до первинних даних

Для системного оцінювання уразливості інформації необхідна система показників, яка відображала або об'єднувала б усі вимоги захисту інформації, а також технологію й умови функціонування інформації на таких етапах:

- у процесі автоматизованого опрацювання інформації;
- у процесі функціонування системи незалежно від опрацювання інформації.

Уразливість інформації в процесі розробки обумовлюється уразливістю утворюваних компонентів систем і утворюваних баз даних.

Умови автоматизованого опрацювання інформації характеризуються сукупністю таких параметрів:

- структурою системи; чим визначається склад об'єктів і елементів, які підлягають захисту;
- наявністю і кількістю ППЦІ та КНОІ;
- кількістю і категоріями осіб, що можуть бути потенційними порушниками статусу інформації, що захищається;
- режимами автоматизованого опрацювання інформації.

Уразливість інформації в процесі функціонування системи, незалежно від процесів опрацювання інформації, обумовлюється тим, що сучасні системи являють собою організаційну структуру з високою концентрацією інформації, що може бути об'єктом випадкових або злочинних впливів навіть у тих випадках, якщо її автоматизоване опрацювання не здійснюється.

За кількісну міру уразливості інформації найбільш доцільно взяти можливість порушення її цілісності або можливість несанкціонованого одержання при існуючих умовах збирання, передачі, обробки і зберігання.

Основними параметрами, що визначають можливість порушення цілісності інформації, є:

1. Кількість і типи тих структурних компонентів, в яких оцінюється уразливість інформації;
2. Кількість і типи ППЦІ, відносно яких оцінюється уразливість;
3. Види інформації, уразливість яких оцінюється.

Конкретний вид уразливості буде залежати від конкретного поєднання значень перерахованих вище параметрів. Основними параметрами уразливості інформації, з погляду несанкціонованого її одержання, є:

1. Кількість і типи структурних компонентів, в яких оцінюється уразливість;
2. Кількість і типи КНОІ, відносно яких оцінюється уразливість;
3. Кількість і типи потенційних порушників, що намагаються порушити уразливість інформації.

Таким чином, помітна достатньо глибока аналогія у формуванні повної множини показників уразливості відносно фізичної цілісності інформації та несанкціонованого її одержання. При наявності такої аналогії сформована уніфікована концепція захисту. Ця аналогія послідовно поширюється на вирішення всіх інших питань, пов'язаних з реалізацією концепції захисту. Тому надалі всі міркування будемо вести відносно ЗІ від несанкціонованого її одержання, маючи на увазі те, що отримані рішення легко можуть бути трансформовані на захист фізичної цілісності інформації.

Неважко помітити з рисунка 2.2, що в структурі два показники займають особливе положення.

Перший позначає уразливість інформації в одному структурному компоненті по одному КНОІ і відносно одного потенційного порушника.

Другий показник характеризує загальну уразливість, тобто уразливість інформації в цілому по всіх потенційно можливих КНОІ відносно всіх потенційно можливих порушників.

Перший показник – базовий, другий – загальний. Тоді інші показники назвемо частково узагальненими.

Для дослідження і практичного вирішення задач ЗІ поряд з розглянутими показниками необхідні ще й такі, що характеризують найбільш несприятливі ситуації з погляду уразливості інформації. Такими є: найуразливіший структурний компонент, найнебезпечніший КНОІ, найнебезпечніший порушник. Вони називаються екстремальними.

Необхідно враховувати також тимчасовий інтервал відносно числа найбільш значущих. Тому для розглянутих тут цілей ЗІ час як параметр уразливості інформації можна розділити на такі інтервали:

1. Дуже малі – інтервали, що можна вважати точками.
2. Малі – інтервали, що не можна зводити до точки.
3. Середні – інтервали, що не можна вважати малими, але на яких заздалегідь можна встановити стан кожного структурного елемента на

кожному його малому інтервалі.

4. Великі – інтервали, для яких не може бути виконана умова середніх інтервалів, але на яких із достатньою точністю все ж можна спрогнозувати послідовність і зміст функціонування основних компонентів.

5. Дуже великі – інтервали, на яких не є можливим виконати умову великих інтервалів.

Відзначимо, що параметри інтервалів істотно залежать від параметрів інформації і конкретних умов її функціонування.

Відповідно до викладеного, загальна класифікація й ідентифікація системи показників інформації зведена в таблицю 2.1.

Таблиця 2.1 – Ідентифікація показників уразливості інформації

ВИД	**Показники уразливості**	**Часовий інтервал оцінок уразливості**				
	найменування	Дуже малий	Малий	Середній	Великий	Дуже великий
ПРОСТІ	Базові	БЗДМ	БЗМЛ	БЗСР	БЗВЛ	БЗДВ
	Частково узагальнені	ЧУДМ	ЧУМЛ	ЧУСР	ЧУВЛ	ЧУДВ
	Загальні	ЗДМ	ЗМЛ	ЗСР	ЗВЛ	ЗДВ
ЕКСТРЕМАЛЬНІ	Найбільш уразливий компонент	УКДМ	УКМЛ	УКСР	УКВЛ	УКДВ
	Найбільш небезпечний КНОІ	ННДМ	ННМЛ	ННСР	ННВЛ	ННДВ
	Найбільш небезпечна категорія	ННБДМ	ННБМЛ	ННБСР	ННБВЛ	ННБДВ

Запитання для самоконтролю

1. Що розуміють під захистом інформації?
2. Що розуміють під надійністю інформації?
3. Які об’єкти захисту існують?
4. У яких зонах здійснюється захист інформації?
5. Чим характеризуються зміни в розвитку обчислювальної техніки?

6. До чого може призвести зниження якості інформації?

7. На які класи розділені шляхи несанкціонованого одержання інформації?

8. Перерахуйте групи можливих шляхів несанкціонованого одержання інформації.

9. Які положення містить у собі системний підхід до ЗІ?

10. Який висновок був отриманий у рамках системно-концептуального підходу до проблем ЗІ? Що випливає з цього висновку?

11. Які елементи визначають концепції ЗІ? Дайте їхні означення.

12. На які дві частини розділені дані елементи?

13. Що необхідно для побудови уніфікованої концепції ЗІ?

ГЛАВА 3
ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Поняття інформаційної безпеки

Словосполучення «інформаційна безпека» у різних контекстах може мати різне значення.

У даному курсі наша увага буде зосереджена на зберіганні, обробці та передачі інформації незалежно від того, якою мовою вона закодована, хто або що є її джерелом та який психологічний вплив вона має на людей. Тому термін «інформаційна безпека» використовується у вузькому змісті так, як це прийнято, наприклад, в англомовній літературі.

Під інформаційною безпекою ми будемо розуміти захищеність інформації й інфраструктуру, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримувальної інфраструктури. (Далі ми пояснимо, що варто розуміти під підтримувальною інфраструктурою.)

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин й інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій.

Із цього положення можна зробити два важливих висновки.

1. Інформаційна безпека може істотно різнитися.

2. Інформаційна безпека не зводиться винятково до захисту від несанкціонованого доступу до інформації, це принципово більш широке поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків й/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі.

Повертаючись до питань термінології, відзначимо, що термін «комп'ютерна безпека» (як еквівалент або замінник ІБ) видається нам занадто вузьким. Комп'ютери – тільки одна зі складових інформаційних систем, і хоча наша увага буде зосереджена в першу чергу на інформації, що зберігається, обробляється й передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових й, у першу чергу, найслабшою ланкою, якою в переважній більшості випадків є людина, яка написала, наприклад, свій пароль на «гірчичнику», наклеєному на монітор.

Відповідно до визначення інформаційної безпеки, вона залежить не тільки від комп'ютерів, але й від інфраструктури, яка її підтримує, до якої

можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговувальний персонал. Ця інфраструктура має самостійну цінність, але нас цікавить, як вона впливає на виконання інформаційною системою запропонованих їй функцій.

Звернемо увагу, що у визначенні ІБ перед іменником «збиток» стоїть прикметник «неприйнятний». Вочевидь, застрахуватися від усіх видів збитків неможливо, тим більш неможливо зробити це економічно доцільним чином, коли вартість захисних засобів і заходів перевищує розмір очікуваного збитку. Іноді таким неприпустимим збитком є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальне (грошове) вираження, а метою захисту інформації стає зменшення розмірів збитків до припустимих значень.

3.2 Основні складові інформаційної безпеки

Інформаційна безпека – багатогранна, можна навіть сказати, багатовимірна сфера діяльності, у якій успіх може принести лише систематичний, комплексний підхід.

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на категорії: забезпечення доступності, цілісності й конфіденційності інформаційних ресурсів і підтримувальної інфраструктури.

Іноді в сукупність основних складових ІБ входить захист від несанкціонованого копіювання інформації, але, на наш погляд, це занадто специфічний аспект із сумнівними шансами на успіх, тому ми не будемо його виділяти.

Пояснимо поняття доступності, цілісності й конфіденційності.

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування й несанкціонованої зміни.

Нарешті, конфіденційність – це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (купуються) для одержання певних інформаційних послуг. Якщо з тих або інших причин надати ці послуги користувачам стає неможливо, це, мабуть, завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим аспектам, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво провідна роль доступності виявляється в різного роду системах керування – виробництвом, транспортом і т. п. Зовні менш драматичні, але також досить неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг,

якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги й т. п.).

Цілісність можна підрозділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (яка стосується коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень із метою виявлення крадіжки, перевпорядкування або дублювання окремих повідомлень.

Цілісність, виявляється, є найважливішим аспектом ІБ у тих випадках, коли інформація слугує «керівництвом до дії». Рецептура ліків, запропоновані медичні процедури, набір і характеристики комплектуючих, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може виявитися в буквальному значенні смертельним. Неприємно й перекручування офіційної інформації, будь-то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – найпроблемніший у нас в країні аспект інформаційної безпеки. На жаль, практична реалізація засобів із забезпечення конфіденційності сучасних інформаційних систем натрапляє в Україні на серйозні труднощі. По-перше, відомості про технічні канали витоку інформації є закритими, так що більшість користувачів позбавлені можливості скласти уявлення про потенційні ризики. По-друге, на шляху використовуваної криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони й технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить перекручені відомості?

Нарешті, конфіденційні моменти є також у багатьох організаціях (навіть у згадуваних вище навчальних інститутах намагаються не розголошувати відомості про зарплату співробітників) і окремих користувачів (наприклад, паролі).

3.3 Важливість і складність проблеми інформаційної безпеки

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні ми не розглядали останню – національному, галузевому, корпоративному або персональному.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, який полягає у тому, що інформаційна безпека є складовою частиною інформаційних технологій – сфери, що розвивається надзвичайно високими темпами. Тут важливі не стільки окремі рішення (закони, навчальні курси, програмно-

технічні засоби), що є на даний час, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ. Варто виходити з того, що необхідно конструювати надійні системи (інформаційної безпеки) із залученням ненадійних компонентів (програм). У принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу ІС.

Наведемо ще кілька цифр. У березні 2000 року був опублікований черговий, четвертий за рахунком, річний звіт «Комп'ютерна злочинність і безпека-2000: проблеми й тенденції» (Issues and Trends: 2000 CS1/FB1 Computer Crime and Security Survey). У звіті відзначається різке зростання кількості звернень до правоохоронних органів із приводу комп'ютерних злочинів (32% із числа опитаних); 30% респондентів повідомили про те, що їхні інформаційні системи були зламані зовнішніми зловмисниками; атакам через Internet піддавалися 57% опитаних; у 55% випадків відзначалися порушення з боку власних співробітників. Примітно, що 33% респондентів на питання «чи були зламані ваші Web-сервери й системи електронної комерції за останні 12 місяців?» відповіли «не знаю».

В аналогічному звіті, опублікованому у квітні 2012 року, цифри змінилися, але тенденція залишилася колишньою: 90% респондентів (переважно з великих компаній й урядових структур) повідомили, що за останні 12 місяців у їхніх організаціях мали місце порушення інформаційної безпеки; 80% констатували фінансові втрати від цих порушень; 44% (223 респонденти) змогли й/або захотіли оцінити втрати кількісно, загальна сума становила більше 455 млн доларів.

Лише 22% респондентів заявили про відсутність порушень інформаційної безпеки. Поряд з поширенням вірусів відзначається різкий ріст кількості зовнішніх атак.

Збільшення кількості атак – ще не найбільша неприємність. Гірше те, що постійно виявляються нові уразливі місця в програмному забезпеченні і, як наслідок, з'являються нові види атак.

Так, в інформаційному листі Національного центру захисту інфраструктури США (National Infrastructure Protection Center, NIPC) від 21 липня 2009 року повідомляється, що за період з 3 по 16 липня 2009 року виявлено дев'ять проблем з ПЗ, ризик використання яких оцінюється як середній або високий (загальна кількість виявлених уразливих місць дорівнює 17). Серед «потерпілих» операційних платформ – майже всі різновиди ОС Unix, Windows, MacOS, так що ніхто не може почуватися спокійно, оскільки нові помилки відразу починають активно використовуватися зловмисниками.

У таких умовах системи інформаційної безпеки повинні вміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам

автоматизованим і скоординованим. Іноді напад триває частки секунди; часом промацування уразливих місць ведеться повільно й розтягується на години, так що підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ – доступності, цілісності або конфіденційності.

Запитання для самоконтролю

1. Які засоби спрямовані на захист інформаційної безпеки?
2. Назвіть основні аспекти ІБ.
3. Що таке захист інформації?
4. Комп’ютерна злочинність у світі.
5. Що розуміють під інформаційною безпекою?
6. Основні складові інформаційної безпеки.
7. Дайте означення конфіденційності.
8. Дайте означення цілісності.
9. Важливість і складність проблеми інформаційної безпеки.
10. Дайте означення доступності.

ГЛАВА 4
КОНЦЕПЦІЇ ТА МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кваліфікація осіб, відповідальних за безпеку інформаційних технологій у межах організацій, повинна бути достатньою для адаптування матеріалів до конкретних потреб організацій.

Керування безпекою інформаційних технологій – це процес, що його використовують для досягнення і забезпечення необхідних рівнів конфіденційності, цілісності, доступності, обліковості, достовірності і надійності. До функцій керування безпекою інформаційних технологій належать:

- визначання цілей, стратегій і методик організування захисту інформаційних технологій;
- визначання необхідних умов під час організування захисту інформаційних технологій;
- ідентифікування й аналізування загроз безпеки для активів інформаційних технологій організації;
- ідентифікування й аналізування ризиків;
- визначання відповідних засобів захисту;
- контроль застосування і функціонування засобів захисту, що необхідно для ефективного захисту інформації і нормального функціонування організації в цілому;
- розробка і реалізація програми компетентності в захисті;
- виявляння і реагування на інциденти.

Для повноцінної реалізації цих функцій керування безпекою в системах інформаційних технологій захист повинен бути невід'ємною частиною загального плану керування організацією (ДСТУ ISO/IEC TR 13335-1:2003).

4.1 Концепція керування безпекою інформаційних технологій

Сприйняття концепцій, що відповідають мікрополітиці й оточенню, у яких працює організація, може дати значний ефект у створенні підходів до захисту в цілому. Крім того, вони можуть вплинути на окремі підрозділи організації, відповідальні за захист. У деяких випадках уряд встановлює чи скасовує відповідальність уведенням у дію відповідних законів. В інших випадках відповідальність призначає власник чи керівник.

Підхід

Для визначання необхідних умов безпеки інформаційних технологій у межах організації потрібно застосовувати системний підхід. Цей підхід також застосовують для організації захисту в інформаційних технологіях і наступному керуванні ним. Процес керування безпекою інформаційних технологій містить такі дії:

1. Розробка стратегії захисту інформаційних технологій;
2. Ідентифікація ролей і обов'язків у межах організації;
3. Керування ризиком, ідентифікацією й оцінюванням:
- активів, що будуть захищені,
- загроз,
- подразнень,
- уражень,
- ризиків,
- засобів захисту,
- залишкових ризиків,
- обмежень;
4. Керування конфігурацією;
5. Керування змінами;
6. Планування випадкових процесів і планування відновлення у випадку непередбачених ситуацій;
7. Вибір засобів захисту та їхнє застосування;
8. Встановлення компетентності щодо захисту разом з:
- експлуатацією,
- контролем безпеки,
- перевіркою,
- переглядом,
- обробкою інцидентів.

Цілі безпеки, стратегії і методики

Цілі безпеки, стратегії і методики треба брати за основу для здійснення ефективного захисту інформаційних технологій в організації. Вони супроводжують діяльність організації й сукупно гарантують стабільність усіх засобів захисту та їхніх взаємозв'язків.

Цілі визначають, чого потрібно досягнути, стратегії визначають, як досягти цих цілей, методики визначають, як виконувати конкретні заходи. Цілі, стратегії і методики можуть бути розроблені за рівнями підпорядкованості організації. Вони мають відображати організаційні вимоги і брати до уваги будь-які зв'язки, вони також мають гарантувати незмінність безпеки на кожному рівні зокрема і на всіх рівнях разом. Безпека – це відповідальність усіх рівнів керівництва організації протягом усіх фаз життєвого циклу системи. Цілі, стратегія і методики мають бути підтримані й модифіковані на підставі результатів періодичного перегляду безпеки (наприклад, аналізу ризику, аудиту захищеності) і змін в цілях підвищення ділової активності.

Методика захисту по суті містить принцип захисту і директиви для організації в цілому. Методики захисту мають детально відображати методики, охоплюючи ті, які стосуються індивідуальних прав, вимог законодавства і стандартів.

Методика захисту інформаційних технологій має відображати істотні принципи безпеки і директиви, застосовувані до корпоративної методики

захисту, та загальне використання систем інформаційних технологій в організації.

Методика захисту системи інформаційних технологій має відображати принципи захисту і директиви у межах методики безпеки інформаційних технологій. Вона має також містити детальний опис специфічних вимог безпеки і засобів захисту, які будуть застосовані, а також метод, використаний для забезпечення відповідного захисту. В усіх випадках важливим є вибір ефективного підходу до потреб діяльності організації.

Цілі, стратегії й методики систем захисту в інформаційних технологіях описують з позиції безпеки. Їх звичайно описують природною мовою, однак системи захисту можуть бути формалізовані з використанням математичної мови. Системи захисту призначені для забезпечення таких критеріїв безпеки інформаційних технологій, як:

- конфіденційність;
- цілісність;
- доступність;
- обліковість;
- достовірність;
- надійність.

Цілі, стратегії й методики визначають рівень безпеки в організації, а також допустимий рівень ризику і непередбачуваних обставин в організації.

4.2 Елементи безпеки

Нижченаведені положення на високому рівні описують головні елементи, задіяні в процесі керування захистом. Кожен з елементів визначений і наведені його основні супутні чинники.

Активи

Наявність відповідного керування активами важлива для забезпечення успіху організації і є головною рисою всіх рівнів керування. До активів організації належать:

- фізичні об’єкти (апаратне забезпечення, засоби зв’язку, будівлі тощо);
- інформація/дані (наприклад, документи, бази даних);
- програмне забезпечення;
- здатність виробляти деяку продукцію чи надавати послуги;
- людські ресурси;
- нематеріальна власність (наприклад, імідж, символіка).

Більшість із цих активів має потребу в певному захисті. У випадку, коли активи не мають належного рівня захищеності, необхідно застосовувати до них механізми оцінювання ризиків.

Якщо йдеться про перспективність програми безпеки організації, то немає сенсу забезпечувати захист і здійснювати його подальшу підтримку,

якщо чітко не визначені активи організації. У більшості випадків процес ідентифікації активів і визначення їхніх розмірів можна виконати на досить високому рівні і без дорогого, детального і тривалого аналізу. Рівень деталізації для цього аналізу визначають значенням часу і вартістю аналізу стосовно цінності активів, виходячи з цілей захисту. Зокрема, ці підходи можна застосовувати до груп активів.

Розглядають такі характеристики активів, як їхня цінність і (або) критичність і різноманітність застосовуваних засобів захисту. Необхідність застосування засобів захисту до активів визначають також їхньою вразливістю до впливу специфічних загроз. Якщо ці аспекти очевидні для власника активів, їх треба зафіксувати на початкових стадіях. Оточення і мікрополітика, у яких діє організація, можуть впливати на активи та їхні характеристики. Наприклад, мікрополітика організації може розглядати як дуже важливі завдання захисту особистої інформації. У діяльності міжнародних організацій і їхніх систем інформаційних технологій вагому роль відіграють оточення і мікрополітика.

Загрози

Активи є об'єктами для багатьох видів загроз. Загроза потенційно є причиною небажаного інциденту, що здатний заподіяти шкоду системі чи організації та її активам. Ця шкода є результатом прямої чи непрямої атаки на інформацію, якою оперує система чи служба інформаційних технологій, наприклад, її несанкціоноване знищення, розкриття, зміна, перекручування, втрата доступності чи втрату взагалі. Загроза може здійснитися, заподіяти шкоду у випадку наявності в активах уразливих місць. Загрози, причиною яких є людина, розділяють на випадкові й навмисні. І випадкові, і навмисні загрози повинні бути ідентифіковані й визначені їхні рівні й імовірність.

Приклади загроз наведені в табл. 4.1.

Таблиця 4.1 – Приклади загроз

Людські		**Довкілля**
Навмисні	**Випадкові**	
Підслуховування Зміна інформації Злом системи Навмисний програмний код Злодійство	Помилки і недогляд Вилучення файлу Неправильна маршрутизація Фізичні ушкодження	Землетрус Блискавка Потоп Пожежі

Статистичні дані накопичуються збиранням інформації про різні типи загроз із довкілля. Ці дані повинні бути отримані і використовуватися організацією в процесі виявляння загрози. Деякі загрози мають спрямовану дію на окремі елементи організації, наприклад, викликають збої інформаційних систем. Загрози можуть мати специфічне територіальне походження, наприклад ушкодження будівель від ураганів чи спалахів

блискавки. Загроза може діяти зсередини організації, наприклад, саботаж службовців, чи зовні, наприклад, навмисний злом чи промислове шпигунство. Шкода, викликана небажаним інцидентом, може мати тимчасовий, легко відновлюваний характер чи остаточний і безповоротний, як у випадку знищення активів.

Обсяги шкоди, заподіяної загрозою, можуть варіюватися в широких межах для кожного конкретного випадку. Наприклад:

- програмний вірус може заподіяти різні обсяги шкоди залежно від його впливу;
- землетрус у зоні специфічного територіального розташування може мати різну силу в кожному конкретному випадку.

Такі загрози часто характеризуються обсягами заподіюваної ними шкоди. Наприклад:

- вірус можна охарактеризувати як такий, що руйнує чи не руйнує;
- силу землетрусу можна виміряти за шкалою Ріхтера.

Прояви загроз можуть впливати на більш ніж один вид активів. У цьому випадку вони ведуть до різних конфліктів, що впливають на активи. Наприклад, програмний вірус може вразити єдину інформаційну систему. Однак той самий програмний вірус, потрапивши на основний мережний файл-сервер, може поширитися на декілька інформаційних систем. Різноманітні загрози чи їх прояв у різних місцях можуть постійно завдавати великої шкоди. Якщо шкода, заподіяна загрозою, є постійною, то можна використовувати універсальний визначений підхід. Однак якщо обсяги заподіяної шкоди змінюються в широких межах, необхідно використовувати конкретизований підхід, що відповідає локалізації загрози.

Загрози характеризуються даними, що містять корисну інформацію. Приклади такої інформації:

- джерело (внутрішнє чи зовнішнє);
- мотивація, наприклад збагачення, конкуренція;
- частота появи;
- серйозність загрози.

Оточення й мікрополітика організації можуть мати істотне значення й обумовлювати вплив загроз на організацію.

У критичних ситуаціях деякі загрози в певних мікрополітичних середовищах не розглядають і вважають безпечними. Всі аспекти щодо оточення й діяльності треба розглядати стосовно загроз.

Вразливості

Вразливості звичайно пов’язані зі слабкими місцями в активах, а саме: у розташуванні організації, процесах, персоналі, керуванні, адмініструванні, апаратному та програмному забезпеченні, в інформації. Їх використовують як потенційну загрозу для заподіяння шкоди системі інформаційних технологій чи діловій активності в цілому. Вразливість сама по собі не є причиною шкоди; вразливість є тільки умовою чи множиною умов, які

можуть допустити вплив загрози на активи. Вразливість, що виникає з різних джерел, наприклад від активів, повинна братися до уваги. Вразливість може зникнути чи втратити актуальність, якщо відбудуться зміни в активах.

Вразливість послаблює експлуатовану систему і може призводити до небажаних наслідків. Вразливість – непряма причина шкоди, заподіюваної загрозою. Наприклад, відсутність механізмів контролювання за доступом до службових і гостьових приміщень – вразливість, що може дати змогу загрозі з легкістю впливати на активи і призводити до їхньої втрати. Специфіка конкретної системи чи організації обумовлює те, що не всі вразливості чутливі до загроз. Треба негайно приділяти увагу вразливості, що має відповідну загрозу. Оскільки оточення може змінюватися динамічно, всі вразливості потрібно постійно перевіряти щодо відкритості до старих і нових загроз.

Аналіз вразливості – це експертиза слабких місць, вразливих до ідентифікованих загроз. Цей аналіз повинен брати до уваги середовище й наявні засоби захисту. Вразливість специфічної системи чи активів до загрози описує способи, якими система чи активи можуть бути ушкоджені.

Ураження

Ураження – наслідок небажаного інциденту, спричинений навмисним чи випадковим впливом на активи. Наслідки можуть бути згубними для деяких активів, нанести ушкодження системі інформаційних технологій, призвести до втрати конфіденційності, цілісності, доступності, обліковості, достовірності чи надійності. Можливі також і такі побічні наслідки, як фінансові втрати частки чи всього ринку, іміджу компанії. Уведення кількісних характеристик уражень дає можливість знаходити компромісне рішення між втратами в результаті небажаного інциденту і витратами на засоби захисту, які страхують від небажаного інциденту. Необхідно враховувати також і частоту появи небажаних інцидентів. Це особливо важливо, коли заподіяна шкода в кожному окремому випадку незначна, проте сумарні втрати як наслідок багатьох випадків протягом періоду часу будуть дуже великими. Запобігання ураженням є важливим складником у зменшенні ризику і виборі засобів захисту.

Кількісні і якісні характеристики ураження можна отримати через:

- визначення фінансових витрат;
- надання емпіричного рангу серйозності ураження, наприклад, від одного до десяти;
- використовування залежностей, обраних із заздалегідь визначеного списку, наприклад: низько, середньо, високо.

Ризик

Ризик – імовірність того, що дана загроза, впливаючи через вразливість організації, заподіє втрати чи пошкодження активів, а значить прямим чи опосередкованим шляхом заподіє збитки організації. Разові чи численні

загрози, що повторюються, можуть скористатися окремою чи множинною вразливістю.

Сценарій ризику описує, як специфічна загроза чи група загроз може скористатися конкретною вразливістю чи групою вразливостей, що шкодять активам. Ризик характеризується комбінацією двох чинників: імовірністю появи небажаного інциденту і його ураженням. Будь-яка зміна стану активів, загроз, вразливостей і засобів захисту може вплинути на ризики. Чим раніше будуть виявлені зміни в самій системі чи в її оточенні, тим більше можливостей для дій, що зменшують ризик.

Засоби захисту

Засоби захисту – засоби, процедури чи механізми, що можуть захистити від загроз, зменшити вразливість, обмежити ураження внаслідок небажаного інциденту, виявити небажані інциденти і полегшити процес відновлення. Ефективний захист звичайно потребує комбінації різних засобів захисту для забезпечення багаторівневого захисту активів. Наприклад, механізми контролю доступу, що їх застосовують у інформаційних системах, повинні супроводжуватися засобами керування аудитом, увагою і навчанням персоналу, безпекою фізичних засобів. Деякі засоби захисту вже існують як частина оточення чи як властивий аспект активів, або вже існують в системі чи організації.

Засоби захисту можуть виконувати одну чи кілька таких функцій: виявляння, стримування, запобігання, обмеження, корекція, відновлювання, контроль й усвідомлення. Відповідний добір засобів захисту – невід'ємна частина правильно виконаної програми захисту. Багато засобів захисту можуть виконувати декілька функцій. Часто вигідніше і дешевше вибрати засоби захисту, що реалізують декілька функцій. Деякі приклади ділянок, де використовують засоби захисту:

- фізичне оточення;
- технічне оточення (апаратні засоби, програмне забезпечення і зв'язок);
- персонал;
- адміністрація.

Поняття безпеки – засоби захисту та їхній взаємозв'язок з персоналом. Оточення і внутрішні умови, в яких діє організація, часто впливають на вибір засобів захисту і на розуміння безпеки організації в цілому. Деякі засоби захисту посилають суворе і чітке повідомлення про тривогу відкритим текстом до підрозділу організації, яка займається захистом. Реагуючи на це повідомлення, важливо точно визначити засоби захисту, що не суперечать мікрополітиці та (або) оточенню, у якому діє організація.

Приклади засобів захисту:

- файрволи в мережі;
- моніторинг і аналіз мережі;
- шифрування з метою забезпечення конфіденційності;
- цифрові підписи;

- програми антивірусів;
- резервні копії інформації;
- безперебійні джерела живлення;
- механізми контролю доступу.

Залишковий ризик

Ризики, зазвичай, лише частково зменшуються за допомогою засобів захисту. Часткове зменшення – єдине, що найчастіше може бути досягнуто, подальші зменшення спричиняють невиправданий ріст вартості. Це показує, що завжди наявні так звані залишкові ризики. Частина оцінок з безпеки або відповідає потребам організації, або допускає залишковий ризик. Цей процес відомий як допускання ризику.

Керування треба здійснювати з урахуванням усіх залишкових ризиків в умовах уражень та імовірності їхньої появи. Рішення про допустимість залишкового ризику повинні приймати ті, хто приймає рішення у разі появи небажаного інциденту і хто уповноважений застосовувати додаткові засоби захисту, якщо рівень залишкового ризику є неприйнятним.

Обмеження

Обмеження звичайно встановлює чи визнає керівництво організації з урахуванням чинників оточення, в якому діє організація. Розглядають, наприклад, такі обмеження:

- організаційні;
- фінансові;
- навколишні;
- персональні;
- часові;
- юридичні;
- технічні;
- мікрополітичні/соціальні.

Усі ці чинники треба враховувати під час вибору і застосування засобів захисту. Періодично наявні та нові обмеження треба переглядати, фіксуючи будь-які зміни. Необхідно також відзначити, що обмеження можуть змінюватися з часом, географією та соціальною еволюцією, а також з мікрополітикою організації. Оточення і мікрополітика, у яких діє організація, можуть негативно впливати на різні елементи безпеки, особливо на загрози, ризики і засоби захисту.

4.3 Процес керування безпекою інформаційних технологій

Керування безпекою інформаційних технологій – тривалий процес, що складається з багатьох інших процесів. Деякі процеси, як керування конфігурацією настроювання і керування змінами, застосовуються не тільки до питань безпеки. Як показує досвід, один із процесів є дуже корисним у керуванні безпекою інформаційних технологій – це керування ризиком і його підпроцес – аналіз ризику. Деякі аспекти керування безпекою

інформаційних технологій охоплюють керування ризиком, аналіз ризику, керування змінами і організацією системи.

Налаштування системи

Налаштування системи – процес фіксації тенденції змін у системі, який виконують формально чи неформально. Первинною метою керування налаштуванням, з погляду безпеки, є гарантування того, що зміни в системі не знизять ефективність засобів захисту і загальну безпеку організації.

Метою налаштування, з погляду безпеки, є розпізнання змін, щоб вони не впливали на безпеку засобів шляхом проведених запобіжних змін у системі інформаційних технологій. У деяких випадках можуть з'явитися причини для змін, що призводять до зниження захищеності. У таких ситуаціях привнесене в захист зниження має бути оцінено, й у відповідь мають бути визначені також керівні рішення на підставі всіх залежних чинників. Іншими словами, усі зміни в системі повинні спричинити відповідні зміни у захисті. Ще одна мета керування налаштуванням полягає в гарантуванні, що зміни в системі відображені в інших документах, а саме: відновлювання після нещасних випадків і плани непередбачених обставин. Якщо зміна дуже важлива, то необхідно проаналізувати деякі чи всі системні засоби захисту.

Керування змінами

Керування змінами – процес визначання потреб в нових засобах захисту у випадках, коли відбуваються зміни в системі інформаційних технологій.

Системи інформаційних технологій і оточення, у якому вони працюють, постійно змінюються. Ці зміни – результат надання нових можливостей інформаційних технологій і послуг чи результат виявлення нових загроз і уражень. Зміни в системах інформаційних технологій містять:

- нові процедури;
- нові можливості;
- модернізацію програмного забезпечення;
- переробку апаратного забезпечення;
- появу нових користувачів у зовнішніх чи анонімних групах;
- додаткову роботу з мережами і зв'язками.

Коли відбувається чи планується зміна в системі інформаційних технологій, важливо визначити ураження в захисті системи, якщо вони були. Якщо в системі є відділ керування конфігурацією чи інша організаційна структура, то повинен бути призначений відповідальний за безпеку інформаційних технологій у відділ для керування спеціальними змінами в системі, а також визначена відповідальність за прийняття рішень залежно від того, чи призведе зміна до уражень у захисті, і якщо так, то яким чином. Для важливіших змін, що охоплюють придбання нових апаратних засобів, програмного забезпечення чи створення послуг, також

потрібен аналіз, що визначає необхідні нові вимоги безпеки. З іншого боку, багато змін у системах насправді незначні і не потребують широкого аналізу, необхідного для важливіших змін. Для обох типів змін повинна бути оцінена величина ризику, виходячи з користі і витрат. Для незначних змін рішення можуть бути прийняті неформально, на зустрічах, але результати і рішення керівництва повинні бути задокументовані.

Керування ризиком

Дії з керування ризиком найбільш ефективні, якщо вони виконуються в процесі всього життєвого циклу системи. Процес керування ризиком сам по собі є важливим циклом активності. У той час, як нові системи можна супроводжувати повним циклом, для успадкованих систем це може бути ініційовано з будь-якого моменту всього життєвого циклу системи. Стратегія може вимагати робити ревізію у певних інтервалах життєвого циклу системи чи у певні часові інтервали. Наступними можуть бути дії з попереднього розгляду-перевірки застосування засобів захисту. Також може виявитися необхідність керування ризиком у процесі створення і розробки системи, це гарантуватиме, що безпека розроблена і реалізована з максимальною ефективністю щодо вартості та часу.

Незалежно від того, які методи чи технічні засоби використовують у керуванні ризиком, важливо забезпечити прийнятний компроміс у зменшенні часових витрат і витрат ресурсів, задіяних у визначанні і застосуванні засобів захисту, поки існує впевненість у відповідному захисті всіх систем.

Керування ризиком – процес порівняння оцінки ризиків з вигодами і (або) витратами на засоби захисту та забезпечення стратегії їхнього застосування й методики безпеки системи, створеної з урахуванням корпоративної методики безпеки інформаційних технологій і завдань бізнесу. Треба розглядати різні типи засобів захисту і проводити аналіз вартості та (або) вигоди. Засоби захисту вибирають з урахуванням ризиків і потенційних уражень. Також треба брати до уваги рівень прийнятного залишкового ризику.

Засоби захисту безпосередньо можуть містити уразливості і призводити до нових ризиків. Тому потрібно з обережністю вибирати відповідні засоби захисту, щоб не тільки знижувати ризики, але і не створювати потенційно нові.

Нижченаведені положення описують додаткові особливості процесів керування ризиком.

Аналіз ризику

Аналіз ризику ідентифікує ризики, що потребують керування чи врахування. З погляду безпеки інформаційних технологій аналіз ризику для систем інформаційних технологій охоплює аналіз номінальної вартості загроз і уражень. Ризики оцінюють відносно потенційного ураження, що може бути викликано порушенням конфіденційності, цілісності, доступності, обліковості, достовірності чи надійності. Результат

оглядового аналізу ризику – положення про найбільш ймовірні ризики стосовно активів.

Аналіз ризику є частиною керування ризиком і може бути виконаний без додаткових витрат часу і ресурсів після оглядового короткого аналізу всіх систем. Це дозволяє встановити, які системи можуть бути адекватно захищені за допомогою практичних вказівок чи базовими засобами керування, і ті системи, що їх можна використовувати після детальнішого аналізу ризику. Це питання практично охоплює комплект інструкцій і базових настанов, які можуть бути використані як базис для домовленості щодо задоволення основних потреб захисту.

Обліковість

Забезпечення ефективного захисту потребує обліковості (звітності) точно визначених завдань і розподілу обов'язків у питаннях безпеки. Обов'язки і обліковість мають бути доручені власникам активів, постачальникам і користувачам ресурсів систем інформаційних технологій. Отже, володіння активами і пов'язані з ними обов'язки щодо захисту з подальшим перевірянням реалізованого захисту є важливими чинниками для ефективного захисту.

Компетентність у захисті

Компетентність у захисті – це істотний елемент ефективного захисту. Відсутність компетентності в захисті і недостатність досвіду в захисті персоналу організації можуть призвести до значного зниження ефективності системи захисту. Людей в організації вважають однією з найслабших ланок захисту. Щоб бути упевненим у належному рівні компетентності в захисті організації, важливо дотримуватися і розвивати програму компетентності захисту. Метою програми компетентності захисту є пояснення робітникам, компаньйонам і компаніям-постачальникам:

– цілей, стратегій і методик захисту;

– потреб у захисті і пов'язаних з ними функцій та обов'язків.

Крім того, має бути розроблена програма, що гарантує розподіл обов'язків із захисту між співробітниками, компаньйонами і компаніями-постачальниками.

Програма компетентності захисту повинна виконуватися на всіх рівнях організації: від вищого керівництва до найнижчої ланки. Необхідно часто розробляти документи, що стосуються підвищення компетентності людей у різних ролях і обов'язках у різних підрозділах організації. Всебічне розуміння програми безпеки розвивається і передається поступово. Кожна стадія формується на основі попередньої, починаючи з концепцій захисту і до обов'язків з виконання і контролю безпеки.

Програми компетентності захисту в межах організації мають ряд етапів. Один з таких етапів – розробка і розподіл документації щодо компетентності в захисті (наприклад, плакатів, бюлетенів, брошур чи документів). Призначення цих матеріалів – збільшити загальну компетенцію службовців і контрактників. Наступний етап – організація курсів для навчання

службовців з питань захисту. Також необхідні поглиблені курси професійного рівня для специфічних аспектів захисту.

У деяких випадках є ефективним об'єднати всі повідомлення з безпеки в окремі навчальні програми. Цей підхід є альтернативою чи повноцінною заміною програми компетентності захисту. Для розвитку програми компетентності захисту, що взаємозалежна з необхідними мікрополітичними й адміністративними умовами даної організації, треба розглядати такі аспекти:

- аналіз потреб;
- програма забезпечення;
- контроль;
- зміст програми компетентності.

Контроль

Використання засобів захисту треба постійно контролювати для гарантії, що вони функціонують правильно, що зміни в оточенні не нейтралізували їхню ефективність і що обліковість активізована і функціонує. Автоматичний перегляд й аналіз системних журналів – ефективний спосіб, що допомагає забезпечити контроль. Цей спосіб також можна використовувати для пошуку небажаних подій, що допоможе перешкодити виникненню цих подій.

Ефективність засобів захисту системи безпеки треба періодично перевіряти. Це здійснюють контролем і гнучкою перевіркою для гарантії, що засоби захисту функціонують і використовуються передбачуваним способом. Вихідні дані багатьох засобів захисту треба перевіряти на наявність вагомих для безпеки подій, наприклад, журналів, які є сигнальною звітною документацією. Загальна система функцій аудиту може надати корисну інформацію про перспективність захисту. Цю інформацію можна відповідно використовувати.

Плани відновлювання після уражень

Таке планування інформує щодо того, як поводитися й виконувати роботу, коли супровідні процеси, разом з системами інформаційних технологій, руйнуються чи стають недоступними.

Ці плани можуть передбачати звернення до можливих комбінацій з численних сценаріїв, що охоплюють:

- різноманітність періодів переривання;
- втрати різних типів засобів;
- повну втрату фізичного доступу до приміщень;
- що необхідно зробити для повернення до стану, що передував порушенню.

Плани відновлювання після нещасних випадків описують як відновити функціювання системи інформаційних технологій після небажаного інциденту та охоплюють:

- критерії, за яких відбуваються катастрофи;
- обов'язки щодо активізації дій з відновлювання;

- відповідальність за різні дії відновлювання;
- опис дій відновлювання.

4.4 Моделі інформаційної безпеки

Результати аналізу об’єктів, які досліджуються, мають конструктивний характер, коли на їхній основі створюються теоретичні фізичні і математичні моделі об’єкта.

Теоретична модель об’єкта, який досліджується, – це сукупність знань, припущень і гіпотез, побудованих у вигляді цілісної логічно витриманої структури, яка відображає основні властивості та характеристики досліджуваного об’єкта, сформульована у термінах і символах, властивих цій науці і необхідних для вирішення цілого класу конкретних завдань.

Таким чином, фізична модель відображає взаємозв’язок і взаємодію фізичних складових з урахуванням фізичних законів досліджуваного об’єкта, а його математична модель – математичний компонент (функції, оператори).

Відомо, що, залежно від постановки завдань досліджень об’єкта, можуть використовуватися різні моделі. Разом з тим, одна математична модель може описувати певне коло досліджуваних об’єктів, різних за своєю фізичною природою.

Фізична модель досліджуваного об’єкта має задовольняти такі вимоги:

- параметри моделі повинні мати реальний фізичний зміст, а їхні основні значення можуть бути отримані шляхом прямих або непрямих вимірів;
- має бути отримана і розроблена методика визначення характеристик параметрів моделі за даними вимірювань, спостережень;
- для математичних об’єктів моделі має бути вказаний клас допустимих операцій і відношень.

Аргументами фізичних і математичних моделей є просторові координати і час.

Відомо, що існує багато моделей для керування безпекою інформаційних технологій. Моделі презентують концепції, необхідні для розуміння процесів керування захистом в інформаційних технологіях. Описувані моделі:

- залежності елементів захисту;
- залежності керування ризиком;
- керування процесом захисту інформаційних технологій.

Концепції, що їх попередньо презентують, і бізнесові цілі організації спільно формують плани, стратегії і методики для убезпечування інформаційних технологій організації. Зміна цілей має гарантувати, що організація буде здатна до ділової активності з допустимими рівнями ризику. Будь-який захист не може бути цілком ефективним, і тому важливо

наперед планувати дії з відновлювання після небажаного інциденту і структурувати захист, щоб обмежити ступінь ушкодженості.

Безпека системи інформаційних технологій є багатовимірною проблемою, яку розглядають у різних аспектах. Тому, щоб визначити і реалізувати загальну й чітку стратегію та методики захисту інформаційних технологій, організація має брати до уваги всі доречні аспекти. Рис. 4.1 показує, що активи є потенційними об'єктами для численних загроз. Цей набір загроз з часом змінюється і лише частково відомий.

Така модель містить:

- оточення із загрозами, що постійно змінюються і тільки частково відомі;
- активи організації;
- уразливості цих активів;
- засоби захисту активів і зменшення наслідків уражень;
- засоби захисту, що зменшують ризики;
- залишкові ризики, прийняті організацією як припустимі.

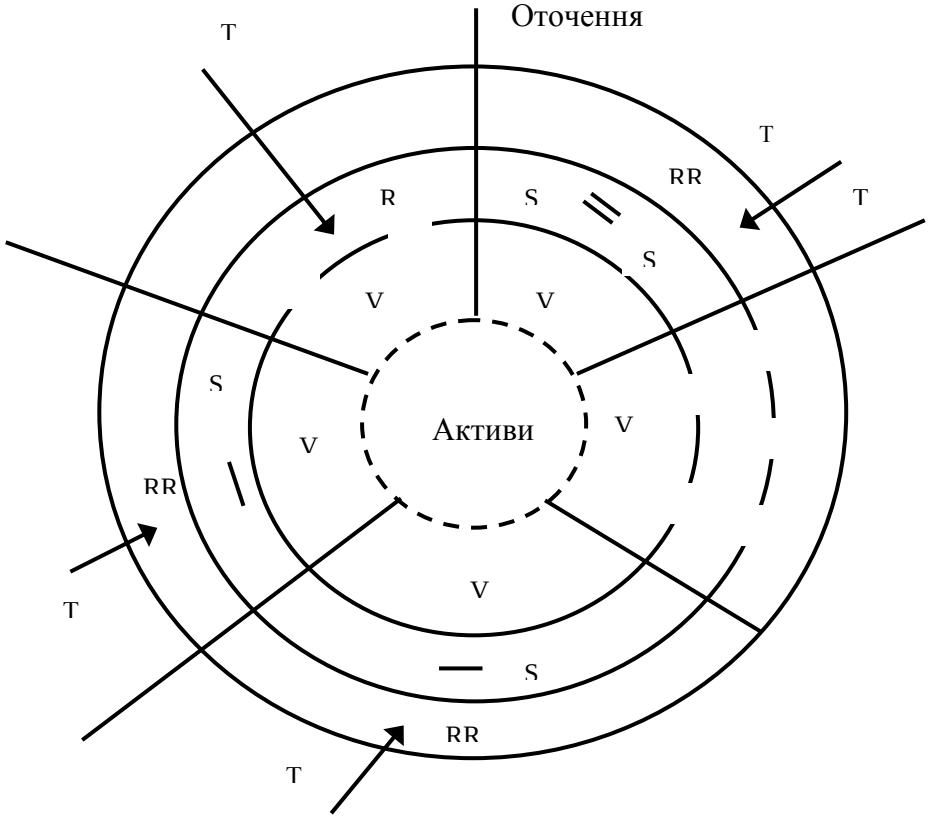


Рисунок 4.1 – Залежності елементів захисту: R – ризик; RR – залишковий ризик; S – засіб захисту; T – загроза; V – вразливість

Як показано на рис. 4.1, деякі засоби захисту можуть бути ефективними для зменшення ризиків, пов'язаних із множинними загрозами і (або)

множинними вразливостями. Іноді потрібно декілька засобів захисту, щоб звести залишковий ризик до припустимого рівня. У деяких випадках, коли ризик допустимий, немає потреби застосовувати засоби захисту, навіть якщо є загрози. В інших випадках уразливість може існувати, але не обов'язкова наявність відомих загроз щодо неї. Засоби захисту можуть забезпечувати контроль наявності загроз в оточенні, щоб запобігти ураженню у разі прояву загрози.

Обмеження, не показані на рис. 4.1, впливають на вибір засобів захисту.

Рисунок 4.2 ілюструє залежність між елементами захисту, тісно пов'язаними з керуванням ризиком. Для наочності відображені тільки основні залежності.

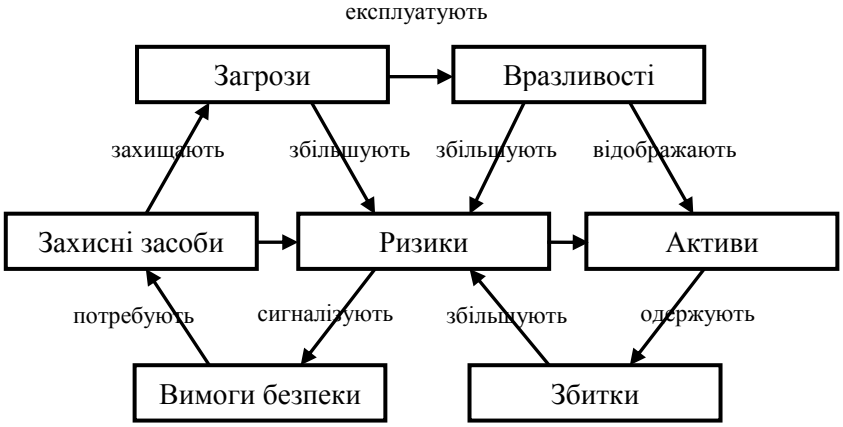


Рисунок 4.2 – Залежність у керуванні ризиком. (Напис на стрілці між будь-якими полями вказує на залежність між ними)

Рисунки 4.3, 4.4 та 4.5 відображають залежності між необхідними умовами захисту і загрозами, уразливостями і вартістю активів відповідно. На цих рисунках проілюстровано перспективи деяких підходів до керування захистом інформаційних технологій. Однак такі підходи можуть не враховувати деякі важливі аспекти.

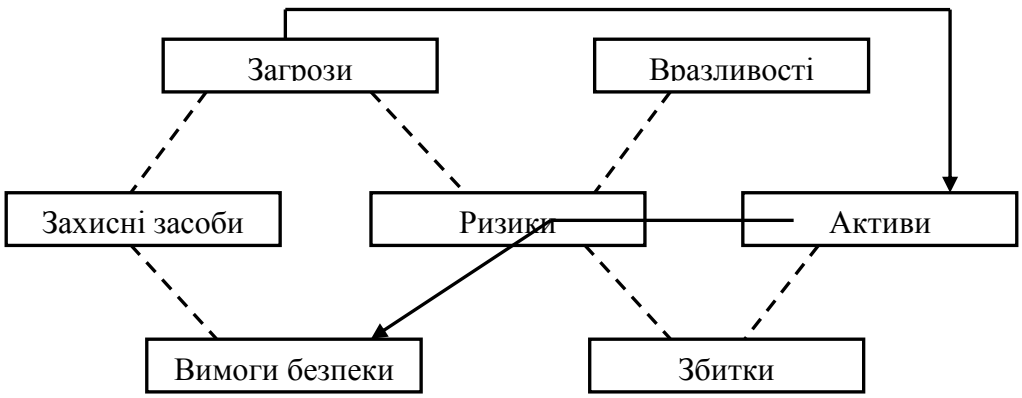


Рисунок 4.3 – Залежності у керуванні ризиком у аспекті загроз

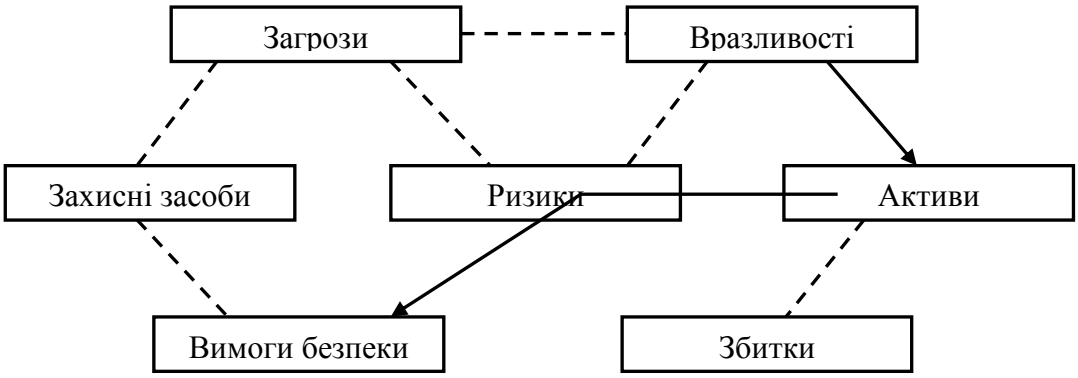


Рисунок 4.4 – Залежності у керуванні ризиком у аспекті вразливостей

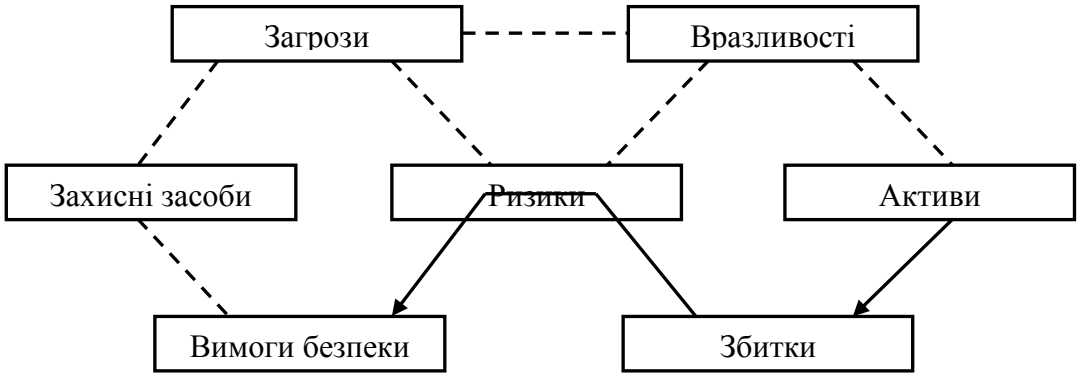


Рисунок 4.5 – Залежності у керуванні ризиком у аспекті ураження

Керування безпекою інформаційних технологій є тривалим процесом, що має враховувати весь життєвий цикл системи безпеки (рис. 4.6).

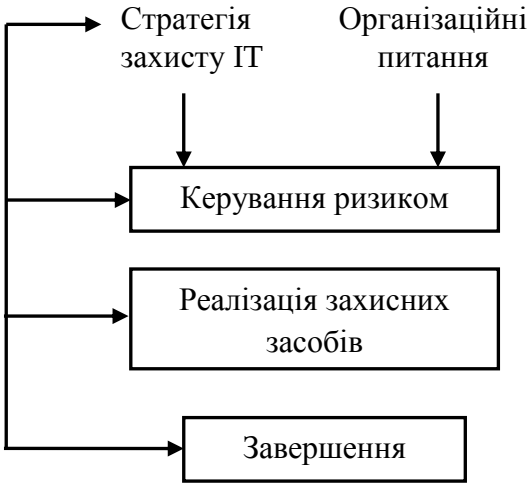


Рисунок 4.6 – Керування процесом захисту інформаційних технологій

Отже, вибір моделі залежить від конкретних вимог організації в цілому та інформаційної системи зокрема.

4.5 Архітектура інформаційної безпеки

Основним документом, що визначає рівні архітектури інформаційної безпеки, є документ ISO 7498-2, який дає їм такі означення (рис. 4.7):

використання поняття «сутність» означає, що взаємодія в мережі може здійснюватися не тільки між людиною і інформаційною системою, але і між програмами, як такі виступають інтелектуальні агенти або віруси;

конфіденційність – властивість інформації бути недоступною або нерозкривною для неуповноважених осіб, сутностей або процесів;

аутентифікація – визначення джерела даних, тобто підтвердження того, що джерелом прийнятих даних є вказане в них джерело, а також як визначення взаємодійної сутності, тобто підтвердження того, що взаємодійна сутність є тим, за кого вона себе видає (peer-entity);

цілісність – визначається як виявлення будь-яких модифікацій, вставок або видалень, що впливають на коректність інформації, зосередженої в інформаційному ресурсі та подаваної у двох формах – без встановлення мережного з'єднання і зі встановленням мережного з'єднання;

управління доступом – визначається як захист від неавторизованого використовування ресурсу, також як захист від використання ресурсу неавторизованим способом (цей рівень іноді плутають з рівнем аутентифікації);

контроль учасників взаємодії – визначається як захист від відмови однієї з сутностей, що беруть участь у взаємодії, від участі у всій взаємодії або її частині і зводиться до контролю учасників з перевіркою джерела, а також контролю даних з перевіркою доставки інформації.

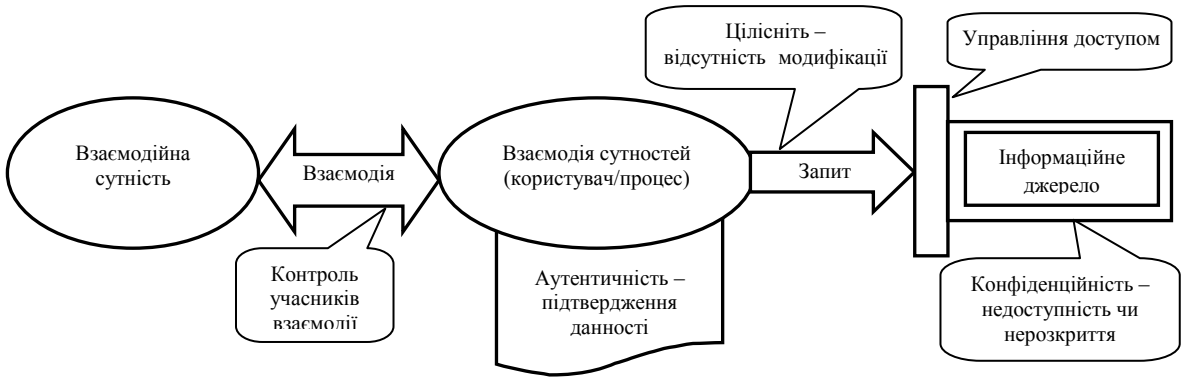


Рисунок 4.7 – Система інформаційної безпеки

Прогрес у сфері ІКТ і глобальних комп'ютерних мереж привів до появи нових методів забезпечення інформаційної безпеки, які, враховуючи природні неточності пристроїв оцифровування і надмірність аналогового відео або аудіосигналу, дозволяють приховувати повідомлення в комп'ютерних файлах (контейнерах) або, на відміну від криптографії, приховувати сам факт передачі інформації.

Методи шифрування діляться на симетричні і асиметричні:

- симетричні (з секретним ключем), використовується один і той же ключ як для шифрування, так і для дешифрування;
- асиметричні методи шифрування з відкритим ключем (public keys, PKI) припускають загальнодоступність ключа шифрування і закритість ключа дешифрування, який неможливо розкрити за ключем шифрування.

Найбільше розповсюдження отримали:

- розроблена Циммерманом (Philip Zimmerman) безкоштовна (freeware) програма PGP (Pretty Good Privacy) для різних платформ, яка забезпечує шифрування пошти і файлів на основі існуючих криптосистем і криптографічних протоколів;
- алгоритми RSA (абревіатура від перших букв імен авторів – Rivest, Shamir і Alderman, 1977 р.) – це система з відкритим ключем, призначена як для шифрування, так і для аутентифікації, заснована на складності розкладання дуже великих цілих чисел на прості співмножники;
- алгоритми IDEA (International Data Encryption Algorithm, автори До. Lai і D. Massey, – шифр з 64-бітових блоків, що повторюються, з 128-бітовим ключем і вісьмома проходами (rounds), дешифрування якого виконується за тим же принципом, що і шифрування (безпека IDEA ґрунтується на використанні трьох несумісних типів арифметичних операцій над 16-бітовими словами);
- алгоритми DES (Data Encryption Standart) – розроблена IBM і затверджена у США в 1977 р. як офіційний стандарт система шифрування з симетричними ключами і 16-кратною перестановкою даних;
- MD5 (Message Digest Algorithm 5) – алгоритм хешування, розроблений компанією RSA Data Security, Inc., що використовується для хешування рядка байтів довільної довжини у 128-бітове значення.

В даний час методи шифрування активно використовуються при створенні електронного цифрового підпису.

Цифровий підпис (digital signature) – це блок даних, що згенеруваний з використанням деякого секретного ключа. В ЄС і США використовуються три варіанти визначення цифрового підпису:

а) перший варіант передбачає, що всі електронні підписи повинні відповідати законодавчим вимогам про підпис;

б) другий варіант передбачає, що електронний підпис має юридичну силу тільки в тому випадку, якщо він:

- дійсно належить особі, яка користується ним;
- може бути перевірений;
- знаходиться виняткова під контролем особи, яка користується ним (електронні цифрові підписи, виготовлені з використанням шифрувальної криптографічної технології, – спочатку опубліковано в John Marshall Journal Computer and Information Law, том XVII № 3, 1999 рік);
- пов’язаний з інформацією таким чином, що у разі зміни інформації, підпис втрачає силу;

в) третій варіант пов'язаний із загальною тенденцією міжнародного законодавства з питань цифрового підпису, направленою на ухвалення більш широкого і всеосяжного визначення електронного підпису на основі другого варіанта як більш нейтрального з технологічної точки зору, не унеможливлює застосування досконаліших технологій в майбутньому і не обмежує виконання підпису з використанням сучасної технології криптографії (Директива 1999/93/ЕС Європейського Парламенту і Поради від 13 грудня 1999 року).

В Директиві ЄС використовується другий варіант і поняття «кваліфікованого електронного підпису», в якому говориться, що такий підпис, якщо він сертифікований і створений надійним способом, відповідає законодавчим вимогам як і поставлений вручну підпис, може використовуватися як доказ у суді.

Не дивлячись на достатньо прозоре загальне означення, розвинуті країни світу дають цьому феномену своє визначення:

- у ФРН електронний підпис визначають як «створена за допомогою приватного ключа печатка до цифрових даних, яка за допомогою відповідного відкритого ключа, забезпеченого сертифікатом ключа підпису, виданим центром сертифікації або державною установою, дозволяє визначити власника ключа підпису і автентичність даних»;

- в Австрії – це «електронні дані, які додані до інших електронних даних або логічно сполучені з останніми і слугують для аутентифікації останніх або для ідентифікації особи, що поставила підпис» (закон локальної дії прийнятий 1 січня 2000 року);

- в США електронний підпис визначають як «електронний звук, символ або процес, приєднаний або логічно сполучений з контрактом або іншим документом (записом) і вироблений або прийнятий особою з метою підписання документа (запису)», а під «особою» розуміється «фізична особа, корпорація, комерційний траст, маєток, траст, партнерство, товариство з обмеженою відповідальністю, асоціація, спільне підприємство, урядове агентство, публічна корпорація, або будь-яка інша юридична або комерційна особа» (закон E-SIGN Act, діє з 30 червня 2000 року і розповсюджується на міжнародні транзакції);

- в російському законі електронний цифровий підпис розуміється як «послідовність символів, отримана в результаті криптографічного перетворення початкової інформації з використанням закритого ключа, що дозволяє користувачу відкритого ключа встановити цілісність і незмінність цієї інформації, а також власника закритого ключа»;

- в українському законі дано таке означення: «електронний цифровий підпис – сукупність даних, отриманих в результаті певного криптографічного перетворення якого-небудь набору даних, яка додається або логічно сполучена з цим набором даних і дає можливість підтвердити його цілісність, а також належність підпису особі, що його підписала». При цьому в українському законі не розкривається значення поняття

«криптографічний» або «криптографія», що робить означення недостатньо чітким.

У зв’язку з цим відзначимо, що в Директиві ЄС виражений тільки намір підвищити надійність цифрового підпису без обмеження її рамками криптографії. Проте на практиці цифровий підпис документа звичайно створюється генерацією дайджесту повідомлення (message digest) з додаванням до нього службової інформації (кореспондент, адресат, час), а потім шифрується секретним ключем того, хто підписує, з використанням того або іншого алгоритму. Зашифрований бітовий стек, що вийшов, і є цифровим підписом.

В цифрових підписах використовуються RSA для підпису і MD5 для обчислення дайджесту. Крім того, для генерації дайджесту повідомлення при створенні цифрового підпису використовуються криптографічні хеш-функції для відображення повідомлення у фіксований розмір (128 і більше бітів) хеш-значення (hash value) таким чином, що вся множина можливих повідомлень розподіляється рівномірно по множині хеш-значень. PGP також може забезпечувати шифрування повідомлень і цифрові підписи, використовуючи ZIP компресію, а також маскуючи координати і дані відправника, що трохи ускладнює процес аналізу трафіку.

Методи стеганографії (steganos – секрет, graphy – запис) забезпечують обмін інформацією з приховуванням самого факту комунікацій і є не альтернативою, а доповненням до криптографії. Суть стеганографічних методів полягає у вкладанні одних інформаційних об’єктів в інші інформаційні об’єкти (контейнери) таким чином, що б операція вкладання не спотворювала приховану інформаційну сутність і об’єкт-контейнер.

4.6 Аналіз моделей моніторингу

З технологічної точки зору концепції законного перехоплення зводяться до задач перехоплення в PSTN, проте PSDN мають іншу природу, а тому концепція перехоплення IP-трафіку вимагає інших підходів і повинна враховувати всі нюанси конвергенції і NGN. У зв'язку з цим можна стверджувати, що основною проблемою перехоплення IP-трафіку є проблема ідентифікація коректних IP-пакетів для перехоплення.

Річ у тому, що в даний час IP-адреси призначаються динамічно (наприклад, протягом сесії), тому використовується термін «тимчасова IP-адреса». Це означає, що IP-адреси, використовувані з метою перехоплення, не можуть коректно ідентифікувати мету і/або трафік. Зрозуміло, дане обмеження не стосується постійних IP-адрес (хост-серверів), які завжди відповідають одному і тому ж користувачу.

Розв’язання цієї проблеми лежить у сфері перевизначення самого поняття IP-перехоплення і розподілу відповідальності за нього між всіма видами провайдингу стосовно тих протоколів і тих видів обслуговування, які їм властиві.

Базисна модель даних перехоплення

Для детального опису особливостей концепції перехоплення IP-трафіку розглянемо, які узагальнені інформаційні сутності в IP-мережах можуть бути предметом перехоплення.

Очевидно, що розгляд всіх мережевих інформаційних об'єктів невід'ємний від їхнього подання у форматах і протоколах обміну в семирівневій моделі OSI ISO (або її аналогах), завдяки яким їхній зміст може бути відновлений в процесі передачі або перехоплення (рис. 4.8).

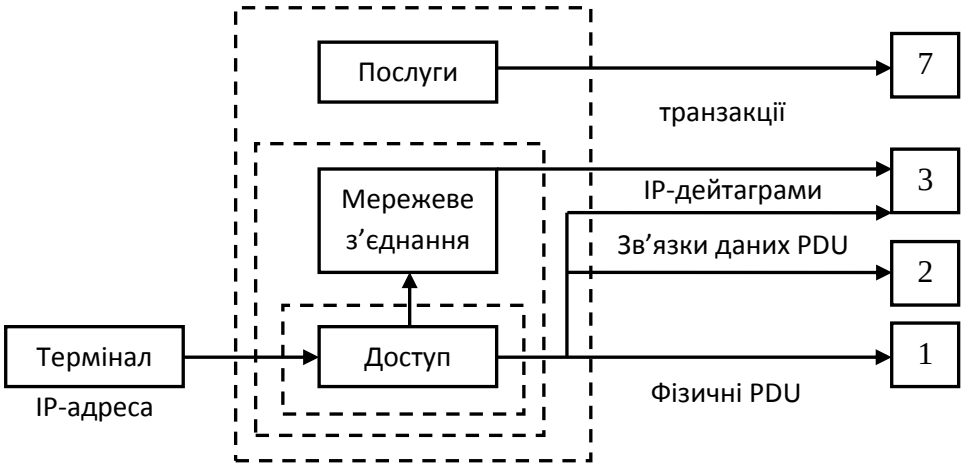


Рисунок 4.8 – Базисна модель даних формату перехоплення

З наведеної моделі видно, що розрізняються не тільки суть і зміст перехоплення, але і ті юридичні особи, яким адресується перехоплення.

Дані відмінності походять із відмінностей у самих задачах і використовуваних технологіях. Так, наприклад, два внутрішні рівні «Доступ» і «Мережеве з'єднання», як правило, здійснюються ISP, а зовнішній рівень – «Послуги» – ICP або ASP.

Таким чином, моделі типового моніторингу, з погляду провайдингу, повинні відповідати на питання – де, ким і коли повинне здійснюватися перехоплення з урахуванням різних рівнів провайдингу.

Перейдемо тепер до аналізу типів IP-перехоплень залежно від того, тимчасовим або постійним є IP-з'єднання.

Перехоплення комутованого з'єднання (dial-up)

При забезпеченні підключення по комутованому каналу (dial-up) IP-з'єднання може бути тільки тимчасовим, і тому до нього застосовні всі наведені вище вимоги в гарантії коректності інформації про об'єкт перехоплення.

В цьому випадку перехопленню підлягають як модемне телефонне з'єднання, так і сервер самого провайдера (рис. 4.9).

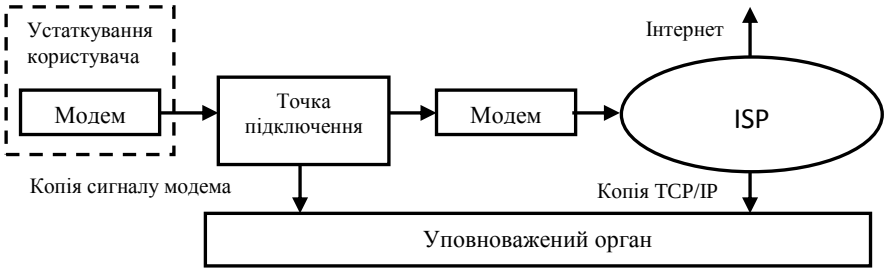


Рисунок 4.9 – Типова модель перехоплення комутованого каналу

Перехоплення постійного з'єднання

Системи, забезпечуючи постійні з'єднання типу виділених каналів, ADSL і LAN, презентують інший клас моделей перехоплення і можуть бути в загальному вигляді подані такою схемою (рис. 4.10).

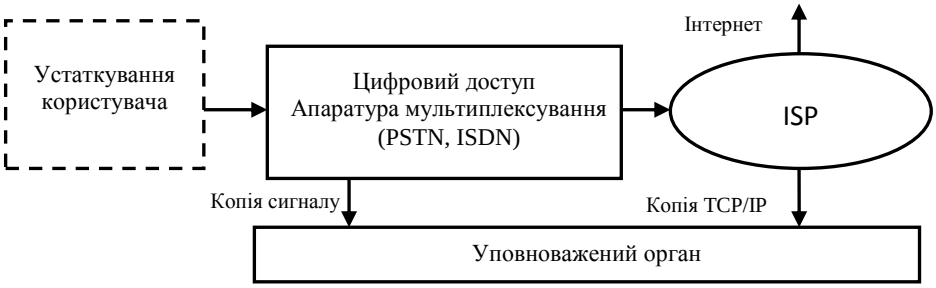


Рисунок 4.10 – Перехоплення через виділений канал

Функціонально GPRS-доступ до Інтернет (наприклад, з використанням RADIUS) перехоплюється аналогічним чином (рис. 4.11).

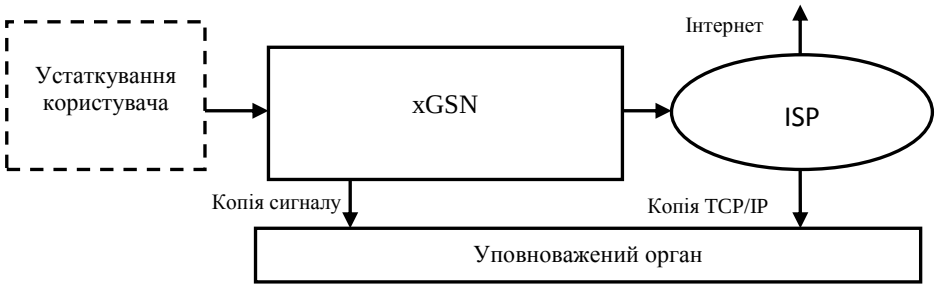


Рисунок 4.11 – Перехоплення GPRS-повідомлень

Вихід в Інтернет через локальну мережу (LAN) може бути організовано різними шляхами, також всіма вищеперерахованими, проте у випадку, якщо це робиться централізовано, то для перехоплення можна застосувати три різні методи підключення (рис. 4.12).

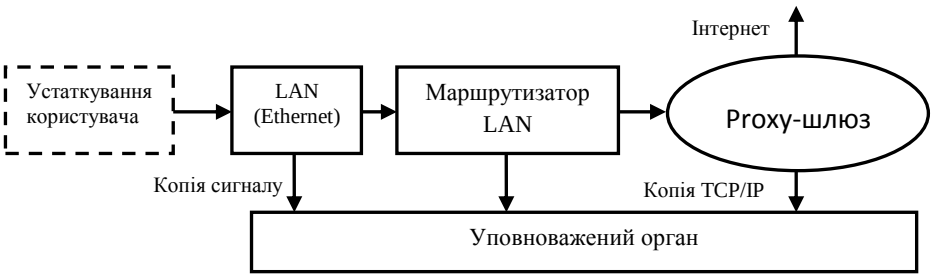


Рисунок 4.12 – Перехоплення в LAN

Наведений аналіз показує, що системи IP-перехоплення розрізнятимуться за:

- технологіями і використовуваними конфігураціями;
- методами взаємодії з системою ISP;
- вартісними характеристиками.

Крім того, сам «моніторинг» розвиватиметься, вбираючи в себе новітні досягнення ІКТ, тому потрібно не тільки дати системам IP-перехоплення робочу класифікацію, але й показати межі їхнього використовування, вартісні характеристики, а також системну єдність. Потрібно зазначити, що він серйозно впливає на функціонування не тільки конкретного ISP, але і всієї системи українського сегменту Інтернет в цілому як з погляду продуктивності, так і з погляду ефективності виконання функцій IP-перехоплення.

Вирішення питань, пов’язаних з упровадженням і використанням систем моніторингу СПД відповідно до рекомендацій ЄС, повинно здійснюватися СБУ в тісній взаємодії з провайдерами України.

Запитання для самоконтролю

1. Які дії містить процес керування безпекою?
2. Цілі безпеки, стратегії і методики.
3. Перелічіть головні елементи, задіяні в процесі керуванням захистом.
4. Охарактеризуйте поняття «залишковий ризик».
5. Охарактеризуйте поняття «обмеження».
6. Що собою являє налаштування системи?
7. Які вимоги повинна задовольняти фізична модель об’єкта?
8. Охарактеризуйте рисунки 4.3, 4.4, 4.5.
9. Який основний документ визначає рівні архітектури інформаційної безпеки?
10. Проаналізуйте основні моделі моніторингу.

ГЛАВА 5
ДОСЛІДЖЕННЯ СТРУКТУРИ ІНФОРМАЦІЙНОГО ПРОЦЕСУ

5.1 Параметри інформаційного процесу і зв'язок між ними

Як відомо, будь-який інформаційний процес визначається зміною параметрів, які його задають, або приведенням одних параметрів (вихідних — $\Phi_1, \Phi_2, ..., \Phi_m$) у відповідність з іншими (вхідними — $x_1, x_2, ..., x_n$) за законом:

$$\begin{cases} \Phi_1 = \varphi_1(x_1, ..., x_n), \\ \Phi_2 = \varphi_2(x_1, ..., x_n), \\ \quad \text{M} \\ \Phi_m = \varphi_m(x_1, ..., x_n), \end{cases} \tag{5.1}$$

де $(x_1, x_2, ..., x_n) \in D \subseteq R^n$.

Нехай $\varphi_i \in C^1(D),\ i = \overline{1,m}$. Припустимо, що значення одного з вихідних параметрів Φ_j однозначно визначається сукупністю значень інших $\Phi_1, ..., \Phi_{j-1}, \Phi_{j+1} ..., \Phi_m$, тобто, якщо $\Omega_0 \subseteq R^{m-1}$ є множина точок, що відповідають деяким точкам $(x_1, x_2, ..., x_n) \in D$, то в Ω_0 буде мати місце функціональна залежність:

$$\Phi_j = f(\Phi_1, ..., \Phi_{j-1}, \Phi_{j+1}, ..., \Phi_m), \tag{5.2}$$

де $f \in C^1(\Omega),\ \Omega \subseteq R^{m-1},\ \Omega \supseteq \Omega_0$, Ω — відкрита множина, а при підстановці (5.1) в (5.2) виходить тотожність відносно $(x_1, x_2, ..., x_n) \in D$:

$$\varphi_j(x_1, ..., x_n) \equiv f(\varphi_1(x_1, ..., x_n), ..., \varphi_{j-1}(x_1, ..., x_n), \varphi_{j+1}(x_1, ..., x_n), ..., \varphi_m(x_1, ..., x_n)). \tag{5.3}$$

У цьому випадку будемо казати, що функція φ_j *залежить від функцій* $\varphi_1, ..., \varphi_{j-1}, \varphi_{j+1} ..., \varphi_m$ у сфері D [12]. У загальному випадку функції $\varphi_1, \varphi_2, ..., \varphi_m$ називаються *залежними* у сфері D, якщо одна з них залежить від інших.

Якщо ані у сфері D, ані в якій-небудь області $E \subseteq D$ не має місця тотожність (5.3), то функції $\varphi_1, \varphi_2, ..., \varphi_m$ називаються *незалежними* в D.

Визначення 5.1. Вихідні параметри інформаційного процесу будуть незалежними (залежними), якщо незалежними (залежними) у сфері D будуть функції (5.1), що їх визначають.

Зауваження 5.1. У випадку незалежності вихідних параметрів їх визначення відповідно до (5.1) може проводитися одночасно (паралельно),

що значно скорочує, при необхідності, час реалізації й аналізу інформаційного процесу. Цей процес можна подати як сукупність не пов'язаних між собою «простих» процесів, результатом кожного з яких є отримання лише одного параметра Φ_i, а дослідження поданого інформаційного процесу зведеться до дослідження скінченної сукупності «простих».

Завдяки зауваженню 5.1 важливою є можливість визначення залежності (незалежності) вихідних параметрів (функцій (5.1)). Відповідь на це питання дають властивості матриці частинних похідних функцій $\varphi_i,\ \ i=\overline{1,m}$, – матриці Якобі неперервного інформаційного процесу:

$$\begin{pmatrix} \frac{\partial\varphi_1}{\partial x_1} & \frac{\partial\varphi_1}{\partial x_2} & \Lambda & \frac{\partial\varphi_1}{\partial x_n} \\ \frac{\partial\varphi_2}{\partial x_1} & \frac{\partial\varphi_2}{\partial x_2} & \Lambda & \frac{\partial\varphi_2}{\partial x_n} \\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda \\ \frac{\partial\varphi_m}{\partial x_1} & \frac{\partial\varphi_m}{\partial x_2} & \Lambda & \frac{\partial\varphi_m}{\partial x_n} \end{pmatrix}. \qquad (5.4)$$

Нехай $n \geq m$. Якщо хоч один визначник m-го порядку, складений з елементів матриці (5.4), відмінний від нуля у сфері D, то в цій області функції $\varphi_i,\ \ i=\overline{1,m}$, а тому і вихідні параметри інформаційного процесу, незалежні. Дійсно, припустимо, що

$$\det\begin{pmatrix} \frac{\partial\varphi_1}{\partial x_1} & \frac{\partial\varphi_1}{\partial x_2} & \Lambda & \frac{\partial\varphi_1}{\partial x_m} \\ \frac{\partial\varphi_2}{\partial x_1} & \frac{\partial\varphi_2}{\partial x_2} & \Lambda & \frac{\partial\varphi_2}{\partial x_m} \\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda \\ \frac{\partial\varphi_m}{\partial x_1} & \frac{\partial\varphi_m}{\partial x_2} & \Lambda & \frac{\partial\varphi_m}{\partial x_m} \end{pmatrix} \neq 0, \qquad (5.5)$$

але якась з функцій, наприклад, φ_m, визначається через інші:

$$\varphi_m = f(\varphi_1,...,\varphi_{m-1}) \qquad (5.6)$$

хоча б у деякій області $E \subseteq D$ (якби відмінним від нуля був інший визначник, то, змінивши нумерацію змінних, можна було б знову прийти до випадку (5.5)).

Продиференціюємо (5.6) за $x_i,\ \ i=\overline{1,m}$:

$$\frac{\partial \varphi_m}{\partial x_i} = \frac{\partial \varphi_m}{\partial \varphi_1}\frac{\partial \varphi_1}{\partial x_i} + \frac{\partial \varphi_m}{\partial \varphi_2}\frac{\partial \varphi_2}{\partial x_i} + ... + \frac{\partial \varphi_m}{\partial \varphi_{m-1}}\frac{\partial \varphi_{m-1}}{\partial x_i}, \quad i = \overline{1,m}. \tag{5.7}$$

З (5.7) випливає, що елементи останнього рядка матриці (5.5) отримуються шляхом додавання відповідних елементів перших $m-1$ рядків, помножених попередньо на множники $\frac{\partial \varphi_m}{\partial \varphi_1},...,\frac{\partial \varphi_m}{\partial \varphi_{m-1}}$. Але тоді визначник (5.5) дорівнює нулю. Отримали суперечність, тому припущення (5.6) хибне.

Розглянемо загальний випадок. Рангом матриці Якобі (5.4) у сфері D назвемо найвищий з порядків визначників, що складаються з елементів цієї матриці і не дорівнюють тотожно нулю в D. Кажуть, що *ранг* r *досягається* в деякій точці $M^0(x_1^0, x_2^0, ..., x_n^0)$ області, якщо визначник r-го порядку в цій точці відмінний від нуля.

Теорема 5.1. Нехай ранг матриці Якобі інформаційного процесу (5.4) у сфері D є r і досягається в точці $M^0(x_1^0, x_2^0, ..., x_n^0) \in D$, при цьому $r = m$. Тоді в D знайдеться така область зміни вхідних параметрів інформаційного процесу, де вихідні будуть незалежними.

Доведення. В умовах теореми існує окіл D_0 точки M^0, в якому r функцій з $\varphi_1, \varphi_2, ..., \varphi_m$, похідні яких входять в визначник r-го порядку, що відрізняється від нуля в M^0, будуть незалежними, а інші будуть залежати від них, звідки при $r = m$ витікає висновок теореми.

5.2 Варіаційна матриця інформаційного процесу

Нехай тепер у сфері D вихідні параметри інформаційного процесу (функції φ_i, $i = \overline{1,m}$) можуть бути як залежними, так і незалежними. Для однаковості викладу всі параметри далі будемо позначати u_i, де $i = \overline{1,N}$, $N = n + m$ (для $i = \overline{1,n}$ u_i відповідають вхідним параметрам). Тоді реалізацію процесу можна формалізувати таким чином:

$$u_k = F_k\left(u_{k_1}, ..., u_{k_{s_k}}\right), n < k \le N, k_1, ..., k_{s_k} < k, \tag{5.8}$$

де всі F_k є досить гладкими функціями своїх аргументів. Як результат процесу розглядається сукупність величин u_k (вихідні параметри). Не накладаючи серйозних обмежень, можна припускати, що результат — це величина u_N.

Співвідношення (5.8) визначають процес обчислення функції (5.2), що є загальною формалізацією інформаційного процесу:

$$\Phi(\boldsymbol{x}_1, ..., \boldsymbol{x}_n) = (\Phi_1, \Phi_2, ..., \Phi_m)^T,$$

чи в нових позначеннях

$$\Phi(u_1,...,u_n)=\left(u_{n+1},u_{n+2},...,u_N\right)^T. \qquad (5.9)$$

Якщо обчислення (5.9) спочатку задані за допомогою (5.8), то при великому N отримати явний вираз функції Φ (тобто функцій φ_i, $i=\overline{1,m}$) через вхідні дані ($u_i, i=\overline{1,n}$) важко й не завжди можливо. Для одержання достатньої умови такого подання кожне рівняння системи (5.8) запишемо в еквівалентному вигляді:

$$F_k\left(u_{k_1},...,u_{k_{s_k}}\right)-u_k = F_k\left(u_{k_1},...,u_{k_{s_k}}\right)-u_k + 0\cdot\sum_{i\neq k,k_1,...,k_{s_k}} u_i = G_k(u_1,u_2,...,u_N)=$$

$$= G_k(x_1,...,x_n,\Phi_1,...,\Phi_m)=0,$$

перетворивши (5.8) в еквівалентну систему рівнянь (у загальному випадку – нелінійну):

$$\begin{cases} \boldsymbol{G}_1(\boldsymbol{x}_1,...,\boldsymbol{x}_n;\Phi_1,...,\Phi_m)=0,\\ \boldsymbol{G}_2(\boldsymbol{x}_1,...,\boldsymbol{x}_n;\Phi_1,...,\Phi_m)=0,\\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\\ \boldsymbol{G}_m(\boldsymbol{x}_1,...,\boldsymbol{x}_n,\Phi_1,...,\Phi_m)=0 \end{cases}. \qquad (5.10)$$

Якщо $G_i\in C^1(D)$, $i=\overline{1,m}$, де $D-n+m$-вимірний прямокутний паралелепіпед

$$\boldsymbol{D}=[\boldsymbol{x}_1^0-\Delta_1,\boldsymbol{x}_1^0+\Delta_1]\times\mathrm{K}\times[\boldsymbol{x}_n^0-\Delta_n,\boldsymbol{x}_n^0+\Delta_n]\times[\Phi_1^0-\overline{\Delta}_1,\Phi_1^0+\overline{\Delta}_1]\times\mathrm{K}\times[\Phi_m^0-\overline{\Delta}_m,\Phi_m^0+\overline{\Delta}_m]$$

з центром в точці $\left(x_1^0,\mathrm{K},x_n^0,\Phi_1^0,\mathrm{K},\Phi_m^0\right)$, координати якої задовольняють систему (5.10), і визначник матриці Якобі для функцій G_i, $i=\overline{1,m}$, за змінними Φ_1,K,Φ_m відмінний від нуля, тобто

$$\det\begin{pmatrix} \frac{\partial \boldsymbol{G}_1}{\partial\Phi_1} & \frac{\partial \boldsymbol{G}_1}{\partial\Phi_2} & \Lambda & \frac{\partial \boldsymbol{G}_1}{\partial\Phi_m}\\ \frac{\partial \boldsymbol{G}_2}{\partial\Phi_1} & \frac{\partial \boldsymbol{G}_2}{\partial\Phi_2} & \Lambda & \frac{\partial \boldsymbol{G}_2}{\partial\Phi_m}\\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda & & & \\ \frac{\partial \boldsymbol{G}_m}{\partial\Phi_1} & \frac{\partial \boldsymbol{G}_m}{\partial\Phi_2} & \Lambda & \frac{\partial \boldsymbol{G}_m}{\partial\Phi_m} \end{pmatrix}\neq 0,$$

тоді в деякому околі точки $\left(x_1^0,\text{K},x_n^0,\Phi_1^0,\text{K},\Phi_m^0\right)$ система (5.10) визначає Φ_1,K,Φ_m у вигляді (5.1), до того ж $\varphi_i \in C^1(D),\quad i=\overline{1,m}$.

Таким чином, інформаційний процес, який визначається за допомогою Φ, можна досліджувати через рекурентні співвідношення (5.8). Для цього система (5.8) для визначення величин u_k еквівалентно перетворюється:

$$F_k\left(u_{k_1},...,u_{k_{s_k}}\right)-u_k=0,\ n<k\le N,\ k_1,...,k_{s_k}<k. \qquad (5.11)$$

Аналіз інформаційного процесу (5.8) з метою встановлення його чутливості до збурних дій може бути формалізований за допомогою дослідження чутливості задачі про розв'язки системи (5.11). Для цього розглядається збурена система:

$$F_k\left(u_{k_1}+\Delta u_{k_1},...,u_{k_{s_k}}\right)-\left(u_k+\Delta u_k\right)=0,\ n<k\le N,\ k_1,...,k_{s_k}<k, \qquad (5.12)$$

де збурення Δu_k малі. Віднімаючи з (5.12) (5.11) і враховуючи подання (5.12) для дійсної функції багатьох змінних, з точністю до нескінченно малих другого порядку, отримаємо систему лінійних алгебраїчних рівнянь відносно збурень Δu_k:

$$\sum_{i=1}^{s_k}\frac{\partial F_k\left(u_{k_1},...u_{k_{s_k}}\right)}{\partial u_{k_i}}\Delta u_{k_i}-\Delta u_k=0,\ n<k\le N,\ k_1,...,k_{s_k}<k \qquad (5.13)$$

Матриця Ψ системи (5.13) – функціональна матриця Якобі функцій

$$y_k=F_k\left(u_{k_1},...,u_{k_{s_k}}\right)-u_k=f_k(u_1,...,u_N)$$

за змінними $u_1,...,u_N$ розміром $m\times N$. Вона зазвичай сильно розріджена. Матриця Ψ має повний ранг, оскільки є нижньою трикутною відносно діагоналі, що проходить через правий нижній кут матриці, на діагоналі знаходяться елементи, які дорівнюють мінус 1. Будемо називати Ψ *варіаційною матрицею інформаційного процесу* (ВМІП) (5.8).

Варіаційна матриця відіграє важливу роль при аналізі структури й властивостей інформаційного процесу, зокрема, при дослідженні його міри чутливості до збурних дій (похибок вхідних даних).

$$\psi_{ij}=\begin{cases}\textit{-1, якщо } j=i+n,\\ \dfrac{\partial F_{i+n}}{\partial u_j},\ \textit{якщо } j \textit{ є одним з чисел } (i+n)_1,...,(i+n)_{s_{i+n}},\\ \textit{0, в інших випадках}\end{cases}.$$

При визначенні $v = F(u)$ в реальних умовах точне значення v отримати не можна. Замість v буде отриманий елемент $\bar{v} \neq v$. При проведенні прямого аналізу похибки, результатом якого є оцінка $\|\bar{v} - v\|$, стає зрозумілим, що якщо така оцінка виявиться великою, це може бути пов'язано з нестійкістю оператора F в околі u. У такій ситуації добре зарекомендував себе обернений аналіз похибок, основна ідея якого полягає в спробі подати реально отриманий елемент $\bar{v}$ як точний результат перетворення F, але не елемента u, а елемента $\bar{u} \neq u$: $\bar{v} = F(\bar{u})$. Про це вже йшла мова вище. Якщо це вдається зробити, то вплив збурних дій оцінюється величиною $\|\bar{u} - u\|$, а $\bar{u} - u$ називається *еквівалентним збуренням*.

Розглянемо процес поширення похибок під час протікання інформаційного процесу (5.8), реалізація якого зводиться до обчислення функції (5.9). При реальних обчисленнях точних формул (5.8) мають місце співвідношення:

$$\begin{array}{l} \bar{u}_k = \bar{F}_k(\bar{u}_{k_1},...,\bar{u}_{k_{s_k}}), \quad n < k \le N, \quad k_1,...k_{s_k} < k, \\ \Updownarrow \\ \bar{u}_k = F_k(\bar{u}_{k_1},...,\bar{u}_{k_{s_k}}) + \eta_k, \quad n < k \le N, \quad k_1,...k_{s_k} < k, \end{array} \tag{5.14}$$

де $\bar{F}_k$ – збурена «близька» до F_k функція, реальне обчислення якої здійснюється при реалізації інформаційного процесу (5.8), $\bar{u}_k$ – реально задана або обчислена величина u_k, η_k – еквівалентна абсолютна похибка (підсумковий результат збурної дії), яка вноситься в результат обчислення F_k.

Подамо (5.14) у вигляді:

$$\bar{u}_k + \varepsilon_k = F_k(\bar{u}_{k_1} + \varepsilon_{k1},...,\bar{u}_{k_{s_k}} + \varepsilon_{k_{s_k}}), \; n < k \le N, k_1,...k_{s_k} < l \tag{5.15}$$

де ε_k – збурення $\bar{u}_k$ (ці збурення вносяться й у вхідні дані). Якщо взяти збурені вхідні дані $u_1 + \varepsilon_1,...,u_n + \varepsilon_n$ і провести з ними точний процес (5.8), то на кожному кроці цього процесу як точний результат отримаємо $\bar{u}_k + \varepsilon_k$.

Сукупність значень ε_k, в якій еквівалентні збурення вхідних даних дорівнюють 0, описує прямий аналіз похибок. Якщо в множині ε_k еквівалентні збурення вихідних даних дорівнюють 0, то маємо обернений аналіз похибок. Інші варіанти ε_k описують змішаний аналіз похибок.

З (5.14), (5.15) отримуємо

$$\varepsilon_k = F_k(\bar{u}_{k_1} + \varepsilon_{k1},...,\bar{u}_{k_{s_k}} + \varepsilon_{k_{s_k}}) - F_k(\bar{u}_{k_1},...,\bar{u}_{k_{s_k}}) - \eta_k, \quad n < k \le N, k_1,...k_{s_k} < k. \tag{5.16}$$

Якщо збурення вхідних даних $\varepsilon_1,...,\varepsilon_n$ відомі, то за допомогою (5.16) можна визначити інші збурення $\varepsilon_k, k > n$ (значення u_k, збурення η_k визначаються реалізацією інформаційного процесу (5.14)), що дасть можливість встановити міру чутливості процесу до похибок вхідних даних (до збурних дій). Розглянемо (5.16) докладно.

Система (5.16) в загальному випадку є нелінійною відносно ε_k. Враховуючи подання (5.4) для дійсної функції багатьох змінних, (5.16) можна замінити лінійною системою:

$$\varepsilon_k = \sum_{i=1}^{s_k} \frac{\partial Fk(\bar{u}_{k_1},...,\bar{u}_{k_{s_k}})}{\partial u_{ki}} \varepsilon_{ki} - \eta_k, \quad n < k \le N, k_1,...k_{s_k} < k.$$

Замінимо реально обчислені величини $\bar{u}_i, i = k_1,...,k_{sk}$ на точні:

$$\sum_{i=1}^{s_k} \frac{\partial Fk(u_{k_1},...,u_{k_{s_k}})}{\partial u_{ki}} \varepsilon_{ki} - \varepsilon_k = \eta_k, \quad n < k \le N, k_1,...k_{s_k} < k \tag{5.17}$$

Матриця системи (5.17) – це ВМІП (5.8), тому система завжди сумісна. Таким чином, величини збурень ε_k визначаються як розв'язки системи лінійних алгебраїчних рівнянь (5.17), властивості якої визначаються властивостями ВМІП.

Оскільки ε_k використовуються для аналізу інформаційного процесу з метою встановлення його чутливості до збурних дій, важливо, щоб ці значення були отримані якнайточніше, для чого матриця системи (5.17) – ВМІП (5.8) – повинна бути добре обумовленою.

ВМІП відіграє важливу роль не тільки при аналізі збурень параметрів, що визначають інформаційний процес.

5.3 Граф інформаційного процесу і його особливості

Довільному інформаційному процесу поставимо у відповідність орієнтований граф (орграф) таким чином. Зіставимо k-й вершині графу

отримання величини u_k. Перші n вершин будуть символізувати введення початкових даних $u_1,...,u_n$ і називатися вхідними, а інші вершини – обчислення u_k як значень функцій F_k з (5.8). Будемо вважати, що дуга йде з i-ї вершини в j-у тоді й тільки тоді, коли при обчисленні величини u_j величина u_i використовується як аргумент. Відповідно до (5.8) дуги не будуть входити в k-у вершину, якщо $k \le n$. Якщо $k > n$, то в k-у вершину будуть входити дуги з вершин з номерами $k_1,...,k_{sk}$.

Будемо називати орграф *дводольним*, якщо множина його вершин V може бути розбита на дві підмножини V_1 і V_2 так, що кожне ребро графу є впорядкованою парою вигляду $< v_1, v_2 >$, де $v_1 \in V_1$, а $v_2 \in V_2$.

Зі способу побудови графу стає очевидною істинність нижченаведних тверджень.

Твердження 5.1. Граф інформаційного процесу є ациклічним.

Теорема 5.2. Вихідні параметри інформаційного процесу будуть незалежними тоді й тільки тоді, коли граф інформаційного процесу буде дводольним.

В графі як моделі інформаційного процесу наочно подані відомості про те, як окремі перетворення при протіканні процесу пов'язані між собою інформаційно, які перетворення в ході їхнього моделювання можуть виконуватися одночасно, які потрібно виконувати пізніше або раніше, ніж інші і т. д. Граф інформаційного процесу описує всю картину поширення інформації при його протіканні, а тому може бути використаний для аналізу інформаційного процесу в цілому, його структури.

Отриманому графу ставиться в співвідношення матриця Ф розміром $m \times N$ з елементами φ_{ij}:

$$\varphi_{ij} = \begin{cases} \textit{-1, якщо } j = i + n, \\ \textit{1, якщо } j \textit{ є одним з чисел } (i+n)_1,...,(i+n)_{s_{i+n}}, \\ \textit{0, в інших випадках} \end{cases}.$$

Очевидно, k-ий стовпець матриці Ф відповідає параметру u_k, а k-ий рядок – параметру u_{k+n}. В k-ому рядку елемент -1 знаходиться в тому стовпці, номер якого відповідає номеру обчислювального параметра, – u_{k+n}. Елементи +1 знаходяться у тих стовпцях, номери яких відповідають номерам аргументів обчислювального параметра, – u_{k+n}. Матриця Ф описує зв'язок параметрів u_k між собою і називається *матрицею інформаційної зв'язності* інформаційного процесу (МІЗІП) (5.8). Очевидний зв'язок матриці зв'язності з ВМІП: структури ненульових елементів обох матриць повністю збігаються.

Для графу інформаційного процесу за МІЗІП заміною ненульових елементів якимись числами можна отримати нескінченну сукупність матриць, кожна з яких є *зваженою* МІЗІП. Будь-яка зважена МІЗІП, окремим випадком якої є й ВМІП, дозволяє однозначно відновити граф інформаційного процесу, а тому може використовуватися для його аналізу.

Для орієнтованого графу, що відповідає інформаційному процесу, стандартно визначається $N \times N$ – матриця суміжності B з елементами b_{ij}

$$b_{ij} = \begin{cases} 1, \text{ якщо з і-ої вершини в j-у йде ребро,} \\ 0, \text{ в інших випадках} \end{cases}$$

і матриця інцидентності A з елементами a_{ij}

$$a_{ij} = \begin{cases} 1, \text{ якщо j-е ребро виходить з і-ої вершини,} \\ -1, \text{ якщо j-е ребро входить в і-у вершину,} \\ 0, \text{ в інших випадках.} \end{cases}$$

Матриця B тісно пов'язана з МІЗІП Ф: Ф – підматриця, яка складається з останніх m рядків матриці $B^T - I$, де I – одинична матриця відповідного розміру. У зв’язку з цим для зведення МІЗІП до більш «придатного», з погляду можливостей її обробки, вигляду за рахунок перенумерації рядків і стовпців можна здійснювати відповідну перенумерацію для матриці суміжності.

До значного зменшення часових витрат, необхідних для дослідження властивостей інформаційного процесу, приводить виявлення й наступне використання його внутрішнього паралелізму на основі відповідного графу [12, 17], тобто можливостей паралельного (одночасного) виконання вхідних до інформаційного процесу операцій.

5.4 Паралельні форми інформаційного процесу

Поява паралельних обчислювальних систем і впровадження їх у практику вирішення великих прикладних задач привела до необхідності аналізу інформаційних процесів з метою визначення можливості їхньої математичної формалізації й обробки в паралельних обчислювальних системах. Результатом аналізу повинно стати виявлення таких частин процесу, які інформаційно між собою не пов’язані. Якщо такі частини знайдені, будемо говорити, що інформаційному процесу властивий *внутрішній паралелізм*.

Будемо використовувати граф $G = (V, E)$ інформаційного процесу, де V – множина вершин, а E – множина впорядкованих пар вершин (ребер), для аналізу його структури, не накладаючи ніяких обмежень на вигляд вхідних і вихідних параметрів. Граф інформаційного процесу не накладає,

загалом кажучи, ніяких обмежень і на порядок виконання операцій, що входять до складу процесу, крім одного: до моменту початку реалізації будь-якої операції повинні закінчити своє виконання всі ті операції, які поставляють для неї параметри-аргументи. Таким чином, граф інформаційного процесу визначає множину припустимих порядків виконання його операцій.

Будь-який інформаційний процес – це процес, що протікає в часі, будь-яка його реалізація породжує певне сортування операцій, що входять до його складу. Це сортування будує розбиття множини операцій (вершин відповідного графу) на такі групи, які виконуються послідовно, а операції всередині групи можуть виконуватися одночасно.

Ототожнюючи інформаційний процес з його графом, будемо припускати, що в графі відображені операції отримання всіх параметрів і зв'язки, вплив яких на реалізацію процесу підлягає вивченню.

Нехай $G = (V, E)$ – довільний орієнтований ациклічний граф з n вершинами. Тоді існує таке натуральне число $s \le n$, що всі вершини графу можна так помітити одним з індексів $1, 2, ..., s$, що якщо ребро йде з вершини з індексом i в вершину з індексом j, то

$$i < j . \qquad (5.18)$$

Така розмітка вершин називається *топологічним сортуванням* графу або *паралельною формою*. Очевидно, що ніякі дві вершини з однаковим індексом не є суміжними. Крім того, для будь-якого натурального $s \le n$, більшого довжини критичного шляху, існує топологічне сортування, при якому використовуються всі s індексів, тобто граф має не єдине топологічне сортування.

Якщо співвідношення (5.18) замінити на $i \le j$, то отримане сортування буде називатися *узагальненим топологічним сортуванням*.

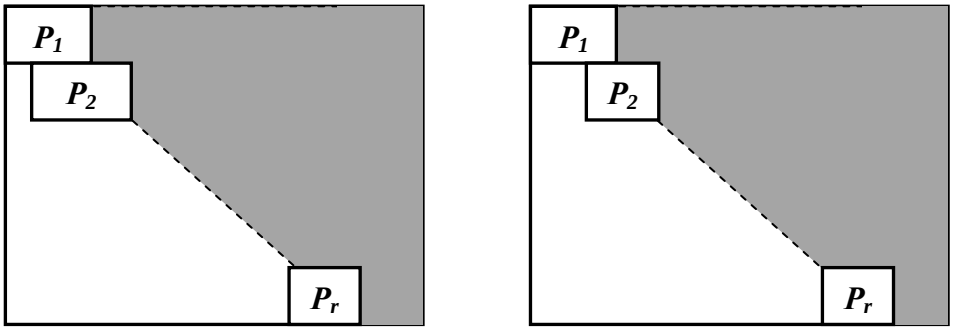
Результатом топологічного сортування є виявлення можливостей паралельного (одночасного) виконання (аналізу) вхідних в інформаційний процес операцій. Ці операції будуть входити в одну групу сортування, яка називається *ярусом паралельної форми*. Сукупність всіх топологічних сортувань графу інформаційного процесу визначає його паралельні форми реалізації (обробки, аналізу). Операції, відповідні вершинам графу одного рівня топологічного сортування, є інформаційно незалежними, а тому можуть виконуватися паралельно. Групи операцій, що відповідають різним топологічним рівням, виконуються послідовно в порядку зростання номерів вершин графу, що входять у них.

Як правило, чим складніший граф, чим більший його розмір, тим важче побудувати його топологічне сортування. Зменшення необхідного часу для цього процесу може бути досягнуте за рахунок розбиття графу на підграфи меншого розміру з наступною побудовою топологічних сортувань

підграфів і відновленням сортування всього графу за сортуваннями підграфів. Крім того, для скорочення часу на аналіз інформаційного процесу можна зменшити розмір графу за допомогою гомоморфної згортки його підграфів.

За допомогою перенумерації вершин графу інформаційного процесу можна спростити його опис. Отже, шляхом перенумерації операцій (5.8) можна спробувати привести МІЗІП і, відповідно, ВМІП до більш зручного вигляду.

Розглянемо довільне топологічне сортування вершин графу інформаційного процесу. Позначимо вершини таким чином: спочатку нумеруються вершини, що потрапили в перший ярус, потім – у другий і т. д., визначаючи тим самим порядок рядків МІЗІП. При впорядкуванні стовпців спочатку нумеруються стовпці, які відповідають аргументам F_1, потім стовпці, що відповідають лише тим аргументам F_2, які ще не були занумеровані, і т. д. При цьому нова нумерація стовпців, відповідно до обчислюваних величин, береться такою, щоб з точністю до викидання стовпців, відповідних вхідним параметрам, вона збігалася з новою нумерацією рядків. Після описаного переставлення рядків і стовпців МІЗІП буде мати вигляд, наведений на рис. 5.1. В кожному рядку P_i існує хоча б один ненульовий елемент, і всі його ненульові елементи дорівнюють 1. В кожному рядку зафарбованої частини знаходиться лише один ненульовий елемент – мінус 1.



а б

Рисунок 5.1 – Структура МІЗІП, коли в інформаційному процесі розмноження інформації присутнє (а); відсутнє (б)

У загальному випадку в кожному стовпці МІЗІП може знаходитися більше однієї одиниці: в l-ому стовпці буде m_l одиниць, якщо m_l операцій, що входять в інформаційний процес, використовують параметр u_l як один зі своїх аргументів, тобто якісь ребра, що виходять з деяких вершин графу інформаційного процесу, визначають перенесення одної інформації. У цьому випадку будемо говорити, що має місце *розмноження інформації*. Якщо розмноження інформації присутнє в інформаційному процесі, то деякі стовпці МІЗІП можуть мати непусті перетинання більш ніж з одним

рядком. При будь-якому переставленні рядків і стовпців ця властивість зберігається. Отже, описані вище переставлення приведуть МІЗІП до вигляду, зображеного на рис. 5.1, а), інакше її вигляд наведений на рис. 5.1, б).

Для формалізації аналізу інформаційного процесу у відповідність його графу можна поставити не лише одну з розглянутих вище двовимірних матриць, але й одновимірний вектор.

Однією з характеристик протікання інформаційного процесу є час його виконання. При безпосередній реалізації визначені моменти виконання всіх операцій (5.8). Порушення певного часу виконання деякої операції в ході процесу є сигналом можливих збоїв, атак, спрямованих на засоби захисту, що забезпечують протікання процесу, і т. п.

Перенумеруємо вершини графу інформаційного процесу довільно й кожній i-й вершині поставимо у відповідність час t_i закінчення виконання відповідної операції. Таким чином, з інформаційним процесом можна зв'язати вектор $t=(t_1,t_2,...,t_n)^T$, який будемо називати *вектором часового розгорнення* процесу, що показує, як протікає процес у часі. Для елементів вектора t природно визначити деякі обмеження, наприклад, задати час h_j для реалізації j-ї операції. Якщо в графі інформаційного процесу існує ребро, що йде з i-ї вершини в j-у, то повинно виконуватися співвідношення: $t_j - t_i \geq h_j$.

Дійсно, час, що проходить від закінчення i-ї операції до закінчення j-ї, містить у собі не тільки час виконання j-ї операції, але й час, який затрачується на передачу інформації, необхідної для виконання j-ї операції. Невід'ємний вектор $h=(h_1,h_2,...,h_n)^T$ будемо називати *вектором реалізації інформаційного процесу*.

З кожним ребром графу можна зв'язати не тільки якусь інформацію, що передається від однієї вершини до іншої. Будь-яке часове розгорнення однозначно визначає час t_i появи цієї інформації й час $t_j - t_i$ її існування, частково в незмінному, частково в перетвореному в j-й вершині вигляді. Можна вважати, що в момент t_j стара інформація повністю закінчує своє існування й народжується нова. Час $t_j - t_i$ *– час затримки інформації на дузі*, яка пов'язує i-у та j-у вершини. При реалізації інформаційних процесів на часи затримок накладаються обмеження знизу. Вони спричиняються часом передачі інформації по каналах і лініях зв'язку, часом зберігання інформації й іншими факторами. Ці обмеження можна задавати аксіоматично й вважати, що час затримки інформації на дузі, що зв'язує i-у і j-у вершини, не менше невід'ємного числа w_{ij}:

$$t_j - t_i \geq w_{ij}.$$

Вектор w з координатами w_{ij} називається *вектором затримок*.

Нехай інформаційний процес починає свою реалізацію в нульовий момент часу, і в кожний додатний цілочисловий момент виконується хоча б одна операція (5.8). Розглянемо відповідне часове розгорнення. Згідно з розгорненням множина вершин графу розбивається на неперетинні підмножини, де в одну підмножину входять ті й тільки ті вершини, які відповідають операціям, що виконуються одночасно. Кожній з побудованих підмножин приписується індекс, що дорівнює моменту виконання відповідних операцій. Очевидно, що отримане розбиття вершин графу інформаційного процесу визначає деяку паралельну форму його протікання. Правильно й те, що будь-яка паралельна форма інформаційного процесу породжує деяке часове розгорнення.

Таким чином, очевидно, що аналіз часових розгорнень є перспективним напрямком в галузі досліджень інформаційних процесів.

5.5 Введення у функціональне дослідження структури інформаційного процесу

Подання часових розгорнень інформаційного процесу у вигляді векторів відповідає математичній формалізації процесу в вигляді (5.8), де виконувані операції ідентифікуються одним цілим параметром. Така ідентифікація при практичному використанні (5.8) призводить до значних незручностей і труднощів.

Будемо вважати вершини графу інформаційного процесу точками скінченновимірного простору (з можливою, в деякому розумінні, «зручною» цілочисловою (хоча це необов'язково) фіксацією координат). Множина вершин буде знаходитися в деякій області D, а часові розгортки можна розглядати як функції, визначені на множині точок-вершин. Таким чином, якщо задано часове розгорнення, то кожній з точок-вершин x ставиться у відповідність число, яке дорівнює часу виконання відповідної операції, тобто часове розгорнення – це деяка функція

$$t(x): D_d \to K, \tag{5.19}$$

де D_d – область визначення, що є дискретною множиною точок x з області D, $K \subseteq Z$ – область значень — дискретна множина, де Z – множина цілих чисел. Часові розгорнення, наведені в такому вигляді, будемо називати *просторово-часовими*.

Будь-яка паралельна форма інформаційного процесу визначає деяку множину часових розгорутнь. При заданні розгорнення у вигляді (5.19) яруси паралельної форми будуть мати явний геометричний зміст: вони визначаються поверхнями рівня (визначення 5.14) для $t(x)$ –

$$t(x) = const\ . \qquad (5.20)$$

Дійсно, нехай множина точок (5.20) містить якісь вершини графу інформаційного процесу. Тоді відповідні вершинам операції виконуються в один момент, тобто утворюють ярус паралельної форми.

Для зручності подальшого аналізу, не обмежуючи значно спільності міркувань, продовжимо яким-небудь прийнятним способом просторово-часові розгорнення (5.19) на всю область **D**. Позначимо відповідні функції $t_D(x)$. Будемо вважати, що функції $t_D(x)$ мають необхідну гладкість.

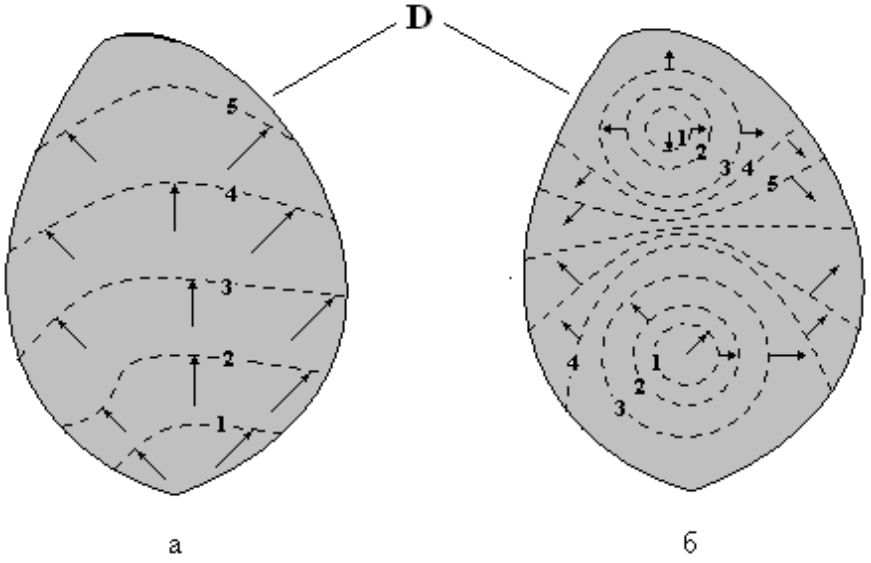


Рисунок 5.2 – Системи поверхонь рівня: однозв'язні (а); багатозв'язні (б)

Нехай **D** — однозв'язна область. Поверхні рівня $t_D(x) = const$ можуть бути як одно- так і багатозв'язними (рис. 5.2 – цифрами відзначені поверхні рівнів, відповідні послідовним значенням t), однак, завдяки припущенням про гладкість функцій $t_D(x)$, зі зміною t вони змінюються неперервно, тому по один бік від них завжди будуть знаходитися вершини, відповідні операціям, що виконуються до часу t, а по інший – вершини, відповідні операціям, що виконуються після часу t. Тоді перенесення інформації від вершин однієї групи до вершин іншої групи здійснюється лише тими ребрами графу інформаційного процесу, які для будь-якої поверхні рівня просторово-часового розгорнення визначають орієнтований розріз графу процесу [12]. Поверхні рівнів показують розподіл потоків інформації в D.

Таким чином, опис паралельних форм інформаційного процесу зводиться до опису поверхонь рівня просторово-часових розгорток і дослідження функцій, що їх визначають, і накреслює новий напрямок у сфері аналізу інформаційних процесів.

Запитання для самоконтролю

1. Коли дійсні функції, що формалізують інформаційний процес, називаються залежними, незалежними?
2. Коли вихідні параметри інформаційного процесу будуть незалежними (залежними)?
3. За рахунок чого у випадку незалежності вихідних параметрів можна значно скоротити час реалізації й аналізу інформаційного процесу?
4. Як визначається матриця Якобі для неперервного інформаційного процесу?
5. Що є достатньою умовою незалежності вихідних параметрів неперервного інформаційного процесу?
6. Що таке варіаційна матриця інформаційного процесу? Яку роль при аналізі структури й властивостей інформаційного процесу відіграє варіаційна матриця?
7. Як варіаційна матриця інформаційного процесу пов’язана з чутливістю процесу до збурних дій?
8. Як інформаційному процесу можна поставити у відповідність орієнтований граф?
9. Які властивості має орієнтований граф, що відповідає інформаційному процесу? Що описує граф інформаційного процесу?
10. Критерій незалежності вихідних параметрів інформаційного процесу.
11. Що називається матрицею інформаційної зв’язності інформаційного процесу?
12. Як пов’язані між собою матриця інформаційної зв’язності й варіаційна матриця інформаційного процесу?
13. Чи можна за зваженою матрицею інформаційної зв’язності однозначно відновити граф інформаційного процесу?
14. Коли інформаційному процесу властивий внутрішній паралелізм?
15. Які обмеження накладає на порядок виконання операцій, що входять до складу інформаційного процесу, граф процесу?
16. Що називається топологічним (узагальненим топологічним) сортуванням, або паралельною формою графу інформаційного процесу? Що є результатом топологічного сортування?
17. Яка сукупність операцій інформаційного процесу називається ярусом паралельної форми?
18. За рахунок чого може бути досягнуто зменшення необхідного часу для побудови топологічного сортування графу інформаційного процесу?
19. Що називається вектором часового розгорнення інформаційного процесу? Про що свідчить порушення певного часу виконання деякої операції в ході протікання процесу?
20. Який вектор називається вектором реалізації інформаційного процесу? Вектором затримок?

ГЛАВА 6
НАЙПОШИРЕНІШІ ЗАГРОЗИ ІНФОРМАЦІЇ

6.1 Основні означення і критерії загроз

Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

Спроба реалізації загрози називається атакою, а той, хто вчиняє таку спробу, – зловмисником. Потенційні зловмисники називаються джерелами загроз.

Найчастіше загроза є наслідком наявності уразливих місць у захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки в програмному забезпеченні).

Проміжок часу від моменту, коли з'являється можливість використати слабке місце, і до моменту, коли прогалина ліквідується, називається вікном небезпеки, асоційованим з даним уразливим місцем. Поки існує вікно небезпеки, можливі успішні атаки на ІС.

Якщо мова йде про помилки в ПЗ, то вікно небезпеки «відкривається» з появою засобів використання помилки й ліквідується при накладенні «латок», які її виправляють.

Для більшості уразливих місць вікно небезпеки існує порівняно довго (кілька днів, іноді – тижнів), оскільки за цей час повинні відбутися такі події:

- повинно стати відомо про засоби використання прогалини в захисті;
- повинні бути випущені відповідні «латки»;
- «латки» повинні бути встановлені в захищуваній ІС.

Ми вже вказували, що нові уразливі місця й засоби їхнього використання з'являються постійно; це значить, по-перше, що майже завжди існують вікна небезпеки й, по-друге, що відстеження таких вікон повинно проводитися постійно, а випуск і накладання «латок» – якомога оперативніше.

Відзначимо, що деякі загрози не можна вважати наслідком якихось помилок або прорахунків; вони існують у самій природі сучасних ІС. Наприклад, загроза відключення електрики або виходу її параметрів за припустимі межі існує внаслідок залежності апаратного забезпечення ІС від якісного електроживлення.

Розглянемо найпоширеніші загрози, яким піддаються сучасні інформаційні системи. Мати уявлення про можливі загрози, а також про уразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, щоб вибирати найбільш економічні засоби забезпечення безпеки. Занадто багато міфів існує в сфері інформаційних технологій (згадаємо все ту ж «Проблему 2000»), тому незнання в цьому випадку веде до перевитрати коштів й, що ще гірше, до концентрації ресурсів там, де вони не дуже потрібні, за рахунок ослаблення дійсно уразливих напрямків.

Підкреслимо, що саме поняття «загроза» у різних ситуаціях найчастіше трактується по-різному. Наприклад, для підкреслено відкритої організації загроз конфіденційності може просто не існувати – вся інформація вважається загальнодоступною; однак у більшості випадків нелегальний доступ є серйозною небезпекою. Іншими словами, загрози, як і все в ІБ, залежать від інтересів суб'єктів інформаційних відносин (і від того, який збиток є для них неприйнятним).

Ми спробуємо подивитися на предмет з точки зору типової (на наш погляд) організації. Втім, багато загроз небезпечні для всіх.

Загрози можна класифікувати за декількома критеріями:

- аспектом інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;
- компонентами інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримувальна інфраструктура);
- способом здійснення (випадкові/навмисні дії природного/техногенного характеру);
- розташуванням джерела загроз (усередині/поза розглянутим ІС).

Як основний критерій ми будемо використовувати перший (за аспектом ІБ), залучаючи при необхідності інші.

6.2 Найпоширеніші загрози доступності

Найчастішими й найнебезпечнішими (з погляду розміру збитку) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів й інших осіб, які обслуговують інформаційні системи.

Іноді такі помилки і є властиво загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють уразливі місця, якими можуть скористатися зловмисники (такими є помилки адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок.

Пожежі й повені не приносять стільки лих, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший засіб боротьби з ненавмисними помилками – максимальна автоматизація й строгий контроль.

Інші загрози доступності класифікуємо за компонентами ІС, на які націлені загрози:

- відмова користувачів;
- внутрішня відмова інформаційної системи;
- відмова підтримувальної інфраструктури.

Звичайно, стосовно користувачів розглядаються такі загрози:

- небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості й при розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);

- неможливість працювати з системою внаслідок відсутності відповідної підготовки (недостатня загальна комп'ютерна грамотність, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією й т. п.);

- неможливість працювати з системою внаслідок відсутності технічної підтримки (неповнота документації, недостатньо довідкової інформації й т. п.).

Основними джерелами внутрішніх відмов є:

- відхід (випадковий або навмисний) від установлених правил експлуатації;

- вихід системи зі штатного режиму експлуатації внаслідок випадкових або навмисних дій користувачів або обслуговувального персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації й т. п.);

- помилки при переконфігуруванні системи;

- відмови програмного й апаратного забезпечення;

- руйнування даних;

- руйнування або ушкодження апаратури.

Стосовно підтримувальної інфраструктури рекомендується розглядати такі загрози:

- порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування;

- руйнування або ушкодження приміщень;

- неможливість або небажання обслуговувального персоналу й/або користувачів виконувати свої обов'язки (цивільні безладдя, аварії на транспорті, терористичний акт або його загроза, страйк і т. п.).

Досить небезпечні так звані «скривджені» співробітники – нинішні й колишні. Як правило, вони прагнуть завдати шкоди організації-«кривдникові», наприклад:

- зіпсувати устаткування;

- вмонтувати логічну бомбу, що згодом зруйнує програми й/або дані;

- видалити дані.

Скривджені співробітники, що були знайомі з порядками в організації, здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

Небезпечні, зрозуміло, стихійні лиха й події, які сприймаються як стихійні лиха: пожежі, повені, землетруси, урагани. За статистикою, на частку вогню, води й тому подібних «зловмисників» (серед яких найнебезпечніший – перебій електроживлення) припадає 13% втрат, нанесених інформаційним системам.

6.3 Деякі приклади загроз доступності

Загрози доступності можуть виглядати грубо – як ушкодження або навіть руйнування устаткування (у тому числі носіїв даних). Таке ушкодження може викликатися природними причинами (найчастіше – грозами). На жаль, джерела безперебійного живлення, що перебувають у масовому використанні, не захищають від потужних короткочасних імпульсів, і випадки вигоряння устаткування – не рідкість.

У принципі, потужний короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати й штучним чином – за допомогою так званих високоенергетичних радіочастотних гармат. Але, напевно, в наших умовах подібну загрозу потрібно все-таки визнати надуманою.

Авторам курсу довелось бути свідками ситуації, коли прорвало трубу з гарячою водою, і системний блок комп'ютера (це була робоча станція виробництва Sun Microsystems) виявився заповнений окропом. Коли окріп вилили, а комп'ютер просушили, він відновив нормальну роботу, але краще таких дослідів не проводити.

Загальновідомо, що періодично необхідно проводити резервне копіювання даних. Однак навіть якщо це виконується, резервні носії найчастіше зберігають недбало (до цього ми ще повернемося під час обговорення загроз конфіденційності), не забезпечуючи їхній захист від шкідливого впливу навколишнього середовища. І коли потрібно відновити дані, виявляється, що ці самі носії ніяк не бажають читатися.

Перейдемо тепер до загроз доступності, які будуть хитріші засмічень каналізації. Мова йтиме про програмні атаки на доступність.

Для виведення системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (звичайно – пропускні шляхи мереж, обчислювальних можливостей процесорів або оперативної пам'яті). За розташуванням джерела загрози таке споживання підрозділяється на локальне й вилучене. При прорахунках у конфігурації системи локальна програма здатна практично монополізувати процесор й/або фізичну пам'ять, звівши швидкість виконання інших програм до нуля.

Стосовно атаки «Papa Smurf» уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети «з'їдають» пропускні шляхи.

Вилучене споживання ресурсів останнім часом проявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес із максимальною швидкістю направляються цілком легальні запити на з'єднання й/або обслуговування. Часом початку «моди» на подібні атаки можна вважати лютий 2000 року, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше – власники й користувачі систем). Відзначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю

мережі й продуктивністю сервера, то захиститися від розподілених атак на доступність украй важко.

Для виведення систем зі штатного режиму експлуатації можуть використовуватися уразливі місця у вигляді програмних й апаратних помилок. Наприклад, відома помилка в процесорі Pentium I дає можливість локальному користувачеві шляхом виконання певної команди «підвісити» комп'ютер, так що допомагає лише апаратний RESET.

Програма «Teardrop» видалено «підвішує» комп'ютери, експлуатуючи помилку в складанні фрагментованих IP-пакетів.

6.4 Шкідливе програмне забезпечення

Одним з найнебезпечніших способів проведення атак є впровадження в системи, які атакують, шкідливого програмного забезпечення. Ми виділимо межі шкідливого ПЗ:

- шкідлива функція;
- спосіб поширення;
- зовнішнє подання.

Частину, що здійснює руйнівну функцію, будемо називати «бомбою» (хоча, можливо, більш вдалими термінами були б «заряд» або «боєголовка»). Загалом кажучи, спектр шкідливих функцій необмежений, оскільки «бомба», як і будь-яка інша програма, може мати яку завгодно складну логіку, але звичайно «бомби» призначаються для:

- впровадження іншого шкідливого ПЗ;
- отримання контролю над системою, яку атакують;
- агресивного споживання ресурсів;
- зміни або руйнування програм й/або даних.

За механізмом поширення розрізняють:

- віруси – код, що має здатність до поширення (можливо, зі змінами) шляхом впровадження в інші програми;
- «хробаки» – код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по ІС й їхнє виконання (для активізації вірусу потрібен запуск зараженої програми).

Віруси звичайно поширюються локально, у межах вузла мережі; для передачі по мережі їм потрібна така зовнішня допомога, як пересилання зараженого файлу. «Хробаки», навпаки, орієнтовані, в першу чергу, на подорожі по мережі.

Іноді саме поширення шкідливого ПЗ викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, «хробаки» «з'їдають» пропускні шляхи мережі й ресурси поштових систем. І з цієї причини для атак на доступність вони не мають потреби у вбудовуванні спеціальних «бомб».

Шкідливий код, що виглядає як функціонально корисна програма, називається троянським. Наприклад, звичайна програма, бувши ураженою

вірусом, стає троянською; часом троянські програми виготовляють вручну й підсовують довірливим користувачам у якому-небудь привабливому пакунку.

Відзначимо, що дані нами означення й наведена класифікація шкідливого ПЗ відрізняються від загальноприйнятих.

Вікно небезпеки для шкідливого ПЗ з'являється з випуском нового різновиду «бомб», вірусів й/або «хробаків» і перестає існувати з відновленням бази даних антивірусних програм і накладенням інших необхідних «латок».

За традицією з усього шкідливого ПЗ найбільша увага громадськості зосереджується на частці вірусів. Однак до березня 1999 року з повним правом можна було стверджувати, що «незважаючи на експонентний ріст числа відомих вірусів, аналогічного росту кількості інцидентів, викликаних ними, не зареєстровано. Дотримання нескладних правил «комп'ютерної гігієни» практично зводить ризик зараження до нуля. Там, де працюють, а не грають, число заражених комп'ютерів становить лише частки відсотка».

У березні 1999 року, з появою вірусу «Melissa», ситуація кардинальним чином змінилася. «Melissa» – це макровірус для файлів MS-Word, що поширюється за допомогою електронної пошти в приєднаних файлах. Коли такий (заражений) приєднаний файл відкривають, він розсилає свої копії за першими 50 адресами з адресної книги Microsoft Outlook. У результаті поштові сервери піддаються атаці на доступність.

У цьому випадку нам хотілося б відзначити два моменти.

1. Як уже говорилося, пасивні об'єкти відходять у минуле; так званий активний уміст стає нормою. Файли, які за всіма ознаками повинні були б належати до даних (наприклад, документи у форматах MS-Word або Postscript, тексти поштових повідомлень), здатні містити інтерпретовані компоненти, які можуть запускатися неявним чином при відкритті файлу. Як і будь-яке в цілому прогресивне явище, таке «підвищення активності даних» має свій зворотний бік (у розглянутому випадку – відставання в розробці механізмів безпеки й помилки в їхній реалізації). Пересічні користувачі ще не скоро навчаться застосовувати інтерпретовані компоненти «у мирних цілях» (або хоча б довідаються про їхнє існування), а перед зловмисниками відкрилося, власне кажучи, необмежене поле діяльності.

2. Інтеграція різних сервісів, наявність серед них мережевих, загальна зв'язність багаторазово збільшують потенціал для атак на доступність, полегшують поширення шкідливого ПЗ (вірус «Melissa» – класичний тому приклад). Образно кажучи, багато інформаційних систем, якщо не вжити захисних заходів, виявляються «в одному човні», так що досить однієї пробоїни, щоб «човен» відразу пішов на дно.

Як це часто буває, слідом за «Melissa» з'явилася на світ ціла серія вірусів, «хробаків» і їхніх комбінацій: «Explorer.zip» (червень 1999), «Bubble Boy» (листопад 1999), «ILOVEYOU» (травень 2000) і т. д. Не те щоб від них був

особливо великий збиток, але суспільний резонанс вони викликали чималий.

Активний вміст, крім інтерпретованих компонентів документів й інших файлів даних, має ще одне популярне обличчя – так звані мобільні агенти. Це програми, які завантажуються на інші комп'ютери й там виконуються. Найбільш відомі приклади мобільних агентів – Java-апплети, що завантажуються на комп'ютер користувача й інтерпретуються Internet-навігаторами. Виявилося, що розробити для них модель безпеки, яка залишає досить можливостей для корисних дій, не так вже й просто; ще складніше реалізувати таку модель без помилок. У серпні 1999 року стали відомі недоліки в реалізації технологій Active й Java у рамках Microsoft Internet Explorer, які давали можливість розміщати на Web-серверах шкідливі апплети, що дозволяють одержувати повний контроль над системою-візитером.

Для впровадження «бомб» часто використовуються помилки типу «переповнення буфера», коли програма, працюючи з областю пам'яті, виходить за межі припустимого й записує в потрібні зловмисникові місця певні дані. Так діяв ще в 1988 році знаменитий «хробак Моріса»; у червні 1999 року хакери знайшли спосіб використати аналогічний метод стосовно Microsoft Internet Information Server (IIS), щоб одержати контроль над Web-сервером. Вікно небезпеки охопило відразу біля півтора мільйона серверних систем.

Не забуті сучасними зловмисниками й випробовані троянські програми. Наприклад, «троянці» Back Orifice й Netbus дозволяють одержати контроль над системами користувачів з різними варіантами MS-Windows.

Таким чином, дія шкідливого ПЗ може бути спрямована не тільки проти доступності, але й проти інших основних аспектів інформаційної безпеки.

6.5 Основні загрози цілісності

На другому місці за масштабами збитків (після ненавмисних помилок і недоглядів) стоять крадіжки й підробки. За даними газети USA Today, ще в 1992 році в результаті подібних протиправних дій з використанням персональних комп'ютерів американським організаціям був нанесений загальний збиток у розмірі 882 мільйони доларів. Можна припустити, що реальний збиток був набагато більшим, оскільки багато організацій зі зрозумілих причин приховують такі інциденти; не викликає сумнівів, що в наші дні збиток від такого роду дій виріс багаторазово.

У більшості випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи й заходами захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні.

Раніше ми відокремлювали поняття статичної й динамічної цілісностей. З метою порушення статичної цілісності зловмисник (як правило, штатний співробітник) може:

- ввести недостовірні дані;
- змінити дані.

Іноді змінюються змістовні дані, іноді – службова інформація.

Можна зробити висновок, що існують не тільки загрози порушення цілісності, але й є небезпека сліпої довіри до комп'ютерної інформації. Заголовки електронного листа можуть бути підроблені; лист у цілому може бути фальсифікований особою, що знає пароль відправника (ми наводили відповідні приклади). Відзначимо, що останнє можливо навіть тоді, коли цілісність контролюється криптографічними засобами. Тут має місце взаємодія різних аспектів інформаційної безпеки: якщо порушено конфіденційність, може постраждати цілісність.

Ще один урок: загрозою цілісності є не тільки фальсифікація або зміна даних, але й відмова від зроблених дій. Якщо немає засобів забезпечити «безвідмовність», комп'ютерні дані не можуть розглядатися як доказ.

Потенційно уразливі, з погляду порушення цілісності, не тільки дані, але й програми. Впровадження розглянутого вище шкідливого ПЗ – приклад подібного порушення.

Загрозами динамічній цілісності є порушення атомарності транзакцій, перевпорядкування, крадіжка, дублювання даних або внесення додаткових повідомлень (мережевих пакетів і т. п.). Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

6.6 Основні загрози конфіденційності

Конфіденційну інформацію можна розділити на предметну й службову. Службова інформація (наприклад, паролі користувачів) не належить до певної предметної області, в інформаційній системі вона відіграє технічну роль, але її розкриття особливо небезпечно, оскільки воно несе в собі одержання несанкціонованого доступу до всієї інформації, у тому числі предметної.

Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться виконувати ролі користувачів не однієї, а цілого ряду систем (інформаційних сервісів). Якщо для доступу до таких систем використовуються багаторазові паролі або інша конфіденційна інформація, то, напевно, ці дані будуть зберігатися не тільки в голові, але й у записній книжці або на листках паперу, які користувач часто залишає на робочому столі, а іноді просто губить. І справа тут не в неорганізованості людей, а в споконвічній непридатності парольної схеми. Неможливо пам'ятати багато різних паролів; рекомендації з їх регулярної (по

можливості – частої) зміни тільки ускладнюють ситуацію, змушуючи застосовувати нескладні схеми чергування або взагалі намагатися звести справу до двох-трьох легких запам'ятовувань (і настільки ж легко вгадуваних) паролів.

Описаний клас уразливих місць можна назвати розміщенням конфіденційних даних у середовищі, де їм не забезпечений (найчастіше – і не може бути забезпечений) необхідний захист. Загроза ж полягає в тому, що хтось не відмовиться довідатися секрети, які самі просяться в руки. Крім паролів, що зберігаються в записних книжках користувачів, у цей клас потрапляє передача конфіденційних даних у відкритому вигляді (у розмові, у листі, по мережі), що уможливлює перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі й т. п.), але ідея одна – здійснити доступ до даних у той момент, коли вони найменш захищені.

Загрозу перехоплення даних варто брати до уваги не тільки при початковому конфігуруванні ІС, але й, що дуже важливо, при всіх змінах. Досить небезпечною загрозою є виставки, на які багато організацій, недовго думаючи, відправляє устаткування з виробничої мережі, з усіма даними, що зберігаються на ньому. Залишаються колишніми паролі, при вилученому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть у межах захищеної мережі організації; в об'єднаній мережі виставки – це занадто суворе випробування чесності всіх учасників.

Ще один приклад зміни, про яку часто забувають, – зберігання даних на резервних носіях. Для захисту даних на основних носіях застосовуються розвинені системи керування доступом; копії ж нерідко просто лежать у шафах й одержати доступ до них може багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються по багатьох каналах, їхній захист може виявитися досить складним та дорогим. Технічні засоби перехоплення добре пророблені, доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може будь-хто, так що цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, але й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але й для комп'ютерів, особливо портативних. Часто ноутбуки залишають без догляду на роботі або в автомобілі, іноді їх просто гублять.

Нетехнічною загрозою конфіденційності є також такі методи морально-психологічного впливу, як маскарад, тобто виконання дій під виглядом особи, що має повноваження доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести зловживання повноваженнями. У багатьох типах систем привілейований користувач (наприклад, системний адміністратор) здатний прочитати кожен (незашифрований) файл, одержати доступ до пошти будь-якого користувача й т. д. Інший приклад – завдання збитків при сервісному обслуговуванні.

Звичайно сервісний інженер одержує необмежений доступ до устаткування й має можливість діяти в обхід програмних захисних механізмів.

Такими є основні загрози, які завдають найбільшої шкоди суб'єктам інформаційних відносин.

Запитання для самоконтролю

1. Назвіть найпоширеніші загрози.
2. Основні означення і критерії загроз.
3. Назвіть найпоширеніші загрози доступності.
4. Основні загрози цілісності.
5. Основні загрози конфіденційності.
6. Що таке вікно небезпеки?
7. Коли з'являється вікно небезпеки?
8. Коли перестає існувати вікно небезпеки?
9. Назвіть найнебезпечніші джерела внутрішніх загроз.
10. Яку загрозу несе агресивне споживання ресурсів?

ГЛАВА 7
ФОРМУВАННЯ ПОВНОЇ МНОЖИНИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Однією з найбільш принципових особливостей проблеми ЗІ є абсолютний характер вимоги повноти всіх загроз інформації, потенційно можливих у сучасних умовах. Навіть один не врахований (не виявлений або не взятий до уваги) дестабілізувальний фактор може значною мірою знизити (або навіть звести нанівець) ефект захисту. Проблема формування повної множини загроз належить до числа яскраво виражених неформалізованих проблем. Це обумовлено тим, що архітектура сучасних засобів автоматизованої обробки інформації, організаційно-структурна і функціональна побудови інформаційно-обчислювальних мереж, технологія й умови обробки, збереження і накопичення інформації схильні до випадкових впливів надзвичайно великого числа факторів, ряд з яких можна класифікувати як дестабілізувальні. Таким чином, виникає ситуація, коли, з одного боку, вимога необхідності розв'язання задачі є абсолютною, а з іншого – регулярні методи розв'язання цієї задачі відсутні.

Оскільки в даний час відсутні скільки-небудь повні і всебічні статистичні дані про дестабілізувальні фактори (задача відбору, накопичення й обробка цих даних є однією зі складових і актуальних задач ЗІ, що підлягають регулярному розв'язанню), то для початкового формування якомога більш повної множини дестабілізувальних факторів найбільш доцільно використовувати експертні оцінки. Проте при цьому не може бути гарантоване формування повної множини дестабілізувальних факторів. Тому назовемо сформовану таким чином множину відносно повною, підкреслюючи цим її повноту відносно можливостей експертних методів.

7.1 Структура і загальний зміст алгоритму формування відносно можливостей експертних методів

Структура і загальний зміст алгоритму формування відносно повної множини дестабілізувальних факторів, які мають вплив на ЗІ, наведені на рисунку 7.1.

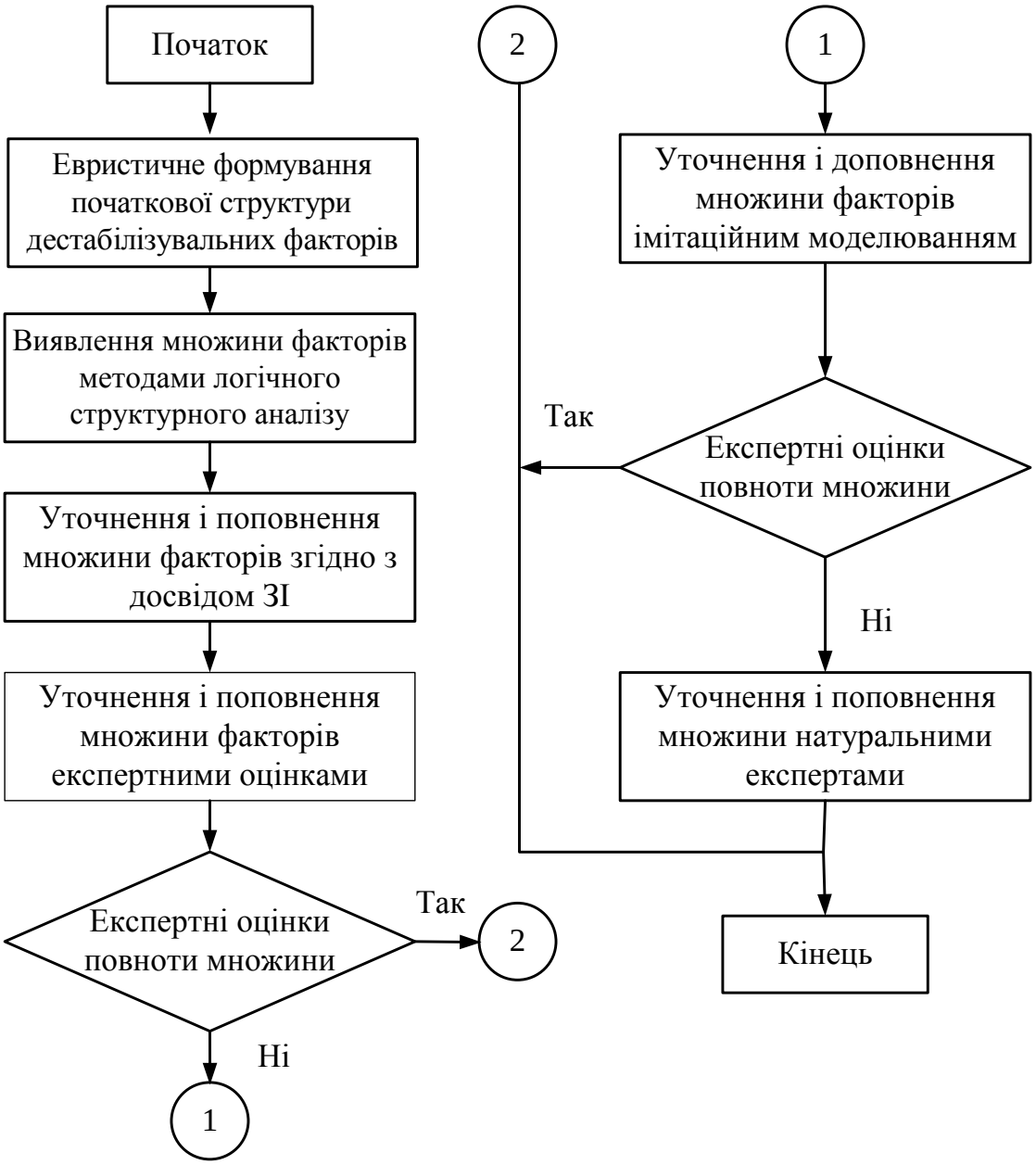


Рисунок 7.1 – Структура загального алгоритму формування відносно повної множини дестабілізувальних факторів

7.2 Причини порушення цілісності інформації

На підставі проведеного аналізу літературних джерел сформулюємо відносно повну множину причин порушення цілісності інформації (ППЦІ). Нагадаємо, що під ППЦІ розуміють такі дестабілізувальні фактори, наслідком прояву яких може бути порушення фізичної цілісності інформації, тобто її викривлення або знищення.

Перелік класів і груп ППЦІ наведено в таблиці 7.1.

Таблиця 7.1 – Класи ППЦІ і перелік потенційно можливих ППЦІ

Найменування групи ППЦІ	Найменування ППЦІ
ВІДМОВИ	
1.1. Відмова основної апаратури	1.1.1. Повний вихід апаратури з ладу 1.1.2. Неправильне виконання функцій
1.2. Відмови програм	1.2.1. Викривлення коду операції 1.2.2. Викривлення адреси вибірки 1.2.3. Викривлення адреси відправлення 1.2.4. Викривлення адреси передачі керування 1.2.5. Знищення фрагментів програми 1.2.6. Неправильне розміщення програм у ЗП
1.3. Відмови людей	1.3.1. Повний вихід із ладу 1.3.2. Систематично неправильне виконання функцій
1.4. Відмови носіїв інформації	1.4.1. Фізичне порушення носія інформації 1.4.2. Погіршення характеристик носія
1.5. Відмови систем живлення	1.5.1. Аварійне відключення живлення 1.5.2. Ушкодження ліній електроживлення 1.5.3. Підвищення напруги, що не відновлюється 1.5.4. Зниження напруги, що не відновлюється
1.6. Відмови систем забезпечення нормальних умов роботи апаратури та персоналу	1.6.1. Відключення систем кондиціонування 1.6.2. Зниження продуктивності систем контролю умов роботи кондиціонування апаратури

Продовження таблиці 7.1

	1.6.3. Незабезпечення персоналу системою кондиціонування 1.6.4. Відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу
1.7. Відмови систем передачі даних	1.7.1. Повний вихід з ладу каналу зв'язку передачі даних 1.7.2. Повний вихід з ладу засобів зв'язку 1.7.3. Неправильне виконання функцій каналом зв'язку 1.7.4. Неправильне виконання функцій засобами зв'язку
1.8. Відмови допоміжних матеріалів	1.8.1. Дефекти паперу для пристрою друкування
ЗБОЇ	
2.1. Збої основної апаратури	2.1.1. Неправильне виконання функцій
2.2. Збої програм	2.2.1. Неправильне виконання коду операції 2.2.2. Неправильне виконання адреси вибірки 2.2.3. Неправильне виконання адреси відправлення 2.2.4. Неправильне виконання адреси передачі керування
2.3. Збої людей	2.3.1. Тимчасовий вихід з ладу 2.3.2. Епізодичне неправильне виконання функцій
2.4. Збої носіїв	2.4.1. Погіршення характеристик носіїв інформації, що відновлюються
2.5. Збої систем живлення	2.5.1. Короткочасне вимикання живлення

Продовження таблиці 7.1

	2.5.2. Короткочасне підвищення напруги 2.5.3. Короткочасне зниження напруги 2.5.4. Короткочасна зміна частоти струму
2.6. Збої системи забезпечення нормальних умов роботи	2.6.1. Короткочасне відключення систем забезпечення кондиціонування 2.6.2. Короткочасне зниження продуктивності систем кондиціонування 2.6.3. Короткочасне відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу
2.7. Збої систем передачі даних	2.7.1. Неправильне виконання функцій передачі даних каналом зв’язку 2.7.2. Неправильне виконання функцій засобами зв’язку
2.8. Збої допоміжних матеріалів	2.8.1. Дефекти в пристроях друкування, що виправляються 2.8.2. Дефекти паперу, що виправляються
ПОМИЛКИ	
3.1. Помилки основної апаратури	3.1.1. Неправильний монтаж схеми процедури апаратури 3.1.2. Неправильний монтаж схеми переходу до процедури 3.1.3. Неправильний монтаж схеми адреси вибірки 3.1.4. Неправильний монтаж схеми адреси відправлення

Продовження таблиці 7.1

3.2. Помилки програми	3.2.1. Неправильний код операції 3.2.2. Неправильна адреса вибірки 3.2.3. Неправильна адреса відправлення 3.2.4. Неправильна передача керування 3.2.5. Неправильне розташування елементів програм
3.3. Помилки людей	3.3.1. Неправильне сприйняття інформації 3.3.2. Неправильний набір інформації 3.3.3. Неправильний вибір процесу 3.3.4. Випадкове втручання в процес
3.4. Помилки системи передачі даних	3.4.1. Неправильна схема комутації каналу передачі даних 3.4.2. Неправильна схема комутації в каналі 3.4.3. Неправильний монтаж схеми в пристроях зв'язку
СТИХІЙНІ ЛИХА	
4.1. Пожежа	4.1.1. Невеличка (локальна) 4.1.2. Середня 4.1.3. Загальна (велика)
4.2. Повінь	4.2.1. Місцева (локальна) 4.2.2. Середня (у межах будинку) 4.2.3. Загальна (міська)
4.3. Землетрус	4.3.1. Легкий 4.3.2. Середній 4.3.3. Сильний
4.4. Ураган	4.4.1. Малий 4.4.2. Середній 4.4.3. Сильний
4.5. Вибух	4.5.1. Легкий 4.5.2. Середній

Продовження таблиці 7.1

	4.5.3. Сильний
4.6. Аварія	4.6.1. Невеличка 4.6.2. Середня 4.6.3. Значна
ЗЛОЧИННІ ДІЇ	
5.1. Запам’ятовування інформації	5.1.1. Запам’ятовування інформації на пристроях наочного відображення інформації 5.1.2. Запам’ятовування бланків з вихідними даними 5.1.3. Запам’ятовування вихідної документації
5.2. Копіювання	5.2.1. Фотографування 5.2.2. Виготовлення неврахованих копій документів 5.2.3. Друкування масивів
5.3. Розкрадання	5.3.1. Розкрадання банків з вихідними даними 5.3.2. Розкрадання магнітних носіїв 5.3.3. Розкрадання вихідних документів
5.4. Підміна	5.4.1. Підміна бланків 5.4.2. Підміна магнітних носіїв 5.4.3. Підміна вихідних документів 5.4.4. Підміна апаратури 5.4.5. Підміна елементів програм
5.5. Підключення	5.5.1. Підключення генератора завад 5.5.2. Підключення реєструвальної апаратури
5.6. Поломка	5.6.1. Поломка апаратури 5.6.2. Ушкодження програм 5.6.3. Ушкодження елементів баз даних 5.6.4. Ушкодження носіїв 5.6.5. Ушкодження документів

Продовження таблиці 7.1

5.7. Диверсія	5.7.1. Створення пожежі 5.7.2. Організація повені 5.7.3. Організація вибуху 5.7.4. Ушкодження системи електроживлення 5.7.5. Ушкодження систем забезпечення нормальних умов роботи апаратури і персоналу
ПОБІЧНІ ЯВИЩА	
6.1. Електромагнітні	6.1.1. Випромінювання пристроїв наочного відображення інформації 6.1.2. Випромінювання процесорів ЕОМ 6.1.3. Випромінювання зовнішніх запам'ятовувальних пристроїв 6.1.4. Випромінювання друкувальних пристроїв 6.1.5. Випромінювання апаратури зв'язку 6.1.6. Випромінювання ліній зв'язку 6.1.7. Випромінювання допоміжної апаратури
6.2. Паразитні наводки	6.2.1. Наводки в комутаторах загального призначення 6.2.2. Наводки в слабкострумових ланцюгах 6.2.3. Наводки в мережах живлення
6.3. Зовнішні електромагнітні випромінювання	6.3.1. Випромінювання біля пристроїв наочного відображення інформації 6.3.2. Випромінювання біля зовнішніх запам'ятовувальних пристроїв 6.3.3. Випромінювання біля друкувальних пристроїв 6.3.4. Випромінювання біля апаратури зв'язку

Продовження таблиці 7.1

	6.3.5. Випромінювання біля ліній зв’язку 6.3.6. Випромінювання біля допоміжних пристроїв 6.3.7. Випромінювання в сховищах носіїв інформації
6.4. Вібрація	6.4.1. Мала 6.4.2. Середня 6.4.3. Велика
6.5. Зовнішні атмосферні умови	6.5.1. Зміна температури 6.5.2. Підвищення вологості повітря 6.5.3. Підвищення запиленості повітря 6.5.4. Підвищення рівня радіації 6.5.5. Зараження повітря отруйними речовинами 6.5.6. Бактеріологічне зараження повітря

7.3 Канали несанкціонованого доступу до інформації

Під каналами несанкціонованого одержання інформації (КНОІ) розуміють такі дестабілізувальні фактори, під дією яких може бути одержання (або небезпека одержання) інформації, яка захищається, особами або процесами, що не мають на це законних повноважень. Об’єктивна необхідність формування повної множини потенційно можливих КНОІ така, як і для ППЦІ. У той же час, труднощі формування повної множини КНОІ значно більші, ніж при вирішенні аналогічної задачі для ППЦІ. Пояснюється це тим, що несанкціоноване одержання інформації пов’язано переважно зі злочинними діями людей, що дуже важко піддаються структуризації. Наведені структури множини і перелік КНОІ сформульовані з використанням методики, викладеної раніше.

Насамперед, було встановлено, що з метою формування більш повної множини КНОІ необхідно побудувати повну класифікаційну структуру. Така структура може бути побудована, якщо за критерії класифікації вибрати такі два показники: перший – що стосується стану інформації і ступінь взаємодії зловмисника з її елементами. Щодо першого критерію, то будуть розрізняти два стани: безвідносно обробки (несанкціоноване одержання інформації може мати місце навіть у тому випадку, якщо вона не обробляється, а просто зберігається) і в процесі безпосередньої обробки.

Повна структуризація другого критерію може бути здійснена виділенням таких його значень:

перше – без доступу (тобто непряме одержання інформації);

друге – з доступом, але без зміни їхнього стану або змісту;

третє – з доступом і зі зміною змісту інформації або стану.

Отже, класифікаційна структура КНОІ буде мати вигляд (таблиця 7.2):

Таблиця 7.2 – Класифікаційна структура КНОІ

Ознака класифікації		***Відношення до стану інформації, що захищається***	
		безвідносно до обробки інформації ***А-канали***	*виявляються в процесі обробки* ***В-канали***
Без доступу	***К-канали***	*1-й КЛАС АК-канали*	*2-й КЛАС ВК-канали*
З доступом	*Без зміни* ***П-канали***	*3-й КЛАС АП-канали*	*4-й КЛАС ВП-канали*
	Зі зміною ***Пи-канали***	*5-й КЛАС Апи-канали*	*6-й КЛАС ВПи-канали*

Повнота поданої класифікаційної структури гарантується тим, що обрані критерії класифікації охоплюють усі потенційно можливі варіанти взаємодії зловмисника з інформацією, а структуризація значень критеріїв здійснюється за методом розподілу цілого на частини.

Таким чином, уся множина потенційно можливих КНОІ може бути строго розділеною на шість класів.

Наступним кроком на шляху вирішення розглянутої задачі є обґрунтування більш повного переліку КНОІ в межах кожного з шести класів.

Отриманий перелік буде виглядати таким чином.

КНОІ першого класу – канали, що виявляються безвідносно обробки інформації і без доступу зловмисника до інформації.

1. Розкрадання носіїв на заводах, де відбувається їхній ремонт.
2. Підслуховування розмов осіб, що стосуються інформації.
3. Провокування на розмови осіб, компетентних щодо інформації.
4. Використання зловмисником візуальних засобів.
5. Використання зловмисником оптичних засобів.
6. Використання зловмисником акустичних засобів.

КНОІ другого класу – канали, що виявляються в процесі обробки інформації без доступу зловмисника до неї.

1. Електромагнітні випромінювання пристроїв відображення.
2. Електромагнітні випромінювання процесорів.
3. Електромагнітні випромінювання зовнішніх запам'ятовувальних пристроїв.
4. Електромагнітні випромінювання апаратури зв'язку.
5. Електромагнітні випромінювання ліній зв'язку.
6. Електромагнітні випромінювання допоміжної апаратури.
7. Електромагнітні випромінювання пристроїв підготовки даних.
8. Паразитні наводки в комунікаціях електропостачання.
9. Паразитні наводки в системах водопостачання і каналізації.
10. Паразитні наводки в мережах теплопостачання і вентиляції.
12. Паразитні наводки в шинах заземлення.
13. Паразитні наводки в ланцюгах газифікації.
14. Паразитні наводки в ланцюгах радіофікації.
15. Паразитні наводки в ланцюгах телефонізації.
16. Паразитні наводки в мережах живлення по ланцюгу 50 Гц.
17. Паразитні наводки в мережах живлення по ланцюгу 400 Гц.
18. Підключення генератора завад.
19. Підключення реєструвальної апаратури.
20. Огляд відходів виробництва, що потрапляють за межі контрольованої зони.

КНОІ третього класу – канали, що виявляються безвідносно обробки інформації з доступом зловмисника до неї, але без зміни інформації.
1. Копіювання бланків із вихідними даними.
2. Копіювання першоносіїв.
3. Копіювання магнітних носіїв.
4. Копіювання пристроїв відображення інформації.
5. Копіювання вихідних документів.
6. Копіювання інших документів.
7. Розкрадання виробничих відходів.

КНОІ четвертого класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до неї, але без зміни останньої.
1. Запам'ятовування інформації на бланках із вихідними даними.
2. Запам'ятовування інформації з пристроїв відображення.
3. Запам'ятовування інформації на вихідних документах.
4. Запам'ятовування службових даних.
5. Копіювання в процесі обробки.
6. Виготовлення дублікатів масивів і вихідних документів.
7. Копіювання роздруківки масивів.
8. Використання програмних пасток.
9. Маскування під зареєстрованого користувача.
10. Використання недоліків операційних систем.

11. Використання недоліків мов програмування.
12. Використання вразливості програмного забезпечення вірусом.

КНОІ п’ятого класу – канали, що виявляються безвідносно обробки інформації з доступом зловмисника до неї та зі зміною останньої.

1. Підміна бланків.
2. Підміна магнітних носіїв.
3. Підміна вихідних документів.
4. Підміна апаратури.
5. Підміна елементів програми.
6. Підміна елементів баз даних.
7. Розкрадання бланків із вихідними даними.
8. Розкрадання магнітних носіїв.
9. Розкрадання вихідних документів.
10. Розкрадання інших документів.
11. Внесення в програми блоків типу «троянський кінь», «бомба» і т. п.
12. Читання залишкової інформації в ОЗП після виконання санкціонованих запитів.

КНОІ шостого класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до інформації та застосуванням її.

1. Незаконне підключення до апаратури.
2. Незаконне підключення до ліній зв’язку.
3. Зняття інформації на шинах живлення пристроїв відображення.
4. Зняття інформації на шинах живлення процесорів.
5. Зняття інформації на шинах живлення апаратури зв’язку.
6. Зняття інформації на шинах живлення ліній зв’язку.
7. Зняття інформації на шинах живлення друкувальних пристроїв.
8. Зняття інформації на шинах живлення зовнішніх запам’ятовувальних пристроїв.
9. Зняття інформації на шинах живлення допоміжної апаратури.

7.4 Методи визначення значень показників уразливості інформації

Для визначення значень показників уразливості інформації розроблений метод, що відповідає природі цих показників і враховує всі фактори, що впливають на значення показників.

У розділі «Система показників уразливості інформації» відзначалося, що з усієї сукупності показників особливе місце займають базові показники, тобто показники, що характеризують уразливість інформації в якому-небудь одному структурному компоненті інформаційної системи (ІС) в одному якому-небудь КНОІ, відносно якогось потенційного порушника. Тоді схему визначення показників уразливості в загальному вигляді можна уявити так (рис. 7.2).

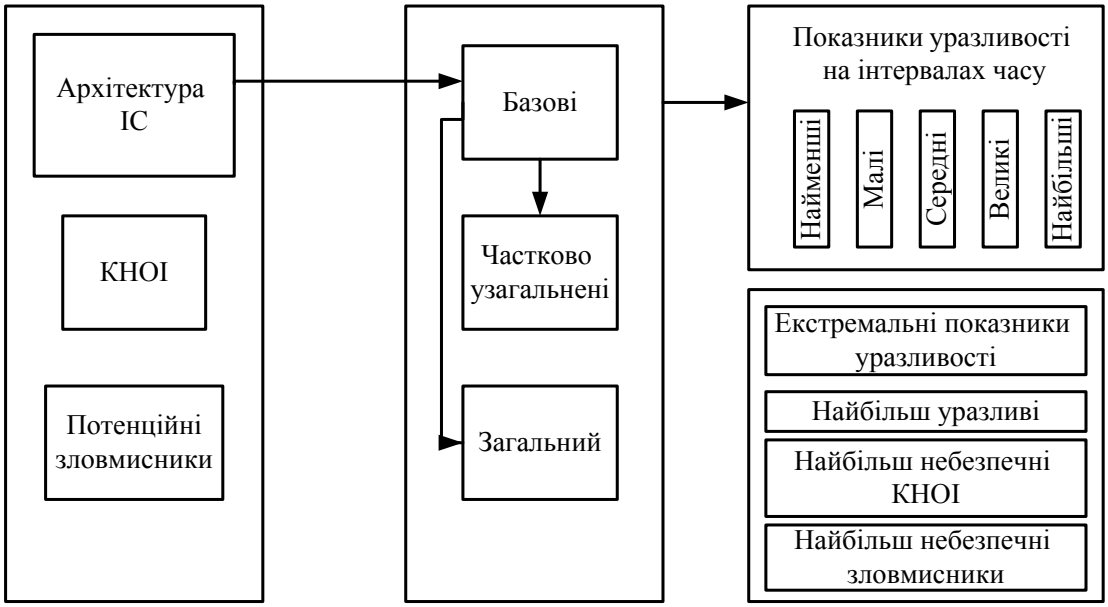


Рисунок 7.2 – Загальна схема визначення показників уразливості інформації

Цю схему можна покласти в основу розробки як методів, так і моделей визначення значень показників уразливості інформації.

Значення базових показників визначається архітектурою ІС (від чого залежить рівень захищеності кожного її структурного компонента), безліччю потенційно можливих КНОІ (від чого залежать потенційні можливості злочинних дій у структурному компоненті), а також чисельністю потенційних порушників і їхніх можливостей здійснювати злочинні дії.

Потенційно можливою є та обставина, що в сучасних ІС несанкціоноване одержання інформації можливо не тільки шляхом безпосереднього доступу до даних, але і багатьма шляхами, що не потребують такого доступу.

Структурну схему потенційно можливих злочинних дій в ІС для найзагальнішого випадку наведено на рис. 7.3.

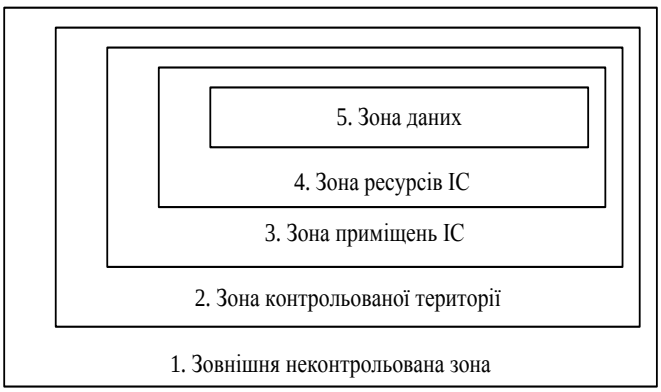


Рисунок 7.3 – Структурна схема потенційно можливих злочинних дій

Виділені зони характеризуються так.

1. **Зовнішня зона, що не контролюється,** – територія навколо ІС, на якій персоналом і засобами ІС не застосовуються ніякі засоби і не здійснюються ніякі заходи для ЗІ.
2. **Зона території, що контролюється,** – територія навколо приміщень ІС, що постійно контролюється персоналом або технічними засобами.
3. **Зона приміщень ІС** – внутрішній простір тих приміщень, у яких розташовані засоби системи.
4. **Зона ресурсів ІС** – та частина приміщень, звідки можливий безпосередній доступ до ресурсів системи.
5. **Зона даних** – та частина ресурсів системи, з якої можливий безпосередній доступ до захищуваної інформації.

Злочинні дії з метою несанкціонованого одержання інформації в загальному випадку можливі в кожній із перерахованих зон. При цьому для несанкціонованого одержання інформації необхідне одночасне настання таких подій.

1. Порушник повинен одержати доступ у відповідну зону.
2. Під час перебування порушника в зоні у ній повинен з'явитися відповідний КНОІ.
3. Відповідний КНОІ повинен бути доступний порушнику.
4. У КНОІ в момент доступу до нього порушника повинна знаходитися інформація, що захищається.

Зробимо висновок щодо загальних залежностей для визначення значень базових показників уразливості. Введемо такі позначення змінних індексів.

Тоді, відповідно до теореми можливостей, можливість несанкціонованого одержання інформації порушником k-ї категорії в j-му КНОІ в 1-й зоні і-го структурного компонента ІС визначається такою залежністю:

$$P_{ijkl}^{(n,l)} = P_{ikl}^{(n,d)} * P_{ijl}^{(n,k)} * P_{ijkl}^{(j,n)} * P_{ijl}^{(n,u)}, \qquad (7.1)$$

де i – поточний ідентифікатор структурного компонента ІС;

j – те ж для КНОІ;

k – те ж для категорії потенційних порушників;

l – те ж для зони злочинних дій.

Введемо такі позначення:

P_{ikl} – можливість доступу порушника *k-ї* категорії в *1-у* зону *і-го* компонента ІС;

P_{ijl} – можливість появи *j-го* КНОІ в *1-й* зоні *і-го* компонента ІС;

P_{ijkl} – можливість доступу порушника *k-ї* категорії до *j-го* КНОІ в *1-й* зоні *i-го* компонента за умови доступу порушника в зону;

P_{ijl} – можливість наявності захищуваної інформації в *j-ому* КНОІ в *1-й* зоні *i-го* компонента в момент доступу туди порушника.

Наведена залежність буде справедлива в тому випадку, коли всі події, відображені в правій частині формули, є незалежними одна від одної, тобто коли поява будь-якої з них впливає на можливість появи інших. В іншому випадку необхідно враховувати коефіцієнти між можливостями залежних подій.

Для базової можливості несанкціонованого одержання інформації байдуже, в якій зоні це одержання інформації мало місце, вона раніше визначена як можливість несанкціонованого одержання інформації в одному компоненті ІС одним порушником якоїсь категорії і в одному КНОІ. Позначимо базову можливість як P_{ijk}, запишемо її в такому вигляді:

$$P_{ijk}^{(n,b)} = 1 - \Pi_{l=1}^{5}\left[1 - P_{ijkl}^{(n,b)}\right] = 1 - \Pi_{l=1}^{5}\left[1 - P_{ikl}^{(n,d)} * P_{ijl}^{(n,k)} * P_{ijkl}^{(j,n)} * P_{ijl}^{(n,u)}\right]. \quad (7.2)$$

Значення частково узагальнених показників можуть визначатися таким чином. Нехай *{k*}* є підмножиною з повної множини потенційно можливих порушників. Тоді можливість несанкціонованого одержання інформації зазначеною підмножиною порушників в *j-му* КНОІ в *i-ому* компоненті ІС $P_{ij}^{(r)}\{k^*\}$ визначається виразом:

$$P_{ij}^{(r)}\{\mathrm{k}^*\} = 1 - \underset{\forall k^*}{\Pi}\left[1 - P_{ijk}^{(b)}\right],$$

де $\forall k^*$ – множення в дужках для усіх k, що входять в підмножину.

Аналогічно, якщо {j*} – підмножина структурних компонент ІС, що викликають інтерес, то уразливість інформаційного компонента даної підмножини КНОІ щодо *k-го* порушника визначається так:

$$P_{i}^{(r)}\{\mathrm{j}^*\}\,\mathrm{k} = 1 - \underset{\forall j^*}{\Pi}\left[1 - P_{ijk}^{(b)}\right].$$

Якщо ж {i*} – підмножина структурних компонент ІС, що викликають інтерес, то уразливість інформації в них у *j-му* КНОІ щодо *k-го* порушника визначається так:

$$P^{(r)}\{\mathrm{i}^*\}\mathrm{jk} = 1 - \underset{\forall i^*}{\Pi}\left[1 - P_{ijk}^{(b)}\right].$$

Кожен з наведених виразів дозволяє робити узагальнення щодо одного якогось параметра.

Для одержання узагальненого виразу необхідно врахувати одночасно підмножини {i*}, {j*},{k*}.

Очевидно, загальний показник уразливості $P^{(r)}$ визначається таким чином:

$$P^{(r)} = 1 - \prod_{\forall i}\left[1 - P_{ijk}^{(b)}\right]\prod_{\forall j}\left[1 - P_{ijk}^{(b)}\right]\prod_{\forall k}\left[1 - P_{ijk}^{(b)}\right].$$

Тепер визначимо вирази, що описують екстремальні показники уразливості. Як уже відзначалося раніше, екстремальними названі показники, які характеризують найбільш несприятливі умови захищеності інформації: найуразливіший структурний компонент ІС, КНОІ, найнебезпечнішу категорію порушників. Позначимо:

i – найбільш уразливий структурний компонент ІС;

j – найбільш небезпечний КНОІ;

k – найнебезпечніша категорія порушників.

Тоді очевидно:

$$\bar{i} = iEp^{y} \to \max \forall i\,,$$

де *i* – є таке *i*, для якого заданий показник уразливості p^y приймає максимальне значення для всіх *i*.

Аналогічно

$$\bar{j} = jEp^{y} \to \max \forall j\,,$$

$$\bar{k} = jEp^{y} \to \max \forall k\,.$$

На підставі проведених досліджень розроблені методи розрахунку показників уразливості інформації з урахуванням інтервалу часу, в якому оцінюється уразливість.

Неважко помітити, що наведені вище вирази є адекватними для таких інтервалів часу, що названі малими. Для інших інтервалів отримані вирази не будуть адекватними, тому що чим більший інтервал часу, тим більше можливостей у порушника для дій і тим більша можливість зміни стану ІС і умов обробки інформації.

Можливі такі підходи для вирішення цієї задачі.

Малими називають інтервали, які не можна зводити до точки, але процеси, що відбуваються на них, відносно уразливості інформації можна вважати однорідними. Тоді природно можна розділити малий інтервал на дуже малі інтервали і на кожному з них визначати уразливість інформації. А оскільки процеси, що відбуваються на малому інтервалі часу,

однорідні, то на кожному інтервалі уразливість буде визначатися однозначно за такою залежністю.

$$P^M = 1 - \prod_{t=1}^{Nt} (1 - P^T),$$

де P^T – уразливість у точці (на дуже малому інтервалі);

P^M – показник уразливості на малому інтервалі;

t – змінний індекс дуже малих інтервалів, на які розбитий малий інтервал;

N_t – загальне число інтервалів.

Неважко помітити, що розглянутий підхід може поширюватися і на інші види інтервалів: великий інтервал уявити деякою послідовністю малих і т. п.

Проте наведені вирази будуть справедливими лише в тому випадку, якщо на всьому розглянутому інтервалі часу умови для злочинних дій залишаються незмінними. У реальних умовах вони можуть змінюватися, причому найбільш важливим фактором, що впливає на можливості злочинних дій, є активні дії системи ЗІ. Технологія функціонування системи ЗІ повинна бути тим сильнішою та активнішою, чим вища уразливість інформації.

З урахуванням цього запишемо:

$$P^T(t) = \oint \left[P^T(t-1) \right], \tag{7.3}$$

тобто значення показника в кожній точці розглянутого інтервалу є деяка функція значення цього показника в попередній точці. Тоді вираз (7.3) можна записати в такому вигляді:

$$P^M = 1 - \prod_{t=1}^{N^t} \left\{ 1 - \oint \left[P^T(t-1) \right] \right\}.$$

Функціональну залежність зумовлюють використовувані засоби захисту і технології функціонування систем ЗІ.

Розглянуті моделі є аналітичними, оскільки вони дозволяють визначати необхідні значення показників уразливості шляхом аналітичних обчислень.

Проте в багатьох практичних ситуаціях конкретні значення вихідних розмірів для визначення базового показника уразливості інформації можуть змінюватися залежно від конкретних ситуацій у ІС і в зовнішньому середовищі і не виражатися у вигляді конкретних формул унаслідок складності вихідних моделей. В той же час часто можна структурувати

системи, що моделюються, та процеси до такого ступеня, що задача може бути вирішена методом моделювання.

Для складних ІС і слабоструктурованих схем функціонування систем обробки найбільш адекватним методом прогнозування показників уразливості буде статистика. Проте для того, щоб статистичним шляхом безпосередньо прогнозувати значення показників уразливості, необхідні багатопараметричні статистичні дані передісторії. В даний час статистичні дані практично відсутні, і одержання їх являє собою дуже складну проблему.

З метою спрощення задачі будемо прогнозувати не безпосередні показники уразливості, а складові величини, що входять у вираз для показників якості. Як випливає з моделей оцінювання показників якості, такими величинами є нижченаведені.

1. Можливість прояву дестабілізувальних факторів (наявності КНОІ).
2. Можливість наявності захищуваної інформації в місці і під час прояву дестабілізувальних факторів.
3. Можливість несанкціонованого одержання інформації під впливом дестабілізувальних факторів, незважаючи на застосування ЗІ.

Розглянемо можливі підходи до прогнозування перерахованих величин.

Можливість прояву дестабілізувальних факторів – P_{ijz}.

При сталому процесі функціонування системи обробки інформації прояв дестабілізувальних факторів можна вважати випадковим пуассоновим процесом. Позначивши *ijz* як інтенсивність потоку *i-го* фактора в *j-му* технічному засобі (ТЗ), що знаходиться в *z-му* стані, то, відповідно до властивостей пуассонового процесу, запишемо

$$P_{ijk} = f_{\text{tijk}} * \sigma_t,$$

де σ_t – інтервал часу, істотно менший того інтервалу, відносно якого визначена величина.

Оскільки для загального випадку інтервал прогнозування цю умову не буде задовольняти, то величину P_{ijk} запишемо в такому вигляді:

$$P_{ijk} = 1 - (1 - \rho_{\text{ijk}}) * ((\Delta t)/(\sigma_t)),$$

де Δt – інтервал прогнозування.

Отже, можна розділити весь період прогнозування Δt на менші інтервали тривалістю σ_t і записати, що

$$\bar{j} = jEp^{y} \rightarrow \max \forall j.$$

Тоді за умови, що $\Delta t >> \sigma_t$, можна записати

$$P_j^M = \frac{\sum_\theta \gamma_{t\theta}\Delta t}{\frac{\Delta t}{\sigma t}} = \frac{\sigma t}{\Delta t}\sum \gamma_{j\theta}.$$

Значення функції визначаються з технологічного графіка обробки інформації в прогнозований період часу.

Аналогічно аналізу попереднього параметра період прогнозування будемо здійснювати на малих інтервалах часу. Введемо функцію N_{in}^{Q}, що є:

1 – якщо *j*-ий засіб захитсу на *k*-му інтервалі часу активно використовується в *i*-ому ТЗ;

0 – не враховується.

З урахуванням того, що $\Delta t >> \sigma_t$, можна записати:

$$P_{ij}^{НП} = \prod_{\forall \eta}\left(1 - P_{шо}^{\eta}\right) * \frac{\sigma}{\Delta e} * \sum N_{от}^{\theta}.$$

де $P_{ij}^{НП}$ – можливість того, що при використанні η*-го* засобу захисту в *j-му* ТЗ несанкціоноване одержання інформації не буде мати місця навіть при появі *і-го* дестабілізувального фактора.

Виходячи з концепції захисту інформації як сукупності взаємозалежних організаційних заходів і технічних систем, синтезованих на основі обраних критеріїв оптимізація з урахуванням обмежень і спрямованих на захист інформації при її формуванні, передаванні, прийомі, обробці та зберіганні з метою збереження її цілісності, формується поняття захищеності інформації в ІС. Поняття захищеності є центральним у силу нижченаведених причин.

1. Сама мета створення системи (моделі) ЗІ є досягненням науково-технічного рівня захищеності інформації в ІС. Таким чином, методологія оцінювання захищеності інформації є, за суттю, методологією наукового обґрунтування кількісних показників досягнення мети системи захисту.

2. Методологія оцінювання захищеності інформації в ІС є, насамперед, методологією наукового обґрунтування норм ефективності ЗІ. Оптимальний або раціональний вибір одиниць виміру і кількісних значень норм ефективності визначає категорії якості системи захисту, структуру і математичний апарат синтезу, аналізу та оптимізації моделі захисту і саму якість захисту. Дійсно, завищені норми ефективності ведуть до підвищення витрат на створення системи захисту, а занижені норми просто не дозволяють досягти цілей захисту.

3. Методологія оцінювання захищеності інформації в ІС є основою для реального рівня захисту інформації в конкретних системах і його порівняння з нормами ефективності захисту, а, отже, є основою для вирішення питань про методи і засоби досягнення системи захисту.

Визначаючи критерії якості захисту, структуру і математичний апарат синтезу, аналізу й оптимізації моделі системи захисту, методологія оцінювання захищеності інформації визначає цілі, засоби і методологію інженерного аналізу, спрямованого на виявлення потенційних стратегій нападу на інформацію в ІС і основні характеристики стратегій нападу, визначення можливих заходів захисту і вимог до їхніх параметрів.

Запитання для самоконтролю

1. Що розуміють під загрозою інформації?
2. Які фактори складають систему дестабілізувальних факторів, як їх визначають?
3. Які існують джерела дестабілізувальних факторів?
4. У яких ситуаціях необхідно оцінювати уразливість інформації?
5. Чим обумовлюється уразливість у процесі функціонування системи?
6. Як виражають кількісну міру уразливості?
7. Що позначають показники, зображені в таблиці 7.2? З якою метою використовують експертні помилки?
8. Що розуміють під КНОІ?
9. Які два показники вибирають за критерії класифікації КНОІ?
10. У чому полягає повнота класифікаційної структури, наведеної на рисунку 7.1?
11. На які 6 класів класифікується КНОІ?
12. Що характеризують базові показники і чим визначаються їхні значення?
13. Чим характеризуються зони, подані на рис. 7.3?
14. Які умови необхідні для несанкціонованого одержання інформації?

ГЛАВА 8
ЗАГАЛЬНІ КРИТЕРІЇ ОЦІНЮВАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Ідучи по шляху інтеграції, у 1990 році Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (TEC) розробили спеціалізовану систему світової стандартизації, а Міжнародна організація зі стандартизації почала створювати міжнародні стандарти щодо критеріїв оцінювання безпеки інформаційних технологій для загального використання, які названі «Common Criteria fon Information Technology Security Evaluation» («Загальні критерії оцінювання безпеки інформаційних технологій») або просто «Common Criteria» («Загальні критерії») (рис. 8.1).

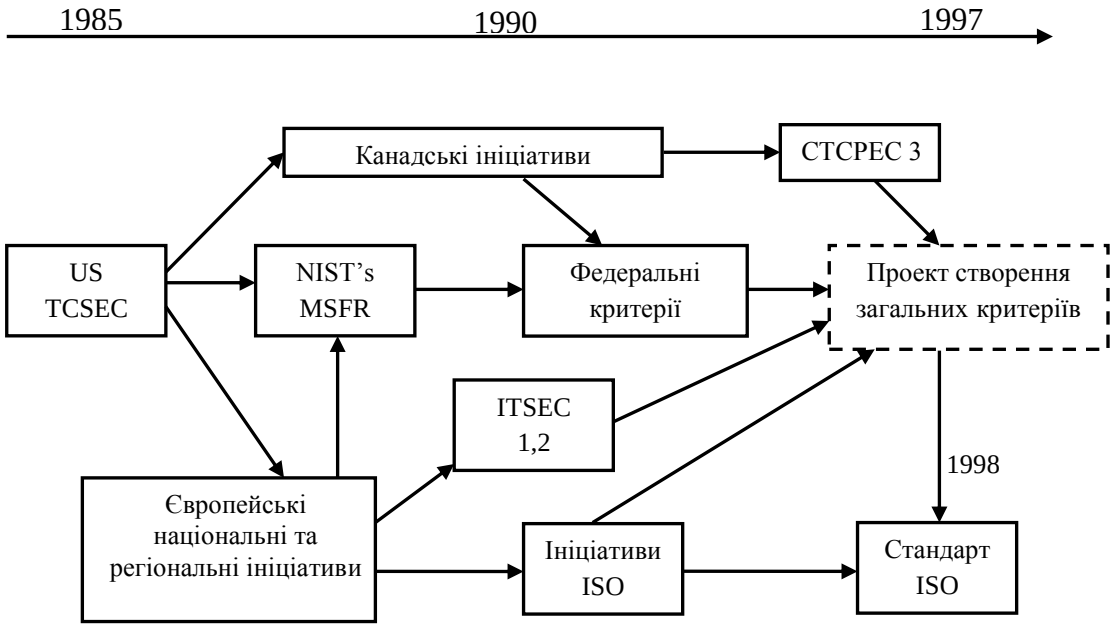


Рисунок 8.1 – Коротка історія загальних критеріїв

У їх розробці брали участь: Національний інститут стандартів і технології та Агентство національної безпеки (США), Організація безпеки комунікацій (Канада), Агентство інформаційної безпеки (Германія), Агентство національної безпеки комунікацій (Нідерланди), Органи виконання програми безпеки і сертифікації інформаційних технологій (Англія), Центр забезпечення безпеки систем (Франція). У подальшому «Загальні критерії» неодноразово редагувались. У результаті 08 червня 1999 року був затверджено Міжнародний стандарт ISO/IEC 15408 під назвою «Загальні критерії оцінки безпеки інформаційних технологій» (рис. 8.2).

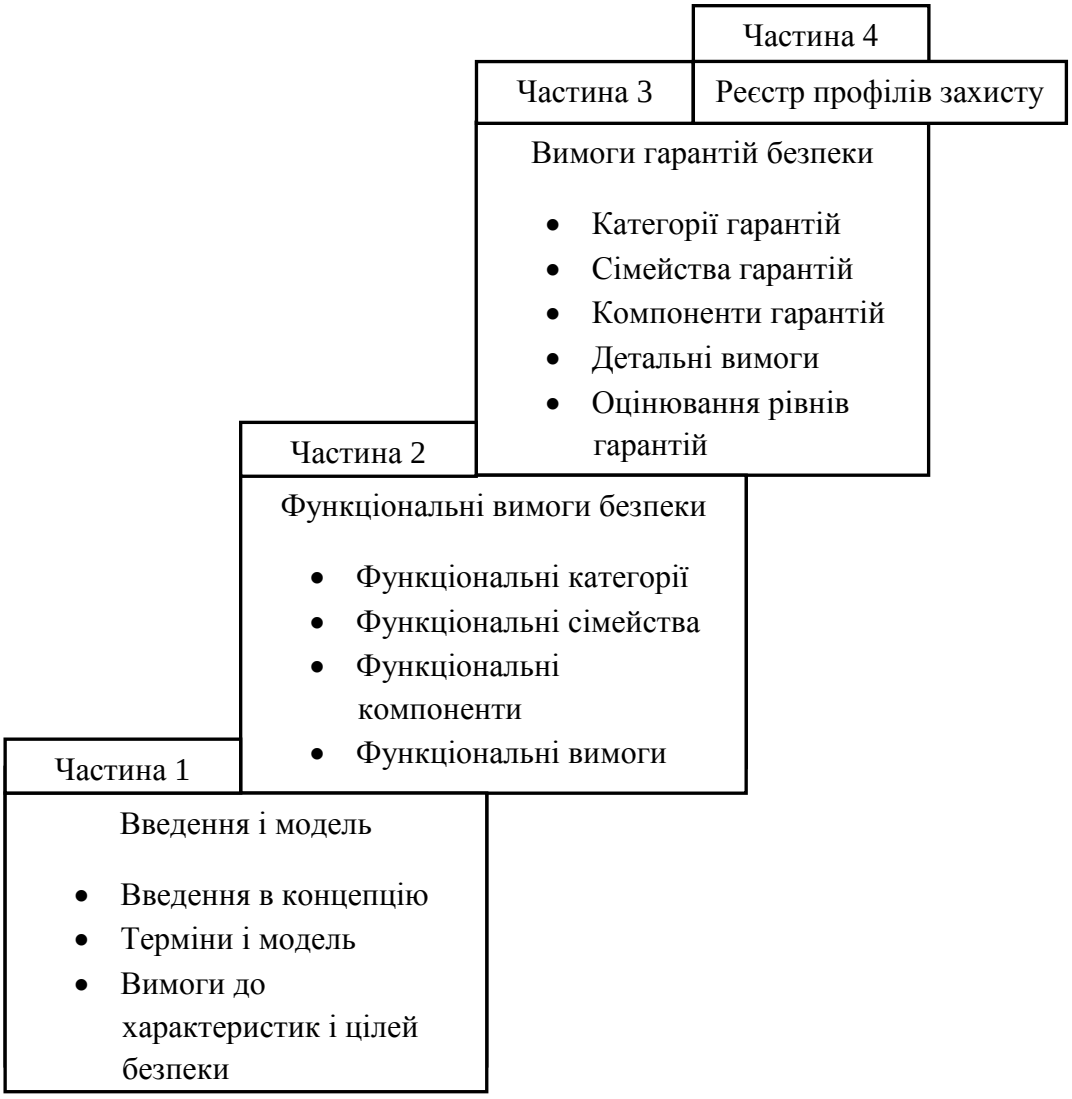


Рисунок 8.2 – Склад стандарту ISO/IEC 15408

«Загальні критерії» узагальнили зміст і досвід використання «Оранжевої книги», розвинули європейські та канадські критерії і втілили у реальні структури концепцію типових профілів захисту федеральних критерії в США. У «Загальних критеріях» наведена класифікація широкого набору вимог безпеки інформаційних технологій, визначено структури їхнього групування і принципи використання (рис. 8.3). Головні переваги «Загальних критеріїв» – повнота вимог безпеки та їхня систематизація, гнучкість у застосуванні і відкритість для подальшого розвитку.

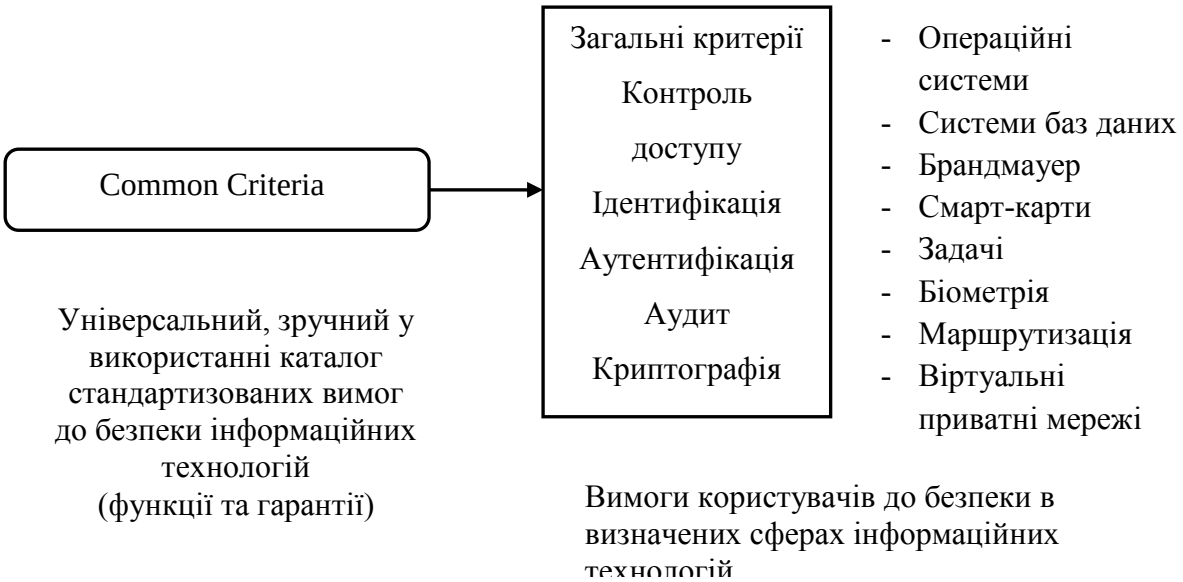


Рисунок 8.3 – Схема класифікації вимог ISO/IEC 15408

Використання методик цього стандарту дозволяє визначити для організації ті критерії, котрі можуть бути основою для вироблення правил і політики безпеки організації. Крім того, ці критерії дозволяють проводити більш повне порівняння результатів оцінення захисних властивостей інформаційних систем за допомогою загального переліку (набору) вимог, а також методів точних вимірів, які проводяться під час отримання оцінки безпеки. На основі цих вимог у процесі оцінювання рівня безпеки встановлюється рівень довіри.

Результати оцінювання безпеки дозволяють визначити для організації необхідний рівень безпеки її інформаційної системи.

Разом з тим у «Загальних критеріях» головну увагу приділено безпеці від несанкціонованого доступу. Модифікації або втрати доступу до інформації у результаті випадкових або навмисних дій і ряд інших аспектів інформаційної безпеки залишились нерозглянутими. Наприклад, оцінювання адміністративних засобів безпеки, оцінювання безпеки від побічних електромагнітних випромінювань, методики оцінювання різних засобів і мір безпеки, критерії для оцінювання криптографічних методів безпеки інформації. Тому необхідно доповнити даний підхід рядом своїх власних апробованих методик оцінювання важливих елементів безпеки. Доповнені таким чином «Загальні критерії оцінювання безпеки інформаційних технологій» можна використовувати як при визначенні вимог до продуктів і систем інформаційних технологій, правил і політики безпеки організації, так і при оцінюванні безпеки інформаційних технологій.

У результаті на практиці стає можливим реалізувати суттєві особливості, а саме:

– охопити увесь спектр інформаційних технологій і врахувати особливості кожної конкретної системи при визначенні вимог та правил безпеки. Пропоновані адаптовані «Загальні критерії оцінювання безпеки інформаційних технологій» призначені для оцінювання безпеки як систем інформаційних технологій розроблених для автоматизації у конкретній сфері призначення, так і окремих продуктів інформаційних технологій, які мають універсальне призначення. Такі «Загальні критерії оцінювання безпеки інформаційних технологій» можуть бути застосовані при оцінюванні безпеки і апаратних засобів, і програмного забезпечення інформаційних технологій;

– уникнути жорсткої класифікації інформаційних технологій за рівнем безпеки. Замість цього стає можливим використовувати сформульовані за ухваленими правилами типові набори вимог до різних видів інформаційних технологій, рівнів безпеки інформації та за іншими класифікаційними ознаками. Перелік типових вимог не регламентується – він формується за результатами проходження ухваленої процедури погодження та апробації. Для оптимального поєднання типових вимог з вимогами, які враховують особливості конкретної сфери застосування інформаційних технологій, використовуються два ключових поняття: профіль безпеки і завдання з безпеки.

Профіль безпеки являє собою функціонально повний, такий, що пройшов апробацію, стандартизований набір вимог, призначений для багаторазового використання.

Завдання з безпеки – це повна комбінація вимог, які є необхідними для створення та оцінювання інформаційної безпеки конкретної системи або продукту інформаційних технологій.

Таким чином, робота з аналізу вимог, які реалізуються на основі стандарту «Загальні критерії оцінювання безпеки інформаційних технологій», дозволяють грамотно задати вимоги до безпеки інформаційних технологій. Результати роботи можуть також використовуватися для порівняльного аналізу різних систем і продуктів інформаційних технологій. В цілому же наводиться розвиток системи структурованих вимог для вибору механізмів забезпечення безпеки при проектуванні і розробці інформаційних технологій:

- пропонувати детальний і структурований перелік вимог для механізмів безпеки, заходів і засобів забезпечення їхньої реалізації. Запропоновані адаптовані «Загальні критерії оцінювання безпеки інформаційних технологій» мають дві категорії вимог: функціональні та вимоги гарантованості. Перші описують функції, які необхідно реалізувати в інформаційних технологіях для забезпечення їхньої безпеки. Другі визначають заходи та засоби, які повинні бути використані у процесі створення інформаційних технологій для повної впевненості у

правильності реалізації механізмів безпеки та в їхній ефективності. Усі вимоги «Загальних критеріїв оцінювання безпеки інформаційних технологій» розбиваються за класами, компонентами і елементами з визначенням залежності одних компонентів від інших. Визначаються допустимі дії над компонентами, які можуть застосовуватися для конкретизації вимог безпеки, що задаються;

- охопити увесь життєвий цикл інформаційних технологій; починаючи від формування цілей і вимог забезпечення безпеки, розробки дієвих політик безпеки і закінчуючи поставкою та налагодженням інформаційних технологій на конкретному об'єкті;
- реалізувати можливість формування наборів вимог і правил безпеки за рівнями безпеки інформаційних технологій, які прирівнюються з іншими системами оцінювання. Запропоноване оцінювання безпеки досягається за рахунок можливості формування профілів безпеки, які відповідають набору вимог та визначають рівні безпеки інформаційних технологій у інших системах;
- гарантувати комплексність підходу до забезпечення безпеки інформаційних технологій.

Адаптація «Загальних критеріїв» дозволяє забезпечити безпеку інформаційних технологій на усіх етапах життєвого циклу інформаційної системи – від етапу аналізу вимог (на етапі формування-замислу інформаційної системи) до реалізації, експлуатації і супроводу системи. Тут передбачені такі рівні розгляду безпеки інформаційних технологій:

- безпека навколишнього середовища (закони, нормативні документи, організаційні заходи, фізичне оточення, що визначають умови застосування інформаційних технологій, а також існуючі та можливі загрози безпеці інформаційних технологій);
- цілі безпеки (наміри, які визначають направленість заходів з протидії виявленим загрозам і забезпечення безпеки);
- вимоги безпеки (отриманий у результаті аналізу цілей безпеки набір технічних вимог для механізмів безпеки і гарантованості їхньої реалізації, що забезпечує досягнення сформульованих цілей);
- специфікації безпеки (проектне подання механізмів безпеки, реалізація яких гарантує виконання вимог безпеки);
- розробка (реалізація механізмів безпеки зі специфікаціями) забезпечення комплексного оцінювання безпеки інформаційних технологій.

Адаптація «Загальних критеріїв» дозволяє оцінити безпеку інформаційних технологій у процесі їх розробки на найбільш важливих етапах. Передбачені такі стадії оцінювання:

- профілі безпеки;
- завдання з безпеки;
- реалізація механізмів безпеки.

У першому випадку встановлюється, що сформований профіль є повним, послідовним, технічно правильним і придатним для використання як типового для ухваленого класу інформаційних технологій. Використання оцінених, апробованих і стандартизованих профілів безпеки дає можливість запобігти витратам на розробку вимог з інформаційної безпеки при створенні систем і виробів та уникнути додаткових витрат на їхнє забезпечення.

Друга стадія покликана встановити, що завдання відповідає вимогам профілю безпеки і має повний, послідовний і технічно правильний набір вимог, необхідних для забезпечення безпеки конкретного об'єкта. Завдання з безпеки належить узгодити в організації і надалі є основним документом, відповідно до якого оцінюється безпека розроблюваної інформаційної системи.

Мета третьої стадії – встановити, що механізми безпеки забезпечують виконання усіх вимог, які викладені у завданні з безпеки, передбачити розширення вимог до безпеки інформаційних технологій.

Адаптація «Загальних критеріїв оцінювання безпеки інформаційних технологій» дозволяє запропонувати найбільш повний набір критеріїв у сфері безпеки інформаційних технологій, які задовольняють вимоги основних категорій і груп користувачів, а також розробників інформаційних систем.

Якщо даний підхід доповнити аналізом з організації режиму інформаційної безпеки організації, тоді отримуємо достатньо дієвий інструмент для оцінювання безпеки інформаційних технологій організацій і розробки ефективних політик безпеки.

Запитання для самоконтролю

1. Коли було затверджено Міжнародний стандарт ISO/IEC 15408 під назвою «Загальні критерії оцінювання безпеки інформаційних технологій»?
2. Який склад стандарту ISO/IEC 15408?
3. Що узагальнили «Загальні критерії»?
4. Що дозволяє визначити для організації використання методик цього стандарту?
5. Що дозволяють визначити для організації результати оцінок захисту?
4. Чому необхідно доповнити даний підхід рядом своїх власних апробованих методик оцінювання важливих елементів захисту?
5. Які суттєві особливості стає можливим реалізувати на практиці?
6. Що дозволяє забезпечити адаптація «Загальних критеріїв»?
7. Що дозволяє оцінити адаптація «Загальних критеріїв»?
8. Які передбачені стадії оцінювання безпеки інформаційних технологій у процесі їхньої розробки на найбільш важливих етапах?

9. Що встановлюється у першому випадку?

10. Що покликана встановити друга стадія?

11. Яка мета третьої стадії?

12. Що дозволяє адаптація «Загальних критеріїв оцінювання безпеки інформаційних технологій»?

13. Що є завданням з безпеки?

14. Що дозволяє робота з аналізу вимог, які реалізуються на основі стандарту «Загальні критерії оцінювання безпеки інформаційних технологій»?

15. Що дає використання оцінених, апробованих і стандартизованих профілів захисту?

16. Коли отримуємо достатньо дієвий інструмент для оцінювання безпеки інформаційних технологій організацій і розробки ефективних політик безпеки?

ГЛАВА 9
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

9.1 Основні поняття

До адміністративного рівня інформаційної безпеки відносять дії керівництва організації загального характеру.

Головна мета заходів адміністративного рівня – сформувати програму робіт у сфері інформаційної безпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ.

Основою програми є політика безпеки, що уособлює підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації повинно усвідомити необхідність підтримки режиму безпеки й виділити значні ресурси на впровадження цих заходів.

Термін «політика безпеки» є не зовсім точним перекладом англійського словосполучення «security policy», однак у цьому випадку калька краще відображає зміст цього поняття, ніж лінгвістично більш правильні «правила безпеки». Ми матимемо на увазі не окремі правила або їхні набори, а стратегію організації у сфері інформаційної безпеки. Для вироблення стратегії й провадження її в життя потрібні, безсумнівно, політичні рішення, прийняті на найвищому рівні.

Під політикою безпеки ми будемо розуміти сукупність документованих рішень, прийнятих керівництвом організації й спрямованих на захист інформації та асоційованих з нею ресурсів.

Таке трактування, звичайно, набагато ширше, ніж набір правил розмежування доступу (саме це означав термін «security policy» в «Оранжевій книзі», в побудованих на її основі нормативних документах інших країн).

ІС організації й пов’язані з нею інтереси суб’єктів – це складна система, для розгляду якої необхідно застосовувати об’єктно-орієнтований підхід і поняття рівня деталізації. Доцільно виділити, принаймні, три таких рівні, що ми вже робили в прикладі й зробимо ще раз далі.

Щоб розглядати ІС предметно, з використанням актуальних даних, варто скласти карту інформаційної системи. Ця карта, зрозуміло, повинна бути виготовлена в об’єктно-орієнтованому стилі, з можливістю варіювати не тільки рівень деталізації, але й видимі межі об’єктів. Технічним засобом складання, супроводу й візуалізації подібних карт може слугувати вільно розповсюджуваний каркас будь-якої системи керування.

9.2 Політика безпеки

Із практичної точки зору політику безпеки доцільно розглядати на трьох рівнях деталізації. До верхнього рівня можна віднести рішення, що

стосуються організації в цілому. Вони носять досить загальний характер й, як правило, виходять від керівництва організації. Зразковий список подібних рішень може містити в собі такі елементи:

- рішення сформувати або переглянути комплексну програму забезпечення інформаційної безпеки, призначення відповідальних за впровадження програми;
- формулювання цілей, які переслідує організація у сфері інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;
- забезпечення бази для дотримання законів і правил;
- формулювання адміністративних рішень з питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

Для політики верхнього рівня мета організації у сфері інформаційної безпеки формулюється в термінах цілісності, доступності й конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані може стояти зменшення числа втрат, ушкоджень або перекручувань даних. Для організації, що займається продажем комп'ютерної техніки, імовірно, важлива актуальність інформації про надавані послуги й ціни та її доступність максимальній кількості потенційних покупців. Керівництво режимного підприємства в першу чергу піклується про захист від несанкціонованого доступу, тобто про конфіденційність.

На верхній рівень виноситься керування захисними ресурсами й координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем і взаємодія з іншими організаціями, що забезпечують або контролюють режим безпеки.

Політика верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть усі комп'ютерні системи організації (або навіть більше, якщо політика регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів). Можлива, однак, і така ситуація, коли в сферу впливу входять лише найбільш важливі системи.

У політиці повинні бути визначені обов'язки посадових осіб з вироблення програми безпеки й впровадження її в життя. У цьому сенсі політика безпеки є основою підзвітності персоналу.

Політика верхнього рівня має справу з трьома аспектами законослухняності й виконавчої дисципліни. По-перше, організація повинна дотримуватися існуючих законів. По-друге, потрібно контролювати дії осіб, відповідальних за вироблення програми безпеки. Нарешті, необхідно забезпечити певний ступінь старанності персоналу, а для цього потрібно виробити систему заохочень і покарань.

Загалом кажучи, на верхній рівень варто виносити мінімум питань. Подібне винесення доцільно, коли воно обіцяє значну економію засобів або коли інакше вчинити просто неможливо.

Тобто необхідно внести в документ, що характеризує політику безпеки організації, такі розділи:

- вступний, що підтверджує занепокоєність вищого керівництва проблемами інформаційної безпеки;
- організаційний, який має опис підрозділів, комісій, груп і т. д., відповідальних за роботу у сфері інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні й інформаційні ресурси та необхідний рівень їхнього захисту;
- штатний, що характеризує заходи безпеки, які застосовуються до персоналу (опис посад з погляду інформаційної безпеки, організація навчання й перепідготовки персоналу, порядок реагування на порушення режиму безпеки й т. п.);
- розділ, що висвітлює питання фізичного захисту;
- керівний розділ, що описує підхід до керування комп'ютерами й комп'ютерними мережами;
- розділ, що описує правила розмежування доступу до виробничої інформації;
- розділ, що характеризує порядок розробки й супроводу систем;
- розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації;
- юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

До середнього рівня можна віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – ставлення до передових технологій (але, можливо, недостатньо перевірених), доступ в Internet (як поєднати можливість доступу до інформації з захистом від зовнішніх загроз), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення й т. д.

Політика середнього рівня повинна для кожного аспекту висвітлювати нижченаведені теми.

Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як ПЗ, що не було схвалено й/або закуплене на рівні організації.

Сфера застосування. Варто визначити, де, коли, як, стосовно кого й чому застосовується дана політика безпеки. Наприклад, чи стосується політика, пов'язана з використанням неофіційного програмного забезпечення, організацій-субпідрядників? Чи стосується вона співробітників, що користуються портативними й домашніми комп'ютерами й змушені переносити інформацію на виробничі машини?

Позиція організації з даного аспекту. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони, вироблення процедури прийому подібного ПЗ й т. п. Позицію можна сформулювати, у більш загальному вигляді, як набір цілей, які

переслідує організація в даному аспекті. Взагалі стиль документів, що визначають політику безпеки (як і їхній перелік), у різних організаціях може суттєво відрізнятися.

Ролі й обов'язки. В «політичний» документ необхідно внести інформацію про посадових осіб, відповідальних за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинно бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, варто знати, хто стежить за виконанням даного правила.

Законослухняність. Політика повинна містити загальний опис заборонених дій і покарань за них.

Точка контакту. Повинно бути відомо, куди варто звертатися за роз'ясненнями, допомогою й додатковою інформацією. Звичайно «точкою контакту» слугують певні посадові особи, а не конкретна людина, що займає в цей момент дану посаду.

Політика безпеки нижнього рівня стосується конкретних інформаційних сервісів. Вона містить у собі два аспекти – мету й правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута політика повинна визначатися більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна однаково регламентувати в рамках всієї організації. У той же час, ці речі настільки важливі для забезпечення режиму безпеки, що рішення, які їх стосуються, повинні прийматися на управлінському, а не на технічному рівні. Наведемо кілька прикладів питань, на які варто дати відповідь щодо політики безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваних сервісом;
- за яких умов можна читати й модифікувати дані;
- як організований вилучений доступ до сервісу.

При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності й конфіденційності, але не можна на цьому зупинятися. Її мета повинна бути більш конкретною. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити мету, щоб лише співробітникам відділу кадрів і бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку мета повинна зв'язувати між собою об'єкти сервісу й дії з ними.

Із цілей виводяться правила безпеки, що описують, хто, що й за яких умов може робити. Чим докладніші правила, чим більш формально вони викладені, тим простіше підтримувати їхнє виконання програмно-технічними засобами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, імовірно, їх доведеться часто переглядати. Керівництво повинно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не

виявляться надмірно зв’язані. Зазвичай найбільш формально висуваються права доступу до об’єктів через особливу важливість даного питання.

9.3 Програма безпеки

Після того, як сформульована політика безпеки, можна приступати до складання програми її реалізації та, безпосередньо, до реалізації.

Щоб зрозуміти й реалізувати яку-небудь програму, її потрібно структурувати по рівнях, звичайно, відповідно до структури організації. У найпростішому й найпоширенішому випадку досить двох рівнів – верхнього, або центрального, який охоплює всю організацію, і нижнього, або службового, який стосується окремих послуг або груп однорідних сервісів.

Програму верхнього рівня очолює особа, відповідальна за інформаційну безпеку організації. У цієї програми такі головні цілі:

- керування ризиками (оцінювання ризиків, вибір ефективних засобів захисту);
- координація діяльності у сфері інформаційної безпеки, поповнення й розподіл ресурсів;
- стратегічне планування;
- контроль діяльності у сфері інформаційної безпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення із забезпечення безпеки, оцінюються технологічні новинки. Інформаційні технології розвиваються дуже швидко, тому необхідно мати чітку політику відстеження й впровадження нових засобів.

Контроль діяльності у сфері безпеки має двосторонню спрямованість. По-перше, необхідно гарантувати, що дії організації не суперечать законам. При цьому варто підтримувати контакти із зовнішніми організаціями, що здійснюють контроль. По-друге, потрібно постійно відслідковувати стан безпеки всередині організації, реагувати на випадки порушень і доопрацьовувати захисні заходи з урахуванням змін, що відбуваються.

Варто підкреслити, що програма верхнього рівня повинна займати певне місце в діяльності організації, вона повинна офіційно прийматися й підтримуватися керівництвом, а також мати певний штат і бюджет.

Мета програми нижнього рівня – забезпечити надійний й економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які варто використовувати механізми захисту; закуповуються та встановлюються технічні засоби; виконується повсякденне адміністрування; відслідковується стан слабких місць і т. п. Звичайно за програму нижнього рівня відповідають адміністратори сервісів.

9.4 Синхронізація програми безпеки з життєвим циклом систем

Якщо синхронізувати програму безпеки нижнього рівня з життєвим циклом захищеного сервісу, можна домогтися більшого ефекту з меншими витратами. Програмісти знають, що додати нову можливість до вже готової системи на порядок складніше, ніж з нуля спроектувати й реалізувати її. Та ж умова виконується для інформаційної безпеки.

У життєвому циклі інформаційного сервісу можна виділити такі етапи.

Ініціація. На даному етапі виявляється необхідність у придбанні нового сервісу, документується його передбачуване призначення.

Закупівля. На даному етапі складаються специфікації, пророблюються варіанти придбання, виконується власне закупівля.

Установлення. Сервіс установлюється, конфігурується, тестується та вводиться в експлуатацію.

Експлуатація. На даному етапі сервіс не тільки працює й адмініструється, але й піддається модифікаціям.

Виведення з експлуатації. Відбувається перехід на новий сервіс.

Розглянемо дії, виконувані на кожному з етапів, більш докладно.

На етапі ініціації оформляється розуміння того, що необхідно придбати новий або значно модернізувати існуючий сервіс; визначається, які характеристики та яку функціональність він повинен мати; оцінюються фінансові й інші обмеження.

З погляду безпеки найважливішою дією тут є оцінювання критичності як самого сервісу, так і інформації, що з його допомогою буде оброблятися. Потрібно сформулювати відповіді на такі запитання:

- якого роду інформація призначається для обслуговування новим сервісом;
- які можливі наслідки порушення конфіденційності, цілісності та доступності цієї інформації;
- які загрози, стосовно яких сервіс та інформація будуть найбільш уразливі;
- чи є які-небудь особливості нового сервісу (наприклад, територіальна розосередженість компонентів), що вимагають прийняття спеціальних процедурних заходів;
- які характеристики персоналу, що відповідає за безпеку (кваліфікація, благонадійність);
- які законодавчі положення й внутрішні правила, яким повинен відповідати новий сервіс?

Результати оцінювання критичності є відправною точкою у складанні специфікацій. Крім того, вони визначають ту міру уваги, яку служба безпеки організації повинна приділяти новому сервісу на наступних етапах його життєвого циклу.

Етап закупівлі – один із найскладніших. Потрібно остаточно сформулювати вимоги до захисних засобів нового сервісу, до компанії, що

може претендувати на роль постачальника, і до кваліфікації, яку повинен мати персонал, що використовує або обслуговує закуплений продукт. Усі ці відомості оформляються у вигляді специфікації, куди входять не тільки апаратура й програми, але й документація, обслуговування, навчання персоналу. Зрозуміло, особлива увага повинна приділятися питанням сумісності нового сервісу з існуючою конфігурацією. Підкреслимо також, що нерідко засоби безпеки є необов'язковими компонентами комерційних продуктів, і потрібно простежити, щоб відповідні пункти не випали зі специфікації.

Коли продукт закуплений, його необхідно встановити. Незважаючи на можливу простоту, встановлення є дуже відповідальною справою. По-перше, новий продукт треба сконфігурувати. Як правило, комерційні продукти постачаються з вимкненими засобами безпеки; їх необхідно ввімкнути й належним чином налаштувати. Для великої організації, де багато користувачів і даних, початкове налаштування може стати досить трудомісткою та відповідальною справою.

По-друге, новий сервіс має потребу в процедурних регуляторах. Варто подбати про чистоту й охорону приміщення, про документи, що регламентують використання сервісу, про підготовку планів на випадок екстрених ситуацій, про організацію навчання користувачів і т. п.

Після прийняття перерахованих заходів необхідно провести тестування. Його повнота й комплексність можуть бути гарантією безпеки експлуатації в штатному режимі.

Період експлуатації – найтриваліший та найскладніший. Із психологічної точки зору найбільшу небезпеку в цей час становлять незначні зміни в конфігурації сервісу, у поводженні користувачів й адміністраторів. Якщо безпеку не підтримувати, вона слабшає. Користувачі не настільки чітко виконують посадові інструкції, адміністратори менш ретельно аналізують реєстраційну інформацію. То один, то інший користувач одержує додаткові привілеї. Здається, що в сутності нічого не змінилося; насправді ж від колишньої безпеки не залишилося й сліду.

Для боротьби з ефектом повільних змін доводиться долучатися до періодичних перевірок сервісу безпеки. Зрозуміло, після значних модифікацій подібні перевірки є обов'язковими.

При виведенні з експлуатації апаратура продається, утилізується або викидається. Тільки в специфічних випадках необхідно піклуватися про фізичне руйнування апаратних компонентів, що зберігають конфіденційну інформацію. Програми, імовірно, просто стираються, якщо інше не передбачено ліцензійною угодою.

При виведенні даних з експлуатації їх звичайно переносять на іншу систему, архівують, викидають або знищують. Якщо архівування робиться з наміром згодом прочитати дані в іншому місці, варто подбати про апаратно-програмну сумісність засобів читання й запису. Інформаційні

технології розвиваються дуже швидко, і через кілька років пристроїв, здатних прочитати старий носій, може просто не виявитися. Якщо дані архівуються в зашифрованому вигляді, необхідно зберегти ключ і засоби розшифрування. Під час архівування й зберігання архівної інформації не можна забувати про підтримку конфіденційності даних.

Запитання для самоконтролю

1. Адміністративний рівень ІБ. Основні поняття.
2. Яка головна мета заходів адміністративного рівня?
3. Політика безпеки.
4. Які цілі політики безпеки верхнього рівня?
5. Що характеризує політику безпеки організації?
6. Що входить у число етапів життєвого циклу інформаційного сервісу?
7. На основі чого будується політика безпеки?
8. Які теми висвітлює політика безпеки середнього рівня?
9. Що стосується політики безпеки нижнього рівня?
10. Програма безпеки.
11. Програма верхнього рівня. Цілі програми.
12. Синхронізація програми безпеки з життєвим циклом систем.
13. Основні етапи життєвого циклу інформаційного сервісу.
14. Якого роду інформація призначається для обслуговування новим сервісом?
15. Які можливі наслідки порушення конфіденційності, цілісності та доступності інформації?
16. Які особливості нового сервісу вимагають прийняття спеціальних процедурних заходів, чи існують вони?
17. Яким законодавчим положенням і внутрішнім правилам повинен відповідати новий сервіс?
18. Програма нижнього рівня. Цілі програми.
19. Програма середнього рівня. Цілі програми.
20. Які теми висвітлює політика безпеки верхнього рівня?

ГЛАВА 10
АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЇ

10.1 Підходи до аналізу ризиків

Перед початком будь-якої діяльності, пов'язаної з аналізом ризиків, організація повинна мати стратегію щодо його здійснення, а її складові частини (методи, технології тощо) мусять бути відображені в методиці безпеки інформаційних технологій. Засоби і критерії для вибору методу аналізу ризиків потрібно погодити з вимогами організації. Стратегія аналізу ризиків має гарантувати, що обраний підхід відповідає оточенню і що він зосереджує зусилля захисту там, де вони необхідні.

Ефективне використання або звернення до детального аналізу всіх систем не є ефективними без урахування серйозності ризиків. Підхід, який забезпечує рівновагу між цими екстремальними показниками, передбачає аналіз високих рівнів посадовцями для встановлення потреб в захисті системи інформаційних технологій, а потім проведення докладного дослідження з урахуванням цих потреб. Потреби в захисті будь-якої організації будуть залежати від її розміру, виду ділової активності, який вона здійснює, її оточення і мікрополітики.

У деяких ситуаціях організація вирішує питання відносно застосування засобів захисту або призупинення їхньої дії на даному етапі. Таке рішення потрібно приймати тільки після того, як організація ретельно здійснить всі аналізи. Якщо таке рішення прийнято, адміністрація повинна знати всі потенціальні ризики, несприятливі ситуації та ймовірність виникнення небажаного інциденту. Без цих відомостей організація може ненавмисно порушити закони або правила і може довести свою ділову активність до потенційного збитку. Рішення про пасивність або відкладання застосування засобів захисту повинні бути прийняті тільки після того, як зроблено докладний розгляд цих та інших можливих несприятливих наслідків.

Між можливістю бездіяльності та визнанням множини ризиків невідомої величини і серйозності можна виділити чотири основних варіанти методики аналізу ризику:

- використання однакового основного підходу до всіх систем незалежно від ризиків, що стоять перед системами, і прийняття того, що рівень захисту ніколи не може бути відповідним;
- використання неформального підходу для аналізу кожного;
- використання змішаного підходу для застосування початкового аналізу ризику високого рівня, щоб визначити системи інформаційних технологій з високим рівнем ризику та такі, що є критичними для ділової активності, з детальним аналізом ризику для цих систем і застосуванням основного підходу до всіх інших систем.

Ці різні можливості щодо напрямків ризиків безпеки обговорюються з подальшими рекомендаціями щодо переваг кожного підходу.

Якщо організація вирішує нічого не робити для захисту чи вкласти кошти в реалізацію заходів захисту, адміністрація повинна знати можливі наслідки такого рішення. Така пасивність має безліч недоліків. Якщо організація впевнена у безпечності своїх систем, вона може тривалий час бути відкритою для серйозних впливів. Організація може бути в конфлікті з законами та розпорядженнями, а її репутація може постраждати, якщо цей конфлікт спричинить порушення у захисті і це покаже, що не було ніякої попереджувальної роботи. Якщо організація мало турбується про захист, не має інших робочих систем перевірки, тоді це може бути життєвою стратегією. Однак така організація не знає, наскільки добрий чи поганий поточний стан безпеки, і для більшості організацій це навряд чи буде прийнятним рішенням.

Перший підхід полягає в тому, що організація за основу безпеки всіх інформаційних технологій систем вибирає стандартні засоби захисту.

Мета основного захисту полягає в тому, щоб установити мінімальну кількість засобів захисту і захистити всі чи деякі системи організації. Використовуючи цей підхід, можна застосувати основний захист у всій організації, і, як відзначено вище, додатково використовувати докладний аналіз ризику для захисту систем з високими рівнями ризику.

Відповідний основний захист можна забезпечити, використавши засоби захисту, які застосовуються для системи інформаційних технологій від найзагальніших загроз. Рівень основного захисту може бути відкоригований відповідно до потреб організації. Докладне оцінювання загроз, вразливостей і ризиків не потрібне. Усе, що треба зробити для здійснення основного захисту, – вибрати ті засоби захисту, що стосуються розглянутої системи інформаційних технологій. Після визначення основного засобу захисту у кожному місці можуть бути визначені засоби захисту, які потрібно конкретно використовувати.

Організація також може, звичайно, створити власну основу, встановлюючи відповідність із типовим оточенням і з діловими цілями.

Переваги використання цього підходу:

- мінімальні витрати для детального аналізу ризику і керування під час забезпечення засобами захисту, оскільки витрачається менше часу і зусиль на вибір засобів захисту;

- основні засоби захисту є рентабельні, ті ж самі або подібні основні засоби захисту можуть бути легко пристосовані до багатьох систем, якщо багато систем організацій працюють у спільному оточенні і якщо потреби захисту порівнянні.

Може виникнути ускладнення в керуванні змінами, що залежить від захисту. Наприклад, якщо система модернізована, можуть виникнути труднощі у визначенні чи є первинні основні засоби захисту, як і раніше, ефективними.

Недоліки цього підходу: якщо базовий рівень захисту визначено як дуже високий, то це може або занадто дорого коштувати, або не забезпечувати необхідного захисту деяких систем; а якщо основний рівень дуже низький, то може виявитися, що для деяких систем немає достатнього рівня захисту.

Якщо всі системи інформаційних технологій організації мають низький рівень необхідних вимог захисту, тоді це найрентабельніша стратегія. У цьому випадку основа повинна бути відповідною рівню захисту, необхідному більшості систем інформаційних технологій. Більшість організацій завжди повинна буде вибирати деяку мінімальну кількість стандартів, щоб захистити секретні дані й узгодити з законами та розпорядженнями, наприклад, із законом захисту даних. Однак там, де системи організації відрізняються в діловій активності, розмірі і складності, цей підхід нелогічний і нерентабельно застосовувати загальний стандарт до всіх систем.

Другий підхід полягає в неформальному, прагматичному аналізі ризику всіх систем. Неформальний підхід базується не на структурованих методах, а на обізнаності і досвіді осіб. Якщо експертизу захисту не можна провести своїми силами, то залучають зовнішніх консультантів.

Перевага цього підходу – ефективність щодо вартості і часу. Немає потреби навчати виконувати неформальний аналіз і його проводять значно швидше, ніж детальний аналіз ризику. Отже, цей підхід ефективний з точки зору вартості та найкраще підходить для малих організацій.

Є, однак, ряд недоліків такого підходу:

- відсутність структурованого підходу збільшує імовірність неврахування деяких ризиків і сфер їхнього впливу;
- існує лише незначне мотивування вибору засобів захисту, отже, складно визначити витрати на них;
- може виникнути складність у керуванні безпекою під час змін без частого аналізу;
- відсутність формального підходу або вичерпного переліку ризиків збільшує імовірність пропустити деякі важливі деталі;
- підтвердження застосування засобів захисту від ризиків у цьому випадку ускладнюється;
- особи, що мають незначний досвід в аналізі ризиків, можуть мати мало інструкцій, які б допомогли їм у виконанні завдань;
- частина пропозицій у минулому керувалася уразливістю, тобто реалізовані засоби захисту ґрунтувалися на певній вразливості, без врахування можливості використання загрозою цієї вразливості, тобто без реальної потреби в засобах захисту;
- оскільки підхід є неформальним, результатам властива суб’єктивність поглядів і упередженість консультанта;
- виникають проблеми, якщо особа, що проводить неформальний аналіз ризику, йде з організації.

Ґрунтуючись на вищевикладених недоліках, цей підхід не вважається ефективним щодо виконання аналізу ризику для багатьох організацій.

Третій підхід полягає в докладному оцінюванні аналізу ризику всіх систем інформаційних технологій організації. Докладний аналіз ризику охоплює визначання та оцінювання активів, а також оцінювання рівнів загроз щодо інформації та її уразливості. Цю інформацію використовують для визначення ризиків. Виконання цього аналізу ризику сприяє ідентифікації, вибору і впровадженню засобів захисту, скоригованих ідентифікованими ризиками стосовно інформації, а також знижує ці ризики до прийнятного визначеного рівня керування. Докладний аналіз ризику може бути ресурсомістким процесом і тому потребує чіткого визначення меж і постійної уваги адміністрації.

Переваги цього підходу:

- визначення рівня захисту відповідно до вимог безпеки для кожної системи;
- додаткова інформація, отримана з детального аналізу ризику, сприяє керуванню змінами, пов’язаними із захистом;
- висока імовірність того, що для всіх систем визначені відповідні засоби захисту.

Недоліки цього підходу:

- він потребує багато часу, зусиль і спеціальних знань для одержання результатів;
- є ймовірність, що вимоги захисту небезпечної системи будуть враховані надто пізно;
- усі системи інформаційних технологій треба розглядати докладно, і буде потрібно багато часу, щоб завершити аналіз.

Четвертий підхід насамперед ідентифікує ті системи, які мають підвищений ризик або є критичними щодо ділової активності, і передбачає високорівневий аналіз ризику. Ґрунтуючись на отриманих при цьому результатах, системи поділяються на ті, які потребують докладного аналізу ризику для досягнення відповідного захисту, і ті, для яких є достатнім базовий захист.

Цей підхід – комбінація кращих положень описаних вище підходів. Таким чином він забезпечує рівновагу та мінімізацію часу і зусиль, що їх витрачають на ідентифікацію засобів захисту, щоб гарантувати відповідну захищеність усіх систем.

Додаткові переваги цього підходу:

- поєднання на початку швидкості і простоти підвищує ймовірність приймання програми аналізу ризиків;
- можливість швидко отримати уявлення про стратегію програми захисту в організації, що може сприяти покращенню планування;
- є можливість побудови безпосередньої стратегічної картини програми безпеки організації, яку можна використовувати під час планування;

- ресурси і кошти можуть бути спрямовані на одержання максимальної вигоди, і системи з імовірно найбільшою потребою в захисті можуть бути враховані на ранніх стадіях;

- наступні дії будуть успішнішими.

Недоліки цього підходу: якщо високорівневий аналіз ризику дає неточні результати, то деяким системам, для яких необхідний докладний аналіз ризику, не буде приділено належної уваги. Звичайно, така ситуація малоймовірна, якщо результати аналізу ризику відповідно перевірені, але в будь-якому випадку такі системи все ж повинні додатково підтримуватися базовими засобами захисту.

У більшості випадків цей підхід є найрентабельнішим рішенням, і його рекомендовано до застосування більшістю організацій.

10.2 Аналіз активів організацій

Докладний аналіз ризику для системи інформаційних технологій містить визначення структури ризиків і оцінку їхніх величин. Необхідність у докладному аналізі ризику може бути визначена без зайвих витрат часу і коштів, коли огляди високого рівня проводять для всіх систем, які супроводжуються докладним аналізом ризику тільки високого рівня чи вирішальних систем.

Аналізують ризик визначенням потенційних несприятливих уражень, небажаних подій та ймовірності їхньої появи. Небажані події можуть впливати на ділову активність службовців чи на будь-який цінний об’єкт організації. Несприятливе ураження в результаті небажаного випадку – складова частина можливих збитків, пов’язаних зі значенням активів і їхніх ризиків. Імовірність появи уражень залежить від того, наскільки привабливі активи для потенційного нападника, від імовірності появи загроз і легкості, з якою уразливість можна використати. Привабливими активами організації можуть бути:

- програмне забезпечення, в тому числі прикладне (наприклад, програми обробки тексту, програми, розроблені для спеціальних цілей);
- апаратура зв’язку (наприклад, телефони, мідний кабель, скловолокно);
- програмно-апаратне забезпечення (наприклад, гнучкі диски, постійна пам’ять на компакт-диску (CD ROM), програмовані ROM);
- документи (наприклад, контракти);
- виготовлені товари;
- служби (наприклад, інформаційні служби, обчислювальні ресурси);
- оточення;
- персонал;
- імідж організації.

Всі активи у встановлених межах огляду повинні бути зафіксовані, і навпаки, будь-які активи, що їх вилучають з огляду з будь-якої причини,

повинні бути вміщені в інший огляд для впевненості, що їх не забудуть і не пропустять.

Наявність відповідного керування активами важлива для забезпечення успіху організації і є головною рисою всіх рівнів керування. До активів організації належать:

- фізичні об'єкти (апаратне забезпечення, засоби зв'язку, будівлі);
- інформація або дані (документи, бази даних);
- програмне забезпечення;
- здатність виробляти деяку продукцію чи надавати послуги;
- людські ресурси;
- нематеріальна власність (символіка).

Більшість із цих активів має потребу в захисті. У випадку, коли активи не мають належного рівня захищеності, необхідно застосовувати до них механізми оцінювання ризиків.

Якщо йдеться про перспективність програми безпеки організації, має сенс забезпечувати захист і здійснювати його подальшу підтримку. У більшості випадків процес ідентифікації активів і визначання їхніх розмірів можна виконати на досить високому рівні і без дорогого, детального і тривалого аналізу. Рівень деталізації для аналізу визначають значеннями часу та вартістю аналізу стосовно цінності активів. У будь-якому випадку рівень деталізації визначають, виходячи з цілей захисту. Зокрема, ці підходи можна застосовувати до груп активів.

Розглядають такі характеристики активів, як їхня цінність або критичність і різноманітність застосовуваних засобів захисту. Необхідність застосування засобів захисту до активів визначають також їхньою вразливістю до впливу специфічних загроз. Якщо ці аспекти очевидні для власника активів, їх треба зафіксувати на початкових стадіях. Оточення і мікрополітика, у яких діє організація, можуть впливати на активи та їхні характеристики. Наприклад, мікрополітика організації може розглядати як дуже важливе завдання захисту особистої інформації. У діяльності міжнародних організацій та їхніх систем інформаційних технологій вагому роль відіграють оточення і мікрополітика.

Активи є об'єктами для багатьох видів загроз. Різноманітні загрози чи їхній прояв у різних місцях можуть постійно завдавати великої шкоди. Якщо шкода, заподіяна загрозою, є постійною, то можна використовувати універсальний, визначений підхід. Однак якщо обсяги заподіяної шкоди змінюються в широких межах, необхідно використовувати конкретний підхід, що відповідає локалізації загрози.

Вихідні дані для оцінювання загрози треба отримувати від власників чи користувачів, від фахівців із планування і фахівців з інформаційних технологій, від фахівців, відповідальних за захист в організації. Перелік можливих загроз може виявитися корисним під час оцінювання загрози. Приблизний перелік наведено нижче.

У разі використання переліків загроз чи більш ранніх оцінювань загроз потрібно знати, що загрози постійно модифікуються, особливо якщо ділове оточення чи інформаційні технології змінюються. Наприклад, сьогоднішні віруси значно складніші ніж ті, що були декілька років тому. Цікаво, що реалізація таких засобів захисту, як перевірка на наявність вірусу майже завжди веде до розробки нових вірусів, що мають імунітет до поточних засобів захисту. Після визначення джерела загрози (хто і що викликало загрозу), її спрямованості (тобто на які елементи системи може вплинути загроза) необхідно визначити імовірність виникнення загрози. У цьому випадку потрібно брати до уваги:

- частоту загроз (як часто вони можуть виникати), спираючись на довідково-статистичні дослідження та інше, якщо статистичні дослідження існують;
- мотивацію, усвідомлені можливості і здатності, ресурси, доступні потенційним нападникам, і привабливі моменти та вразливості активів системи інформаційних технологій для потенційного нападника і навмисних джерел загрози;
- такі географічні чинники, як близькість до хімічних чи нафтових заводів, можливість появи критичних метеорологічних умов, і чинники, що можуть впливати на людські помилки і несправність устаткування, випадкові джерела загрози.

Залежно від ступеня точності може виникнути необхідність розбивати активи на складові та встановлювати зв’язки загроз із складовими. Наприклад, у фізичних активах можуть спочатку розглядати «центральні сервери даних», а коли визначено, що ці сервери перебувають у різних місцях, то розглядають окремо «центральний сервер даних 1» і «центральний сервер даних 2», тому що можуть бути дещо різні загрози і з різними впливами. Так само програмні активи можна спочатку розцінювати як «прикладне програмне забезпечення», а пізніше розбити на кілька видів «прикладного програмного забезпечення». Прикладом стосовно активів даних може слугувати початкове визначення як «кримінального досьє», а пізніше поділ на «текст кримінального досьє» і «зараження кримінального досьє».

У разі завершення оцінювання загроз буде отримано перелік ідентифікованих загроз, активів чи груп активів, на які загрози можуть впливати, і оцінок ймовірностей появи загроз у градації «високо», «середньо» чи «низько».

10.3 Побудова моделей загроз

Необхідно здійснити аналіз об’єктів захисту, ситуаційний план умов функціонування організації, оцінити ймовірність прояву загроз та очікувану шкоду від їхньої реалізації, підготувати дані для побудови окремої моделі загроз.

Обстеження має бути проведено комісією, склад якої визначається відповідальною за технічний захист інформації особою, і затверджується наказом керівника організації.

У ході обстеження необхідно:

- провести аналіз умов функціонування організації, її розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;
- дослідити засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;
- визначення схеми і системи життєзабезпечення організації (електроживлення, заземлення, пожежної та охоронної сигналізації тощо), а також інженерних комунікацій та металоконструкцій;
- дослідити інформаційні потоки та технологічні процеси обробки інформації;
- визначити наявність і технічний стан засобів забезпечення технічного захисту інформації;
- перевірити наявність в організації нормативних документів, які забезпечують функціонування системи захисту інформації з обмеженим доступом, організацію проектування будівельних робіт з урахуванням вимог технічного захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційну діяльність;
- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, проводів тощо;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтажу;
- визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів технічного захисту інформації.

Матеріали обстеження необхідно використовувати під час розробки окремої моделі загроз, яка має містити:

- генеральний та ситуаційний плани організації, схеми розташування засобів і систем забезпечення інформаційної діяльності, а також інженерних комунікацій, які виходять за межі контрольованої території;
- схему та опис каналів витоку інформації, каналів спеціального впливу і шляхи несанкціонованого доступу до інформації з обмеженим доступом;
- оцінку шкоди, яка передбачається від реалізації загроз.

Розглянемо приклад, коли джерелами загроз можуть бути навмисні або ненавмисні дії юридичних і фізичних осіб. Загрози можуть здійснюватися:

1. Технічними каналами, що охоплюють канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали, а саме:

- звичайними електромагнітними випромінюваннями і наводками (електромагнітні випромінювання, що утворюються під час роботи засобів забезпечення інформаційної діяльності під впливом електричних і магнітних полів на випадкові антени у процесі акусто-електричних

перетворень, під час виконання адитивної високочастотної генерації та паразитної модуляції шляхом взаємного впливу кіл технічних засобів, призначених і не призначених для обробки інформації з обмеженим доступом, і кіл електроживлення, електроосвітлення, сигналізації та управління, під час хибних комутацій і несанкціонованих дій користувачів);

- акустичними, лазерно-акустичними каналами (випромінювання звукового та ультразвукового діапазонів частот);
- оптичними каналами (електромагнітні випромінювання інфрачервоного, видимого та ультрафіолетового діапазонів частот);
- радіо-, радіотехнічними каналами (електромагнітні випромінювання в діапазоні радіочастот);
- хімічними каналами (хімічні речовини різної природи, що використовуються як сировина, утворюються в нових технологічних процесах, під час розробки нових матеріалів, проведення випробувань спеціальної техніки та виробів і містяться у навколишньому середовищі);
- іншими каналами (радіаційними, магнітометричними тощо);

2. Каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

3. Несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування підкладних пристроїв чи програм та вкорінення вірусів (рис. 10.1).

В деяких випадках людина може розглядатися як носій інформації. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або змін фізичних властивостей носія.

Опис загроз і схематичне подання шляхів їхнього здійснення становлять окрему модель загроз. При аналізі загроз використовуються три терміни: загрози, вразливі місця і захист інформації.

Загрози з'являються тому, що існують системи або процеси, а не тому, що є якісь конкретні їхні недоліки. Так загроза пожежі існує для всіх приміщень незалежно від обсягу проведених на них протипожежних заходів. Загрози безпеки інформаційній системі можуть бути пов'язані з працівником (порушником), об'єктом (несправне обладнання або програмне забезпечення) або подією (пожежа, землетрус, зсув тощо).

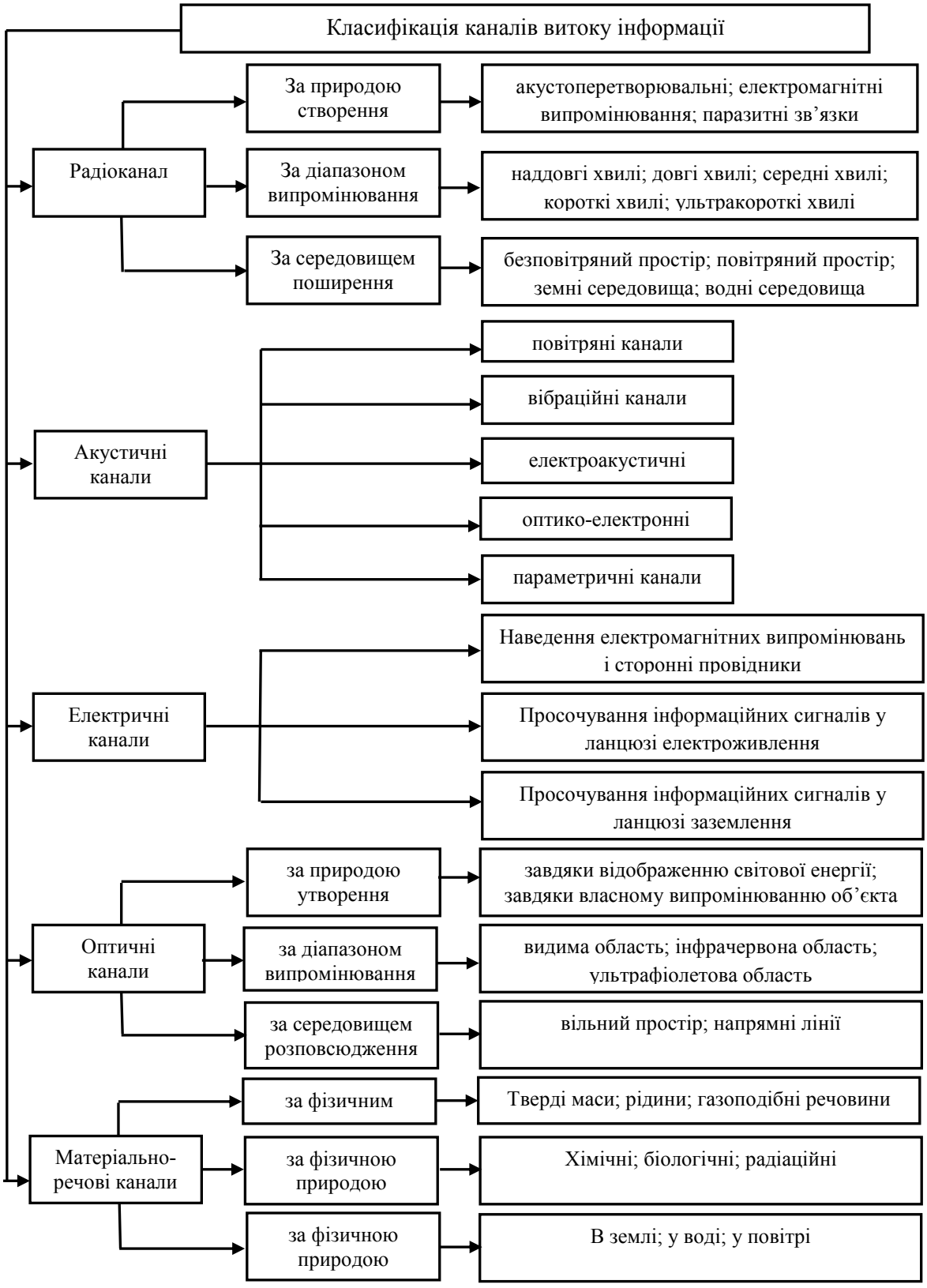


Рисунок 10.1 – Канали витоку інформації

На рис. 10.2 наведено варіант структурованої бази потенційних загроз для інформації, яка базується на наведених вище обґрунтуваннях.

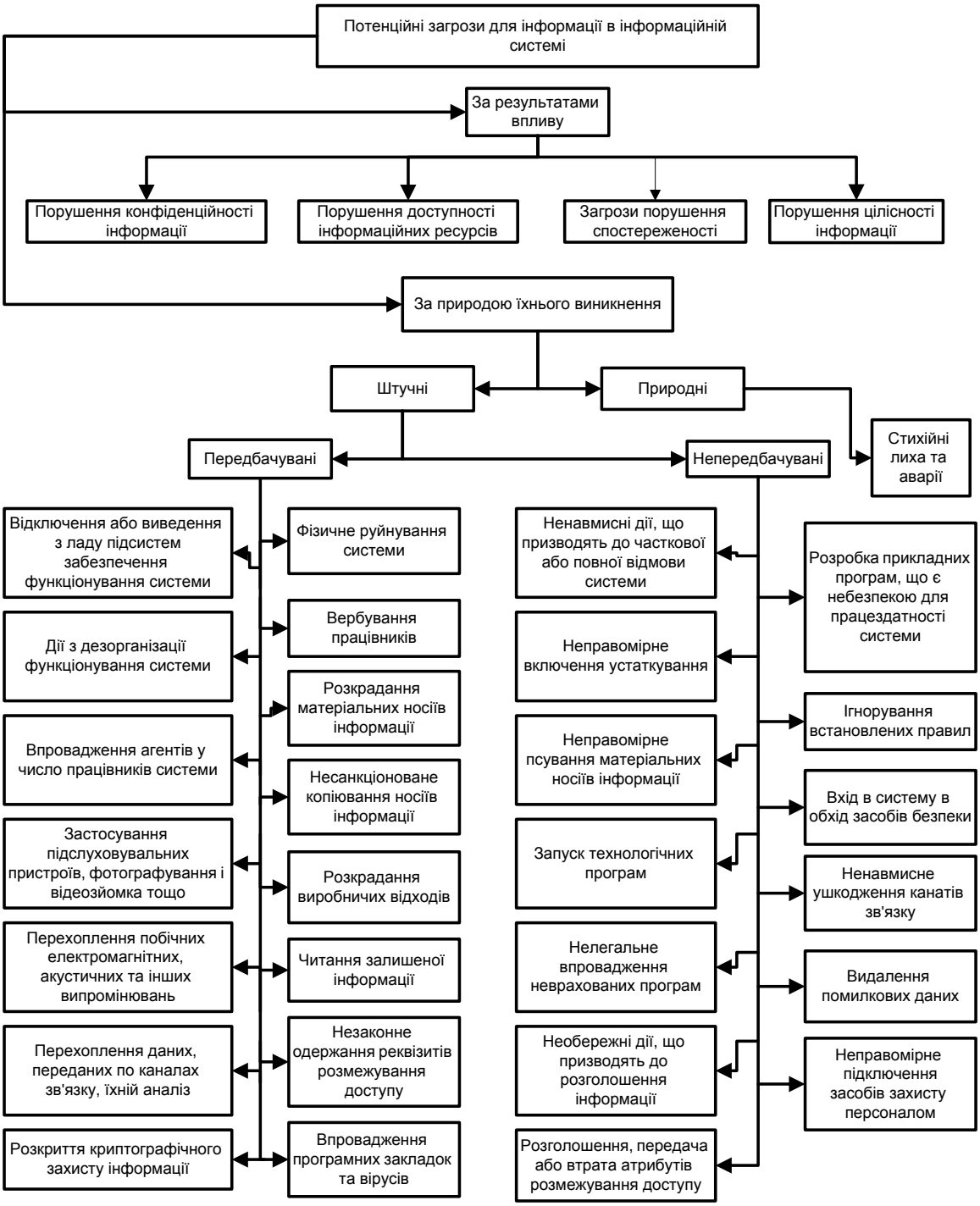


Рисунок 10.2 – Структурована база потенційних загроз для інформації в інформаційній системі

Для виділення типових уразливих місць в інформаційних системах можна скористатися описом протоколів обміну на основі еталонної моделі взаємозв’язку відкритих систем у вигляді ієрархії взаємодії прикладних процесів, що складається з семи рівнів:

- фізичного – керування фізичним каналом;
- канального – керування інформаційним каналом;
- мережевого – керування мережею;
- транспортного – керування передачею;
- сеансового – керування сеансом;
- представницького – керування представленням;
- прикладного – програми користувачів.

У цьому зв’язку можна виділити такі напрямки впливів:
- крадіжка цифрових носіїв;
- крадіжка результатів видачі (документів);
- зловмисні дії користувача програми;
- несанкціонований віддалений доступ;
- помилки в роботі користувачів чи програмно-технічного засобу;
- використання ліній зв’язку не за призначенням (перехоплення);
- неправильна робота ліній зв’язку (підробка).

Підходи до виявлення загроз

Різні підходи у виявленні загроз безпеці інформації в інформаційних системах наведено в табл. 10.1 з точки зору еталонної моделі взаємозв’язку відкритих систем.

Таблиця 10.1 – Різні підходи до виявлення загроз безпеці інформації в інформаційних системах з точки зору еталонної моделі взаємозв’язку відкритих систем

Загрози безпеки інформації	Рівні еталонної моделі взаємозв’язку відкритих систем						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Землетруси	+	+	+	+	+	+	+
Пожежі	+	+	+	+	+	+	+
Урагани	+	+	+	+	+	+	+
Електромагнітні бурі	+	+	+	+	+	+	+
Радіозаглушувальні лінії зв’язку	+	+					
Віруси					+	+	+
Спеціальні програмно-технічні впливи			+		+	+	+
Вбудовані дефекти			+				
Руйнування	+	+	+	+	+	+	+
Підробка			+				+
Розсекречування						+	+
Дешифрування		+				+	+
Декодування						+	+
Перехоплення інформації		+	+	+	+	+	+
Крадіжка інформації і її носіїв							

Продовження таблиці 10.1

Втрата інформації			+	+			+
Неправомірні дії щодо інформації					+	+	+
Загрози безпеки інформації	Рівні еталонної моделі взаємозв'язку відкритих систем						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Помилка в роботі							**+**
Затримка інформації	+	+	+	+	+		
Інформаційне заглушування						+	+
Порушення доступу законних користувачів						+	+
Побічні електромагнітні випромінювання і наведення	**+**	+				+	

Користуючись цією таблицею, можна побудувати модель загроз для кожної конкретної організації.

Як порушник розглядається особа, яка може одержати доступ до інформації з внесеними до складу інформаційної системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами інформаційної системи. Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень містить функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з інформаційною системою – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску цих програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням інформаційної системи, тобто впливом на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;
- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів інформаційної системи, аж до внесення до складу інформаційної системи власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про інформаційну систему і комплекс засобів захисту.

У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, що є

адекватною реальному порушнику для певної інформаційної системи. При розробці моделі порушника визначається:

- припущення про категорії осіб, до яких може належати порушник;
- припущення про кваліфікацію порушника і його технічну оснащеність (про використані для здійснення порушення методи і засоби);
- припущення про мотиви дій порушника (цілі, які переслідує порушник);
- обмеження та припущення про характер можливих дій порушників.

Стосовно інформаційної системи порушники можуть бути внутрішніми (з числа персоналу системи):

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби;
- співробітники підрозділу розробки і супроводу програмного забезпечення (прикладні та системні програмісти);
- технічний персонал, що обслуговує приміщення (прибиральники, електрики, сантехніки та інші працівники, що мають доступ у приміщення, де розташована автоматизована система);
- керівники різних рівнів посадової ієрархії, або зовнішні (сторонні особи):
- відвідувачі (запрошені з будь-якого приводу);
- представники організацій, що взаємодіють з питань забезпечення життєдіяльності установи (енергопостачання, водопостачання, теплопостачання);
- представники організацій-конкурентів або особи, що діють за їхнім завданням;
- особи, що випадково або навмисно порушили пропускний режим (без мети порушення безпеки інформаційної системи);
- будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви порушень: безвідповідальність, самоствердження, корисливий інтерес.

Усіх порушників можна класифікувати таким чином.

1. За рівнем знань про інформаційну систему:

- знає функціональні особливості інформаційної системи, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;
- має високий рівень знань і досвід роботи з технічними засобами системи та їхнього обслуговування;
- має високий рівень знань у галузі програмування, проектування та експлуатації інформаційних систем;
- знає структуру, функції та механізм дії засобів захисту, їхні сильні і слабкі сторони.

2. За рівнем можливостей (використаним методом і засобом):

- застосовуючи агентурні методи оволодіння відомостями;

- застосовуючи пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- використовуючи тільки штатні засоби та недоліки системи захисту (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, що можуть бути потай пронесені через охорону;

- застосовуючи методи та засоби активного впливу (модифікація і залучення додаткових технічних засобів, підключення до каналів передачі даних. Упровадження програмних закладок та використання спеціальних інструментальних і технологічних програм).

3. За часом дії:

- у процесі функціонування інформаційної системи (під час роботи опонентів системи);

- у період неактивних компонентів системи (у неробочий час, під час планових перерв, перерв з метою обслуговування та ремонту тощо);

- як у процесі функціонування інформаційної системи, так і в період активності компонентів системи.

4. За місцем дії:

- без доступу на контрольовану територію організації;

- з контрольованої території без доступу у приміщення;

- усередині приміщень, але без доступу до технічних засобів інформаційної системи;

- з робочих місць кінцевих користувачів інформаційної системи;

- з доступом у зону даних (баз даних, архівів тощо);

- з доступом у зону керування засобами забезпечення безпеки системи.

Класифікаційна модель порушника для інформації в інформаційній системі наведена на рис. 10.3.

Визначення конкретних значень характеристик можливих порушників у значній мірі є суб'єктивним. Модель порушника, побудована з урахуванням особливостей конкретної предметної сфери та технології обробки інформації може бути подана перерахуванням декількох варіантів його виду. Кожен вид порушника можна класифікувати за характеристиками, наведеними вище. Методи перевірки отриманих моделей, їхньої відповідності реальній системі та порядок визначення потенційно вразливих місць у системі є обов'язковим при створенні моделі. Так, помилки персоналу можуть становити 55%, нечесні співробітники – 10%, скривджені особи – 9%, зовнішній напад – 1÷3%, віруси – 4%, проблеми фізичного захисту (стихійні лиха, порушення й електроживлення (зниження або підвищення напруги, коливання потужності опалення тощо) – 20%.

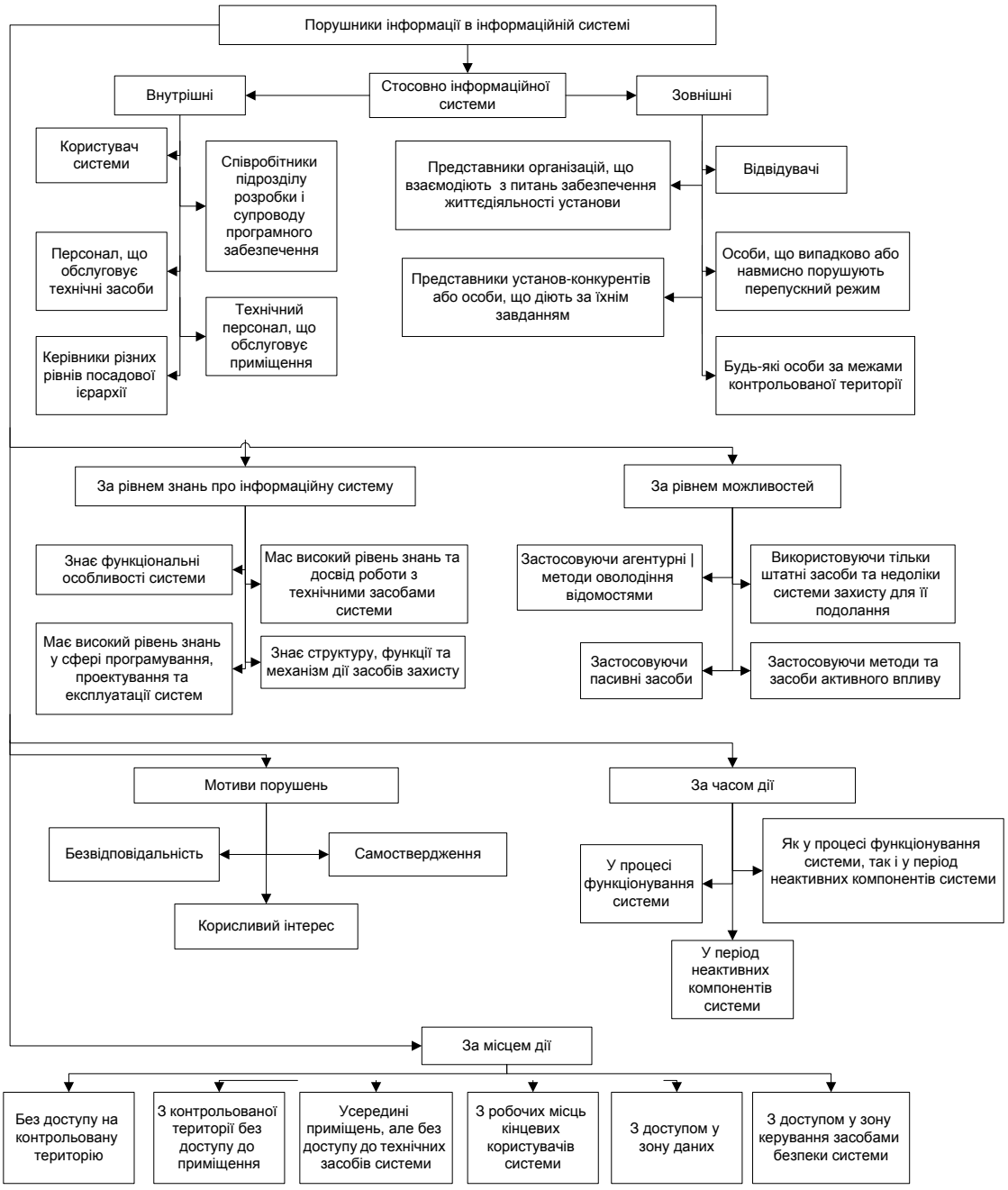


Рисунок 10.3 – Класифікаційна модель порушника в інформаційній системі

10.4 Аналіз функціонування інформаційної системи

При аналізі функціонування інформаційних систем потрібно розглядати всі можливі варіанти комбінацій, загроз на основі використання їхнього об’єднання та перетину. Так, наприклад, для інформаційної системи обробки інформації з обмеженим доступом задано конкретний скінченний вектор загроз

$$X_n = (x_1, \ldots, x_n), \; n \in N \qquad (10.1)$$

де {x} – множина потенційних загроз різного характеру, N – натуральна множина чисел.

Тоді аналіз функціонування даної інформаційної системи базується на розв'язанні таких операторних рівнянь:

$$y_k = L_k\left[\mathrm{Y}_{i=1}^{m} x_i, \mathrm{I}_{j=1}^{q} x_j\right], k \in N \qquad (10.2)$$

де $y_к$ – це відгук інформаційної системи при вхідній дії об'єднання $\mathrm{Y}_{i=1}^{m} x_i$ та перетину $\mathrm{I}_{j=1}^{q} x_j$ потенційних загроз;

$L_k[\ ]$ – відповідний оператор дії інформаційної системи на вказану комбінацію вхідних потенційних загроз.

Сучасні інформаційні системи обробки інформації з обмеженим доступом є адаптованими до різних комбінацій потенційних загроз, тому їх функціонування можна описати певною послідовністю відповідних операторів дії залежно від конкретної комбінації вхідних потенційних загроз.

У більшості випадків математичні моделі потенційних загроз є випадковими, а послідовність (10.2) – детермінованими, інтегральними диференціальними операторами. Тому методологія аналізу функціонування інформаційної системи є статистичною.

При створенні інформаційних систем обробки інформації з обмеженим доступом аналіз операторних рівнянь (10.2) є певним станом, результати якого дають можливість сформулювати рекомендації забезпечення захисту інформації з подальшою їхньою реалізацією у конкретній інформаційній системі на основі деталізації технічних характеристик розробки структури системи використання відповідної елементної бази, засобів обчислювальної техніки і т. д.

Витрати на систему захисту інформації з обмеженим доступом в інформаційній системі від несанкціонованого доступу необхідно порівнювати і приводити у відповідність з цінністю захищуваної інформації та інших інформаційних ресурсів, що підлягають захисту, а також зі збитками, що можуть бути завдані несанкціонованим доступом.

Варто відзначити, що для досягнення поставленої мети несанкціонованих дій зловмисники використовують не одну, а деяку сукупність загроз.

Зупинимось на основних етапах оцінювання дій загроз в інформаційних системах обробки інформації, які мають чітку логічну послідовність у часі при вирішенні складних науково-технічних проблем, до яких належить і проблема захисту інформації в інформаційних системах.

Етап розробки фізичних і математичних моделей потенційних загроз і досліджуваних інформаційних систем.

Методологія проведення етапу теоретичних досліджень базується на:

- обґрунтуванні і постановці завдань;
- виборі методів вирішення завдань;
- аналізі результатів теоретичних досліджень.

Етап імітаційних досліджень, як правило, зводиться до комп'ютерного моделювання.

Етап моделювання по суті є основним етапом аналізу функціонування інформаційної системи обробки інформації, при цьому моделюється та оцінюється дія загроз для всіх можливих підсистем захисту інформації. Методологія і результати моделювання визначають цінність сучасних новітніх інформаційних технологій, розробкою яких на сьогодні займаються дослідники і фахівці всіх розвинених країн світу. Для сучасних інформаційних технологій характерним є:

- методологія їхнього створення базується на використанні результатів фундаментальних теоретичних досліджень та інформації з обмеженим доступом;
- адаптація до широкого кола автоматизованих систем;
- значна фінансова вартість використання таких високоінтелектуальних технологій.

Етап створення інформаційних систем є найтривалішим за часом, комплексним за своїм змістом.

Відмітимо лише деякі характерні особливості виконання цього етапу:

- на основі отриманих теоретичних результатів і моделювання обґрунтовується структура конкретної системи з заданими інформаційними та технічними характеристиками;
- специфіка функціонування кожної системи визначається класом завдань, які розв'язуються такою системою в основному на базі розробки програмного математичного забезпечення;
- завдання захисту інформації при створенні системи є одними з головних і, в основному, визначають специфіку, цінність, адаптацію до загроз самої системи.

На етапі налаштування, випробувань і введення в експлуатацію інформаційних систем є можливість формування бази знань функціонування розробленої системи з метою визначення життєвого циклу системи на основі:

- розрахунків характеристик надійності;
- розробки методології регламентних і ремонтних робіт;
- створення відповідних баз даних вимірювань поточних характеристик і параметрів механізмів, пристроїв системи;
- методик прогнозу стану системи та інших.

Завдання аналізу дій загроз в інформаційних системах

База знань функціонування інформаційної системи обробки містить складову компоненту бази знань захисту інформації.

Необхідно відмітити, що до завдань захисту інформації відносять класичні завдання виявлення корисних сигналів при дії завад, завдання визначення їхніх характеристик, завдання розпізнавання.

Як правило, для вирішення таких завдань використовуються статистичні методи теорії випадкових процесів і математичної статистики.

Найбільш обґрунтований підхід до аналізу функціонування інформаційної системи зводиться до аналізу такої структурної схеми (рис. 10.4)

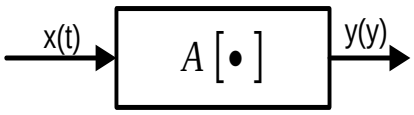


Рисунок 10.4 – Структурна схема еквівалентної системи,
де x(t), t є T – вхідна дія; *A[.]* – оператор перетворення вхідної дії;
y(t) – відгук оператора.

Але на практиці, залежно від рівня деталізації, практична структурна схема аналізу досліджуваної системи має такий вигляд (рис. 10.5).

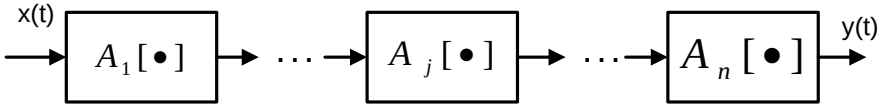


Рисунок 10.5 – Практична структурна схема системи

Таким чином, на практиці аналіз функціонування системи зводиться до аналізу перетворення вхідної дії x(t) складовим оператором

$$\boldsymbol{A}[\bullet] = \boldsymbol{A}_1[\bullet]...\boldsymbol{A}_j[\bullet]...\boldsymbol{A}_n[\bullet] = \prod^n \boldsymbol{A}_j[\bullet]. \qquad (10.3)$$

Як приклад розглянемо лінійну систему з двох лінійних функцій, які описуються відповідними імпульсними перехідними функціями $\{\varphi_j(t), j = 1,2\}$ і мають постійні у часі параметри, тобто (рис. 10.6 та 10.7).

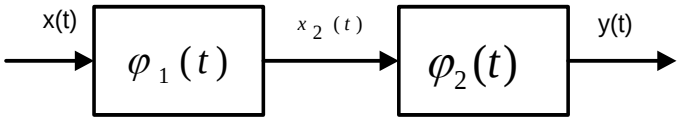


Рисунок 10.6 – Структура лінійної системи

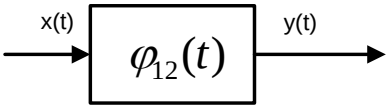


Рисунок 10.7 – Структурна схема еквівалентної лінійної системи

Відповідні співвідношення опису відгуку лінійної системи мають такий вигляд

$$x_1(t) = \int_{-\infty}^{\infty} \varphi_1(t-\tau)x(\tau)d\tau,$$

$$x_2(t) = \int_{-\infty}^{\infty} \varphi_1(t-\tau)x_1(\tau)d\tau = \int_{-\infty}^{\infty} \varphi_2(t-\tau)\int_{-\infty}^{\infty} \varphi_2(t-s)x(s)d\tau\, ds = \int_{-\infty}^{\infty} \varphi_2(t-\tau)x(\tau)d\tau,$$

де $x_{12}(t) = \int_{-\infty}^{\infty} \varphi_2(t-\tau)\varphi_1(\tau)d\tau$,

для n-модульної лінійної системи маємо

$$\varphi_{L..n(t)} = \int_{-\infty}^{\infty}\ldots \int_{-\infty}^{t-\tau_1-\ldots-\tau_{n-31}} \int_{-\infty}^{t-\tau_1-\ldots-\tau_{n=2}} \varphi_n(t-\tau_1-\ldots\tau_{n-1})\varphi_{n-1}(\tau_{n-1})\ldots\varphi_1(\tau_1)d\tau_{n-1}\ldots d\tau_1.$$

У більшості випадків оператор (10.3) складається з лінійних і нелінійних операторів відповідних модулів інформаційної системи.

Наведений приклад підтверджує факт використання класичних результатів теорії сигналів і систем для аналізу інформаційних систем обробки сигналів.

Основні завдання оцінювання дій загроз в інформаційних системах обробки інформації можна умовно поділити на дві групи, які тісно взаємопов’язані між собою, а саме:

А) завдання аналізу функціонування інформаційної системи відповідно до загроз;

Б) завдання аналізу функціонування інформаційної системи за наявності загроз.

Коло завдань групи Б) значно ширше порівняно з завданнями групи А), але саме результати розв’язання задач групи А) є необхідною умовою отримання оцінки дії загроз. Розглянемо принципово нові завдання групи Б).

Обґрунтувати і розробити фізичні і математичні моделі потенційних загроз, визначити їхні основні характеристики, базуючись на опублікованих результатах досліджень. Обґрунтувати множину потенційних загроз і визначити імовірні шляхи та методи їхньої реалізації на основі результатів аналізу функціонування конкретної інформаційної системи: класу основних задач і галузей використання результатів їхнього розв’язку; специфіки і характеру досліджуваної інформації; рівня конфіденційності інформації; оцінки умовної цінності інформації у технічному і економічному аспектах.

У більшості випадків моделі загроз описуються випадковими функціями. Наприклад, неоднорідний пуассонів випадковий процес з незалежними приростами може описувати певну послідовність появи загроз, які відбуваються випадково за часом й інтенсивністю.

Завдання випадкових моделей загроз базується на визначенні послідовності скінченних вимірів. У більшості випадків на практиці обмежуються аналізом досліджуваних випадкових процесів у рамках кореляційної теорії. При цьому використовується одновимірна та двовимірна функції розподілу досліджуваного випадкового процесу. Як правило, вибір того чи іншого закону розподілу ймовірностей формується як та чи інша статистична гіпотеза, підтвердження якої обґрунтовується результатами статистичної обробки даних вимірів досліджуваної загрози. По суті, задача ідентифікації досліджуваної загрози зводиться до обчислення статистичної оцінки її характеристик, параметрів на основі обробки даних вимірів і підтвердження статистичної гіпотези належності моделі загрози до відповідного класу випадкових процесів, наприклад, гауссового, стаціонарного, періодичного, лінійного та інших. При заданих характеристиках, параметрах моделей і пристроїв інформаційної системи, моделей загроз, аналізуються дії у рамках проведення:

- теоретичних досліджень;
- моделювання;
- статистичної обробки даних вимірювань експериментальних досліджень на основі постановки відповідних задач, обґрунтування застосування методів їхнього розв’язання та отримання результатів розв’язання задач.

Аналіз отриманих результатів дає можливість оцінити технічні, економічні витрати від здійснення загроз.

Результати розв’язання послідовності задач, наведених вище, дають можливість приступити до вирішення складної науково-технічної проблеми захисту інформації у досліджуваній інформаційній системі.

Нижче наведено приклади вразливостей в різних зонах захисту, висновки з аналізу загроз в інформаційних системах, також приклади загроз, що могли б скористатися цими вразливостями. Дані приклади можна використовувати як довідкову інформацію в процесі оцінювання вразливостей. Варто також підкреслити, що в деяких випадках інші загрози також можуть використовувати ці вразливості.

Оточення та інфраструктура:

- відсутність фізичного захисту будівель, дверей і вікон (може використовувати, наприклад, загроза злодійства);
- недостатнє чи недбале використання фізичного контролю за доступом до будівель, кімнат (може використовувати, наприклад, загроза навмисного пошкодження);
- нестійкість енергосистеми (може використовувати, наприклад, загроза нестабільності енергоживлення);

- розташування в зоні ймовірного затоплення (може використовувати, наприклад, загроза затоплення).

Апаратні засоби:

- відсутність графіка періодичної заміни (може використовувати, наприклад, загроза погіршення носіїв даних);
- чутливість до змін напруги (може використовувати, наприклад, загроза нестабільності енергоживлення);
- чутливість до коливань температури (може використовувати, наприклад, загроза екстремальних значень температури);
- чутливість до вологості, пилу, вогкості (може використовувати, наприклад, загроза запилення);
- чутливість до електромагнітного випромінювання (може використовувати, наприклад, загроза електромагнітного випромінювання);
- недостатній супровід/неправильна інсталяція даних (може використовувати, наприклад, загроза помилки обслуговуючого персоналу);
- відсутність ефективного керування змінами конфігурації (може використовувати, наприклад, загроза помилки персоналу, що займається експлуатацією).

Програмні засоби:

- неповні чи незрозумілі для розробників технічні вимоги (може використовувати, наприклад, загроза програмної помилки);
- відсутність чи недостатність випробування програмного забезпечення (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженими користувачами);
- складний інтерфейс користувача (може використовувати, наприклад, загроза помилки персоналу, що займається експлуатацією);
- відсутність таких ідентифікаційних і пізнавальних механізмів, як автентифікація користувача (може використовувати, наприклад, загроза нелегального проникнення користувача);
- відсутність контрольних точок (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженим користувачем);
- відомі «дірки» в програмному забезпеченні (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженими користувачами);
- незахищені таблиці паролів (може використовувати, наприклад, загроза несанкціонованого доступу користувача);
- недостатнє керування паролями (паролі, які легко підібрати, зберігання паролів у відкритому вигляді, недостатня частота зміни; може використовувати, наприклад, загроза нелегального проникнення користувача);
- неправильний розподіл прав доступу (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженим чином);

- неконтрольоване завантаження і використання програмного забезпечення (може використовувати, наприклад, загроза зловмисної програмної закладки);

- немає механізмів «виходу з системи» у разі від'єднання робочої станції від системи (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженими користувачами);

- відсутність ефективного керування змінами (може використовувати, наприклад, загроза програмної помилки);

- відсутність документації (може використовувати, наприклад, загроза помилки оперативного персоналу);

- відсутність запасних копій (може використовувати, наприклад, загроза зловмисної програмної закладки чи загроза пожежі);

- розповсюджування чи багаторазове використання носіїв даних без відповідного очищення (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженими користувачами).

Зв'язок:

- незахищені лінії зв'язку (може використовувати, наприклад, загроза підслуховування);

- погані кабельні з'єднання (може використовувати, наприклад, загроза витоку даних з каналів зв'язку);

- відсутність ідентифікування і підтвердження відправника й одержувача (може використовувати, наприклад, загроза нелегального проникнення користувача);

- передавання паролів у відкритому вигляді (може використовувати, наприклад, загроза доступу до мережі неуповноваженими на те користувачами);

- відсутність підтвердження посилання чи одержання повідомлень (може використовувати, наприклад, загроза невизнання участі);

- вилучений доступ (може використовувати, наприклад, загроза доступу до мережі неуповноваженими на те користувачами);

- незахищений чутливий потік даних (може використовувати, наприклад, загроза підслуховування);

- недостатнє керування мережею (гнучкість маршрутизації; може використовувати, наприклад, загроза перевантаження трафіка);

- незахищені з'єднання загального використання (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженими на те користувачами).

Документи:

- зберігання в незахищеному вигляді (може використовувати, наприклад, загроза злодійства);

- відсутність обережності у використанні (може використовувати, наприклад, загроза злодійства);

- несанкціоноване копіювання (може використовувати, наприклад, загроза злодійства).

Персонал:

- відсутність персоналу (може використовувати, наприклад, загроза, пов'язана з недостатньою кількістю персоналу);
- неконтрольована зовнішня робота некомпетентним персоналом (може використовувати, наприклад, загроза злодійства);
- недостатнє навчання питанням захисту (може використовувати, наприклад, загроза помилки оперативного персоналу);
- відсутність компетентності в захисті (може використовувати, наприклад, загроза помилок користувача);
- неправильне використання програмного забезпечення і устаткування (може використовувати, наприклад, загроза помилки оперативного персоналу);
- відсутність заходів контролю (може використовувати, наприклад, загроза використання програмного забезпечення неуповноваженим на те коритувачем);
- відсутність методик для правильного використання засобів телекомунікації і пересилання повідомлень (може використовувати, наприклад, загроза використання мережних засобів неуповноваженим на те коритувачем);
- неадекватні процедури прийому на роботу (може використовувати наприклад, загроза навмисного збитку).

Загальні причини вразливостей:

- окремі місця недоліків (може використовувати, наприклад, загроза недоліків послуг зв'язку);
- неадекватне реагування служб підтримки (може використовувати, наприклад, загроза відмови апаратури).

Важливо визначити, наскільки небезпечні вразливості, іншими словами, як легко ними можна скористатися. Вразливість має бути оцінена стосовно кожної загрози у відповідній ситуації. Наприклад, система може мати вразливість до загроз нелегального проникнення користувача і використання ресурсів. Вразливість нелегального проникнення користувача може бути високою через відсутність механізмів авторизації користувачів. З іншого боку, вразливість зловживання ресурсами може бути низькою, тому що навіть без механізмів авторизації користувачів ресурси, якими вони могли б зловживати, обмежені.

Результатом цього кроку повинен бути перелік вразливостей і оцінок легкості їхнього використання, наприклад, у градації «високо», «середньо» і «низько».

Модель загроз складається з таких етапів:

- збирання та попередня підготовка інформації (складання запитальника);
- методи моделювання та інтерпретації інформації;

- аналіз та коригування моделі;

- оформлення результатів.

На етапі збирання та попередньої підготовки інформації в першу чергу необхідно знайти відповіді на запитання:

- хто, вірогідніше за все, може напасти на конкретну інформацію;

- яку інформацію, скільки грошей та інших засобів можуть отримати порушники.

Щоб відповісти на ці запитання, необхідно знати:

- чи є в інформаційній системі та мережі інформація з обмеженим доступом, котра має цінність для порушника;

- чи є в системі інформація з грифом обмеження доступу;

- чи є інформація, котра може бути особливо цікавою для порушників;

- наскільки достатньо система захищена від нападів;

- які вразливі місця системи;

- які засоби захисту вже застосовувались?

При цьому необхідно чітко знати відповіді на такі запитання:

- яка вірогідність того, що хто-небудь нападе на конкретну інформаційну систему;

- наскільки вірогідна кожна з виявлених конкретних загроз?

Перший етап (складання запитальника) є теоретичним. Необхідно уявити можливі напади, котрі можуть бути: вандали занесуть вірус, щоб завдати збитку, крадії можуть за замовленням украсти обладнання і програмне забезпечення, може виникнути пожежа, повінь, землетрус.

Методи моделювання та інтерпретації інформації починаються з ряду запитань:

- хто може напасти на інформаційну систему;

- які засоби можуть використовувати нападники;

- які ресурси і компоненти системи можуть бути вкрадені або порушені?

Другий етап є конкретним. Які є вразливі місця систем з урахуванням загроз? Якщо загрози видаються мінімальними, необхідно виявити потенційно вразливі місця. Мінімальні загрози можуть стати великими, а загрози, вірогідність котрих не врахована, – матеріалізуватися. Що необхідно зробити з вразливими місцями – це окреме питання. Мета цього етапу полягає у виявленні та переліченні загроз.

Тепер, коли відомі вразливі місця інформаційної системи з пов’язаними з ними загрозами, можна визначити, які методи захисту інформаційної системи вже застосовуються і що ще необхідно зробити.

Іноді достатньо простих і недорогих заходів, щоб забезпечити необхідний рівень захисту системи. Іноді, щоб як слід захистити систему, необхідно вкласти великі гроші. На цьому етапі потрібно прийняти рішення. Зрозуміло, що ступінь захисту системи, який необхідно забезпечити, залежить як від ступеня її вразливості, так і від коштів, виділених на ці роботи. Якщо рівень загроз мінімальний, витрати і зусилля

на організацію захисту будуть мінімальні. Якщо рівень загроз великий, витрати і зусилля на організацію захисту значно збільшуються.

Бажано розділити потреби в забезпеченні захисту на три категорії:

- перша категорія – це невідкладні потреби, які необхідно вирішити прямо зараз. Зламаний замок, ненавчений співробітник, дірки в огорожі тощо;

- друга категорія - це середньотермінові потреби, а саме: зміни, які необхідно зробити в поточному фінансовому році (модернізація наявного захисного обладнання);

- третя категорія – це довготермінові потреби, витрати на них необхідно вносити в бюджет наступних років, це пов’язано з модернізацією системи в цілому і прогнозованими потребами в наступному.

Незалежно від того, що вирішено на подальший час, повинен бути план дій в надзвичайних умовах. Якщо зловмисник знайшов доступ до системи, необхідно швидко знайти гроші, «закрити двері комори і очистити стайню».

У процесі аналізу та коригування моделі загроз необхідно перерахувати усі цінності, що їх необхідно захищати в даній інформаційній системі. Приблизний перелік таких цінностей:

- програмне забезпечення (операційна система, прикладні програми, стандартні прикладні та робочі програми, системні утиліти, комунікаційні програми);

- фізичні цінності – системи життєзабезпечення (енергозабезпечення, водопостачання, опалення, освітлення);

- споруди;
- інформаційна система;
- витратні матеріали (папір, магнітні носії інформації);
- резервне обладнання;
- приміщення з встановленим обладнанням тощо.

10.5 Оцінювання активів організації

Оцінювання активів організації – істотний етап всього процесу аналізу ризиків. Значення цінності, визначене для активів, мусить бути виражене в поняттях, що стосуються майна і об’єктів, залучених до ділової активності. Для оцінювання активів організація має спочатку зробити перелік усіх наявних активів; щоб забезпечити адекватне оцінювання всіх активів, доцільно згрупувати їх за типами, наприклад, інформаційні активи, програмні матеріальні носії інформації, фізичні матеріальні носії інформації і служби. Також корисно визначити власника кожного з активів, що буде відповідати за визначення значень цих активів.

Наступним кроком є вибір і погодження використовуваних шкал і критеріїв специфічних оцінювань активів. Оскільки в більшості

організацій зазвичай є значне різноманіття активів, швидше за все, цінності деяких активів можуть бути визначені у вартісному виразі та будуть оцінені в національній валюті, в той час як інші, виражені в якісному значенні, можуть бути оцінені діапазоном значень від «дуже низько» до «дуже високо». Рішення про використання шкали кількісних оцінок замість шкали якісних оцінок є компетенцією організації і має залежати від оцінюваних активів. Обидва види оцінювань можна застосовувати до тих самих активів.

Типові градації, використовувані для якісного оцінювання активів, такі: «незначно», «дуже низько», «низько», «середньо», «високо», «дуже високо» і «критично». Вибір діапазону значень залежить від вимог організації до безпеки, розміру організації та інших чинників, визначених для організації.

Критерії, що використовуються як основа для кожного з активів, мають бути зафіксовані в певних значеннях. Це, зазвичай, один з найважчих аспектів оцінювання активів, тому що значення деяких активів, імовірно, доведеться визначити суб'єктивно і, швидше за все, це будуть визначати багато різних осіб. Можливі критерії, використовувані для визначання значень активів, охоплюють вартість їхнього придбання, заміни чи вартість повторного створення; їхні значення можуть бути абстрактними, наприклад, значення гарного іміджу організації чи її репутації.

Ще однією основою для оцінювання активів є витрати, спричинені втратою конфіденційності, цілісності чи доступності в результаті інциденту. Ця оцінка надає три важливих доповнення значень активів як додаток вартості відшкодування, заснований на оцінюванні потенційного збитку чи несприятливого зниження ділової активності, що випливатиме з інцидентів захисту і буде залежною від нього множиною обставин. Треба зазначити, що цей підхід дозволяє врахувати збитки чи інші втрати коштів як необхідну складову формули оцінювання ризику.

Багато активів можуть мати декілька значень, наданих в процесі оцінювання. Наприклад, план ділової активності може бути оцінений на підставі зусиль, необхідних для розробки плану розвитку, що, в свою чергу, ґрунтується на зусиллях, пов'язаних з накопиченням даних, а також на їхньому значенні для конкурентів. Кожна з отриманих оцінок з великою ймовірністю матиме різні значення. Присвоєне значення може бути максимальним серед усіх можливих значень чи може бути сумою деяких чи всіх можливих значень. Остаточний аналіз, що припускає визначення значення чи значень активів, має бути чітко детермінованим, тому що надане остаточне значення враховують під час визначання ресурсів, що будуть залучені для захисту активів.

Зрештою всі оцінки активів мають бути зведені до спільної основи. Це може бути виконано за допомогою критеріїв. Критерії, які можна використовувати для визначання можливих збитків, зумовлюються втратою конфіденційності, цілісності чи доступності активів:

- порушення законів і (або) розпоряджень;
- порушення ділової активності;
- зміна з позитивного на негативний вплив на репутацію;
- порушення, пов’язані з особистою інформацією;
- втрата особистої безпеки;
- несприятливий вплив на законність діяльності;
- порушення комерційної конфіденційності;
- порушення громадського порядку;
- фінансові втрати;
- збої в діловій активності;
- втрата безпеки відносно оточення.

Ці критерії – приклади положень, які потрібно враховувати під час оцінювання активів. Для визначення оцінок організація має вибрати критерії, що залежать від типу вимог безпеки і ділової активності.

Необхідно також враховувати, що деякі з критеріїв, наведених вище, можуть не відповідати потребам конкретної організації і можуть бути додані інші, відмінні від них.

Після визначення критеріїв, які необхідно брати до уваги, організація мусить погодити шкалу, яка буде використовуватися для всієї організації. Перший крок складається з визначення кількості використовуваних рівнів. Немає загальних правил, що дозволяють визначити кількість найбільш прийнятних рівнів. Більша кількість рівнів забезпечує вищий рівень деталізації оцінок, але іноді вищий рівень диференціації ускладнює в цілому загальну оцінку для організації. Звичайно, можна використовувати будь-яке число рівнів від трьох (наприклад, «низько», «середньо» і «високо») до десяти, якщо воно не суперечить підходу, використовуваному організацією для всього процесу оцінювання ризику.

Також організація може визначити власні межі для таких значень матеріальних носіїв інформації, як «низько», «середньо» чи «високо». Ці межі повинні бути визначені відповідно до обраних критеріїв. Наприклад, можливий фінансовий збиток: він повинен бути визначений у вартісному виразі, однак під час розгляду втрат особистої безпеки фінансове значення не буде відповідним. Наостанок, в компетенції організації вирішити, що необхідно розглядати як «низький» чи «високий» збиток: збиток, що може бути великим для малої організації, може бути незначним для дуже великої організації.

Після досягнення мети щодо ідентифікації активів за допомогою огляду всіх активів системи інформаційних технологій треба визначити цінність активів. Ця цінність відображає важливість активів для діяльності організації, їх можна виразити в таких термінах захисту, «як потенційно небажані порушення ділової активності в результаті розкриття», «зміни, недоступності або знищення інформації» або «інших активів системи інформаційних технологій». Отже, ідентифікація активів та їхнє

оцінювання, засновані на ділових потребах організації, є провідними чинниками при визначенні ризиків.

Вихідними даними для оцінювання активів повинні забезпечувати власники і користувачі активів. Особи, що аналізують ризик, повинні формулювати перелік активів. Вони мусять звертатися по допомогу до тих, хто займається плануванням ділової активності, фінансами, інформаційними системами та іншою залежною діяльністю, для того, щоб визначити цінність кожного з цих активів. Встановлення цінності потрібно пов'язувати з вартістю придбання і отримання активів і з потенційними поразками від втрати конфіденційності, цілісності, доступності, достовірності та надійності. Кожен з ідентифікованих активів має певну цінність для організації. Проте не завжди є прямий чи простий спосіб встановлення фінансової цінності для всіх параметрів. Також необхідно встановити цінність чи ступінь важливості параметра для нефінансових, тобто, для якісних характеристик, термінів в організації. Інакше буде важко визначити рівень захисту і кількість ресурсів, які організація має залучити, щоб захистити матеріальні носії. Наприклад, для подібних визначень цінності можна використовувати шкалу, де вона виражена у градації: «низько», «середньо», «високо» або більш детальну – «дуже низько», «низько», «середньо» , «високо», «дуже високо».

Організація також повинна визначити власні межі для оцінювання збитків як «низькі» або «високі». Наприклад, фінансовий збиток, що міг би бути згубним для малої організації, може спричинити незначні чи часткові втрати для великої організації. Варто підкреслити на цій стадії, що метод для оцінювання повинен давати не тільки кількісну оцінку, але і якісну оцінку там, де кількісна оцінка неможлива чи недоцільна (наприклад, існує потенційна можливість втрати життєздатності чи репутації організації). Необхідно надавати чіткі обґрунтування обраних критеріїв оцінювання.

Також потрібно визначити залежності одних активів від інших, тому що це може впливати на їхню цінність. Наприклад, конфіденційність даних треба зберігати протягом усього процесу обробки, тобто вимоги програми захисту обробки даних повинні залежати безпосередньо від значення, що відображає конфіденційність оброблюваних даних. Якщо бізнес-процес спирається на цілісність певних даних, вироблених програмою, вхідні дані цієї програми повинні забезпечувати відповідну надійність. Крім того, цілісність активів буде залежати від апаратних засобів і програмного забезпечення, що використовуються для її зберігання та обробки. Також апаратні засоби залежать від електроживлення тощо. Така інформація щодо залежностей буде допомагати під час ідентифікування залежних загроз і, особливо, вразливостей. Це також допоможе під час визначення дійсних цінностей матеріальних носіїв (прямих залежностей відносин) і, отже, гарантувати відповідний рівень захищеності.

Цінність активів, від яких залежать інші активи, можуть змінюватися таким чином:

- якщо цінність залежних активів (дані) нижча чи дорівнює цінності розглянутих активів (програмне забезпечення), цінності залишаються незмінними;
- якщо цінність залежних активів (дані) вища цінності розглянутих активів (програмне забезпечення), цінність має бути збільшена згідно з:
- рівнем залежності;
- цінністю інших активів.

Організація може мати деякі активи, що мають бути доступними більше одного разу, такі як копії чи програми, подібні тим, що їх використовують у більшості організацій. Важливо враховувати цей факт під час оцінювання активів. Ці копії легкодоступні. Тому, з одного боку, треба потурбуватися про визначення всіх шляхів доступу; з іншого – потрібно шукати шляхи зменшення можливостей доступу.

Кінцевим результатом є перелік активів та їхніх цінностей щодо розкриття (забезпечення конфіденційності), зміни (забезпечення цілісності), доступності чи знищення (забезпечення доступності) і вартості відшкодування.

Величина економічної шкоди та інші наслідки, завдані або такі, що можуть бути завдані від втрати або витоку інформації, має бути меншою від витрат на забезпечення збереженості інформації, тобто має місце така умовна формалізація у вигляді

$$C = E + I > B,$$

де С – сукупні економічні витрати, завдані або такі, що можуть бути завдані внаслідок втрати або витоку інформації, викладеної в документі;

Е – економічна шкода: матеріальні збитки, спричинені або такі, що можуть бути спричинені внаслідок втрати або витоку інформації, викладеної в документі;

І – інші наслідки: втрати, які відбулися або можуть відбутися внаслідок втрати або витоку інформації, які економічно важко обраховуються у кількісному виразі (погіршення або розрив відносин та зв’язків з партнерами (одним або кількома), витрати на відновлення відносин та зв’язків, зрив договорів на впровадження нової продукції, людський фактор тощо);

В – витрати на забезпечення збереженості інформації, викладеної в документі.

Людський фактор відіграє дуже важливу роль в справі ефективного здійснення заходів щодо захисту активів від актів несанкціонованого доступу. Незважаючи на процес створення технічних засобів забезпечення безпеки активам, ніяка технологія не в змозі замінити добре підготовлених або тих, що мають високу мотивацію, працівників служби захисту

інформації з обмеженим доступом. Ефективність роботи найскладнішого сучасного обладнання залежить від рівня і навичок працівників, які мусять бути професіоналами у своїй справі.

Запитання для самоконтролю

1. Назвіть чотири основних варіанти методики аналізу ризику.
2. Що може бути привабливими активами організації для потенційного порушника?
3. Які головні характеристики активів?
4. Охарактеризуйте канали витоку інформації.
5. Назвіть основні підходи до виявлення загроз.
6. Охарактеризуйте класифікаційну модель порушника в інформаційній системі.
7. На чому базується методологія проведення етапу теоретичних досліджень?

ГЛАВА 11
КЕРУВАННЯ РИЗИКАМИ

11.1 Реалізація змішаного підходу до аналізу ризиків

Аналіз ризиків високого рівня

Спочатку необхідно провести початковий аналіз ризику високого рівня, щоб вибрати підхід (основний чи докладний аналіз ризику), що відповідає кожній системі інформаційних технологій. Цей аналіз ризику високого рівня розглядає практичну цінність системи інформаційних технологій, оброблену інформацію і ризики з точки зору ділової активності організації. Вихідні дані для вирішення вибору відповідного для системи інформаційних технологій підходу можна використовувати такі підстави:

– ділові цілі, що їх досягають за допомогою системи інформаційних технологій;

– рівень залежності ділової активності організації від системи інформаційних технологій, тобто, чи впливає функція, яку розглядає організація, на її виживання або ефективність ділової активності, залежної від цієї системи, чи на конфіденційність, цілісність, доступність, обліковість, достовірність і надійність інформації, оброблюваної цією системою;

– рівень інвестування в цю систему інформаційної технології в умовах розробки, підтримування чи заміни системи;

– активи системи інформаційних технологій, для яких організація безпосередньо надала значення.

Коли ці положення оцінені, рішення прийняти легко. Якщо цілі системи важливі для ділової активності організації, якщо витрати на заміну системи високі чи якщо значення активів мають високі рівні ризику, то необхідний детальний аналіз ризику для системи. Кожна з цих умов може бути достатньою для необхідності детального аналізування ризику.

Загальне правило застосування: якщо відсутність захисту системи інформаційних технологій може спричинити істотну шкоду чи ушкодження в організації, її діловим процесам чи її активам, то необхідний докладний аналіз ризику для визначання потенційних ризиків. У всіх інших випадках для досягнення відповідного рівня захисту досить застосування основного підходу.

Основний підхід

Мета основного захисту полягає в тому, щоб установити мінімальну кількість засобів захисту і захистити всі чи деякі системи інформаційних технологій організації. Використовуючи цей підхід, можна застосувати основний захист у всій організації, і, як відзначено вище, додатково використовувати докладний аналіз ризику для захисту систем

інформаційних технологій з високими рівнями ризику чи систем, вирішальних для справи. Використання основного підходу зменшує капіталовкладення, які організація повинна робити у здійснення аналізу ризику.

Відповідний основний захист можна забезпечити, використовуючи каталоги засобів захисту, які містять перелік засобів захисту для системи інформаційних технологій від найзагальніших загроз. Рівень основного захисту може бути відкоригований відповідно до потреб організації. Докладне оцінювання загроз, вразливостей і ризиків не потрібне. Усе, що потрібно зробити для здійснення основного захисту, – це вибрати ті частини каталогу засобів захисту, що стосуються розглянутої системи інформаційних технологій. Після визначення засобів захисту, уже реалізованих на місці, їх порівнюють із засобами захисту, перерахованими в основному каталозі. Ті, яких немає на місці, повинні бути реалізовані.

Основні каталоги можуть визначити засоби захисту, які потрібно конкретно використовувати, або вони можуть пропонувати перелік необхідних вимог захисту, врахованих в будь-яких засобах захисту, відповідних розглянутій системі. Обидва підходи мають переваги. Одна з цілей основного підходу – узгодженість засобів захисту по всій організації, якої можна досягти обома підходами.

Кілька уже наявних документів надають перелік основних засобів захисту. Також іноді схожі оточення можна спостерігати серед компаній того самого промислового сектора. Після експертизи основних вимог їх можна застосовувати для основних каталогів захисту, які можуть використовувати багато різних організацій. Наприклад, каталоги основних засобів захисту могли б бути отримані від:

– міжнародних і державних організацій зі стандартизації;
– стандартів чи рекомендацій промислового сектора;
– іншої організації, бажано з подібними діловими цілями і відповідного розміру.

Організація може, звичайно, також створити власну основу, встановлюючи відповідність із типовим оточенням і з діловими цілями.

Докладний аналіз ризику

Докладний аналіз ризику для системи інформаційних технологій містить визначення структури ризиків і оцінку їхніх величин. Необхідність у докладному аналізі ризику може бути визначена без зайвих витрат часу і коштів, коли огляди високого рівня проводять для всіх систем. Такі огляди супроводжуються докладним аналізом ризику тільки високого рівня чи вирішальних систем.

Аналізують ризик визначанням потенційних несприятливих уражень, небажаних подій та ймовірності їхньої появи. Небажані події можуть впливати на ділову активність службовців чи на будь-який цінний об’єкт організації. Несприятливе ураження в результаті небажаного випадку –

складова частина можливих збитків, пов’язаних із значенням активів і їхніх ризиків. Імовірність появи уражень залежить від того, наскільки привабливі активи для потенційного нападника, від імовірності появи загроз і легкості, з якою уразливість можна використати. Результати аналізу ризику приведуть до ідентифікації і вибору засобів захисту, що їх можна використовувати для зменшення визначених ризиків до припустимого рівня.

Докладний аналіз ризику містить глибоку перевірку на кожному з кроків, показаних на рис. 11.1. Цим керуються при виборі перевірених засобів захисту як частини процесу керування ризиком. Необхідні вимоги для цих засобів захисту наведені в методиці безпеки системи інформаційних технологій і пов’язані з планом безпеки інформаційної технології. Множина інцидентів і зовнішніх чинників, що можуть впливати на необхідні вимоги захисту системи, може спричинити перегляд усього аналізу ризику чи його частини. Це такі впливи: недавні інциденти, істотні зміни системи, заплановані зміни чи наслідки інцидентів, які потрібно розглядати.

Існує ряд методів для ефективного аналізу ризику, починаючи від контрольного переліку основних підходів і закінчуючи основними методами структурованого аналізу. Можна використовувати автоматизовані (за допомогою інформаційної системи) чи звичайні базові інструкції. Також важливо, щоб методи гармонізували з мікрополітикою організації.

Після завершення детального огляду аналізу ризиків системи результати огляду (активи та їхня значимість, загрози, вразливості і рівні ризиків, а також визначені засоби захисту) повинні бути збережені, наприклад, у базі даних. Очевидно, методи, що використовують засоби програмного забезпечення, здійснюють це набагато простіше. Таке подання, згадуване іноді як модель, можна використовувати, щоб досягти істотного ефекту, оскільки через якийсь час відбуваються зміни в конфігурації, в оброблюваних типах інформації, у сценаріях загроз тощо. У цьому разі вихідними даними стають тільки самі зміни для визначання впливу на необхідні засоби захисту. Надалі такі моделі можна швидко використовувати для досліджування різних параметрів, обговорювати у процесі розробки нової системи, використовувати для інших подібних систем.

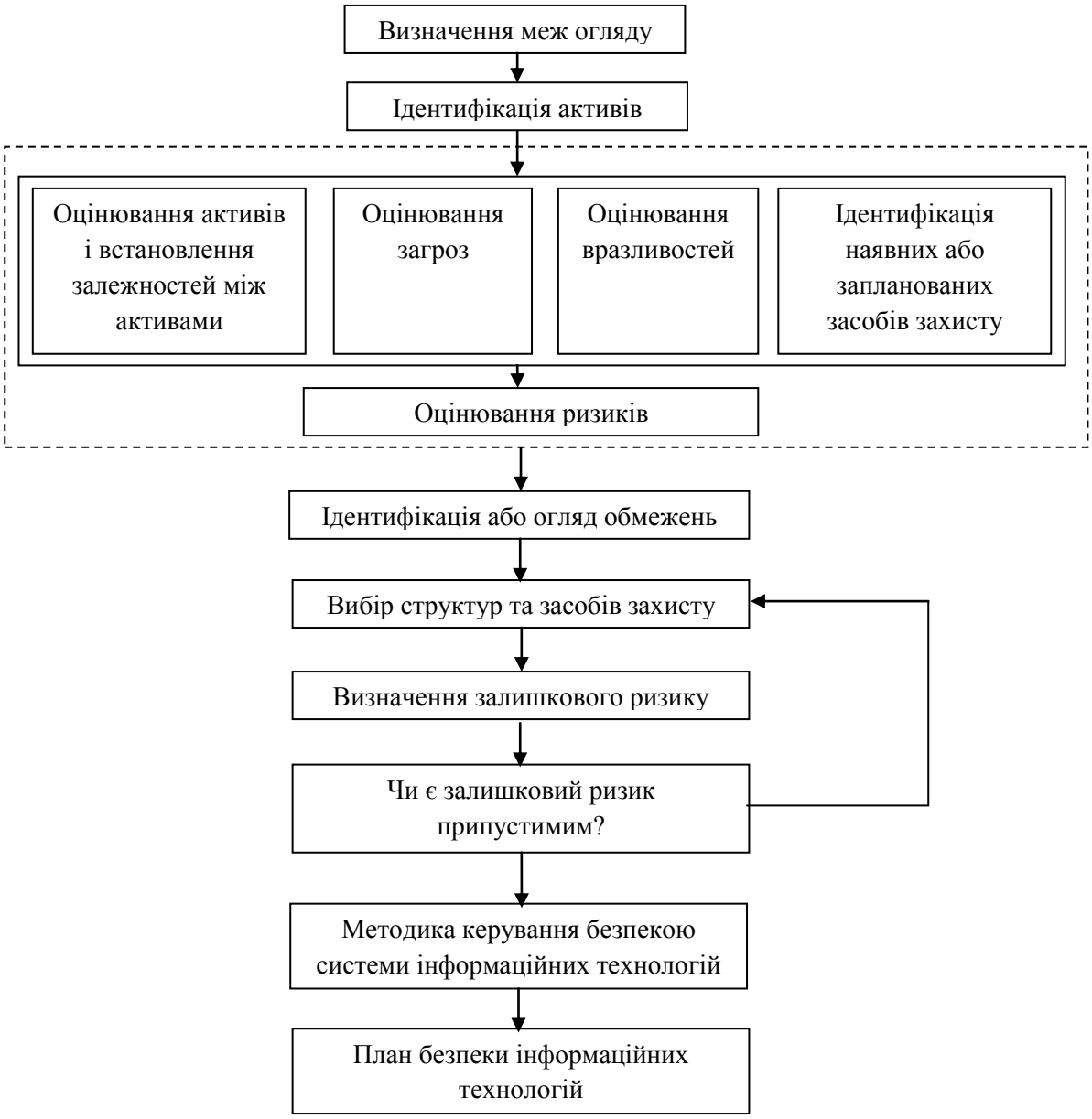


Рисунок 11.1 – Керування ризиком з використанням детального аналізу ризику

Визначання меж огляду

Як показано на рис. 11.1, перед збиранням подібної інформації для ідентифікації активів і їхнього оцінювання потрібно визначити межі огляду. Точне визначання меж у цій стадії дає змогу уникнути непотрібної роботи і поліпшити якість аналізу ризику. Кінцевий опис чітко визначить, що з наведеного нижче треба розглядати під час огляду аналізу ризиків для розглянутої системи інформаційних технологій:

– активи інформаційних технологій (наприклад, апаратні засоби, програмне забезпечення, інформація);

– люди (наприклад, персонал, субпідрядники, інший зовнішній персонал);

– оточення (наприклад, будівлі, обладнання);
– діяльність (виконувані роботи).

11.2 Ідентифікація та оцінювання активів

Актив – це компонент або частина всієї системи, для якої організація безпосередньо визначає цінність і, отже, яка потребує захисту. Для ідентифікації активів треба брати до уваги те, що система інформаційних технологій складається не тільки з апаратних засобів і програмного забезпечення. Наприклад, типи активів можуть бути такими:

– інформація (дані) (наприклад, файли, що містять фінансові подробиці, інформація про продукцію);

– апаратні засоби (наприклад, інформаційна система, пристрій для друку);

– програмне забезпечення, в тому числі прикладне (наприклад, програми обробки тексту, програми, розроблені для спеціальних цілей);

– апаратура зв'язку (наприклад, телефони, мідний кабель, скловолокно);

– програмно-апаратне забезпечення (наприклад, гнучкі диски, постійна пам'ять на компакт-диску (CD ROM), програмовані ROM);

– документи (наприклад, контракти);

– грошові засоби (кошти) (наприклад, у банкоматах);

– вироблені товари;

– служби (наприклад, інформаційні служби, обчислювальні ресурси);

– конфіденційність і служби довіри (наприклад, служби оплати);

– устаткування оточення;

– персонал;

– імідж організації.

Всі активи у встановлених межах огляду повинні бути визначені і навпаки, будь-які активи, що їх вилучають з меж огляду з будь-якої причини, повинні бути вміщені в інший огляд, для впевненості, що їх не забудуть і не пропустять.

11.3 Оцінювання загроз

Загроза потенційно може нашкодити системі інформаційних технологій та її активам за умов прояву. Якщо загроза трапиться, то це може вплинути на систему інформаційних технологій і викликати небажані інциденти і, відповідно, порушення. Загрози можуть мати природне чи людське походження і можуть бути випадковими чи навмисними. Випадкові і навмисні джерела загроз повинні бути визначені, а імовірність їхньої появи необхідно оцінити. Важливо, щоб ніяка залежна загроза не була пропущена, тому що це може спричинити пошкодження чи ослаблення в системі захисту інформаційної технології.

Вихідні дані для оцінювання загрози треба отримувати від власників активів чи користувачів, від персоналу відділу кадрів, від фахівців із планування і фахівців інформаційних технологій, і від людей, відповідальних за захист організації.

В главі 6 наведено детальний перелік типових загроз. Перелік можна використовувати в процесі оцінювання загроз. Загрози можуть бути викликані одним чи кількома навмисними або випадковими (природними) подіями. Перелік наводить для кожної такої загрози її тип, де Д (навмисна), А (випадкова), Е (навколишня). Д – використовують для всіх навмисних дій, націлених на активи інформаційної технології, А – використовують для визначання всіх людських дій, що можуть призводити до ушкодження активів ІТ, Е – використовують для всіх інцидентів, що не ґрунтуються на людських діях.

Також доцільно ознайомитись з іншими каталогами загроз (можливо, специфічними для вашої організації чи ділової активності), тому що не можна скласти єдиний вичерпний перелік. Деякі з найзагальніших проявів загроз такі:

– помилки і виправлення;

– обман і злодійство;

– саботаж службовців;

– втрата фізичного та інфраструктурного супроводу:

– навмисний злом, наприклад, несанкціоноване проникнення;

– модифікація коду;

– промислове шпигунство.

У разі використання каталогів загроз чи більш ранніх оцінювань загроз потрібно знати, що загрози постійно модифікуються, особливо якщо ділове оточення чи інформаційні технології змінюються. Наприклад, віруси 90-их ХХ ст. значно складніші, ніж 80-их. Цікаво, що реалізація таких засобів захисту, як перевірка на наявність вірусу майже завжди веде до розробки нових вірусів, що мають імунітет до поточних засобів захисту. Після визначення джерела загрози (хто і що викликали загрозу) та її спрямованості (тобто на які елементи системи може вплинути загроза) необхідно визначити імовірність виникнення загрози. У цьому випадку потрібно брати до уваги:

– частоту загроз (визначити, як часто вони можуть виникати, спираючись на досвід, статистичні дослідження, якщо статистичні дослідження існують, тощо);

– мотивацію, усвідомлені можливості та здатності, ресурси, доступні потенційним нападникам, і привабливі моменти та вразливості активів системи інформаційних технологій для потенційного нападника і навмисних джерел загроз;

– такі географічні чинники, як близькість до хімічних чи нафтових заводів, можливість появи критичних метеорологічних умов, і чинники, що

можуть впливати на людські помилки і несправність устаткування, випадкові джерела загроз.

Залежно від ступеня точності може виникнути необхідність розбивати активи на складові та встановлювати зв'язки загроз із складовими. Наприклад, у фізичних активах можуть спочатку розглядати «центральні сервери даних», а коли визначено, що ці сервери перебувають у географічно різних місцях, то розглядають окремо «центральний сервер даних 1» і «центральний сервер даних 2», тому що можуть бути деякі різні загрози і з різними впливами. Так само програмні активи можна спочатку розцінювати як «прикладне програмне забезпечення», а пізніше розбити на кілька видів «прикладного програмного забезпечення». Прикладом щодо активів даних може слугувати таке початкове означення як «кримінальне досьє», а пізніше поділ на «текст кримінального досьє» і «зображення до кримінального досьє».

У разі завершення оцінювання загроз буде отримано перелік ідентифікованих загроз, активів чи груп активів, на які загрози можуть впливати, та оцінок ймовірностей появи загроз у градації «високо», «середньо» чи «низько».

11.4 Оцінювання вразливостей

Ця оцінка містить визначення недоліків у фізичному оточенні, організації, процедурах, персоналі, керуванні, адмініструванні, апаратних засобах, програмному забезпеченні чи апаратурі зв'язку, які можуть використовуватись загрозами для заподіяння шкоди активам і діяльності, яку вони супроводжують. Сама присутність вразливостей не заподіює шкоди, для чого повинна ще існувати загроза, яка використовує цю вразливість. Вразливість, для якої не існує відомих загроз, не вимагає застосування засобів захисту, але вона все-таки повинна бути ідентифікована і контролюватися щодо змін. Треба зазначити, що неправильно реалізовані засоби захисту чи такі, що працюють зі збоями, або засоби захисту, що їх використовують неправильно, можуть приховувати в собі вразливості.

Вразливості можуть бути пов'язані з властивостями чи атрибутами активів, які можна використати у спосіб або з метою, іншими від визначених у момент купівлі чи виготовлення активів. Наприклад, одна з властивостей постійного запам'ятовувача з перезаписуванням – та, що інформація, яка зберігається в ньому, може бути стерта і змінена. Це – один з конструктивних критеріїв постійного запам'ятовування з перезаписом. Проте ця властивість також надає можливість недозволеного знищення інформації на постійному запам'ятовувачі з перезаписуванням. Це може бути вразливістю.

Оцінювання ідентифікує вразливості, що можуть використовуватись загрозами, та оцінює імовірний рівень їхньої недостатності, тобто легкості

використання. Наприклад, деякими активами легко розпоряджатися, їх легко приховати чи транспортувати – ці властивості можуть спричинити вразливості. Вихідні дані для оцінювання вразливості повинні бути отримані від власників активів чи користувачів, від фахівців і експертів з устаткування систем інформаційних технологій з апаратного та програмного забезпечення. Приклади вразливостей:

– незахищені зв'язки (наприклад Internet);

– непідготовлені користувачі;

– неправильний вибір і використовування паролів;

– відсутність відповідного контролю за доступом (логічним і (або) фізичним);

– відсутність резервного копіювання інформації чи програмного забезпечення;

– розташування на ділянках, де можливі повені.

Ідентифікація наявних і (або) запланованих засобів захисту

Засоби захисту, ідентифіковані після огляду аналізу ризику, повинні бути доповненням до вже наявних і запланованих засобів захисту. Важливо, щоб наявні і заплановані засоби захисту були визначені як частина цього процесу, щоб уникнути непотрібної роботи чи витрат, наприклад, під час дублювання засобів захисту. Може виявитися, що для наявних чи запланованих засобів захисту немає обґрунтувань. У цьому випадку потрібно перевірити, чи потрібно засіб захисту вилучити і замінити іншим, більш прийнятним, чи треба лишити його для подальшого виконання своїх функцій (наприклад через вартість).

Крім того, потрібно виконати перевірку, щоб установити, після огляду аналізу ризику, чи сумісні обрані засоби захисту з наявними і запланованими засобами захисту, тобто, що обрані та наявні засоби захисту не суперечать один одному.

Під час визначення наявних засобів захисту необхідно перевірити, чи правильно вони функціонують. Якщо захисний засіб, на який покладено певну функцію захисту, не функціонує в процесі ділової активності, він є джерелом можливої вразливості.

Результат цього кроку – перелік всіх наявних і запланованих засобів захисту і стан їх впровадження та використання.

11.5 Оцінювання ризиків

Ризики – функція цінності активів стосовно небезпеки, імовірності загроз, що трапляються і можуть викликати потенційні порушення в діловій активності, легкості використання вразливості ідентифікованими загрозами, і будь-яких наявних чи запланованих засобів захисту, що можуть зменшувати ризик.

Є різні напрямки встановлення зв'язків цих чинників, наприклад, значення, надані активам, вразливостям і загрозам, поєднуються, щоб одержати значення вимірювань ризику.

Аналіз ризиків складається з багатьох стадій, що були обговорені в цій та інших главах цього навчального посібника. Стадії:

– визначання і оцінювання активів (оцінювання потенційних порушень ділової активності);

– оцінювання загроз;

– оцінювання вразливостей;

– оцінювання наявних або запланованих заходів захисту;

– оцінювання ризиків.

Прикінцевий етап повинен визначити повноту ризиків. Як відзначено раніше, активи, що мають цінність і певний рівень вразливості, перебувають у небезпеці щоразу, коли з'являється загроза. Оцінювання ризиків – це комбінація потенційних порушень ділової активності, небажаних інцидентів, рівнів оцінених загроз і вразливості. Ризики – вимір впливів, яким можуть бути піддані система і пов'язана з нею організація.

Мета аналізу ризику полягає в тому, щоб визначити і оцінити ризики, яким піддано систему інформаційних технологій та її активи, щоб визначити і вибрати відповідні і вмотивовані заходи захисту. Під час оцінювання ризиків необхідно враховувати деякі положення, також порушення та імовірність порушення.

Порушення може бути оцінено кількома способами, з використанням кількісних, наприклад, вартісних оцінок якості (може бути засноване на використанні таких ознак, як «помірковано» чи «несприятливо»), чи комбінації обох. Щоб визначити імовірність прояву загрози, потрібно встановити часовий інтервал, у якому активи будуть мати цінність чи повинні бути захищені. На імовірність прояву загрози впливають такі фактори:

– привабливість активів, особливо коли розглядають навмисну людську загрозу;

– простота перетворення активів на матеріальну винагороду, особливо якщо розглядають навмисну людську загрозу;

– технічні можливості носія загрози, що використовується для навмисної людської загрози;

– імовірність загрози;

– чутливість до вразливостей експлуатації щодо технічних і нетехнічних вразливостей.

11.6 Приклади використання методів аналізу ризиків

Багато методів використовують таблиці і поєднують суб'єктивні та емпіричні виміри. На поточний момент не існує правильного чи неправильного методу для використання. Важливо, щоб організація

використовувала методи, що є найбільш зручними і надійними; це дозволить їх багаторазово використовувати. Нижче наведено кілька прикладів методів, заснованих на таблицях.

Приклад 1

Матриця з визначеними цінностями

До методів аналізу ризику даного типу відносять такі, які оцінюються в поняттях затрат на заміну чи відновлення фактичних чи уявних фізичних активів (тобто кількісні виміри). Ці витрати потім перетворюються за шкалою в такі ж якісні оцінки, що і для активів даних (див. нижче). Фактичні чи запропоновані програмні активи оцінюють так само, як і фізичні активи з визначенням затрат на придбання чи модернізацію, і потім перетворюються в ті самі якісні оцінки, що й для активів даних. Додатково, якщо знайдено прикладне програмне забезпечення, що має власні вимоги з конфіденційності чи цілісності (наприклад, якщо сам програмний код є комерційно значущий), його оцінюють так само, як і активи даних.

Значення для активів даних одержують опитуванням обраного персоналу («власників даних»), який може авторитетно говорити відносно даних, встановлювати цінність і критичність даних, що знаходяться в користуванні, зберігаються, обробляються чи надають доступ. Опитування полегшують оцінювання значень і критичності активів даних в аспектах очікуваних найгірших сценаріїв, у результаті прояву порушень ділової активності через неуповноважене розкриття, неуповноважені зміни, невизнання участі, недоступність протягом різних проміжків часу і знищення.

Оцінювання виконують на підставі рекомендацій з оцінювання активів даних, що враховують такі положення, як:

– особиста безпека;
– персональна інформація;
– правові та регуляторні зобов’язання;
– правова діяльність;
– комерційні й економічні інтереси;
– фінансові втрати/зупинка діяльності;
– суспільний порядок;
– ділова методика і діяльність;
– втрата принципу «доброї волі».

Рекомендації полегшують ідентифікацію значень в числовій шкалі (значення від 0 до 4 показано нижче в матриці прикладу), дають змогу визначити, де можливо, кількісні і логічні значення і значення якісні там, де кількісні значення не придатні, наприклад, схильність до небезпеки людського життя.

Наступні основні дії – складання пар опитувальних листів для кожної загрози і пов’язаної з нею групи активів, що допоможе оцінити рівні загроз (імовірність появи загрози) і рівні вразливості (легкість використання їх

загрозами спричиняє порушення). Кожна відповідь на питання оцінюється кількістю балів. Ці бали накопичуються в базі знань і порівнюються з діапазонами. Це дає змогу ідентифікувати рівні загроз у градаціях «високо», «низько», і рівні вразливості так, як показано нижче в матриці прикладу, диференційовано за релевантними типами враження. Інформація, необхідна для заповнення опитувальних листів, повинна бути зібрана шляхом опитування відповідних представників технічних відділів, перевіркою фізичного розташування й оглядами документації.

Типи розглядуваних загроз згруповані в широких межах: від несанкціонованих дій, непередбачених природних впливів, помилок людей до несправностей устаткування/програм/каналів зв'язку.

Цінності активів, рівні загроз і вразливостей стосовно кожного типу вражень розміщені в матриці, зображеній нижче, призначеній для визначання для кожної комбінації ризику в діапазоні від 1 до 8. Значення розміщені в матриці структурованим чином. Приклад наведено в таблиці 11.1.

Таблиця 11.1 – Цінності активів, рівні загроз і вразливостей стосовно кожного типу вражень

	Рівні	**Низько**			**Середньо**			**Високо**		
	Рівні вразли-вості	**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Цінність активу	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для кожного активу необхідно розглядати пов'язані з ним вразливості і відповідні загрози. Якщо існує вразливість без відповідної загрози чи загроза без відповідної вразливості, то не існує ніякого ризику (але все-таки повинна бути обережність у випадку, якщо положення зміниться). Тепер відповідний рядок у матриці може бути ідентифікований номінальною вартістю, а відповідний стовпець може бути ідентифікований серйозністю загрози і вразливості. Наприклад, якщо актив має значення цінності 3, загроза і вразливість «низько», величина ризику – 3. Припустимо, що актив має значення цінності 2, рівень загроз – «низько», і вразливість «високо», тоді величина ризику – 4. Розмірність матриці, в термінах кількості категорій серйозності загроз, категорій серйозності вразливостей і кількості категорій оцінювання активів, може бути відкоригована відповідно до потреб організації. Додаткові стовпці і рядки

передбачають додаткові аспекти і величини ризику. Суть цього підходу полягає в ранжуванні врахованих ризиків.

Приклад 2

Ранжування загроз величинами ризику

Можна використовувати матрицю чи таблицю (таблиця 11.2) для описування зв'язків чинників зниження (цінності активів) і ймовірності появи загрози (беручи до уваги аспекти вразливості).

Таблиця 11.2 – Зв'язки чинників зниження цінності активів, ймовірності загрози, аспекти вразливості

Тип загрози 00	**Зниження значення активів (b)**	**Імовірність появи загрози (c)**	**Величина ризику (d)**	**Ранг загрози (e)**
Тип А	5	2	10	2
Тип Б	2	4	8	3
Тип В	3	5	15	1
Тип Г	1	3	3	5
Тип Д	4	1	4	4
Тип Е	2	4	8	3

Перший крок складається з оцінювання зниження (значення активів) у визначеній шкалі, наприклад, від 1 до 5, для кожної загрози активам (стовпець 2 в таблиці).

Другий крок складається з оцінювання імовірності появи загрози у певній шкалі, наприклад, від 1 до 5, для кожної загрози (стовпець 3 в таблиці). Третій крок передбачає визначання величини ризику шляхом множення (b·c). Нарешті, загрози можуть бути ранжовані залежно від їхнього коефіцієнта «схильності». Варто помітити, що в цьому прикладі 1 приймають якнайнижче порушення і найнижчу ймовірність появи.

Як показано вище, ця процедура припускає різні загрози з різними порушеннями та імовірністю появи, що порівнюються і ранжуються згідно з пріоритетом. В деяких ситуаціях може виникнути необхідність зіставити вартісні значення з емпіричними масштабами, використаними тут.

Приклад 3

Оцінювання значення для частоти і ризиків можливого збитку

У цьому прикладі акцент зроблено на вилученні небажаних інцидентів і на визначенні, яким системам повинен бути наданий пріоритет. Це здійснюється визначанням двох значень для кожного активу і ризику, що в комбінації дадуть оцінку для кожного з активів. Коли всі оцінки активів для системи підсумовані, то цим визначена величина ризику системи інформаційних технологій.

Спочатку надають значення для кожного з активів. Це значення залежить від потенційного збитку, що може виникати у разі загрози активам. Для кожної загрози активам надають ціннісне значення активам.

Потім оцінюють значення частоти. Цю оцінку отримують на підставі комбінації імовірності прояву загрози і легкості використання вразливості, як показано в таблиці 11.3.

Таблиця 11.3 – Комбінації імовірності прояву загрози і легкості використання вразливості

Рівні загроз	**Низько**			**Середньо**			**Високо**		
Рівні вразливості	НС	С	В	НС	С	В	НС	С	В
Значення частоти	0 1	1	2	1 2	2	3	2 3	3	4

Далі визначають величину «актив/загроза» пошуком перетину значень активів і частоти в таблиці 11.4 Множину оцінок активів/загроз підсумовують для одержання загальної суми оцінок активів. Це обчислення можна використовувати для диференціювання активів, що формують частину системи.

Підсумковий крок полягає в підсумовуванні всіх сумарних оцінок активів системи, що дозволяє одержати оцінки для всієї системи. Ці дані можна використовувати для диференціювання систем і встановлювання пріоритетів у системі захисту.

Таблиця 11.4 – Значення активів і частоти

	Значення активів				
Значення частоти	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

У наступних прикладах всі значення вибрано навмання.

Припустимо, що система S має три активи A_1 A_2 і A_3. Також припустимо, що є дві загрози T_1 і T_2 системі S. Нехай значення A_1 дорівнює 3, аналогічне значення активу A_2 дорівнює 2, а значення активу A_3 дорівнює 4.

Якщо для A_1 і T_1 імовірність загрози низька, а легкість використання вразливості – середня, то значення частоти дорівнює 1 (див. табл. 11.3).

Величина активів/загроз A_1/T_1 може бути отримана з таблиці 11.4 як перетин значення активу – 3 і значення частоти – 1, і її значення – 4. Точно так само для A_1/T_2 припустимо, що імовірність загрози «середня», а легкість використання вразливості «висока», одержимо величину $A_1/T_2 = 6$.

Тепер може бути обчислена загальна оцінка активів A_1/T_1: 4 + 6 = 10. Сумарну величину активів обчислюють для кожного активу і відповідної загрози. Сумарну величину системи обчислюють додаванням

$$ST = A_1T + A_2T + A_3T.$$

Тепер можуть бути зіставлені різні системи з метою встановлення пріоритетів, а також різних активів в межах однієї системи.

Приклад 4

Розходження між припустимими і неприпустимими ризиками

Це ще один шлях вимірювання ризиків, що ґрунтується на розходженні між припустимими і неприпустимими ризиками. В основі його лежить принцип, що виміри ризиків використовують тільки для ранжування ризиків в оцінках того, де необхідні найшвидші дії і де той самий результат може бути досягнутий з меншою кількістю зусиль.

У цьому підході використовують матрицю, що з чисел містить тільки T і N, які визначають, є відповідний ризик припустимим (T) чи ні (N). Наприклад, таблиця прикладу 4 може бути зведена до таблиці 11.5.

Таблиця 11.5 – Зведена таблиця прикладу 4

	Значення активів				
Значення частоти	**0**	**1**	**2**	**3**	**4**
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N

Варто відзначити, що це лише умовні приклади, а провести лінію між припустимими ризиками можна з урахуванням особливостей функціонування інформаційної системи.

Незалежно від того, який шлях обрано для вимірювання ризику, результатом цього кроку повинен бути перелік вимірюваних ризиків для кожного з уражень у розкритті, зміні, недостачі і знищенні для розглянутої системи інформаційних технологій. Виміри ризику допоможуть ідентифікувати ті ризики, які під час вибору засобів захисту треба розглядати в першу чергу. Використовуваний метод повинен мати можливість багаторазового застосування і легко налаштовуватися.

Як зазначено раніше, різні програмні засоби автоматизації можна використовувати для супроводу усього чи частини процесу аналізу ризику. Якщо організація вирішує використовувати певний інструмент, то вона повинна бути впевнена у відповідності підходу з використанням цього інструмента методиці і стратегії безпеки інформаційної технології. А також зусилля повинні бути прикладені для одержання точних вихідних даних, тому що інструмент може працювати настільки точно, наскільки вихідні дані дозволяють.

Запитання для самоконтролю

1. В чому полягає змішаний підхід?
2. Які основні переваги змішаного підходу?
3. Як залежать засоби захисту один від одного?
4. Охарактеризуйте рис. 11.1.
5. Дайте означення поняття «активи системи».
6. Як здійснюється оцінювання загроз?

ГЛАВА 12
ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ, КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЇ

12.1 Ідентифікація та аутентифікація

Ідентифікацію та аутентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й аутентифікація – це перша лінія оборони, «прохідна» інформаційного простору організації.

Ідентифікація дозволяє суб'єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка дійсності».

(Помітимо в дужках, що походження україномовного терміна «аутентифікація» не зовсім зрозуміле. Англійське «authentication» скоріше можна прочитати як «аутентикація»; важко сказати, звідки в середині узялося ще «фі» – може, з ідентифікації? Проте, термін устоявся, він закріплений у Керівних документах України, використаний у численних публікаціях, тому виправити його вже неможливо.)

Аутентифікація буває однобічною (звичайно клієнт доводить свою дійсність серверу) і двосторонньою (взаємною). Приклад однобічної аутентифікації – процедура входу користувача в систему.

У мережевому середовищі, коли сторони ідентифікації/аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти:

- що слугує аутентифікатором (тобто використовується для підтвердження дійсності суб'єкта);
- як організований (і захищений) обмін даними ідентифікації/аутентифікації.

Суб'єкт може підтвердити свою дійсність, пред'явити принаймні одну з сутностей:

- щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і т. п.);
- щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);
- щось, що є частиною його самого (голос, відбитки пальців і т. п., тобто свої біометричні характеристики).

У відкритому мережевому середовищі між сторонами ідентифікації/аутентифікації не існує перевіреного маршруту; це значить, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими й використаними для перевірки дійсності. Необхідно

забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни й/або відтворення даних. Передача паролів у відкритому вигляді, мабуть, незадовільна; не рятує становище й шифрування паролів, тому що воно не захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація й аутентифікація ускладнені не тільки через мережеві загрози, але й з цілого ряду причин. По-перше, майже всі аутентифікаційні сутності можна довідатися, украсти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача й системного адміністратора, з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже його посаду могла зайняти інша людина), а це не тільки клопітно, але й підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб захисту, тим він дорожчий.

Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід у мережу – це, у першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежний обіг, то багаторазова ідентифікація/аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід у мережу став нормою.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ідентифікації й аутентифікації.

Цікаво відзначити, що сервіс ідентифікації/аутентифікації може стати об’єктом атак на доступність. Якщо система сконфігурована так, що після певної кількості невдалих спроб пристрій введення ідентифікаційної інформації (такий, наприклад, як термінал) блокується, то зловмисник може припинити роботу легального користувача буквально декількома натисканнями клавіш.

12.2 Парольна аутентифікація

Голова перевага парольної аутентифікації – простота й звичність. Паролі давно вбудовані в операційні системи й інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх варто визнати найслабшим засобом перевірки дійсності.

Щоб пароль краще запам’ятався, його найчастіше роблять простим (ім’я подруги, назва спортивної команди й т. п.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Відома класична історія про радянського розвідника Рихарда Зорге, об’єкт уваги якого через слово говорив «карамба»; зрозуміло, цим же словом відкривався надсекретний сейф.

Іноді паролі з самого початку не зберігаються в таємниці, тому що мають стандартні значення, зазначені в документації, і далеко не завжди після встановлення системи відбувається їхня зміна.

Уведення пароля можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на якийсь час власника пароля. Теоретично, в подібних випадках більш правильно залучити засоби керувань доступом, але на практиці так ніхто не робить: а таємниця, яку знають двоє, вже не таємниця.

Пароль можна вгадати «методом грубої сили», використовуючи, скажімо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна скачати до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Проте важливі заходи дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити букви, цифри, знаки пунктуації й т. п.);
- керування терміном дії паролів: їхня періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему, це утруднить застосування «методу грубої сили»:
- навчання користувачів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може породжувати тільки благозвучні й, отже, паролі, які добре запам'ятовуються).

Перераховані заходи доцільно застосовувати завжди, навіть якщо поряд з паролями використовуються інші методи аутентифікації.

12.3 Одноразові паролі

Розглянуті вище паролі можна назвати багаторазовими: їхнє розкриття дозволяє зловмисникові діяти від імені легального користувача. Набагато сильнішим засобом, стійким до пасивного прослуховування мережі, є одноразові паролі.

Найбільш відомим програмним генератором одноразових паролів є система S/KEY компанії Bellcore. Ідея цієї системи полягає в нижчевикладеному. Нехай є однобічна функція f (тобто функція, обчислити обернену до якої за прийнятний час неможливо). Ця функція відома й користувачеві, і серверу аутентифікації. Нехай, далі, є секретний ключ K, відомий тільки користувачеві.

На етапі початкового адміністрування користувача функція f застосовується до ключа K n разів, після чого результат зберігається на

сервері. Після цього процедура перевірки дійсності користувача виглядає так:

- сервер надсилає на систему користувача число *(n-1)*;
- користувач застосовує функцію до секретного ключа *K (n-1)* разів і відправляє результат по мережі на сервер аутентифікації;
- сервер застосовує функцію *f* до отриманого від користувача значення й порівнює результат з раніше збереженою величиною. У випадку збігу дійсність користувача вважається встановленою, сервер запам'ятовує нове значення (прислане користувачем) і зменшує на одиницю лічильник *(n)*.

Насправді реалізація влаштована дещо складніше (крім лічильника сервер посилає значення, використовуване функцією *f*), але для нас зараз це неважливо. Оскільки функція *f* не обернена, перехоплення пароля, так само як і одержання доступу до сервера аутентифікації, не дозволяють взнати секретний ключ *K* і передбачити наступний одноразовий пароль.

Система S/KEY має статус Internet-стандарту (RFC 1938).

Інший підхід до надійної аутентифікації складається в генерації нового пароля через невеликий проміжок часу (наприклад, кожних 60 секунд), для чого можуть використовуватися програми або спеціальні інтелектуальні карти (з практичної точки зору такі паролі можна вважати одноразовими). Серверу аутентифікації повинен бути відомий алгоритм генерації паролів й асоційовані з ним параметри; крім того, годинники клієнта й сервера повинні бути синхронізовані.

Сервер аутентифікації Kerberos

Kerberos – це програмний продукт, розроблений у середині 1980-х років у Массачусетському технологічному інституті, зазнав з тих часів принципових змін. Клієнтські компоненти Kerberos присутні в більшості сучасних операційних систем.

Kerberos призначений для вирішення такого завдання. Є відкрита (незахищена) мережа, у вузлах якої зосереджені суб'єкти – користувачі, а також клієнтські й серверні програмні системи. Кожен суб'єкт має секретний ключ. Щоб суб'єкт *C* міг довести свою дійсність суб'єктові *S* (без цього *S* не стане обслуговувати *C*), він повинен не тільки назвати себе, але й продемонструвати знання секретного ключа. *C* не може просто надіслати *S* свій секретний ключ, по-перше, тому, що мережа відкрита (доступна для пасивного й активного прослуховування), а, по-друге, тому, що *S* не знає (і не повинен знати) секретний ключ *C*. Потрібен менш прямолінійний спосіб демонстрації знання секретного ключа.

Система Kerberos являє собою довірену третю сторону (тобто сторону, якій довіряють усе), що володіє секретними ключами суб'єктів, яких обслуговують, і допомагає їм у попарній перевірці дійсності.

Щоб за допомогою Kerberos одержати доступ до *S* (звичайно це сервер), *C* (як правило, клієнт) посилає Kerberos запит, що містить відомості про нього (клієнта) і про запитувану послугу. У відповідь Kerberos повертає так званий квиток, зашифрований секретним ключем

сервера, і копію частини інформації з квитка, зашифровану секретним ключем клієнта. Клієнт повинен розшифрувати другу порцію даних і переслати її разом з квитком серверу. Сервер, розшифрувавши квиток, може порівняти його вміст із додатковою інформацією, присланою клієнтом. Збіг свідчить про те, що клієнт зміг розшифрувати призначені йому дані (адже вміст квитка нікому, крім сервера й Kerberos, недоступний), тобто продемонстрував знання секретного ключа. Виходить, клієнт – саме той, за кого себе видає. Підкреслимо, що секретні ключі в процесі перевірки дійсності не передавалися по мережі (навіть у зашифрованому вигляді) – вони тільки використовувалися для шифрування. Як організований первинний обмін ключами між Kerberos і суб'єктами і як суб'єкти зберігають свої секретні ключі – питання окреме.

Проілюструємо описану процедуру (рис. 12.1).

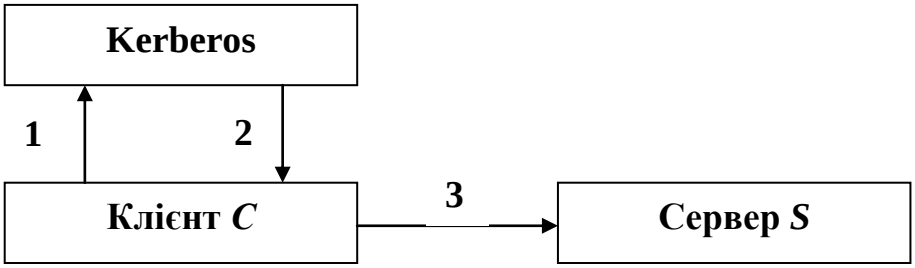


Рисунок 12.1 – Перевірка сервером *S* дійсності клієнта *C*

1. **Клієнт *C* → Kerberos**: c, s,… (клієнт надає Kerberos інформацію про себе і про запитуваний сервіс)
2. **Kerberos → клієнт *C*:** (d1) Kc, (Tc.s) Ks (Kerberos повертає квиток, закодований ключем сервера, і додаткову інформацію, закодовану ключем клієнта)
3. **Клієнт *C* → сервер *S*:** d2, (Tc.s) Ks (клієнт посилає на сервер квиток і додаткову інформацію)

Тут c та s – відомості (наприклад, ім'я), відповідно, про клієнта й сервер, dl та d2 – додаткова (стосовно квитка) інформація, Tc.s – квиток для клієнта *C* на обслуговування в сервера *S*, Kc й Ks – секретні ключі клієнта й сервера, {info}K – інформація info, зашифрована ключем K.

Наведена схема – вкрай спрощена версія реальної процедури перевірки дійсності. Більш докладний розгляд системи Kerberos можна знайти, наприклад, у статті В. Галатенко «Сервер аутентифікації Kerberos» (Jet Info, 1996, 12-13). Нам же важливо відзначити, що Kerberos не тільки стійкий до мережевих загроз, але й підтримує концепцію єдиного входу в мережу.

12.4 Ідентифікація/аутентифікація за допомогою біометричних даних

Біометрія являє собою сукупність автоматизованих методів ідентифікації й/або аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. До числа фізіологічних характеристик належать особливості відбитків пальців, сітківки й роговиці очей, геометрія руки й особи й т. п. До поведінкових характеристик відносять динаміку підпису (ручний), стиль роботи з клавіатурою. На стику фізіології й поведінки знаходяться аналіз особливостей голосу й розпізнавання мови.

Біометрією в усьому світі займаються дуже давно, однак довгий час усе, що було пов'язане з нею, відрізнялося складністю й дорожнечею. Останнім часом попит на біометричні продукти, в першу чергу у зв'язку з розвитком електронної комерції, постійно й досить інтенсивно зростає. Це зрозуміло, оскільки, з точки зору користувача, набагато зручніше «пред'явити» себе самого, ніж щось запам'ятовувати. Попит породжує пропозицію, тому на ринку з'явилися відносно недорогі апаратно-програмні продукти, орієнтовані, в основному, на розпізнавання відбитків пальців.

У загальному вигляді робота з біометричними даними організована в такий спосіб. Спочатку створюється й підтримується база даних характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються, і результат обробки (названий біометричним шаблоном) заноситься в базу даних (такі вихідні дані, як результат сканування пальця або роговиці, звичайно не зберігаються).

Надалі для ідентифікації (і одночасно аутентифікації) користувача процес зняття й обробки повторюється, після чого виробляється пошук у базі даних шаблонів. У випадку успішного пошуку особистість користувача та її дійсність вважаються встановленими.

Для аутентифікації досить зробити порівняння з одним біометричним шаблоном, обраним на основі попередньо введених даних.

Звичайно біометрію застосовують разом з іншими аутентифікаторами, такими, наприклад, як інтелектуальні карти. Іноді біометрична аутентифікація є лише першим рубежем захисту й слугує для активації інтелектуальних карт, що зберігають криптографічні секрети; у такому випадку біометричний шаблон зберігається на тій же карті.

Активність у сфері біометрії дуже велика. Організовано відповідний консорціум (http://www.biometrics.org). Активно ведуться роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу й т. п.), публікується маса рекламних статей, у яких біометрія подається як засіб забезпечення надбезпеки, що став доступним широким масам.

На наш погляд, до біометрії варто ставитися досить обережно. Необхідно враховувати, що вона піддана тим же загрозам, що й інші методи аутентифікації. По-перше, біометричний шаблон порівнюється не з результатом первинної обробки характеристик користувача, а з тим, що прийшов до місця порівняння. А, як відомо, під час маршрутизації багато чого може відбутися. По-друге, біометричні методи не надійніші, ніж база даних шаблонів. По-третє, варто враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в «польових» умовах, коли, наприклад, до пристрою сканування роговиці можуть піднести муляж і т. п. По-четверте, біометричні дані людини змінюються, так що база шаблонів має потребу в супроводі, що створює певні проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка «пробоїна» для біометрії виявляється фатальною. Паролі, при всій їхній ненадійності, у крайньому випадку, можна змінити. Загублену аутентифікаційну карту можна анулювати й завести нову. Палець же, око або голос змінити не можна. Якщо біометричні дані виявляться скомпрометовані, доведеться, як мінімум, робити істотну модернізацію всієї системи.

12.5 Керування доступом. Основні поняття

Із традиційної точки зору засоби керування доступом дозволяють специфікувати і контролювати дії, які суб’єкти (користувачі й процеси) можуть виконувати над об’єктами (інформацією й іншими комп’ютерними ресурсами). У даному підрозділі мова йде про логічне керування доступом, що, на відміну від фізичного, реалізується програмними засобами. Логічне керування доступом – це основний механізм багатокористувацьких систем, покликаний забезпечити конфіденційність і цілісність об’єктів й, певною мірою, їхню доступність (шляхом заборони обслуговування неавторизованих користувачів).

Розглянемо формальну постановку завдання в традиційному трактуванні. Є сукупність суб’єктів і набір об’єктів. Завдання логічного керування доступом полягає в тому, щоб для кожної пари «об’єкт-об’єкт-суб’єкт-об’єкт» визначити безліч припустимих операцій (залежних від деяких додаткових умов) і контролювати виконання встановленого порядку.

Відношення «об’єкт-об’єкт-суб’єкт-об’єкт» можна подати у вигляді матриці доступу, у рядках якої перераховані суб’єкти, у стовпцях – об’єкти, а в клітинках, розташованих на перетині рядків і стовпців, записані додаткові умови (наприклад, час і місце дії) і дозволені види доступу. Фрагмент матриці може виглядати, наприклад, так (табл. 12.1).

Таблиця 12.1 – Фрагмент матриці доступу

	Файл	Програма	Лінія зв’язку	Реляційна таблиця
Користувач – 1	orw системної консолі	e	rw з 8:00 до 18:00	
Користувач – 2				a
«o» – означає дозвіл на передачу прав доступу іншим користувачам «r» – читання, «w» – запис, «e» – виконання, «a» – додавання інформації				

Тема логічного керування доступом – одна з найскладніших у сфері інформаційної безпеки. Справа в тому, що саме поняття об’єкта (а тим більше видів доступу) змінюється від сервісу до сервісу. Для операційної системи до об’єктів належать файли, пристрої та процеси. Стосовно файлів і пристроїв звичайно розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення й додавання. Окремим правом може бути можливість передачі повноважень доступу іншим суб’єктам (так зване право володіння). Процеси можна створювати й знищувати. Сучасні операційні системи можуть підтримувати й інші об’єкти.

Для систем керування реляційними базами даних об’єкт – це база даних, таблиця, подання, збережена процедура. До таблиць застосовуються операції пошуку, додавання, модифікації й видалення даних, у інших об’єктів інші види доступу.

Розмаїтість об’єктів і застосовуваних до них операцій веде до принципової децентралізації логічного керування доступом. Кожен сервіс повинен сам вирішувати, чи дозволити конкретному суб’єктові ту або іншу операцію. Теоретично це узгоджується з сучасним об’єктно-орієнтованим підходом, на практиці ж призводить до значних труднощів. Головна проблема в тім, що багатьом об’єктам можна одержати доступ за допомогою різних сервісів (можливо, при цьому доведеться перебороти деякі технічні труднощі). Так, до реляційних таблиць можна дістатися не тільки засобами СУБД, але й шляхом безпосереднього читання файлів або дискових розділів, підтримуваних операційною системою (розібравшись попередньо в структурі зберігання об’єктів бази даних). У результаті при заданні матриці доступу потрібно брати до уваги не тільки принцип розподілу привілеїв для кожного сервісу, але й існуючі зв’язки між сервісами (доводиться піклуватися про узгодженість різних частин матриці). Аналогічні труднощі виникають при експорті/імпорті даних, коли інформація про права доступу, як правило, губиться (оскільки на новому сервісі вона не має сенсу). Отже, обмін даними між різними сервісами становить особливу небезпеку з точки зору керування доступом, а при проектуванні й реалізації різнорідної конфігурації необхідно подбати про погоджений розподіл прав доступу суб’єктів до об’єктів і про мінімізацію числа способів експорту/імпорту даних.

Контроль прав доступу виробляється різними компонентами програмного середовища – ядром операційної системи, сервісами безпеки, системою керування базами даних, програмним забезпеченням проміжного шару (таким, як монітор транзакцій) і т. д. Проте можна виділити загальні критерії, на підставі яких вирішується питання про надання доступу й загальні методи зберігання матриці доступу.

При ухваленні рішення про надання доступу звичайно аналізується така інформація:

- ідентифікатор суб'єкта (ідентифікатор користувача, мережева адреса комп'ютера й т. п.). Подібні ідентифікатори є основою довільного (або дискреційного) керування доступом;
- атрибути суб'єкта (мітка безпеки, група користувача й т. п.). Мітки безпеки – основа примусового (мандатного) керування доступом.

Матрицю доступу, через її розрідженість (більшість клітинок – порожні), нерозумно зберігати у вигляді двовимірного масиву. Звичайно її зберігають по стовпцях, тобто для кожного об'єкта підтримується список «допущених» суб'єктів разом з їхніми правами. Елементами списків можуть бути імена груп і шаблони суб'єктів, що є значною допомогою адміністраторові. Деякі проблеми виникають тільки при видаленні суб'єкта, коли доводиться видаляти його ім'я з усіх списків доступу; втім, ця операція відбувається нечасто.

Списки доступу – винятково гнучкий засіб. З їхньою допомогою легко виконати вимогу про гранулярність прав з точністю до користувача. За допомогою списків нескладно додати права або явно заборонити доступ (наприклад, щоб покарати декількох членів групи користувачів). Безумовно, списки є кращим засобом довільного керування доступом.

Переважна більшість операційних систем і систем керування базами даних реалізує саме довільне керування доступом. Основа перевага довільного керування – гнучкість. Загалом кажучи, для кожної пари «об'єкт-об'єкт-суб'єкт-об'єкт» можна незалежно задавати права доступу (особливо легко це робити, якщо використовуються списки керування доступом). На жаль, у «довільного» підходу є ряд недоліків. Розосередженість керування доступом призводить до того, що довіреними повинні бути багато користувачів, а не тільки системні оператори або адміністратори. Через неуважність або некомпетентність співробітника, що знає секретну інформацію, цю інформацію можуть довідатися і всі інші користувачі. Отже, довільність керування повинна бути доповнена твердим контролем за реалізацією обраної політики безпеки.

Другий недолік, що здається основним, полягає в тому, що права доступу існують окремо від даних. Ніщо не заважає користувачеві, що має доступ до секретної інформації, записати її в доступний всім файл або замінити корисну утиліту її «троянським» аналогом. Подібне «розділення» прав і даних істотно ускладнює проведення декількома системами

погодженої політики безпеки й, головне, робить практично неможливим ефективний контроль узгодженості.

Повертаючись до питання подання матриці доступу, вкажемо, що для цього можна використовувати також функціональний спосіб, коли матрицю не зберігають у явному вигляді, а щораз обчислюють вміст відповідних клітинок. Наприклад, при примусовому керуванні доступом застосовується порівняння міток безпеки суб'єкта та об'єкта.

Зручною надбудовою над засобами логічного керування доступом є обмежувальний інтерфейс, коли користувача позбавляють самої можливості спробувати зробити несанкціоновані дії, внести в число видимих йому об'єктів тільки ті, до яких він має доступ. Подібний підхід звичайно реалізують у межах системи меню (користувачеві показують лише припустимі варіанти вибору) або за допомогою таких обмежувальних оболонок, як restricted shell в ОС Unix.

На закінчення підкреслимо важливість керування доступом не тільки на рівні операційної системи, але й у межах інших сервісів, що входять до складу сучасних додатків, а також, наскільки це можливо, на «стиках» між сервісами. Тут на перший план виходить існування єдиної політики безпеки організації, а також кваліфіковане й погоджене системне адміністрування.

12.6 Рольове керування доступом

При великій кількості користувачів традиційні підсистеми керування доступом стають украй складними для адміністрування. Число зв'язків у них пропорційно добутку кількості користувачів на кількість об'єктів. Необхідні рішення в об'єктно-орієнтованому стилі, здатні ці складнощі понизити.

Таким рішенням є рольове керування доступом (РКД). Суть його в тому, що між користувачами та їхніми привілеями з'являються проміжні сутності – ролі. Для кожного користувача одночасно можуть бути активними кілька ролей, кожна з яких дає йому певні права (рис. 12.2).

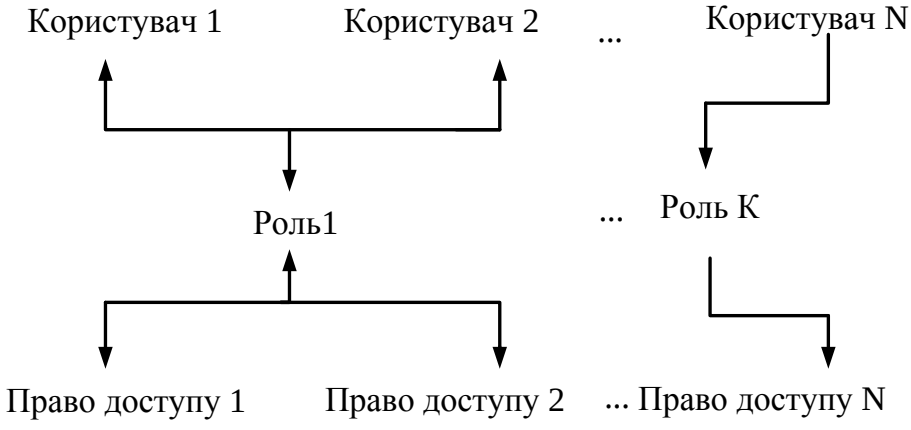


Рисунок 12.2 – Користувачі, об'єкти й ролі

Рольовий доступ нейтральний стосовно конкретних видів прав і способів їхньої перевірки; його можна розглядати як об'єктно-орієнтований каркас, що полегшує адміністрування, оскільки він дозволяє зробити підсистему розмежування доступу керованою при якій завгодно великій кількості користувачів насамперед за рахунок встановлення між ролями зв'язків, аналогічних успадкуванню в об'єктно-орієнтованих системах. Крім того, ролей повинно бути значно менше, ніж користувачів. У результаті число адміністрованих зв'язків стає пропорційним сумі (а не добутку) кількості користувачів й об'єктів.

Рольовий доступ розвивається більше 10 років (сама ідея ролей, зрозуміло, є значно старшою) як на рівні операційних систем, так і у рамках СУБД й інших інформаційних сервісів. Зокрема, існують реалізації рольового доступу для Web-серверів.

У 2001 році Національний інститут стандартів і технологій США запропонував проект стандарту рольового керування доступом (див. http://csrc.nist.gov/rbac/), основні положення якого ми й розглянемо.

Рольове керування доступом оперує такими основними поняттями:

- користувач (людина, інтелектуальний автономний агент і т. п.);
- сеанс роботи користувача;
- роль (звичайно визначається відповідно до організаційної структури);
- об'єкт (сутність, доступ до якої розмежовується; наприклад, файл ОС або таблиця СУБД);
- операція (залежить від об'єкта; для файлів ОС – читання, запис, виконання й т. п.; для таблиць СУБД – вставляння, видалення й т. п., для прикладних об'єктів операції можуть бути більш складними);
- право доступу (дозвіл виконувати певні операції над певними об'єктами).

Ролям приписуються користувачі й права доступу; можна вважати, що вони (ролі) іменують відносини «багато хто до багатьох» між користувачами й правами. Ролі можуть бути приписані багатьом користувачам; один користувач може бути приписаний декільком ролям. Під час сеансу роботи користувача активізується підмножина ролей, яким він приписаний, у результаті чого він стає власником об'єднання прав, приписаних активним ролям. Одночасно користувач може відкрити кілька сеансів.

Між ролями може бути визначене відношення часткового порядку, так зване успадкуванням. Якщо роль r_2 є спадкоємицею r_1, то всі права r_1 приписуються r_2, а всі користувачі r_2 приписуються r_1. Очевидно, що успадкування ролей відповідає успадкуванню класів в об'єктно-орієнтованому програмуванні, тільки правам доступу відповідають методи класів, а користувачам – об'єкти (екземпляри) класів.

Відношення успадкування є ієрархічним, причому права доступу й користувачі поширюються по рівнях ієрархії назустріч один одному. У

загальному випадку успадкування є множинним, тобто в однієї ролі може бути кілька попередниць (і, природно, декілька спадкоємиць, яких ми будемо називати також спадкоємицями).

Можна уявити собі формування ієрархії ролей, починаючи з мінімуму прав (і максимуму користувачів), приписуваних ролі «співробітник», з поступовим уточненням складу користувачів і додаванням прав (ролі «системний адміністратор», «бухгалтер» і т. п.), аж до ролі «керівник» (що, втім, не означає, що керівникові надаються необмежені права; як й іншим ролям, відповідно до принципу мінімізації привілеїв, цій ролі доцільно дозволити тільки те, що необхідно для виконання службових обов'язків). Фрагмент подібної ієрархії ролей показаний на рис. 12.3.

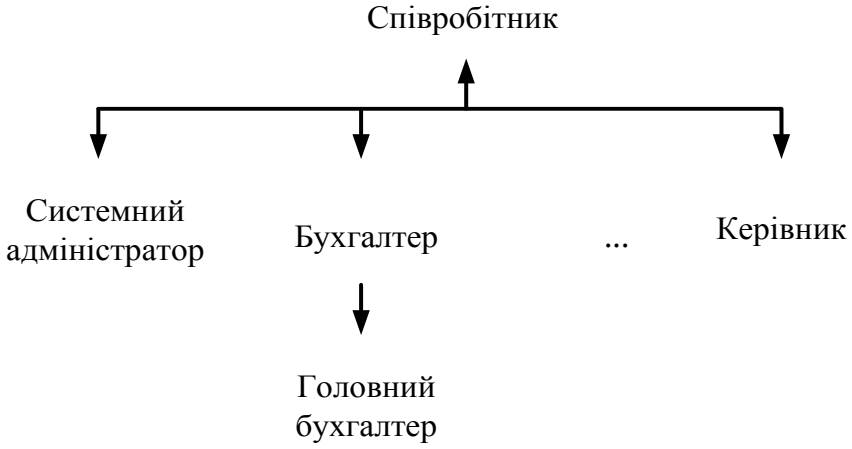


Рисунок 12.3 – Фрагмент ієрархії ролей

Для реалізації ще одного згадуваного раніше важливого принципу інформаційної безпеки вводиться поняття поділу обов'язків, причому у двох виглядах: статичному й динамічному.

Статичний поділ обов'язків накладає обмеження на приписування користувачів ролям. У найпростішому випадку членство в деякій ролі забороняє приписування користувача певній сукупності інших ролей. У загальному випадку дане обмеження задається як пара «безліч ролей – число» (де безліч складається, принаймні, з двох ролей, а число повинно бути більшим 1), так що ніякий користувач не може бути приписаний зазначеному (або більшому) числу ролей з заданої кількості. Наприклад, може існувати п'ять бухгалтерських ролей, але політика безпеки допускає членство не більш ніж у двох таких ролях (тут число дорівнює 3).

При наявності успадкування ролей обмеження набуває більш складного вигляду, але суть залишається простою: при перевірці членства в ролях потрібно враховувати приписування користувачів ролям-спадкоємицям.

Динамічний поділ обов'язків відрізняється від статичного тільки тим, що розглядаються ролі, одночасно активні (у різних сеансах) для даного користувача (а не ті, котрим користувач статично приписаний). Наприклад,

один користувач може відігравати роль і касира, і контролера, але не одночасно; щоб стати контролером, він повинен спочатку закрити касу. Тим самим реалізується так зване тимчасове обмеження довіри, що є аспектом мінімізації привілеїв.

Розглянутий проект стандарту містить специфікації трьох категорій функцій, необхідних для адміністрування РКД.

1. **Адміністративні функції** (створення й супровід ролей та інших атрибутів рольового доступу): створити/видалити роль/користувача, приписати користувача/право ролі або ліквідувати існуючу асоціацію, створити/видалити відношення успадкування між існуючими ролями, створити нову роль і зробити її спадкоємицею/попередницею існуючої ролі, створити/видалити обмеження для статичного/динамічного поділу обов'язків.

2. **Допоміжні функції** (обслуговування сеансів роботи користувачів): відкрити сеанс роботи користувача з активацією якого мається на увазі набір ролей; активувати нову роль, деактивувати роль; перевірити правомірність доступу.

3. **Інформаційні функції** (одержання відомостей про поточну конфігурацію з урахуванням відносин успадкування). Тут проводиться поділ на обов'язкові й необов'язкові функції. До числа перших належить одержання списку користувачів, приписаних ролі, і списку ролей, яким приписаний користувач.

Усі інші функції віднесені до розряду необов'язкових. Це одержання інформації про права, які приписані ролі, про права заданого користувача (які він має як член певної сукупності), про активні на даний момент сеансу ролі і права, про операції, які роль/користувач правочинен зробити з заданим об'єктом, про статичний/динамічний розподіл обов'язків.

Можна сподіватися, що запропонований стандарт допоможе сформувати єдину термінологію й, що більш важливо, дозволить оцінювати РУД-продукти з єдиних позицій, за єдиною шкалою.

12.7 Керування доступом в Java-середовищі

Java – це об'єктно-орієнтована система програмування, тому й керування доступом у ній спроектовано й реалізовано в об'єктному стилі. Із цієї причини розглянути Java-середовище для нас дуже важливо. Докладно про Java-технологію й безпеку Java-середовища розказано в статті А. Таранова й В. Цишевского «Java у три роки» (Jet Info, 1998, 11-12). З дозволу авторів далі використовуються її фрагменти.

Насамперед, зупинимося на еволюції моделі безпеки Java. В JDK 1.0 була запропонована концепція «пісочниці» (sandbox) – замкненого середовища, – у якій виконуються потенційно ненадійні програми (апплети, що надійшли по мережі). Програми, що розташовуються на

локальному комп'ютері, вважалися абсолютно надійними, і їм було доступно все, що доступно віртуальній Java-машині.

У число обмежень, що накладаються «пісочницею», входить заборона на доступ до локальної файлової системи, на мережеву взаємодію з усіма хостами, крім джерела апплета, і т. п. Незалежно від рівня безпеки, що досягається при цьому, (а проблеми виникали й з розподілом свій/чужий, і з визначенням джерела апплета), накладені обмеження варто визнати занадто обтяжливими: можливості для змістовних дій в апплетів майже не залишається.

Щоб упоратися з цією проблемою, в JDK 1.1 увели розподіл джерел (точніше, розповсюджувачів) апплетів на надійні та ненадійні (джерело визначалося за електронним підписом). Надійні апплети прирівнювалися в правах до «рідного» коду. Зроблене послаблення вирішило проблеми тих, кому прав не вистачало, але захист залишився неешелонованим й, отже, неповним.

В JDK 1.2 сформувалася модель безпеки, використовувана й в Java 2. Від моделі «пісочниці» відмовилися. Сформувалися три основні поняття:

- джерело програми;
- право й сукупність;
- політика безпеки.

Джерело програми визначається парою (URL, розповсюджувачі програми). Останні задаються набором цифрових сертифікатів.

Право – це абстрактне поняття, згідно з яким, як і прийнято в об'єктному середовищі, стоять класи й об'єкти. У більшості випадків право визначається двома ланцюжками символів – ім'ям ресурсу й дією. Наприклад, ресурсом може виступати файл, а дією – читання. Найважливішим методом «правових» об'єктів є implies. Він перевіряє, чи витікає одне право (запитуване) з іншого (наявного).

Політика безпеки задає відповідність між джерелом і правами програм, що надійшли з нього (формально можна вважати, що кожному джерелу відповідає своя «пісочниця»). В JDK 1.2 «рідні» програми не мають яких-небудь привілеїв у плані безпеки, і політика стосовно них може бути будь-якою. У результаті вийшов традиційний для сучасних ОС і СУБД механізм прав доступу з такими особливостями:

- Java-програми виступають не від імені користувача, що їх запустив, а від імені джерела програми. (Це досить глибоке й прогресивне трактування, якщо його правильно розвинути);
- немає поняття власника ресурсів, що міг би змінювати права; останні задаються винятково політикою безпеки (формально можна вважати, що власником усього є той, хто формує політику);
- механізми безпеки забезпечені об'єктною обгорткою.

Досить важливим поняттям у моделі безпеки JDK. 1.2 є контекст виконання. Коли віртуальна Java-машина перевіряє права доступу об'єкта до системного ресурсу, вона розглядає не тільки поточний об'єкт, але й

попередні елементи стека викликів. Доступ надається тільки тоді, коли потрібне право мають усі об’єкти в стекові. Розробники Java називають це реалізацією принципу мінімізації привілеїв.

На перший погляд, врахування контексту вважається логічним. Не можна допускати, щоб виклик якого-небудь методу розширював права доступу хоча б з тієї причини, що доступ до системних ресурсів здійснюється не прямо, а за допомогою системних об’єктів, що мають усі права.

На жаль, подібні твердження суперечать одному з основних принципів об’єктного підходу – принципу інкапсуляції. Якщо об’єкт А звертається до об’єкта В, він не може й не повинен знати, як реалізований У і якими ресурсами він користується для своїх цілей. Якщо А має право викликати який-небудь метод У з певним значенням аргументів, У зобов’язаний обслужити виклик. В іншому випадку при формуванні політики безпеки доведеться враховувати можливий перелік викликів об’єктів, що, звичайно ж, нереально.

Розробники Java усвідомлювали цю проблему. Щоб упоратися з нею, вони ввели поняття привілейованого інтервалу програми. При виконанні такого інтервалу контекст ігнорується. Привілейована програма відповідає за себе, не цікавлячись передісторією. Аналогом привілейованих програм є файли з бітами перевстановлення ідентифікатора користувача/групи в ОС Unix, що зайвий раз підтверджує традиційність підходу, реалізованого в JDK 1.2. Відомі загрози безпеки, які привносять подібні файли. Тепер цей не найкращий засіб ОС Unix перейшов до Java.

12.8 Можливий підхід до керування доступом у розподіленому об’єктному середовищі

Вважається, що на сьогодні проблема керування доступом існує в трьох майже не пов’язаних між собою проявах:

- традиційні моделі (дискреційна й мандатна);
- модель «пісочниця» (запропонована для Java-середовища й близької їй системі Safe-Tel);
- модель фільтрації (використана в міжмережевих екранах).

На наш погляд, необхідно об’єднати існуючі підходи на основі їхнього розвитку й узагальнення.

Формальна постановка завдання розмежування доступу може виглядати в такий спосіб.

Розглядається сукупність об’єктів (у сенсі об’єктно-орієнтованого програмування). Частина об’єктів може бути контейнерами, що групують об’єкти-компоненти, які задають для них загальний контекст та виконують загальні функції й реалізують перебір компонентів. Контейнери або вкладені один у одного, або не мають загальних компонентів.

З кожним об’єктом асоційований набір інтерфейсів, забезпечених дескрипторами (ДЕ). До об’єкта можна звернутися тільки за допомогою ДЕ. Різні інтерфейси можуть надавати різні методи й бути доступними для різних об’єктів.

Кожен контейнер дозволяє опитати набір ДЕ об’єктів-компонентів, що задовольняють деяку умову. Результат, що повертається, у загальному випадку залежить від зухвалого об’єкта.

Об’єкти ізольовані один від одного. Єдиним видом міжоб’єктної взаємодії є виклик методу.

Передбачається, що використовуються надійні засоби аутентифікації й захисту комунікацій. У плані розмежування доступу локальні й вилучені виклики не розрізняються.

Передбачається також, що дозвіл або заборона на доступ не залежать від можливого паралельного виконання методів (синхронізація є окремою проблемою, що тут не розглядається).

Розмежовується доступ до інтерфейсів об’єктів, а також до методів об’єктів (з урахуванням значень фактичних параметрів виклику). Правила розмежування доступу (ПРД) задаються у вигляді предикатів над об’єктами.

Розглядається завдання розмежування доступу для виділеного контейнера СС, компонентами якого повинні бути зухвалий й/або викликуваний об’єкти. ДЕ цього контейнера є загальновідомим. Уважається також, що між зовнішніми, стосовно виділеного контейнера, об’єктами можливі будь-які виклики.

Виконання ПРД контролюється монітором обігів.

При виклику методу ми будемо розділяти дії, вироблені зухвалим об’єктом (ініціація виклику) і викликуваним методом (прийом і завершення виклику).

При ініціації виклику може вироблятися перетворення ДЕ фактичних параметрів до вигляду, доступного викликуваному методу («трансляція інтерфейсу»). Трансляція може мати місце, якщо викликуваний об’єкт не входить у той же контейнер, що й зухвалий.

Параметри методів можуть бути вхідними й/або вихідними. При прийомі виклику виникає інформаційний потік із вхідних параметрів у викликуваний об’єкт. У момент завершення виклику виникає інформаційний потік з викликуваного об’єкта у вихідні параметри. Ці потоки можуть фігурувати в правилах розмежування доступу.

Структуруємо сукупність всіх ПРД, виділивши чотири групи правил:

- політика безпеки контейнера;
- обмеження на викликуваний метод;
- обмеження на зухвалий метод;
- обмеження, що їх накладають добровільно.

Правила, загальні для всіх об’єктів, що входять у контейнер З, назвемо політикою безпеки даного контейнера.

Нехай метод M_1 об'єкта O_1 у точці P_1 свого виконання повинен викликати метод M об'єкта O. Правила, які повинен задовольняти M, можна розділити на чотири підгрупи:

- правила, що описують вимоги до формальних параметрів виклику;
- правила, що описують вимоги до семантики M;
- реалізаційні правила, що накладають обмеження на можливі реалізації M;
- правила, що накладають обмеження на викликуваний об'єкт O.

Метод M об'єкта O, потенційно доступний для виклику, може висувати до зухвалого об'єкта такі групи вимог:

- правила, що описують вимоги до фактичних параметрів виклику;
- правила, що накладають обмеження на зухвалий об'єкт.

Можна виділити три різновиди предикатів, що відповідають семантиці й/або особливостям реалізації методів:

- твердження про фактичні параметри виклику методу M у точці P_1;
- предикат, що описує семантику методу M;
- предикат, що описує особливості реалізації методу M.

Перераховані обмеження можна назвати добровільними, оскільки вони відповідають реальній поведінці об'єктів і не пов'язані з якими-небудь зовнішніми вимогами.

Запропонована постановка завдання розмежування доступу відповідає сучасному етапу розвитку програмування, вона дозволяє відобразити найскладнішу політику безпеки, знайти баланс між багатством виразних можливостей й ефективністю роботи монітора обігів.

Запитання для самоконтролю

1. Ідентифікація й аутентифікація. Керування доступом.
2. Що використовується як аутентифікатор в мережевому середовищі?
3. Парольна аутентифікація.
4. Заходи, які дозволяють підвищити надійність парольного захисту.
5. Одноразові паролі.
6. Основні поняття рольового керування доступом.
7. Що собою являє Internet-стандарт (RFC 1938)?
8. Основні поняття керування доступом.
9. Ідентифікація/аутентифікація за допомогою біометричних даних.
10. Керування доступом. Основні поняття.
11. Рольове керування доступом.
12. Які засоби об'єктно-орієнтованого підходу використовує рольове керування доступом?
13. Основні поняття рольового керування доступом.
14. Назвіть категорії функцій, необхідних для адміністрування РКД.
15. Керування доступом в Java-середовищі.
16. Особливості механізму прав доступу.

ГЛАВА 13
ВИБІР ЗАСОБІВ БЕЗПЕКИ

Настанову з вибору засобів безпеки застосовують тоді, коли приймають рішення про вибір засобів безпеки інформаційної системи:

– відповідно до типу і характеристик інформаційної системи;

– відповідно до загального оцінювання загроз та наявних потреб безпеки;

– відповідно до результатів детального аналізу ризиків.

Перехресні посилання зроблені для того, щоб показати, де вибір засобів безпеки може бути підтриманий використанням загальнодоступних довідників, що містять опис засобів безпеки (ДСТУ ISO/IEC TR 13335-4:2005).

13.1 Вступ до вибору засобів безпеки та концепція базової безпеки

При виборі засобів безпеки з використанням концепції базової безпеки використовуються два головних підходи до вибору засобів безпеки, а саме: використання базового підходу та проведення детального дослідження ризиків.

Проведення детального аналізу ризику має ту перевагу, що досягається повна картина ризиків. Це необхідно для вибору тих засобів безпеки, що зумовлені ризиками і, відповідно, мають бути реалізовані. Це запобігає забезпеченню занадто великої чи занадто малої безпеки. Оскільки цей підхід може вимагати значної кількості часу, зусиль та кваліфікації, він найбільш підходить для інформаційних систем з високим ризиком, тоді як простіший підхід може виявитись достатнім для систем з низьким рівнем ризику. Використання високорівневого аналізу ризиків може визначити системи з низьким рівнем ризику. Цей високорівневий аналіз ризиків не потребує формалізованого чи складного процесу. Засоби захисту для систем з низьким рівнем ризику можуть бути обрані шляхом застосування базової безпеки. Базова безпека забезпечує мінімальний рівень безпеки, визначений організацією для кожного типу інформаційної технології системи. Цей рівень базової безпеки досягається реалізацією мінімального набору засобів безпеки, що відомі як базові засоби.

Внаслідок відмінностей в процесі вибору засобів безпеки в цьому розділі розглядають два різні шляхи застосування базового підходу:

– використання базового підходу, в якому засоби безпеки рекомендовано вибирати відповідно до типу та характеристик інформаційної технології розглядуваної системи;

– використання базового підходу, в якому засоби безпеки рекомендовано вибирати відповідно до проблем та загроз безпеки, також враховувати і розглядувану систему.

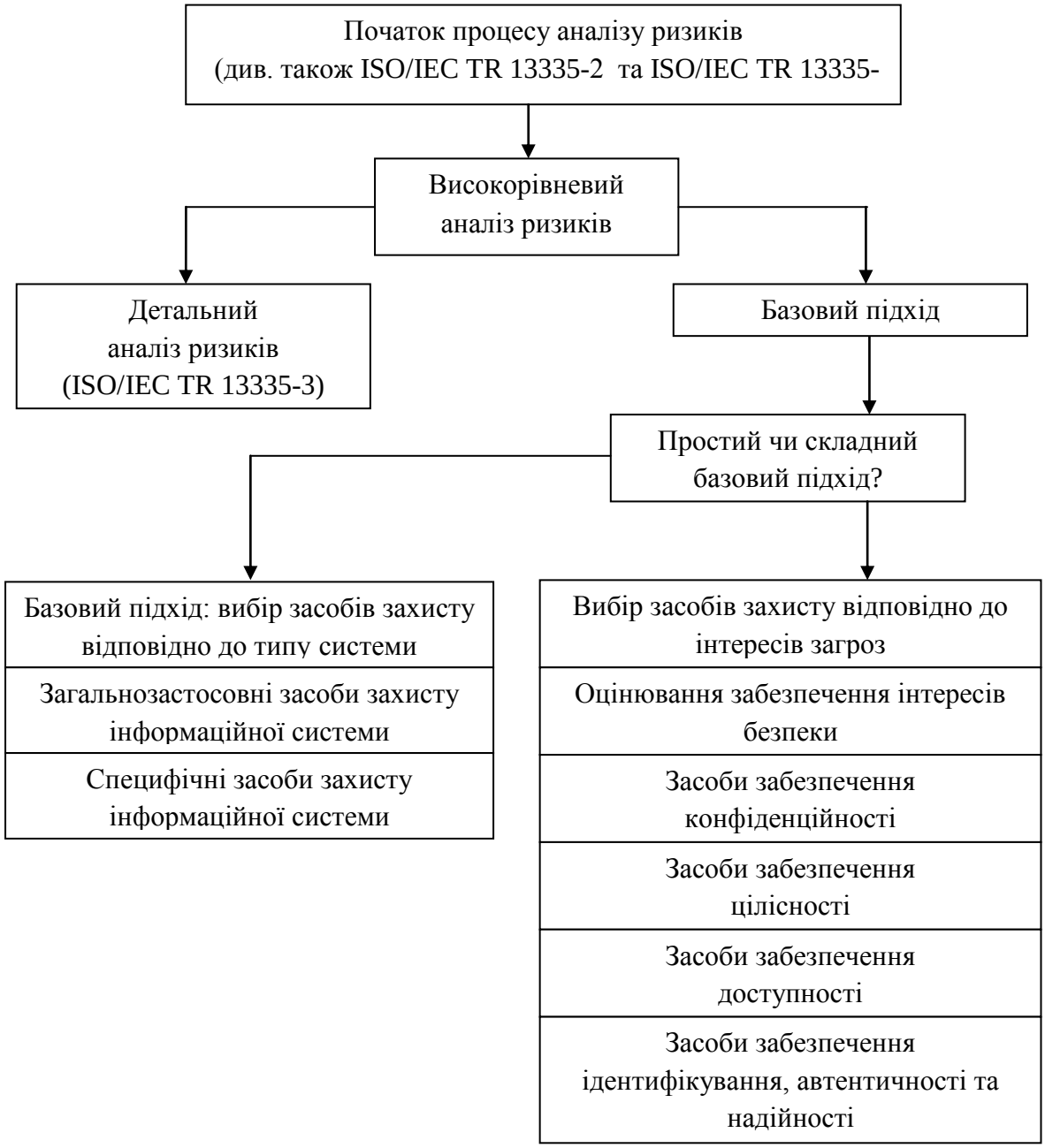


Рисунок 13.1 – Способи вибору засобів безпеки

Базовий підхід треба вибирати відповідно до ресурсів, які можуть бути витрачені у процесі вибору усвідомлених проблем безпеки, а також типу і характеристик інформаційної розглядуваної системи. Якщо організація не бажає витрачати багато часу та зусиль на вибір засобів безпеки (з будь-якої причини), то можна скористатися базовим підходом, що пропонує засоби безпеки без подальшого оцінювання. Однак якщо ділові процеси організації до певної міри залежать від інформаційної системи чи послуг та (або) оброблювана інформація контрольована, то дуже ймовірно, що будуть необхідні додаткові засоби безпеки. В цьому випадку наполегливо рекомендується проводити високорівневий огляд важливості інформації та

можливих загроз для того, щоб мати краще уявлення про засоби безпеки, потрібні для найефективнішої безпеки інформаційної системи. Якщо ділові процеси організації суттєво залежать від інформаційної системи чи послуг, а (або) оброблювана інформація є дуже чутливою, ризики можуть бути високі, і детальний аналіз ризиків є найкращим шляхом визначення прийнятних засобів безпеки.

Специфічні засоби безпеки повинні призначатися на основі детального аналізу ризиків, якщо:

– діяльність чи потреби безпеки не відповідають рішенням, запропонованим у цих розділах;

– детальніше оцінювання є виправданим у разі потенційно високих ризиків, чи важливості інформаційної системи для діяльності організації.

Треба зазначити, що навіть коли виконаний детальний аналіз ризиків, все ще доцільно застосувати до системи базові засоби безпеки.

Перше рішення, яке повинна ухвалити організація, – використовувати базовий підхід сам по собі чи як частину більш повної стратегії аналізу ризиків. У разі прийняття цього рішення треба зазначити, що під час використання базового підходу самого по собі результатний процес вибору засобів безпеки може дати менш оптимізовану безпеку, ніж прийнята ширша стратегія аналізу ризиків. Однак менші кошти та ресурси, необхідні для вибору засобів забезпечення безпеки та досягнення, принаймні, мінімального рівня безпеки для всіх інформаційних систем, можуть бути причинами для прийняття рішення про використання тільки базового підходу.

Базова безпека для інформаційної системи може бути досягнута через визначення та застосування набору відповідних засобів безпеки, що є прийнятним за обставин наявності низького ризику, тобто вони задовольняють, принаймні, мінімальні потреби безпеки. Наприклад, прийнятні засоби безпеки можуть бути визначені через каталоги, що містять набори засобів безпеки від більшості загальних загроз для різних типів інформаційних технологій. Ці каталоги засобів безпеки містять інформацію про категорії засобів безпеки чи про окремі засоби, але загалом не зазначають, які засоби безпеки треба застосовувати в конкретних обставинах. Можливо, якщо інформаційні системи організації (чи частини організації) є дуже схожі за природою та послугами, які вони надають, засоби безпеки, вибрані за базовим підходом, можуть бути застосовані до всіх систем інформаційних технологій. На рис. 13.2 показано різні способи використання базового підходу.

Якщо організація вирішує впровадити базову безпеку до організації в цілому або її підрозділів, необхідно вирішити, для яких підрозділів організації прийнятні засоби безпеки, і який рівень безпеки повинен забезпечувати цей захист. У більшості випадків, коли використовують базову безпеку, не застосовують менший рівень безпеки, доки не будуть реалізовані додаткові засоби безпеки, обґрунтовані та необхідні для

керування середніми й великими ризиками. Як альтернативу базова безпека може визначити середній рівень для організації, тобто дозволяються винятки вище і нижче базового рівня, якщо вони були обґрунтовані, наприклад, результатами аналізу ризиків.

Однією з переваг базової безпеки є те, що її застосовують до груп інформаційних систем, і всюди в цій групі можна покладатися на певний рівень безпеки. В цих умовах зазвичай найкориснішим є розробити і вести базовий каталог засобів безпеки в межах організації чи відділу.

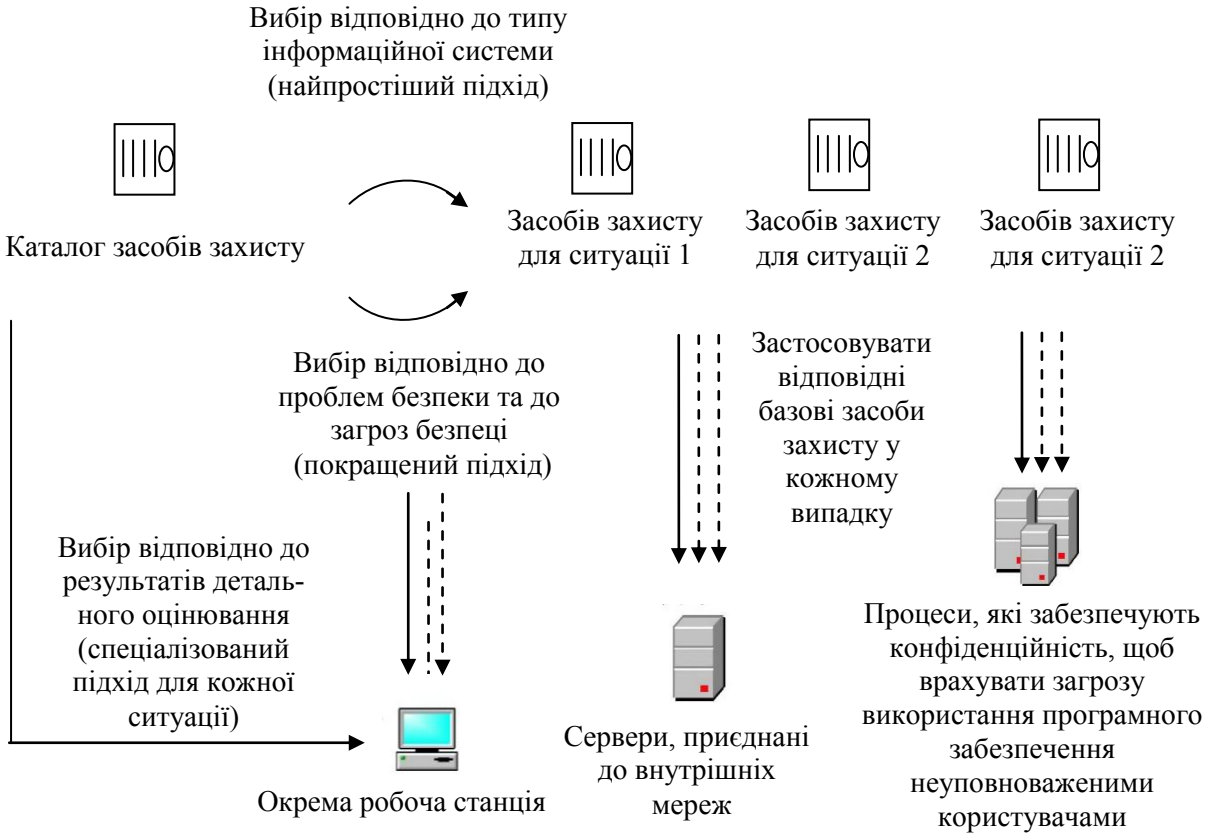


Рисунок 13.2 – Базове оцінювання під час вибору засобів безпеки

13.2 Базове оцінювання

Процес вибору засобів безпеки завжди потребує певного знання типу та характеристик розглядуваної інформаційної системи (наприклад, окрема робоча станція або робоча станція, під'єднана до мережі), оскільки це суттєво впливає на вибрані засоби безпеки. Корисно мати інфраструктури, які містять будівлі, кімнати тощо. Інший важливий чинник, пов'язаний з вибором засобів безпеки, – це оцінювання наявних і (або) запланованих засобів безпеки. Це звільняє від зайвої роботи та марнування часу, зусиль та коштів. Тому настійно рекомендується оцінювання використовувати як основу для вибору засобів безпеки. Коли вибирають засоби безпеки, потрібно брати до уваги вимоги бізнесу та підхід організації до безпеки. Нарешті, необхідно визначити, чи надають ці результати оцінювання

достатньо інформації для вибору базових засобів безпеки, чи необхідне детальніше оцінювання або детальний аналіз ризиків.

Визначання типу інформаційної системи

Для оцінювання наявної чи запланованої інформаційної системи її треба порівняти з нижченаведеними компонентами та визначити складники, визначальні для системи. Компоненти для вибору такі:

– окрема робоча станція;

– робоча станція (клієнт без спільних ресурсів), під'єднана до мережі;

– сервер чи робоча станція зі спільними ресурсами, під'єднана до мережі.

Визначення фізичних умов та умов навколишнього середовища

Оцінювання оточення охоплює визначання фізичної інфраструктури, що підтримує наявну чи заплановану інформаційну систему так само, як і пов'язані з нею наявні та (або) заплановані засоби безпеки. Оскільки всі засоби безпеки мають бути сумісними з навколишнім середовищем, оцінки є істотними для успішного вибору. Нижченаведені питання можуть надати допомогу під час дослідження інфраструктури. Повинен також враховуватися вплив навколишнього середовища та будь-які інші обставини.

Розташування та будівля:

– де розташована будівля – на своїй власній ділянці з огорожею по периметру, чи на вулиці і в місці з інтенсивним рухом транспорту тощо?

– будівля зайнята однією організацією чи багатьма?

– якщо будівля зайнята багатьма організаціями, то хто ці мешканці?

– де знаходяться зони безпеки?

Керування доступом:

– хто має доступ до будівлі?

– чи є система керування фізичним доступом?

– наскільки міцна конструкція будівлі?

– наскільки міцні двері, вікна тощо та як вони захищені?

– чи охороняється будівля, якщо так, то цілодобово чи тільки протягом робочого часу?

– чи є в будівлі та (або) кімнаті, в якій розташоване критичне інформаційне обладнання, сигналізація для безпеки від вторгнень?

Безпека на місці:

– як захищається кімната (кімнати), що містить інформаційну систему?

– яка система виявлення пожежі, сигналізація та система гасіння встановлені, та де вони знаходяться?

– яка система виявлення витоку води/рідини, можливості її виведення та сигналізації?

– чи є такі допоміжні засоби, як система безперебійного живлення, водопровід та кондиціювання повітря (для контролю температури та вологості)?

Відповідаючи на ці питання, можна легше виявити наявні фізичні та пов’язані з ними засоби безпеки. Варто відмітити, що під час дослідження місцезнаходження будівлі необхідно одночасно з’ясувати все, що стосується дверей, замків та контролю і порядку фізичного доступу; ця процедура не займає багато часу.

Оцінювання наявних/планованих засобів безпеки

Після оцінювання умов навколишнього середовища та компонентів інформаційної системи треба визначити всі інші засоби безпеки: вже наявні та заплановані. Це необхідно, щоб уникнути повторного вибору наявних чи запланованих засобів, а знання цих засобів безпеки допомагає вибрати інші засоби, що будуть діяти разом з ними. Коли вибирають засоби безпеки, треба розглядати сумісність наявних засобів безпеки з вибраними. Засіб безпеки може бути несумісним з іншими засобами безпеки чи унеможливлюватиме успішну діяльність та безпеку.

Для визначення наявних чи планованих засобів безпеки можуть бути корисними такі дії:

– перегляньте документи, що містять інформацію про засоби безпеки (наприклад, плани чи концепції інформаційної безпеки); якщо процес убезпечення добре документований, всі наявні чи заплановані засоби та статус їхньої реалізації повинні бути там перераховані;

– перевірте з відповідальними особами (наприклад, керівник інформаційної безпеки, управитель будинком чи директор-розпорядник) та користувачами, які засоби безпеки дійсно реалізовані для розглядуваної інформаційної системи;

– продивіться схему розташування засобів безпеки в будівлі, порівняйте запроваджені засоби безпеки зі списком тих, що мають бути, та перевірте як запроваджено засоби безпеки, чи працюють вони коректно та ефективно.

Може бути виявлено, що наявні засоби безпеки перевищують поточні потреби. В цьому випадку треба розглянути можливість видалення цих засобів. Якщо розглядати вилучення надлишкових засобів чи засобів, що не є необхідними, треба взяти до уваги чинники безпеки та вартості. Оскільки засоби безпеки впливають один на одного, видалення надлишкових засобів може зменшити загальну безпеку. Треба зазначити, що іноді дешевше залишити ці засоби на місці, ніж вилучати їх, або, особливо якщо засоби безпеки мають високу вартість обслуговування, дешевше вилучити їх.

13.3 Засоби безпеки

Огляд засобів безпеки, які можна реалізувати для підвищення безпеки

Деякі з цих засобів є механізмами, інші можуть розглядатися, як процедури, яких потрібно дотримуватись. Організаційні та фізичні засоби, що можуть бути застосовані в інформаційних системах. Засоби безпеки,

специфічні для окремих інформаційних технологій систем. Треба зазначити, що засоби безпеки описані незалежно від способу, яким вони можуть бути вибрані, тобто, деякі з цих засобів безпеки можуть бути вибрані одним способом, інші можуть бути визначені тільки після проведення детального аналізу ризиків.

Для полегшення опису різних типів засобів безпеки вводяться категорії цих засобів.

Керування інформаційною безпекою та політика безпеки

Ця категорія засобів безпеки містить всі ті засоби, що стосуються керування інформаційною безпекою, планування якої повинно містити відповідальність за ці процеси та іншу діяльність, що стосується безпеки. Мета цих засобів безпеки – досягнути прийнятного рівня безпеки в організації.

Політика інформаційної безпеки

Треба розробити письмовий документ, який має містити правила, вказівки та практичні рекомендації з керування цінностями, їхній захист і поширення в організації. Він повинен містити відомості про необхідність документів з інформаційної безпеки та настанову щодо їх змісту.

Політика безпеки інформаційної системи

Для кожної інформаційної системи має бути розроблена політика її безпеки, що описує засоби захисту, які існують чи мають бути реалізовані. Також вона повинна містити процедури, що стосуються безпеки цієї системи, також, за потреби, виклад проблем безпеки та (або) ризиків, що обґрунтовують засоби безпеки.

Керування інформаційною безпекою

Керування інформаційною безпекою має бути формалізованим та скоординованим у межах організації відповідно до її розміру, наприклад, заснуванням комітету інформаційної безпеки та призначенням особи (часто керівник інформаційної безпеки), відповідальної за безпеку кожної інформаційної системи.

Розподіл обов'язків

Обов'язки стосовно інформаційної безпеки організації повинні бути чітко задокументовані та розподілені відповідно до політики інформаційної безпеки та політики безпеки інформаційної системи.

Організація інформаційної безпеки

Всі ділові процеси, що можуть підтримати інформаційну безпеку (наприклад, закупки, співробітництво з іншими організаціями), повинні бути організовані так, щоб надійно забезпечити цю підтримку.

Визначення і оцінювання цінностей

Мають бути визначені всі цінності в організації та в інформаційно-технологічній системі і оцінене їхнє значення для ведення бізнесу.

Затвердження інформаційних систем

Затвердження інформаційних систем повинно відбуватися відповідно до політики інформаційної безпеки. Процес затвердження має метою

виявити, чи реалізовані засоби безпеки дійсно забезпечують відповідний рівень безпеки. Треба брати до уваги, що інформаційна система може охоплювати мережі та основні засоби зв'язку.

Перевірка узгодженості безпеки

Важливо, щоб підтримувалась узгодженість з усіма необхідними засобами безпеки, законами, правилами та нормами, оскільки будь-який засіб безпеки, правило чи політика можуть працювати до тих пір, поки користувачі їх застосовують, а системи узгоджуються з ними. Засоби захисту в цій сфері наведено нижче:

– узгодженість з політикою інформаційної безпеки та засобами безпеки. Треба проводити регулярні перевірки для гарантування того, що всі засоби безпеки, впроваджені на місці, як зазначено в політиці безпеки та інших важливих документах, наприклад, документах процедур безпеки та надзвичайних планах, реалізовані коректно і використовуються коректно та ефективно (кінцевими користувачами також), також, за необхідності, проведено тестування;

– узгодженість з правовими та регуляторними вимогами. Перевірки узгодженості, згадані вище, повинні підтвердити, що виконуються всі правові та регуляторні вимоги в країні, чи країнах, де задіяна інформаційна система; там, де це законодавство охоплює питання безпеки та недоторканності даних, копіювання програмного забезпечення, безпеки записів, що ведуться в організації, зловмисного використання інформаційних систем чи криптографії.

Реагування на порушення

Кожен в організації має бути обізнаним з необхідністю звітувати про порушення безпеки, в тому числі і збої програмного забезпечення та виявлену недосконаліть так швидко, як це можливо. Організація повинна забезпечити схему звітування, яка зробить це можливим. Реагування на порушення містить:

– звітування про порушення безпеки. Кожен працівник повинен усвідомлювати, що він зобов'язаний звітувати про порушення безпеки. Інструментальні засоби також можуть визначати порушення та звітувати про них. Для полегшення ефективного реагування на порушення організація повинна впровадити схему звітування та точки контакту в організації;

– звітування про недосконаліть безпеки. Якщо користувачі помічають будь-яку недосконаліть системи, що стосується безпеки, вони повинні повідомити про неї відповідальну особу так швидко, наскільки це можливо;

– звітування про збої програмного забезпечення. Якщо користувачі помічають будь-які збої програмного забезпечення, що стосуються безпеки, вони повинні звітувати про них відповідальній особі так швидко, наскільки це можливо;

– керування інцидентами. Має бути процес керування, що забезпечує захист від інцидентів, їх виявлення та звітування, відповідне реагування на інцидент. Інформація про порушення повинна збиратися і оцінюватись, щоб унеможливити інциденти в майбутньому та зменшити збитки від них.

Персонал

Засоби безпеки в цій категорії повинні зменшувати ризики безпеки, що виникають від помилок або зловмисного чи незловмисного порушення правил безпеки персоналом (який працює постійно чи тимчасово). Засоби безпеки в цій сфері наведено нижче:

– засоби безпеки для постійного та тимчасового штату. Всі працівники мають знати свої обов'язки щодо безпеки. Усі процедури стосовно безпеки, яких слід дотримуватись персоналу, мають бути сформульовані у документі. Працівників треба перевіряти перед влаштуванням на роботу, та, за потреби, підписувати договір про нерозголошення інформації;

– засоби безпеки для договірного персоналу. Договірний персонал (наприклад, прибиральниці чи найманий персонал) треба контролювати так само, як інших відвідувачів. Договірний, звичайно довгостроковий, персонал повинен підписувати договір про нерозголошення перед тим, як отримає доступ (фізичний чи логічний) до інформаційних систем організації;

– обізнаність у питаннях безпеки та навчання. Для підтримання поінформованості весь персонал, що використовує, розробляє, підтримує чи має доступ до інформаційних систем, повинен отримувати регулярні інструкції та інші матеріали. Це має забезпечити персоналу розуміння важливості для бізнесу оброблюваної інформації, пов'язаних з нею загроз, ризиків тощо, і, отже, розуміння того, для чого потрібні засоби безпеки. Користувачі також мають бути навчені використовувати обладнання коректно, щоб унеможливити помилки. Для вибраного персоналу, наприклад, керівників інформаційної безпеки, адміністраторів безпеки, можливо, необхідне більш специфічне навчання безпеці;

– дисциплінарний процес. Всі працівники повинні знати про наслідки порушень (зловмисних чи незловмисних) політики безпеки організації в цілому та політик безпеки окремих інформаційних систем, або будь-яких інших задокументованих домовленостей, пов'язаних з безпекою.

Питання експлуатації

Засоби безпеки в цій сфері охоплюють процедури підтримання безпечного, правильного та надійного функціонування інформаційних систем та пов'язаних з цим систем. Більшість цих засобів безпеки може бути реалізована шляхом запровадження організаційних процедур. Експлуатаційні засоби безпеки треба запроваджувати в поєднанні з іншими, наприклад, фізичними та технічними засобами. Засоби безпеки в сфері питань експлуатації наведено нижче:

– керування конфігурацією та змінами. Керування конфігурацією – це процес відстежування змін інформаційних систем. Основна його мета

щодо безпеки – переконатися, що ці зміни в інформаційних технологічних системах не зменшують ефективність засобів захисту та безпеки в цілому. Керування змінами може сприяти визначенню нових включень засобів безпеки, коли трапляються зміни в інформаційних технологічних системах;

– керування навантаженнями. Керування навантаженнями треба використовувати, щоб уникнути збоїв через неадекватні потужності. Коли оцінюються необхідні навантаження для інформаційної системи, треба брати майбутні навантаження та поточні тенденції;

– документація. Всі аспекти конфігурацій та діяльності інформаційних технологій систем повинні документуватися для забезпечення неперервності та стабільності. Безпеку інформаційної системи також треба документувати в частині політики безпеки інформаційної системи, в документах процедур безпеки та звітах і планах, що стосуються стратегії забезпечення неперервності бізнесу. Документація має бути актуалізованою та доступною;

– обслуговування. Інформаційні системи потрібно правильно обслуговувати для забезпечення постійної надійності, доступності та цілісності. Всі вимоги безпеки, що мають задовольнятись постачальниками обслуговування, повинні бути повністю задокументовані в договорах на обслуговування. Обслуговування треба виконувати відповідно до договору з постачальником та тільки уповноваженим персоналом;

– відстеження змін, що стосуються безпеки. Зміни впливів, загроз, вразливостей та ризиків, а також їхніх характеристик треба відстежувати. Відстежування має охоплювати як нові, так і старі аспекти. Стан навколишнього середовища, в якому розташована система, також треба відстежувати;

– результати аудиту та ведення журналів. Можливості аудиту та ведення журналів серверів (наприклад, записування результатів аудиту та засоби аналізу), мереж (наприклад, засоби аудиту брандмауерів та маршрутизаторів) і програмного забезпечення (наприклад, засоби аудиту програм обміну повідомленнями чи програм оброблення транзакцій) потрібно використовувати для запису деталей подій, що стосуються безпеки. Вони охоплюють деталі подій, визнаних неповноважними чи помилковими, а також деталі звичайних подій, що мають бути проаналізовані пізніше. Результати аудиту та журнали необхідно регулярно переглядати для виявлення неповноважних дій, що дозволить приймати відповідні коригувальні заходи. Події, записані в журналах, треба аналізувати також з метою виявлення повторення схожих подій, що можуть вказувати на наявність вразливостей чи загроз, засоби безпеки від яких є неадекватними. Такий аналіз може також виявити закономірності в непов’язаних, на перший погляд, подіях, що може дозволити ідентифікувати людей, які виконують неповноважні дії, чи причину проблеми з безпекою.

Примітка. В тексті «можливості аудиту» систем та програмного забезпечення, а також «можливості ведення журналі обліку» використовують для позначення одного й того ж. Доки такі можливості можна використовувати для підтримування аудиту фінансової цілісності, вони задовольняють тільки частину вимог для такої діяльності, і читач повинен усвідомлювати використання цієї термінології;

– тестування безпеки. Тестування безпеки потрібно використовувати, щоб всі інформаційні системи та всі пов'язані програмні компоненти працювали безпечно. Тестування безпеки здійснюють, щоб перевірити на відповідність вимогам безпеки, визначеним у політиці безпеки інформаційної системи та планах проведення тестування, а також має бути встановлено критерій прийняття для демонстрації того, що необхідний рівень безпеки досягнуто;

– контроль носіїв інформації. Контроль носіїв інформації охоплює низку засобів безпеки для забезпечення фізичної безпеки та безпеки, що стосується навколишнього середовища, і також обліку дисків, роздруківок та інших носіїв інформації. Контроль носіїв інформації охоплює маркування, ведення журналів, перевіряння цілісності, безпеку від фізичного доступу, від навколишнього середовища, передавання та безпечне знищення;

– гарантоване вилучення інформації. Конфіденційність інформації, попередньо записаної на запам'ятовувальний пристрій, має бути вилучена, якщо ця інформація більше не потрібна. Треба забезпечити, щоб файли, які містять конфіденційні матеріали, були стерті та фізично перезаписані, або ж знищені іншим способом – активація функцій вилучення не завжди це робить. Засоби, схвалені відповідальним персоналом (наприклад, керівником інформаційної безпеки), мають бути доступні всім користувачам для повного та безпечного вилучення даних;

– розподіл обов'язків. Для мінімізації ризиків і можливостей зловживання правами бажано запроваджувати розподіл обов'язків там, де це потрібно та можливо. Зокрема, обов'язки та функції, що в поєднанні можуть привести до обминання засобів безпеки чи аудиту, або надмірних привілеїв для працівника, потрібно тримати роздільно;

– правильне використання програмного забезпечення. Щоб матеріал не копіювався, необхідно забезпечити захист авторського права через виконання ліцензійної угоди для використання комерційного програмного забезпечення;

– контроль змін програмного забезпечення. Контроль змін може бути запроваджений для підтримання цілісності програмного забезпечення, коли вносять зміни (контроль змін програмного забезпечення застосовується тільки до програм, оскільки керування конфігурацією та змінами, що застосовується до інформаційних систем та їхнього оточення як цілого). Необхідно встановити процедури контролю змін до програмного забезпечення, що керують всіма змінами та гарантують, що

безпека підтримується протягом всього процесу. Вони охоплюють авторизацію змін, розгляд безпеки проміжних рішень та перевірку безпеки остаточного рішення.

Планування безперервності бізнесу

Для безпеки бізнесу, особливо критичних ділових процесів, від наслідків збоїв чи катастроф та для мінімізації пошкоджень, спричинених такими подіями, має існувати чинник ефективної неперервності бізнесу, охоплюючи планування непередбачуваних обставин, відновлення після катастроф, стратегію і план(и). Він містить такі засоби безпеки:

– стратегія неперервності бізнесу. Стратегія безперервності бізнесу, охоплюючи планування непередбачуваних обставин, відновлення після катастроф, повинна бути сформульована та задокументована відповідно до розглядуваної інформаційної системи, на основі визначених потенційних ударів, спричинених недоступністю, модифікаціями та знищенням, нанесених недружнім бізнесом;

– план неперервності бізнесу. На основі стратегії неперервності бізнесу потрібно розробити та задокументувати план(и) неперервності бізнесу, охоплюючи плани непередбачуваних обставин та відновлення після катастроф;

– тестування та оновлення плану неперервності бізнесу. Перед прийняттям план безперервності бізнесу має бути ретельно відтестований для гарантування того, що він працює в «реальних» обставинах, та доведений до відома всіх відповідних працівників. Оскільки плани безперервності бізнесу можуть швидко старіти, важливо їх регулярно обновляти. Стратегію безперервності бізнесу треба, за необхідності, обновляти;

– резервування. Для всіх важливих файлів та інших ділових даних, важливих системних програм та документації потрібно робити резервні копії. Частоту резервування потрібно узгоджувати з важливістю інформації й планом безперервності бізнесу. Резервні копії необхідно зберігати у безпечному та віддаленому місці, а відновлення перевіряти регулярно для надійності.

Фізична безпека

Засоби безпеки в цій сфері пов’язані з фізичним захистом. їх треба розглядати в поєднанні з визначенням навколишнього середовища. Положення поширюються на будівлі, безпечні зони, кімнати та офіси. Вибір засобів безпеки залежить від того, яка частина будівлі розглядається. Засоби безпеки в цій сфері наведено нижче:

– матеріальна безпека. Фізичні засоби для безпеки будівлі охоплюють паркани, фізичний контроль доступу, міцні стіни, двері та вікна. Зони будівлі, які підлягають безпеці, треба захищати від несанкціонованого доступу за допомогою системи контролю фізичного доступу, охорони тощо. Зони безпеки можуть бути необхідними для такого обладнання, як сервери, з відповідним програмним забезпеченням та даними, що

підтримують важливі ділові операції. Доступ до таких зон безпеки повинен обмежуватись мінімальною кількістю необхідного персоналу, а подробиці треба записувати в журналі обліку. Все обладнання для діагностування та контролю треба надійно зберігати та ретельно контролювати під час використання;

– протипожежна безпека. Обладнання та прилеглі зони, в тому числі і підхід до них, треба захищати від поширення вогню з будь-якого місця в будівлі чи з суміжних будівель. Небезпека загоряння поблизу кімнат/зон, де розміщено обладнання, має бути мінімізована. Також треба забезпечити захист від вогню, що займається та (або) поширюється на всі кімнати/зони, де розташоване ключове обладнання. Засоби мають умикати сигналізацію на виявлення вогню та диму і систему гасіння. Потрібно потурбуватися про те, щоб захист від пожежі не призвів до пошкодження систем від води чи інших засобів гасіння;

– захист від води/рідини. Цінне обладнання не треба розташовувати на майданчиках, де можливі значні затоплення та витоки води чи іншої рідини. Відповідний захист має бути забезпечений там, де є значна загроза затоплення;

– захист від стихійних лих. Будівлі, де розміщено ключове обладнання, треба захищати від ударів блискавки. Також це обладнання безпосередньо треба захищати від цих ударів. Безпеку від інших стихійних лих можна досягти, уникаючи районів, де вони можуть статися (якщо це можливо), а також запроваджуючи стратегії та планування неперервності бізнесу;

– захист від крадіжок. Для контролю запасів кожна одиниця обладнання має бути ретельно облікована та занесена до опису майна. Охоронцям/реєстраторам треба перевіряти обладнання чи носії інформації на предмет винесення їх з кімнати/зони чи будівлі без авторизації. Інформація з грифом секретності та патентоване програмне забезпечення, що зберігається на портативних носіях інформації (наприклад, флешках або дисках), потрібно захищати відповідно;

– електричне живлення та кондиціювання повітря. За потреби обладнання треба захищати від збоїв живлення. Треба забезпечити придатне електропостачання, а також, за потреби, впровадити безперебійне живлення. Інша мета безпеки – забезпечити необхідну температуру та вологість;

– прокладання кабелю. Кабелі електричного живлення та зв’язку, які передають дані чи підтримують інформаційні послуги, потребують захисту від перехоплення, пошкодження чи перевантаження. Кабелі мають бути фізично захищені від випадкового чи зловмисного пошкодження, вибрані та прокладені відповідно до їх призначення; ретельне планування, що передбачає майбутні розробки, дозволяє уникнути багатьох проблем. Там, де це обґрунтовано і можливо, кабелі треба захищати від прослуховування.

Ідентифікація та автентифікація

Ідентифікація є засобом, яким користувач надає системі заявлену ідентичність. Автентифікація – це метод визначення дійсності цієї заявки. Нижченаведені способи – це приклади, як досягти автентифікації (можливі інші способи класифікації механізмів автентифікації).

1. Автентифікація на основі інформації, якою володіє користувач

Паролі є найтиповішим способом забезпечення автентифікації на основі того, чим володіє користувач і що пов'язано з процесом ідентифікації користувача. Призначення паролів та їхню регулярну зміну треба контролювати. Якщо користувачі вибирають паролі самостійно, вони повинні знати загальні правила створення і поводження з паролями. В цьому питанні може допомогти програмне забезпечення, наприклад, для обмеження використання простих чи шаблонних паролів і символів. Якщо необхідно чи бажано, копії паролів слід захищати, щоб дозволити авторизований доступ, якщо користувач не має в розпорядженні чи забув свій пароль. Автентифікації на основі інформації, якою володіє користувач, також може використовувати криптографічні методи чи протоколи автентифікації. Цей тип ідентифікації та автентифікації також може бути використаний для віддаленої автентифікації.

2. Автентифікація на основі того, чим володіє користувач

Об'єктами, якими володіє користувач для цілей автентифікації, можуть бути модулі пам'яті та інтелектуальні модулі. Звична реалізація таких модулів пам'яті – магнітний матеріал на звороті кредитної картки. Автентифікація забезпечується на основі того, чим володіє користувач (картка), та того, що він знає (PIN-код). Типовими прикладами інтелектуальних модулів є смарт-картки.

3. Автентифікація на основі того, ким є користувач

Технології біометричної автентифікації використовують унікальні характеристики чи риси людини для визначення її особистості. Це можуть бути відбитки пальців, форма руки, знімок сітківки ока, а також голос чи письмовий підпис. Відповідні деталі треба безпечно зберігати на смарт-картках чи в системі.

Контроль логічного доступу та аудит

Засоби захисту в цій сфері реалізують для:

– обмеження доступу до інформації, інформаційних систем, мереж, додатків, системних ресурсів, файлів та програм;

– запису деталей помилок та дій користувача в журнали аудиту та аналізу записаних деталей для виявлення порушень безпеки і реагування на них відповідним чином.

Звичний метод для впровадження контролю доступу – це використання списків контролю доступу, що визначають, до яких файлів, ресурсів тощо користувачу дозволено доступ, і які форми цей доступ може мати. Засоби безпеки в сфері контролю логічного доступу та аудиту наведено нижче.

1. Політика контролю доступу

Для кожного користувача чи групи користувачів треба чітко визначити політику контролю доступу. Ця політика має надавати права доступу відповідно до таких ділових потреб, як доступність, продуктивність та принцип «необхідного знання». Загальна ідея така: «максимальна кількість прав, яка вважається необхідною, мінімальна кількість прав, яка вважається можливою». Під час призначення прав доступу потрібно брати до уваги підхід організації до безпеки (наприклад, відкритий чи обмежувальний) та способи забезпечення потреб організації і прийнятності системи для користувача.

2. Доступ користувачів до інформаційних систем

Контроль доступу до інформаційних систем застосовують для запобігання будь-якого неавторизованого доступу до інформаційних систем. Має бути можливою ідентифікація та перевірка ідентичності кожного авторизованого користувача та ведення журналів успішності чи неуспішності спроби. Контроль доступу до інформаційних систем можна посилити паролями чи будь-яким іншим методом автентифікації.

3. Доступ користувачів до даних, служб та програм

Контроль доступу треба застосовувати для захисту даних чи служб інформаційної системи або в мережі від несанкціонованого доступу. Це може бути зроблено за допомогою відповідних механізмів ідентифікації та автентифікації, відповідних інтерфейсів між мережевими службами та конфігурації мережі, яка гарантує лише авторизований доступ до інформаційних служб (обмежувальний розподіл прав). Для запобігання несанкціонованого доступу до програм потрібно запроваджувати рольовий контроль доступу, що дозволяє доступ відповідно до ділових обов’язків користувача.

4. Перегляд і оновлення прав доступу

Усі права доступу, що надаються користувачам, мають регулярно переглядатися та оновлюватись, якщо потреби безпеки чи ділові потреби доступу змінились. Права привілейованого доступу треба переглядати частіше, щоб уникнути їх нецільового використання. Права доступу негайно скасовують, якщо вони більше не потрібні.

5. Журнали аудиту

Усю роботу з супроводу інформаційних технологій треба записувати в журнали обліку, а ці журнали обліку регулярно перевіряти; це охоплює успішні та неуспішні спроби входу в систему, ведення журналу обліку доступу до даних, функцій системи тощо. Також необхідно вести журнали обліку збоїв і регулярно переглядати ці журнали. Всі ці дані потрібно використовувати відповідно до законодавства про захист даних та приватного життя, наприклад, їх можна зберігати тільки обмежений строк та використовувати тільки для виявлення порушень захисту.

Захист від зловмисного коду

Зловмисний код може потрапляти до систем через зовнішні сполучення, а також через файли та програмне забезпечення, занесені на переносних носіях інформації. Якщо не реалізовані відповідні засоби захисту, цей код можна не виявити, доки він не призвів до пошкоджень. Зловмисний код може призводити до компрометації безпеки засобів безпеки (наприклад, перехоплення та розкриття паролів), незловмисного розкриття інформації, внесення незловмисних змін до інформації, втрати цілісності системи, руйнування інформації, та (або) до несанкціонованого використання системних ресурсів.

Зловмисний код може бути таких видів:

– віруси;

– черв'яки;

– троянські коні.

Переносниками зловмисного коду є:

– програми, що запускаються;

– файли даних (що містять макроси, наприклад, текстові документи чи таблиці);

– активний вміст сторінок Інтернету.

Зловмисний код може поширюватись через:

– електронні носії інформації;

– інші знімні носії інформації;

– електронну пошту;

– мережі;

– завантаження (по каналах зв'язку).

Зловмисний код може бути введений внаслідок зловмисних дій користувача чи у разі взаємодії системних рівнів, що може бути невидимою для користувачів. Захистити від зловмисного коду можна, використавши засоби захисту, наведені нижче.

1. Сканери

Різні форми зловмисного коду можуть бути виявлені та видалені спеціальним сканувальним програмним забезпеченням та програмами перевірки цілісності. Сканери можуть працювати в закритому чи відкритому режимах. Робота сканера у відкритому режимі забезпечує активний захист, тобто виявлення (і, можливо, видалення) зловмисного коду перед тим, як відбулося зараження та інформаційній системі заподіяна шкода. Є сканери для окремих інформаційних систем, робочих станцій, файлових серверів, серверів електронної пошти та брандмауерів. Однак користувачі та адміністратори мають знати про те, що на сканери не можна покладатися у виявленні всіх зловмисних кодів (чи навіть всього коду певного типу), оскільки постійно з'являються нові форми зловмисного коду.

2. Програми перевірки цілісності

Зазвичай, для доповнення засобів захисту, що забезпечується сканерами, потрібні інші форми засобів захисту. Наприклад, контрольні суми можна використовувати для перевірки того, чи була програма модифікована. Програми перевірки цілісності мають бути складовою частиною технічних засобів захисту від зловмисного коду. Ця техніка може бути використана тільки для файлів даних і програм, що не зберігають інформацію про статус для подальшого використання.

3. Контроль за обігом переносних носіїв інформації

Неконтрольований обіг носіїв інформації (особливо електронних носіїв інформації) може призвести до зростання ризику введення зловмисного коду в інформаційні системи організації. Контроль за обігом носіїв може бути досягнуто використанням:

– спеціального програмного забезпечення;

– процедурних засобів захисту.

4. Процедурні засоби безпеки

Потрібно розробити настанови для користувачів та адміністраторів, що окреслюють процедури та правила мінімізації проникнення зловмисного коду. Такі настанови мають стосуватися питання завантаження ігор та інших виконуваних програм, використання різних видів Інтернет-служб та важливих файлів різних типів. За необхідності, потрібно виконувати незалежний перегляд вихідного чи виконуваного коду. Треба запроваджувати навчання, що стосується питань безпеки, та дисциплінарні заходи і відповідні процедури за недотримання задокументованих процедур і правил запобігання зловмисному коду.

Керування мережею

Ця сфера охоплює теми планування, експлуатації та адміністрування мереж. Правильна конфігурація та адміністрування мереж є ефективним методом зменшення ризиків.

1. Процедури експлуатації

Запровадження процедур експлуатації та обов’язків необхідне для забезпечення правильного та безпечного функціонування мереж. Вони містять документацію щодо експлуатації та запровадження процедур реагування у разі порушення безпеки.

2. Планування системи

Для забезпечення надійного функціонування та адекватних мережевих потужностей необхідне розвинене планування, підготовка та моніторинг (охоплюючи статистику завантаження). Для нових систем треба застосовувати критерій прийняття, треба здійснювати контроль за змінами та реагування на них.

3. Конфігурація мережі

Прийнятна конфігурація мережі є істотною для її надійного функціонування. Вона містить стандартизований підхід до конфігурації серверів в організації, та, що дуже важливо, хорошу документацію. Більше

того, необхідно пересвідчитися, що сервери, задіяні для спеціальних цілей, використовуються тільки для цих цілей (наприклад, ніякі інші задачі не запускаються на брандмауері), і що є достатній захист від збоїв.

4. Відокремлення мережі

Для мінімізації ризиків та можливостей зловживання в мережі під час її експлуатації, ділові зони, що мають справу з критичними діловими питаннями та інформацією, треба відокремлювати логічно чи фізично. Також засоби розробки треба відокремлювати від засобів експлуатації.

5. Моніторинг мережі

Для визначення слабких місць у наявній конфігурації мережі треба здійснювати моніторинг мережі. Він дозволяє перебудовувати структуру мережі за допомогою аналізу робочого навантаження та допомагає визначити нападників.

6. Виявлення вторгнень

Спроби вторгнень до систем чи мереж та успішний несанкціонований вхід потрібно виявляти так, щоб організація могла відреагувати відповідним та ефективним чином.

Криптографія

Криптографія – це математичні методи перетворення даних для забезпечення безпеки. Їх можна застосовувати для багатьох різних цілей в інформаційній безпеці, наприклад, криптографія може допомогти забезпечити конфіденційність та (або) цілісність даних, неспростовність і посилені методи ідентифікації та автентифікації. Застосовуючи криптографію, треба подбати про те, щоб дотримувалися всі правові та регуляторні вимоги в цій сфері. Один з найважливіших аспектів криптографії – адекватна система керування ключами. Послуги штемпелювання часу можна використовувати для підтримки окремих програм криптографічних засобів захисту.

Приклад

Криптосистема, заснована на еліптичних кривих

У 1985 році Коблиць і Міллер незалежно один від одного запропонували використовувати для побудови криптосистем алгебраїчні структури, визначені на безлічі точок на еліптичних кривих. Розглянемо випадок визначення еліптичних кривих над простими кінцевими полями довільної характеристики і над полями Галуа характеристики 2.

Нехай $p > 3$ – просте число. Нехай $\alpha,\ b \in GF(p)$ такі, що $4a^2 + 27b^2 \neq 0.$ Еліптичною кривою E над полем $GF(p)$ називається безліч розв'язків $(x,\ y)$ рівняння $y^2 = x^3 + ax + b$ над полем $GF(p)$ разом з додатковою точкою $\infty,$ названою точкою в нескінченності.

Подання еліптичної кривої у вигляді розв'язання називається еліптичною кривою у формі Вейерштрасса.

Позначимо кількість точок на еліптичній кривій E через $\#E$. Верхня і нижня межі для $\#E$ визначаються теоремою Хассе:

$$p+1-2\sqrt{p} \le \#_E \le p+1+2\sqrt{p}\,.$$

Задамо бінарну операцію на E (в адитивному запису) нижченаведеними правилами:

(I) $\infty+\infty=\infty$;

(II) $\forall(x,\ y)\ \in\ E,\ (x,\ y)+\infty=(x,\ y)$;

(III) $\forall(x,\ y)\ \in\ E,\ (x,\ y)+(x,\ -y)=\infty$;

(IV) $\forall(x_1,\ y_1)\ \in\ E,\ (x_2,\ y_2)\ \in\ E,\ x_1\neq x_2,\ (x_1,\ y_1)+(x_2,\ y_2)=(x_3,\ y_3)$,

де $x_3=\lambda^2-x_1-x_2$,
$y_3=\lambda(x_1-x_3)-y_1$,
$\lambda=\dfrac{y_2-y_1}{x_2-x_1}$;

(V) $\forall(x_1,\ y_1)\ \in\ E,\ y_1\neq 0,\ (x_1,\ y_1)+(x_1,\ y_1)=(x_2,\ y_2)$,

де $x_2=\lambda^2-2x_1$,
$y_2=\lambda(x_1-x_3)-y_1$
$\lambda=\dfrac{3x_1^2+a}{2y_1}$.

Безліч точок еліптичної кривої E, заданої в такий спосіб операцією, утворить абелеву групу.

Якщо $\#_E=p+1$, то крива E називається суперсингулярною.

Еліптична є суперсингулярною кривою E над полем $GF(2^m)$ характеристики 2 та задається в такий спосіб. Нехай $m>3$ – ціле число. Нехай $a,\ b\ \in\ GF(2^m),\ b\ \neq\ 0$. Еліптична крива E над полем $GF(2^m)$ називається безліччю розв'язань $(x,\ y)$ рівняння

$$y^2+xy=x^3+ax+b$$

над полем $GF(2^m)$ разом з додатковою точкою ∞, названою точкою в нескінченності.

Кількість точок на кривій E також визначається теоремою Хассе:

$$q+1-2\sqrt{q} \le \#E \le q+1+2\sqrt{q}\,,$$

де $q = 2^m$. Більш того, $\# E$ парне.

Операція додавання на E у цьому випадку задається такими правилами:

(I) $\infty + \infty = \infty$;

(II) $\forall (x,\ y) \in E,\ (x,\ y) + \infty = (x,\ y)$;

(III) $\forall (x,\ y) \in E,\ (x,\ y) + (x,\ x + y) = \infty$;

(IV) $\forall (x_1,\ y_1) \in E,\ (x_2,\ y_2) \in E,\ x_1 \neq x_2,\ (x_1,\ y_1) + (x_2,\ y_2) = (x_3,\ y_3)$,

де $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$,

$y_3 + \lambda(x_1 + x_3) + x_3 + y_1$,

$\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$.

(V) $\forall (x_1,\ y_1) \in E,\ x_1 \neq 0,\ (x_1,\ y_1) + (x_1,\ y_1) = (x_2,\ y_2)$,

де $x_2 = \lambda^2 + \lambda + a$,

$y_2 = x_1^2 + (\lambda + 1)x_3$,

$\lambda = x_1 + \dfrac{y_1}{x_1}$.

У цьому випадку безліч точок еліптичної кривої E, заданої в такий спосіб операцією, також утворить абелеву групу.

Користуючись операцією додавання точок на кривій, можна природним чином визначити операцію множення точки $P \in E$ на довільне ціле число n:

$$n = P + P + \Lambda + P,$$

де операція додавання виконується n раз.

Тепер побудуємо однобічну функцію, на основі якої можна буде створити криптографічну систему.

Нехай E – еліптична крива, $P \in E$ – точка на цій кривій. Виберемо ціле число $n < \# E$. Тоді як пряму функцію виберемо добуток n. Для його обчислення за оптимальним алгоритмом буде потрібно не менше $2 \cdot \log_2 n$ операцій додавання. Обернену задачу сформулюємо в такий спосіб: за заданою еліптичною кривою E, точкою $P \in E$ і добутком n знайти n.

В даний час усі відомі алгоритми розв'язання цієї задачі потребують експонентного часу.

Для встановлення захищеного зв'язку два користувачі A і B спільно вибирають еліптичну криву E і точку P на ній. Потім кожен з користувачів вибирає своє секретне ціле число, відповідно a і b. Користувач A обчислює добуток a, а користувач B – добуток b. Далі вони обмінюються обчисленими значеннями. При цьому параметри самої кривої, координати точки на ній і значення добутків є відкритими і можуть передаватися по незахищених каналах зв'язку.

Потім користувач A множить отримане значення на a, а користувач B множить отримане ним значення на b. У силу властивостей операції множення на число $a\,b \equiv b\,a$. Таким чином, обидва користувачі одержать загальне секретне значення (координати точки ab), яке вони можуть використовувати для одержання ключа шифрування. Відзначимо, що зловмиснику для відновлення ключа буде потрібно розв'язати складну, з обчислювальної точки зору, задачу визначення a і b за відомими E, P, a і b.

Різні способи використання криптографії описано нижче.

1. Безпека конфіденційності даних

В обставинах, коли важливо зберігати конфіденційність, тобто коли інформація є надзвичайно чутливою, треба розглядати засоби безпеки, що зашифровують інформацію для зберігання чи передавання мережею. Під час вирішення питання про використання засобів шифрування треба брати до уваги:

– відповідні державні закони та норми;

– вимоги до керування ключами та труднощі, які треба подолати для гарантування того, що справжні поліпшення безпеки досягаються без створення нових вразливостей;

– прийнятність використовування механізмів шифрування для розгорнення та рівень необхідної безпеки.

2. Безпека цілісності даних

За обставин, коли важливим є цілісність даних, що зберігаються чи обробляються, для безпеки цих даних треба розглянути хеш-функції, цифрові підписи та (або) засоби забезпечення цілісності. Засоби безпеки цілісності гарантують безпеку від випадкової чи зловмисної зміни, долучення чи вилучення інформації. Засоби цифрових підписів можуть забезпечувати безпеку, схожу на засоби цілісності повідомлень, але також мають властивості, що дозволяють уможливити неспростовність. У разі вирішення питання про використання цифрових підписів чи інших засобів забезпечення цілісності треба брати до уваги:

– відповідні державні закони та норми;

– відповідну інфраструктуру відкритих ключів;

– вимоги до керування ключами та труднощі, які потрібно подолати для гарантування того, що справжнього поліпшення безпеки досягають без створення нових вразливостей.

3. Неспростовність

Методи криптографії (наприклад, засновані на використанні цифрових підписів) можуть бути використані для повідомлень, комунікацій та транзакцій з метою підтвердження чи спростування відправлення, передавання, подання, доставлення, оповіщення про отримання тощо.

4. Автентичність даних

У ситуаціях, коли є важливою автентичність даних, для підтвердження достовірності даних може бути використаний цифровий підпис. Ця необхідність проявляється особливо, коли використовуються дані, на які посилається третя сторона, або коли велика кількість людей залежать від точності даних джерел, на які посилаються. Цифрові підписи також можна використовувати для підтвердження факту, що дані створені чи передані певною особою.

5. Керування ключами

Керування ключами охоплює технічні, організаційні та процедурні аспекти, необхідні для використання будь-якого механізму криптографії. Метою керування ключами є безпечне адміністрування та керування криптографічними ключами та пов'язаною з ними інформацією. Керування ключами охоплює генерування, реєстрування, сертифікування, дереєстрування, поширення, встановлення, зберігання, архівування, відгук, виведення та знищення ключового матеріалу. На додаток, важливо розробляти систему керування ключами так, щоб зменшити ризик компрометування ключа та використання ключа не уповноваженими на це особами. Процедури керування ключами залежать від використовування алгоритму наміру щодо використання ключів та політики безпеки.

13.4 Базовий підхід: вибір засобів безпеки відповідно до типу системи

Є два різні набори засобів безпеки, механізмів та (або) процедур, які можна застосовувати для безпеки інформаційних систем. З одного боку, є доволі багато організаційних категорій засобів безпеки, які є загальноприйнятими для кожної інформаційної системи за конкретних обставин, незалежно від окремих компонентів. Внаслідок їх загальної застосовності, засоби, які належать до цих категорій, потрібно завжди розглядати. До того ж, багато з них є недорогими для впровадження, оскільки вони стосуються організаційних структур та процедур.

З іншого боку, є специфічні засоби безпеки інформаційної системи – вибір цих засобів безпеки залежить від типу та характеристик розглядуваної інформаційної системи.

Звичайно, можливо, що одна чи більше з цих категорій або специфічних засобів безпеки не є застосовними до інформаційної системи. Наприклад, шифрування може не бути необхідним, якщо відправлена чи

отримана інформація не потребує конфіденційності, а цілісність може бути перевірена іншим чином.

Перед реалізацією вибраних засобів безпеки необхідно ретельно перевірити, чи їх немає серед наявних та (або) запланованих.

Якщо засоби безпеки вибрані відповідно до інших критеріїв (наприклад, базові та додаткові засоби), остаточний набір засобів для впровадження треба робити обережно. Після перегляду декількох інформаційних систем, потрібно розглянути, чи можна запровадити базову безпеку для всієї організації.

Інша можливість вибору засобів безпеки без детального розгляду – це застосування баз, пов'язаних з конкретним використанням. Але перед вибором того, які засоби безпеки треба впроваджувати, корисно розглянути потреби та проблеми безпеки.

Засоби безпеки загального застосування

Категоріями загального застосування засобів безпеки є:

– керування інформаційною безпекою та політикою безпеки;
– перевірка узгодженості безпеки;
– реагування на порушення;
– персонал;
– питання експлуатації;
– планування неперервності бізнесу та
– фізична безпека.

Засоби безпеки, які належать до цих категорій, формують основу успішного керування інформаційною безпекою, їх не треба недооцінювати. Також важливо забезпечити взаємодію цих засобів з більш технічними засобами. Організація визначає обсяги робіт у цих сферах, залежно від її потреб, проблем та доступних ресурсів.

Звичайно, багато інших категорій засобів безпеки застосовні в більшості випадків, але спосіб реалізації зазвичай є відповідним конкретним обставинам (наприклад, засоби, які забезпечують контроль доступу для мережі, відрізняються від тих засобів, що забезпечують контроль доступу для автономної інформаційної системи).

Коли засоби безпеки вибирають з категорій загальнозастосовних засобів, корисно розглядати розмір організації так само, як потреби безпеки, оскільки він впливає на межі, в яких реалізуються ці засоби безпеки. Наприклад, маленька організація не буде мати ні потреби, ні персоналу для створення комітету інформаційної безпеки, проте має бути хтось, хто виконує ці функції. Тому всі засоби безпеки мають бути відповідно зважені, коли б це не знадобилося.

Специфічні засоби безпеки інформаційної системи

На додаток до засобів захисту загального застосування для кожного відповідного типу системного компонента треба вибирати специфічні засоби безпеки системи. Нижченаведена таблиця дає приклад того, як починати процес вибору специфічних засобів системи. В цьому прикладі

«X» означає засоби, що мають реалізовуватись за нормальних обставинах, а «(X)» означає засоби, що можуть бути необхідними за деяких обставин (табл. 13.1).

Таблиця 13.1 – Як починати процес вибору специфічних засобів системи

	Автономна робоча станція	Робоча станція (клієнт без спільних ресурсів), під'єднана до мережі	Сервер чи робоча станція зі спільними ресурсами, під'єднана до мережі
Автентифікація			
Автентифікація на основі інформації, що є в наявності у користувача	X	X	X
Автентифікація на основі дечого, що є в наявності у користувача	X	X	X
Автентифікація на основі того, ким є користувач	(X)	(X)	(X)
Контроль логічного доступу та аудит			
Політика контролю доступу			X
Доступ користувачів до інформаційних систем	X	X	X
Доступ користувачів до даних, служб та програм	X	X	X
Перегляд і оновлення прав доступу			X
Журнали аудиту	X	X	X
Зловмисний код			
Сканери	X	X	X
Програми перевірки цілісності	X	X	X
Контроль за обігом переносних носіїв інформації	X	X	X
Процедурні засоби безпеки	X	X	X
Керування мережею			
Методика експлуатації			X
Планування системи			X
Конфігурація мережі			X
Відокремлення мережі			X
Моніторинг мережі			X
Виявлення вторгнень			X
Криптографія			
Безпека конфіденційності даних	(X)	(X)	(X)
Безпека цілісності даних	(X)	(X)	(X)
Неспростовність		(X)	(X)
Автентичність даних	(X)	(X)	(X)
Керування ключами	(X)	(X)	(X)

13.5 Вибір засобів безпеки відповідно до проблем і загроз безпеці

Вибір засобів безпеки відповідно до проблем та загроз безпеці можна здійснювати таким чином.

Перший крок – визначити та оцінити проблеми безпеки. Потрібно розглянути вимоги до конфіденційності, цілісності, доступності, спостережності, автентичності та надійності. Міцність та кількість вибраних засобів захисту має відповідати оціненим проблемам безпеки.

Другий крок – для кожної проблеми безпеки визначають типові загрози і для кожної загрози пропонувати засоби безпеки інформаційної системи, що розглядається. У такий спосіб можна задовольнити специфічні потреби безпеки та досягти безпеки там, де вона дійсно необхідна.

Оцінювання проблем безпеки

Для ефективного вибору прийнятних засобів безпеки, необхідно розуміти проблеми безпеки підтримуваних ділових операцій інформаційною системою, що розглядається. За допомогою визначення проблем безпеки, беручи до уваги відповідні загрози, що можуть призвести до цих проблем, потрібно вибирати засоби безпеки.

Якщо оцінювання, проведене згідно з положеннями цього підрозділу, виявляє дуже великі проблеми безпеки, рекомендується деталізованіший підхід для визначання прийнятної безпеки.

Проблеми безпеки мають містити:

– втрату конфіденційності;

– втрату цілісності;

– втрату доступності;

– втрату спостережності;

– втрату автентичності;

– втрату надійності.

Оцінювання має охоплювати саму інформаційну систему, інформацію, що зберігається чи обробляється на ній, та ділові операції, які вона виконує. Це оцінювання визначає цілі вибраних засобів безпеки. Різні частини інформаційної системи або інформація, що зберігається чи обробляється, можуть мати різні проблеми безпеки. Важливо пов’язувати проблеми безпеки безпосередньо з цінностями, оскільки це впливає на загрози, які можуть з’являтися, і, таким чином, на вибір засобів безпеки.

Значимість проблем безпеки може бути оцінена залежно від того, чи спричиняє порушення безпеки серйозні ушкодження діловій діяльності, чи ж тільки завдає легкої шкоди, чи не впливає зовсім. Наприклад, якщо конфіденційна інформація організації, несанкціоноване розкриття цієї інформації конкуренту може дозволити йому зробити дешевші пропозиції і, таким чином, заподіяти серйозні збитки бізнесу організації. З іншого боку, якщо оброблювана інформаційною системою інформація доступна широкому загалу, несанкціоноване розкриття не заподіє ніяких збитків.

Розгляд можливих загроз може допомогти з'ясувати проблеми безпеки. Оцінювання, описане нижче, треба проводити окремо для кожної цінності, оскільки проблеми безпеки для різних цінностей можуть бути різними. Однак, якщо є достатні знання з проблем безпеки, цінності з однаковими чи схожими діловими потребами та проблемами безпеки можуть бути об'єднані в групи.

Якщо інформація, оброблювана системою, є різнотипною, різні її типи можуть вимагати окремого розгляду. Безпека, що надається інформаційній системі, має бути достатньою для всіх типів оброблюваної інформації. Таким чином, якщо певна інформація потребує високого рівня безпеки, всю систему треба захищати належним чином. У випадку, якщо кількість інформації з великими потребами безпеки незначна, є сенс розглянути перенесення цієї інформації в іншу систему, якщо це не заважає діловим процесам.

Коли всі можливі втрати конфіденційності, цілісності, доступності, спостережності, автентичності та надійності визначені як можлива причина тільки незначної втрати, вважається достатньою наявна безпека системи. Коли будь-яка з цих втрат визначена як можлива причина серйозних збитків, треба оцінити, чи потрібно підбирати інші засоби безпеки.

Втрата конфіденційності

Розглянемо, які збитки можуть виникнути внаслідок втрати конфіденційності цінностей, що розглядаються (зловмисної чи незловмисної). Наприклад, втрата конфіденційності може призвести до:

– втрати суспільної довіри чи погіршення репутації;

– судової відповідальності, також до відповідальності за порушення законодавства про безпеку даних;

– несприятливі наслідки організаційної політики;

– загрози власній безпеці;

– фінансових втрат.

Відповідно до відповідей на поставлені вище питання, має бути вирішено, якими будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

Втрата цілісності

Розглянемо, які збитки можуть виникнути внаслідок втрати цілісності згаданих цінностей (зловмисної чи незловмисної). Наприклад, втрата цілісності може призвести до:

– прийняття неправильних рішень;

– обману;

– порушення ділових функцій;

– втрати суспільної довіри чи погіршення репутації;

– фінансових втрат;

– судової відповідальності, також до відповідальності за порушення законодавства про захист даних.

Залежно від відповідей на поставлені вище питання, треба вирішити, якими будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

Втрата доступності

Розглянемо, які збитки можуть виникнути внаслідок довготермінової втрати доступності до програм чи доступності до інформації, тобто переривання яких ділових функцій призведе до невчасної відповіді на запит чи невчасного виконання. Також має бути розглянута крайня форма втрати доступності, остаточна втрата даних та (або) фізичне руйнування апаратного чи програмного забезпечення. Наприклад, втрата доступності до критичних програм чи доступності до критичної інформації може призвести до:

– прийняття неправильних рішень;

– неможливості виконувати ризиковані задачі;

– втрати суспільної довіри чи погіршення репутації;

– фінансових втрат;

– судової відповідальності, також відповідальності за порушення законодавства про захист даних, недотримання строків виконання, вказаних в контракті;

– суттєвих затрат на відновлення.

Треба зазначити, що величина збитків внаслідок втрати доступності може досить сильно відрізнятися у різні періоди часу. Коли це дійсно так, то доречно розглянути всі збитки, що можуть виникнути в ці різні періоди часу, та оцінити їх для кожного періоду як значні, незначні чи нульові (ця інформація буде використовуватись у виборі засобів захисту).

Залежно від наданих відповідей на поставлені вище питання треба вирішити, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

Втрата спостережності

Розглянемо, які збитки можуть виникнути внаслідок втрати спостережності за користувачами системи чи суб’єктами (наприклад, програмами), що виконують доручення користувача. Цей розгляд також має охоплювати автоматично згенеровані повідомлення, які можуть стати причиною проведення дії. Наприклад, втрата спостережності може призвести до:

– маніпуляції системою з боку користувачів;

– обману;

– індустріального шпіонажу;

– дій, що не прослідковуються;

– помилкових обвинувачень;

– судової відповідальності, також відповідальності за порушення законодавства про захист даних.

Залежно від відповідей на поставлені вище питання має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

Втрата автентичності

Розглянемо, які збитки можуть виникнути внаслідок втрати автентичності даних та повідомлень, незалежно від того, хто їх використовує: люди чи система. Це особливо важливо в розподілених системах, де прийняті рішення поширюються на широкий загал, чи у разі використання довідкової інформації. Наприклад, втрата автентичності може призвести до:

– обману;

– використання в правильному процесі неправильних даних, що призводить до неправильного результату;

– маніпуляції організацією з боку сторонніх осіб;

– індустріального шпіонажу;

– помилкових обвинувачень та

– судової відповідальності, також відповідальності за порушення законодавства про захист даних.

Залежно від наданих відповідей на поставлені вище питання має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

Засоби конфіденційності

Типи загроз, що впливають на конфіденційність, наведено нижче разом з засобами безпеки від цих загроз. Якщо це важливо для вибору засобів безпеки, треба брати до уваги тип і характеристики інформаційної системи.

Потрібно відмітити, що більшість засобів захисту розраховано на ряд загроз та забезпечує захист через підтримування загального ефективного керування інформаційною безпекою. Тому вони не перераховані тут детально, але їхній вплив не треба недооцінювати, і їх треба впроваджувати для загальної ефективної безпеки.

Підслуховування

Один із шляхів отримання доступу до контрольованої інформації – це підслуховування, наприклад, записування інформації з лінії чи підслуховування телефонної розмови. Засоби захисту від цього наведено нижче.

Фізичні засоби. До них належать кімнати, стіни, будівлі тощо, що роблять підслуховування неможливим чи важким. Інший шлях зробити це – створити шуми. У випадку використання телефонів певний захист від підслуховування може забезпечити відповідне прокладення кабелю.

Інформаційна політика безпеки. Інший шлях уникнути підслуховування – забезпечити правила стосовно того, коли, де, та за яких умов треба обмінюватись контрольованою інформацією.

Захист конфіденційності даних. Ще один шлях захиститись від прослуховування – зашифровувати повідомлення перед відправленням.

Електромагнітне випромінювання

Електромагнітне випромінювання може бути використане нападником, щоб отримати інформацію, яка обробляється інформаційною системою. Засоби безпеки від електромагнітного випромінювання наведено нижче.

Фізичні засоби. Це може бути екранування кімнат, стін тощо, що не дозволить електромагнітному випромінюванню проходити через таке екранування.

Безпека конфіденційності даних. Треба відмітити, що ця безпека ефективно застосовується тільки до тих пір, доки інформація зашифрована. Для інформації, яку обробляють, відображають чи друкують, цю безпеку не застосовують.

Використання інформаційних систем з низьким рівнем випромінювання. Але і в цьому випадку обладнання з вбудованим захистом може бути застосовано.

Зловмисний код

Зловмисний код може призводити до втрати конфіденційності, наприклад, через перехоплення та розкриття паролів. Засоби захисту від нього наведено нижче.

Захист від зловмисного коду

Оскільки один із шляхів отримання паролів – це введення зловмисного коду для їх перехоплення, має бути безпека від таких програм.

Реагування на порушення. Своєчасно надані звіти про будь-які незвичні порушення можуть зменшити збитки у разі ураження зловмисним кодом. Виявлені вторгнення можна використовувати для виявлення спроб отримати вхід до системи чи мережі.

Керування мережею. Ще один спосіб отримання контрольованого матеріалу – приховування користувача в потоці, наприклад, електронної пошти.

Безпека конфіденційності даних. Якщо, з деяких причин, вищезгаданий тип безпеки неможливий чи недостатній, можна впровадити додаткову безпеку під час шифрування важливих даних.

Приховування ідентичності користувача

Приховування ідентичності користувача можна використовувати, щоб уникнути автентифікації, а також всіх служб та функцій безпеки, пов’язаних з нею. В результаті, кожного разу це може призводити до проблем конфіденційності, коли приховування уможливлює доступ до контрольованої інформації. Засоби захисту в цій сфері наведено нижче.

Автентифікація. Приховування стає більш важким, коли застосовують засоби ідентифікації та автентифікації, що базуються на поєднанні чогось

відомого, чогось наявного, а також внутрішніх характеристиках користувача.

Контроль логічного доступу та аудит. Контроль логічного доступу не може відрізняти уповноваженого користувача від когось, хто видає себе за цього авторизованого користувача, але використання механізмів контролю доступу може звузити сферу впливу. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Хибне направлення/перенаправлення повідомлень

Хибне направлення – це зловмисне чи незловмисне хибне спрямування повідомлень, тоді як перенаправлення можна застосовувати як для добрих, так і для недобрих цілей. Перенаправлення може виконуватись, наприклад, для підтримування цілісності доступності. Хибне направлення чи перенаправлення повідомлень може призводити до втрати конфіденційності, якщо воно дозволяє несанкціонований доступ до цих повідомлень. Засоби захисту проти цього наведено нижче.

Керування мережею. Засоби безпеки від хибного направлення та перенаправлення.

Безпека конфіденційності даних. У випадках помилкового пере-направлення, щоб запобігти несанкціонованому доступу, повідомлення треба шифрувати.

Збої програмного забезпечення

Збої програмного забезпечення можуть впливати на безпеку конфіденційності, якщо це програмне забезпечення захищає конфіденційність, наприклад, програми контролю доступу чи шифрування, або ж якщо збої програмного забезпечення спричиняють зациклювання, наприклад, в операційній системі. Засоби безпеки конфіденційності в цьому випадку наведено нижче.

Реагування на порушення. Кожен, хто помічає некоректну роботу програмного забезпечення, повинен звітувати про це відповідальній особі так швидко, як це можливо.

Експлуатація. Деяких збоїв програмного забезпечення можна уникнути за допомогою тестування програм перед використанням та за допомогою контролю змін програмного забезпечення.

Крадіжки

Крадіжки можуть піддавати небезпеці конфіденційність, якщо вкрадений компонент інформаційних технологій має будь-яку контрольовану інформацію, що може стати доступною крадію. Засоби безпеки від крадіжок наведено нижче.

Фізичні засоби. Це може бути матеріальний захист, що робить доступ у будівлю, зону чи кімнату, яка містить обладнання, складнішим, або це можуть бути специфічні засоби безпеки від крадіжок.

Персонал. Засоби безпеки персоналу (контроль зовнішнього персоналу, угоди конфіденційності тощо) мають бути наявними для ускладнення крадіжок.

Безпека конфіденційності. Цей засіб безпеки треба впроваджувати, якщо можлива крадіжка обладнання що містить контрольовану інформацію.

Контроль носіїв інформації. Будь-який носій, що містить контрольований матеріал, треба захищати від крадіїв.

Несанкціонований доступ до інформаційних систем, даних, служб та програм

Несанкціонований доступ до інформаційних систем, даних, служб та програм може бути загрозою, якщо можливий доступ до будь-яких контрольованих матеріалів. Засоби безпеки від несанкціонованого доступу охоплюють відповідну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи та відокремлення мережі на мережевому рівні.

Автентифікації. Відповідні засоби ідентифікації та автентифікації використовують в поєднанні з контролем логічного доступу для запобігання несанкціонованого доступу.

Контроль логічного доступу та аудит. Треба використовувати засоби безпеки для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Перегляд та аналіз журналів аудиту може виявити несанкціоновану діяльність людей з правами доступу до системи.

Відокремлення мережі. Для ускладнення несанкціонованого доступу треба зробити відокремлення мережі.

Фізичний контроль доступу. Крім логічного контролю доступу, безпеку можна забезпечити фізичним контролем доступу.

Контроль носіїв інформації. Якщо контрольовані дані зберігаються на інших носіях інформації, для безпеки цих носіїв від несанкціонованого доступу потрібно застосовувати контроль носіїв інформації.

Безпека конфіденційності даних. Якщо, з деяких причин, вищезазначений тип безпеки неможливий чи недостатній, може бути забезпечена додаткова безпека під час шифрування збережуваних контрольованих даних.

Несанкціонований доступ до носіїв даних

Несанкціонований доступ до носіїв даних, на яких зберігається якийсь конфіденційний матеріал, та їх використання можуть впливати на безпеку конфіденційності. Засоби захисту конфіденційності наведено нижче.

Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичної безпеки, обліку носіїв інформації та гарантоване вилучення інформації, що зберігалася, щоб ніхто не міг отримати конфіденційний матеріал з попередньо очищеного носія. Спеціальні заходи безпеки треба вжити для таких переносних носіїв інформації, як машинні носії та папір.

Фізична безпека. Відповідна безпека кімнат (міцні стіни та вікна, а також фізичний контроль доступу) та аксесуари безпеки можуть захистити від несанкціонованого доступу.

Безпека конфіденційності даних. Додаткова безпека контрольованої інформації на носіях даних може бути забезпечена за допомогою шифрування матеріалу. Необхідна добра система керування ключами для безпроблемного застосування шифрування.

Засоби контролю цілісності

Типи загроз, що можуть впливати на безпеку цілісності, наведено нижче разом із засобами безпеки від цих загроз. Якщо це важливо для вибору засобів безпеки, потрібно враховувати тип і характеристики інформаційної системи.

Варто відмітити, що більшість засобів безпеки забезпечує більш «загальну» безпеку, тобто вони націлені на певні загрози та забезпечують безпеки через підтримування загального ефективного керування безпекою інформації. Тому вони не описані тут детально, але їх вплив не треба недооцінювати, і їх потрібно впроваджувати для загальної ефективної безпеки.

Псування носіїв даних

Псування носіїв даних загрожує цілісності інформації, що зберігається на цих носіях. Якщо цілісність є важливою, треба застосовувати нижченаведені засоби безпеки.

Контроль носіїв інформації. Достатній контроль носіїв повинен охоплювати перевірку цілісності, щоб з'ясувати, що збережені файли були пошкоджені.

Резервування. Потрібно виконувати резервування всіх важливих файлів, ділових даних тощо. Якщо помічена втрата цілісності, наприклад, через контроль носіїв чи тестування резервних копій, тоді треба використати запасну копію чи попередню копію для відновлення цілісності файлів.

Безпека цілісності даних. Для безпеки цілісності даних на запам'ятовувальному пристрої можуть бути впроваджені криптографічні методи.

Помилки обслуговування

Якщо обслуговування виконують нерегулярно чи під час обслуговування трапляються помилки, то цілісність інформації знаходиться під загрозою. Засоби безпеки цілісності в цьому випадку наведено нижче.

Обслуговування. Належне обслуговування – це найкращий шлях уникнення помилок обслуговування. Воно охоплює задокументовані та перевірені процедури обслуговування й належний нагляд за роботою.

Резервування. Якщо трапляються помилки обслуговування, для відновлення цілісності пошкодженої інформації можна використовувати резервні копії.

Безпека цілісності даних. Для безпеки цілісності інформації можна використовувати криптографічні методи.

Зловмисний код

Зловмисний код може призвести до втрати цілісності, наприклад, якщо дані чи файли змінені особою, що отримала несанкціонований доступ за допомогою зловмисного коду чи самим цим кодом. Засоби безпеки від цього наведено нижче.

Безпека від зловмисного коду. Оскільки один із способів отримання паролів – це введення зловмисного коду для їхнього перехоплення, то має бути безпека від таких програм.

Реагування на порушення. Своєчасне звітування про будь-які незвичні порушення може зменшити збитки у разі ураження зловмисним кодом. Виявлення вторгнень треба використовувати для виявлення спроб виконати вхід до системи чи мережі.

Керування мережею. Ще один спосіб несанкціонованого доступу – приховування користувача в потоці, наприклад, електронної пошти.

Безпека цілісності даних. Якщо, з деяких причин, вищезгаданий тип безпеки неможливий чи недостатній, треба забезпечити додаткову безпеку у разі використання таких криптографічних методів, як цифрові підписи.

Неспростовність

Засоби для забезпечення неспростовності треба застосовувати, коли важливо мати підтвердження того, що повідомлення було відправлено та (або) отримано, і що мережа передала це повідомлення. Існують специфічні криптографічні засоби безпеки як основа неспростовності (цілісність даних та неспростовність).

Збої програмного забезпечення

Збої програмного забезпечення можуть зруйнувати цілісність даних та інформації, яку обробляють за допомогою цього програмного забезпечення. Засоби безпеки цілісності наведено нижче.

Звітування про некоректне функціонування програмного забезпечення. Звітування про збої, проведене швидко, наскільки це можливо, допомагає зменшити збитки, якщо такі збої виникають.

Експлуатація. Контроль за безпекою можна використовувати для гарантування того, що програмне забезпечення функціонує коректно, а контроль змін програмного забезпечення допоможе уникнути проблем через оновлення чи внесення змін до програмного забезпечення.

Резервування. Резервні копії, наприклад, створені раніше, можна використовувати для відновлення цілісності даних, що були оброблені програмним забезпеченням, яке не функціонує коректно.

Безпека цілісності даних. Для безпеки цілісності даних можна використовувати криптографічні методи.

Збої постачання (живлення, кондиціонування повітря)

Збої постачання можуть викликати проблеми цілісності, якщо через них виникли інші збої. Наприклад, збої постачання можуть спричинити збої апаратного забезпечення, технічні пошкодження чи проблеми з накопичувачами інформації. Засоби безпеки від цих специфічних проблем

можна знайти у відповідних підпунктах; засоби захисту від збоїв постачання наведено нижче.

Живлення та кондиціонування повітря. Потрібно використовувати засоби безпеки живлення та кондиціонування повітря, наприклад, безпека від сплесків напруги, коли необхідно уникнути будь-яких проблем, пов’язаних зі збоями постачання.

Резервування. Резервування потрібно використовувати для відновлення пошкодженої інформації.

Технічні пошкодження

Технічні пошкодження, наприклад, у мережі, можуть зруйнувати цілісність будь-якої інформації, що зберігається чи обробляється в цій мережі. Засоби безпеки від технічних пошкоджень наведено нижче.

Експлуатація. Керування конфігурацією та змінами, так само, як керування потужностями, треба використовувати, щоб уникнути збоїв у будь-якій системі чи мережі. Документацію та обслуговування використовують для забезпечення безперебійної роботи системи чи мережі.

Керування мережею. Для мінімізації ризиків технічних пошкоджень потрібно використовувати методику експлуатації, планування системи та належну конфігурацію мережі.

Електричне живлення та кондиціонування повітря. Потрібно використовувати засоби безпеки живлення та кондиціонування повітря, наприклад, захист від коливань напруги, коли необхідно уникнути будь-яких проблем, пов’язаних зі збоями постачання.

Резервування. Резервування треба використовувати для відновлення пошкодженої інформації.

Помилки передавання

Помилки передавання можуть зруйнувати цілісність інформації, що передається. Засоби безпеки цілісності наведено нижче.

Прокладання кабелю. Ретельне планування та прокладання кабелю допоможе уникнути помилок, наприклад, якщо помилка спричинена перевантаженням.

Керування мережею. Мережевим обладнанням потрібно належним чином керувати та обслуговувати його, щоб уникнути помилок передавання.

Безпека цілісності даних. Для безпеки від випадкових помилок передавання в протоколах передавання даних можна використовувати контрольні суми та циклічні надлишкові коди. Для безпеки цілісності даних від зловмисних атак під час передавання використовують криптографічні методи.

Несанкціонований доступ до інформаційних систем, даних, служб та програм

Несанкціонований доступ до інформаційних систем, даних, служб та програм може бути загрозою цілісності інформації, якщо можлива

несанкціонована модифікація. Засоби безпеки від несанкціонованого доступу охоплюють належну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи та поділ мережі на мережевому рівні.

Автентифікація. Для запобігання несанкціонованому доступу відповідні засоби ідентифікації та автентифікації потрібно використовувати разом з контролем логічного доступу.

Контроль логічного доступу та аудит. Треба використовувати засоби безпеки для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Перегляд та аналіз журналів аудиту можуть виявити недозволені дії працівників, що суперечать правам доступу до системи.

Поділ мережі. Для ускладнення несанкціонованого доступу треба зробити поділ мережі.

Фізичний контроль доступу. Крім логічного контролю доступу, безпека може забезпечуватись фізичним контролем доступу.

Контроль носіїв інформації. Якщо контрольовані дані зберігаються на інших носіях інформації (наприклад, дисках або флешках), для захисту цих носіїв від несанкціонованого доступу потрібно застосовувати контроль носіїв інформації.

Цілісність даних. Для захисту цілісності даних під час зберігання чи передавання використовують криптографічні методи.

Використання несанкціонованих програм та даних

Використання несанкціонованих програм та даних піддає небезпеці цілісність інформації, яка зберігається та обробляється з системою, якщо програми та дані використовуються для зміни інформації несанкціонованим шляхом, або якщо програми та дані містять зловмисний код (наприклад ігри). Засоби безпеки від цього наведено нижче.

Інформування про безпеку та навчання. Всі працівники мають бути попереджені про те, що вони не повинні інсталювати та використовувати жодне програмне забезпечення без дозволу керівника інформаційної безпеки або будь-кого, хто може відповідати за безпеку системи.

Резервування. Резервування треба використовувати для відновлення пошкодженої інформації.

Автентифікація. Відповідні засоби ідентифікації та автентифікації потрібно використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

Контроль логічного доступу та аудит. Контроль логічного доступу має гарантувати, що тільки уповноважені особи можуть застосовувати програмне забезпечення для обробки та зміни інформації. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Безпека від зловмисного коду. Перед використанням всі програми та дані треба перевіряти на наявність зловмисного коду.

Несанкціонований доступ до носіїв даних

Несанкціонований доступ та використання носія даних може піддавати небезпеці цілісність, оскільки він дозволяє несанкціоновану зміну інформації, що зберігається на цьому носії. Засоби безпеки цілісності наведено нижче.

Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичної безпеки, ідентифікованості носіїв інформації, для запобігання несанкціонованому доступу, а перевірка цілісності – для виявлення будь-якого порушення цілісності інформації на носії. Спеціальні заходи запровадити для безпеки таких легкозмінних носіїв інформації, як диски, флешки, папір тощо.

Фізичний захист. Відповідна безпека кімнат (міцні стіни та вікна, а також максимально можливий контроль фізичного доступу) та аксесуари безпеки можуть захистити від несанкціонованого доступу.

Цілісність даних. Для безпеки цілісності даних під час їхнього зберігання на носії інформації використовують криптографічні методи.

Помилки користувача

Помилки користувача можуть зруйнувати цілісність інформації. Засоби безпеки від них наведено нижче.

Інформування про безпеку та навчання. Всі користувачі мають бути навчені належним чином, щоб уникнути помилок під час обробки інформації. Це навчання має охоплювати тренування на визначення дій процедури експлуатації чи безпеки.

Резервування. Резервні копії, наприклад, створені раніше, можна використовувати для відновлення цілісності даних, які було знищено через помилки користувача.

Засоби безпеки доступності

Типи загроз, що можуть піддавати небезпеці доступність, наведено нижче разом із засобами безпеки від цих загроз. Якщо це важливо для вибору засобів безпеки, треба враховувати тип і характеристики інформаційної системи.

Потрібно відмітити, що більшість засобів безпеки забезпечує «загальну» безпеку, тобто вони не націлені на окремі загрози, а забезпечують безпеку через підтримування загального ефективного керування інформаційною безпекою. Тому вони не описані тут детально, але їхній вплив не треба недооцінювати, і вони мають бути реалізовані для загальної ефективної безпеки.

Вимоги до доступності можуть коливатися від некритичних за часом даних або інформаційних технологій систем (але втрата таких даних та непрацездатність таких систем все ще вважається критичною) до надто критичних за часом даних або систем. Перші треба захищати резервуванням, в той час як останні можуть потребувати наявності резервної системи.

Руйнівний напад

Інформація може бути знищена під дією руйнівних нападів. Засоби безпеки проти них наведено нижче.

Дисциплінарний процес. Всі працівники мають бути попереджені про наслідки у випадку, якщо вони (зловмисно чи незловмисно) знищать інформацію.

Контроль носіїв інформації. Всі носії інформації мають бути відповідно захищеними від несанкціонованого доступу, використовуючи фізичний захист та облік всіх носіїв.

Резервування. Треба робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація недоступні (з будь-якої причини), для відновлення інформації треба використовувати резервну копію чи попередню резервну копію.

Матеріальна безпека. Для запобігання несанкціонованому доступу, що сприятиме несанкціонованому руйнуванню обладнання чи інформації, треба використовувати фізичний контроль за доступом.

Автентифікація. Відповідні засоби ідентифікації та автентифікації потрібно використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

Контроль та аудит логічного доступу. Контроль логічного доступу повинен гарантувати, що не буде несанкціонованого доступу до інформації, який може її знищити. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Псування носіїв даних

Псування носіїв даних загрожує доступності інформації, що зберігається на цих носіях. Якщо доступність є важливим чинником, потрібно застосовувати нижченаведені засоби безпеки.

Контроль носіїв інформації. Регулярне тестування носіїв даних має виявляти будь-яке псування, бажано до того, як інформація стане дійсно недоступною. Носії мають зберігатись у такий спосіб, щоб не було ніякого зовнішнього впливу, який міг би спричинити псування.

Резервування. Треба робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація недоступна (з будь-якої причини), для відновлення інформації треба використовувати резервну копію чи попередню резервну копію.

Збої комунікаційного обладнання та служб

Збої комунікаційного обладнання та служб загрожують доступності інформації, що передається за допомогою цих послуг. Залежно від причин збою, може бути корисним розглянути положення «Збої програмного забезпечення», «Збої постачання» чи «Технічні несправності».

Надлишковість та резервування. Надмірне запровадження компонентів комунікаційних служб може бути використано для зниження ймовірності збоїв комунікаційних служб. Залежно від розміру максимально припустимого простою, запасне обладнання також можна використовувати

для задоволення потреб. У будь-якому випадку, дані конфігурації та розташування мають бути також зарезервовані для забезпечення доступності у випадку надзвичайної ситуації.

Керування мережею. Мережевим обладнанням треба належним чином керувати та обслуговувати його, щоб уникнути помилок.

Прокладання кабелю. Ретельне планування та прокладання кабелю можуть запобігти пошкодженням; якщо є підозра, що лінію може бути пошкоджено, цю версію потрібно перевірити.

Неспростовність. Якщо потребують підтвердження мережевого доставляння, посилання чи отримання повідомлення, треба застосовувати неспростовність; тоді пошкодження комунікацій чи зниклу інформацію можна легко виявити.

Вогонь, вода

Інформація та обладнання можуть бути знищені вогнем та (або) водою. Засоби безпеки від вогню та води наведено нижче.

Фізична безпека. Всі будівлі та кімнати, які містять обладнання чи носії, що зберігають важливу інформацію, треба належним чином захищати від вогню і води.

План неперервності бізнесу. Для безпеки бізнесу від згубних впливів вогню та води потрібно розробити план неперервності бізнесу та доступні резервні копії важливої інформації.

Помилки обслуговування

Якщо обслуговування виконують нерегулярно чи в процесі його виконання трапляються помилки, то доступність інформації знаходиться під загрозою. Засоби безпеки в цьому випадку наведено нижче.

Обслуговування. Належне обслуговування – це найкращий шлях уникнути помилок обслуговування.

Резервування. Якщо трапляються помилки обслуговування, для відновлення доступності втраченої інформації можна використовувати резервні копії.

Зловмисний код

Зловмисний код можна використовувати, щоб обійти автентифікацію та всі служби і функції безпеки, пов’язані з нею. Внаслідок цього він може призвести до втрати доступності, наприклад, якщо дані чи файли знищені особою, яка отримала несанкціонований доступ за допомогою зловмисного коду, чи безпосередньо зловмисним кодом.

Засоби безпеки проти нього наведено нижче.

Безпека від зловмисного коду. Перед використанням всі програми та дані треба перевіряти на наявність зловмисного коду.

Реагування на порушення. Своєчасне звітування про будь-які незвичні порушення може обмежити пошкодження від ураження зловмисним кодом. Виявлення вторгнень можна використовувати, щоб виявити спроби входу до системи чи мережі.

Приховування особистості користувача

Приховування особистості користувача можна використовувати, щоб обійти автентифікацію, а також усі служби та функції безпеки, пов'язані з нею. В результаті, воно може призводити до проблем доступності кожного разу, коли це приховування дозволяє вилучити або знищити інформацію. Засоби безпеки в цій сфері наведено нижче.

Автентифікація. Приховування стає важчим, якщо застосовують засоби ідентифікації та автентифікації, які базуються на комбінаціях чогось відомого, чогось наявного, а також внутрішніх характеристик користувача.

Контроль та аудит логічного доступу. Контроль логічного доступу не може відрізнити авторизованого користувача від когось, хто видає себе за цього авторизованого користувача, але використання механізмів контролю доступу може зменшити сферу впливу. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Безпека від зловмисного коду. Оскільки один із шляхів отримання паролів – це введення зловмисного коду для їхнього перехоплення, має бути безпека від таких програм.

Керування мережею. Ще один спосіб неуповноваженого доступу – приховування користувача в потоці, наприклад, електронної пошти.

Резервування даних. Резервування даних не може захистити від приховування особистості користувача, але зменшує вплив подій, пов'язаних з пошкодженнями, що виникають внаслідок цього.

Неправильне направлення/перенаправлення повідомлень

Неправильне направлення – це зловмисне чи незловмисне неправильне спрямування повідомлень, у той час, як перенаправлення можна застосовувати як для добрих, так і для недобрих цілей. Перенаправлення можна виконувати, наприклад, для підтримування цілісності доступності. Неправильні направлення та перенаправлення повідомлень призводять до втрати доступності повідомлень. Засоби безпеки проти цього наведено нижче.

Керування мережею. Засоби безпеки від неправильного направлення та перенаправлення.

Неспростовність. Якщо є потреба підтвердити мережеве доставляння, відправлення або отримання повідомлення, треба застосовувати неспростовність.

Зловживання ресурсами

Зловживання ресурсами може призвести до недоступності інформації чи служб. Засоби безпеки від цього наведено нижче.

Персонал. Весь персонал має бути попереджений про наслідки зловживання ресурсами; за потреби треба запровадити дисциплінарні заходи.

Експлуатація. Для виявлення несанкціонованих дій за системою потрібно слідкувати, а для мінімізації можливостей зловживання привілеями потрібно запровадити розподіл обов'язків.

Автентифікація. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу,

Контроль та аудит логічного доступу. Треба використовувати засоби захисту для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Керування мережею. Для мінімізації можливостей зловживання ресурсами в мережах треба застосовувати відповідну конфігурацію та розподіл мережі.

Стихійні лиха

Для безпеки від втрати інформації та послуг через стихійні лиха треба застосовувати такі засоби безпеки.

Безпека від стихійних лих. Всі будівлі мають бути захищені, наскільки це можливо, від стихійних лих.

План неперервності бізнесу. Має бути наявний та повністю перевірений план неперервності бізнесу для кожної будівлі, резервних копій всієї важливої інформації, мають бути доступні служби та ресурси.

Збої програмного забезпечення

Збої програмного забезпечення можуть знищити доступність даних та інформацію, що обробляється цим програмним забезпеченням. Засоби безпеки доступності наведено нижче.

Звітування про збої програмного забезпечення. Звітування про збої якомога швидше допоможе обмежити пошкодження у випадку їхнього виникнення.

Експлуатація. Тестування безпеки можна використовувати для гарантування коректного функціонування програмного забезпечення, а контроль змін програмного забезпечення допоможе уникнути проблем цих програм, спричинених оновленнями чи іншими змінами програмного забезпечення.

Резервування. Резервні копії, наприклад, зроблені останніми, можна використовувати для відновлення даних, оброблених програмним забезпеченням, що функціонує некоректно.

Збої постачання (живлення, кондиціонування повітря)

Збої постачання можуть викликати проблеми доступності, якщо через них виникли інші збої. Наприклад, пошкодження постачання можуть спричинити збої апаратного забезпечення, технічні пошкодження чи проблеми з накопичувачами інформації. Засоби безпеки від цих специфічних проблем можна знайти у відповідних підпунктах; засоби захисту від збоїв постачання наведено нижче.

Живлення та кондиціонування повітря. Треба використовувати засоби безпеки живлення та кондиціонування повітря, наприклад, захист від сплесків напруги, коли необхідно уникнути будь-яких проблем, пов’язаних зі збоями постачання.

Резервування. Необхідно робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація втрачені через збої постачання, для відновлення інформації потрібно використовувати резервну копію чи попередню резервну копію.

Технічні пошкодження

Технічні пошкодження, наприклад, у мережах, можуть знищити доступність будь-яких матеріальних носіїв інформації, що зберігається чи обробляється в цій мережі. Засоби безпеки від технічних пошкоджень наведено нижче.

Експлуатація. Керування конфігурацією та змінами, так само, як і керування потужностями, треба використовувати, щоб уникнути збоїв в будь-якій інформаційній технології системи. Документацію та обслуговування використовують для забезпечення безпроблемної роботи системи.

Керування мережею. Для мінімізації ризиків технічних пошкоджень треба використовувати методику експлуатації, планування системи та відповідну конфігурацію мережі.

План неперервності бізнесу. Для безпеки бізнесу від згубних ефектів технічних пошкоджень треба розробити план неперервності бізнесу та доступні резервні послуги, ресурси та копії важливої інформації.

Крадіжки

Крадіжки явно піддають небезпеці доступність інформації та інформаційних технологій обладнання. Засоби безпеки від крадіжок наведено нижче.

Фізичні засоби. Це може бути матеріальний захист, що робить доступ в будівлю, зону чи кімнату, яка містить обладнання та інформацію, складнішим, або це можуть бути специфічні засоби від крадіжок.

Персонал. Для ускладнення крадіжок мають бути наявні засоби безпеки персоналу (контроль зовнішнього персоналу, угоди конфіденційності тощо).

Контроль носіїв інформації. Будь-який носій, що містить важливий матеріал, треба захищати від крадіжок.

Перевантаження каналів

Перевантаження каналів загрожує доступності інформації, що передається по цих каналах. Засоби безпеки доступності наведено нижче.

Надлишковість та резервування. Надлишкова реалізація компонентів комунікаційних послуг може бути використана для зниження ймовірності збоїв комунікаційних служб. Залежно від розміру максимального припустимого простою запасне обладнання також треба використовувати для задоволення вимог. У будь-якому випадку, дані конфігурації та розташування мають бути також зарезервовані для забезпечення доступності у випадку надзвичайної ситуації.

Керування мережею. Щоб уникнути перевантаження треба використовувати відповідну конфігурацію, керування та адміністрування мереж і комунікаційних послуг.

Помилки передавання

Помилки передавання можуть зруйнувати доступність інформації, що передається. Засоби безпеки доступності наведено нижче.

Прокладання кабелю. Ретельне планування та прокладання кабелю може допомогти уникнути помилок передавання, наприклад, якщо помилка викликана перевантаженням.

Керування мережею. Керування мережею не може захистити від помилок передавання, а може використовуватись для виявлення проблем, що виникають через помилки передавання та підняття тривоги в таких випадках. Це дозволяє своєчасно реагувати на такі проблеми.

Несанкціонований доступ до інформаційних систем, даних, служб та програм

Несанкціонований доступ до інформаційних систем, даних, служб та програм може бути загрозою доступності інформації, якщо можливий несанкціонований доступ. Засоби безпеки від несанкціонованого доступу охоплюють відповідну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи та поділ мережі на мережевому рівні.

Автентифікація. Відповідні засоби ідентифікації та автентифікації потрібно використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

Контроль та аудит логічного доступу. Треба використовувати засоби безпеки для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Перегляд та аналіз журналів аудиту може виявити неуповноважені дії співробітників з правами доступу до системи.

Поділ мережі. Щоб несанкціонований доступ до мережі був важчим, треба здійснити поділ мережі.

Контроль фізичного доступу. Крім логічного контролю доступу безпеку можна забезпечувати фізичним контролем доступу.

Контроль носіїв інформації. Якщо важливі дані зберігаються на інших носіях інформації (наприклад, дисках), для безпеки цих носіїв від несанкціонованого доступу потрібно застосовувати контроль носіїв інформації.

Використання несанкціонованих програм та даних

Використання несанкціонованих програм та даних піддає небезпеці доступність інформації, що зберігається та обробляється в системі, в якій це відбувається, якщо програми та дані використовують для вилучення матеріальних носіїв інформації несанкціонованим шляхом, або якщо програми та дані містять зловмисний код (наприклад, ігри). Засоби безпеки від цього наведено нижче.

Інформування про безпеку та навчання. Всі працівники мають бути попереджені про те, що вони не повинні запускати жодне програмне забезпечення без дозволу керівника інформаційної безпеки або будь-кого, хто може відповідати за безпеку системи.

Резервування. Резервні копії треба використовувати для відновлення пошкодженої інформації.

Автентифікація. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

Контроль та аудит логічного доступу. Контроль логічного доступу повинен гарантувати, що тільки уповноважені особи можуть застосовувати програмне забезпечення для обробляння та вилучення матеріальних носіїв інформації. Перегляд та аналіз журналів аудиту може виявити несанкціоновані дії.

Безпека від зловмисного коду. Перед використанням всі програми та дані треба перевіряти на наявність зловмисного коду.

Несанкціонований доступ до носіїв даних

Несанкціонований доступ та використання носія даних може піддавати небезпеці доступність, оскільки він може спричинити несанкціоноване знищення інформації, яка зберігається на цьому носії. Засоби безпеки конфіденційності наведено нижче.

Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичного захисту, обліку носіїв інформації для запобігання несанкціонованому доступу до інформації, що зберігається на цих носіях. Спеціальні заходи треба вжити для захисту легкозмінних носіїв інформації: диски, папір тощо.

Фізична безпека. Відповідний захист кімнат (міцні стіни та вікна, а також контроль фізичного доступу) та аксесуари безпеки захищають від несанкціонованого доступу.

Помилки користувача

Помилки користувача можуть знищити доступність інформації. Засоби безпеки від них наведено нижче.

Інформування про безпеку та навчання. Всі користувачі мають бути відповідно навчені, щоб уникнути помилок під час обробляння матеріальних носіїв інформації. Це навчання повинно охоплювати тренування, яке навчає таким діям, як процедури експлуатації чи безпеки.

Резервування. Резервні копії, наприклад, створені попереднього разу, можна використовувати для відновлення інформації, що була знищена через помилки користувача.

Засоби безпеки спостережності, автентичності та надійності

Сфера застосування спостережності, автентичності та надійності дуже відрізняється в різних галузях. Ці відмінності означають, що можна застосувати багато різних засобів безпеки. Тому нижче наведено загальну настанову.

Засоби безпеки забезпечують «загальну» безпеку, тобто вони спрямовані на низку загроз та забезпечують захист через підтримування загального ефективного керування інформаційною безпекою. Тому вони не наведені тут, але їхній вплив не потрібно недооцінювати, тому їх потрібно впроваджувати для загального ефективного захисту.

Спостережність

Для захисту спостережності можна розглядати будь-яку загрозу, що може призвести до неможливості пов'язати якісь дії з конкретним об'єктом чи суб'єктом. Деякі приклади таких загроз: спільне використання облікового запису, відсутність трасування дій, приховування особистості користувача, збої програмного забезпечення, несанкціонований доступ до інформаційних систем, даних, служб та програм, а також слабка автентифікація особистості.

Є два типи спостережності, які необхідно розглянути. Один пов'язаний з визначенням користувачів, відповідальних за конкретні дії над інформацією та інформаційними системами. Цю функцію виконують журнали аудиту. Інший тип пов'язаний з ідентифікованістю між користувачами в системі. Його можна досягнути через послуги неспростовності, розділення знань та подвійний контроль.

Багато засобів безпеки можна використовувати для впровадження неспростовності чи сприяти її запровадженню. Можна застосовувати засоби, що залежать від таких чинників: політика безпеки, інформування про безпеку та контроль і аудит логічного доступу до одноразових паролів та контролю носіїв інформації. Впровадження політики володіння інформацією є необхідною умовою спостережності. Вибір специфічних засобів безпеки буде залежати від певного використання спостережності в конкретній сфері.

Автентичність

Може бути зменшена будь-яка загроза, яка може призводити до того, що суб'єкт, система чи процес не будуть упевнені в автентичності об'єкта. Наприклад, ситуації, що можуть призвести до виникнення цього, містять неконтрольовані зміни даних, неперевірене джерело даних та джерело даних, що не підтримується.

Багато засобів безпеки можна використовувати для впровадження автентичності чи сприяти її впроваджено. Можна застосовувати засоби від підписаних довідкових даних, контролю та аудиту логічного доступу до використання цифрових підписів. Вибір специфічних засобів безпеки буде залежати від визначеного використання автентичності в конкретній сфері.

Надійність

Будь-яка загроза, що може призвести до суперечливої поведінки систем чи процесів, зменшить рівень надійності. До таких загроз належать продуктивність системи та ненадійне обслуговування. Втрата надійності може проявитися в неякісний роботі з клієнтами чи втраті довіри клієнтів.

Багато засобів захисту можна використовувати для впровадження надійності чи сприяти її впровадженню. Можна застосовувати такі засоби, як плани неперервності бізнесу, введення надлишковості у фізичну архітектуру та обслуговування системи до ідентифікації та автентифікації, контролю і аудиту логічного доступу. Вибір специфічних засобів безпеки буде залежати від визначеного використання автентичності в конкретній сфері.

13.6 Вибір засобів безпеки відповідно до детальних оцінок

Вибір засобів безпеки відповідно до детальних оцінок здійснюють згідно з принципами, наведеними в попередніх розділах. Детальний аналіз ризиків дозволяє враховувати спеціальні вимоги та обставини інформаційної системи та її цінностей. Відмінність від використання, наведеного у попередніх розділах, – це обсяг робіт та подробиці, зібрані протягом процесу оцінювання. Тому можливе кваліфіковане обґрунтування вибраних засобів безпеки.

В ISO/IEC TR 13335-3 описано керування інформаційною безпекою. Крім того, наведено інші питання, можливі варіанти стратегії аналізу ризиків та рекомендований підхід до аналізу ризиків. Головними варіантами стратегій для використання в організації є:

– використання базового підходу для всіх інформаційних технологій систем;

– використання детального аналізу ризиків для всіх інформаційних технологій систем;

– використання «рекомендованого підходу», тобто дотримуватися високорівневого аналізу ризиків для всіх інформаційних технологій систем, базового підходу для інформаційних технологій систем малого ризику і детального аналізу ризиків для інформаційних технологій систем високого ризику.

Якщо для визначення засобів безпеки було вирішено використовувати детальний аналіз ризиків для всіх інформаційних технологій систем, інформація про те, як вибирати засоби захисту, і як ефективно використовувати результати детального аналізування ризиків. Проте може використовуватися інформація про засоби безпеки для специфічних інформаційних технологій систем та зв’язок між проблемами безпеки, загрозами і засобами безпеки.

Принципи вибору

Є чотири основних аспекти, на які спрямований засіб безпеки: впливи, загрози, вразливості та ризики самі по собі. Засоби спрямовують на самі ризики, коли приймається рішення зменшити чи уникнути ризиків, а не приймати їх, наприклад, для зменшення ризику – проведення страхування, а прикладом, щоб уникнути ризику, є переміщення контрольованої інформації в іншу інформаційну систему. Компоненти, що всі разом

створюють ризики, тобто впливи, загрози та вразливості, є головними цілями засобів безпеки. Способи, якими засоби можна направляти на ці аспекти, такі:

1) загрози – засоби безпеки можуть зменшити ймовірність виникнення загрози (наприклад, розглянемо загрозу втрати даних через помилки користувача, тоді навчальний курс для користувачів зменшить кількість цих помилок) чи, у випадку зловмисного нападу, вони можуть спинити його через збільшення технічної складності успішної атаки;

2) вразливість – засоби безпеки можуть усунути вразливість чи зробити її менш серйозною (наприклад, якщо внутрішня мережа, що з'єднана з зовнішньою мережею, вразлива до несанкціонованого доступу, то реалізація відповідного брандмауера зробить з'єднання менш вразливим, а роз'єднання усуне цю вразливість);

3) вплив – засоби безпеки можуть зменшити чи усунути вплив (якщо зловмисний вплив являє собою недоступність інформації, він зменшується через створення копій інформації, які надійно зберігаються в іншому місці, та готовність до активування плану неперервності бізнесу). Добре організований облік і аналіз журналів аудиту та засобів сигналізації може допомогти ранньому виявленню інциденту та знизити зловмисний вплив на бізнес.

Як і де використовують засіб безпеки, може бути суттєва різниця від тієї користі, яку отримано завдяки його запровадженню. Дуже часто загрози можуть використовувати більше ніж одну вразливість. Тому, якщо засіб безпеки використовують, щоб запобігти виникненню такої загрози, він може бути спрямованим на декілька вразливостей одночасно. Обернене також спаведливо – засіб безпеки, що захищає вразливість, може бути спрямованим на декілька безпек. Ці переваги слід розглядати, за можливості, під час вибору засобів безпеки. Ці додаткові переваги потрібно завжди документувати, щоб мати повноту вимог безпеки, які задовольняє будь-який засіб безпеки.

Взагалі, засоби безпеки можуть забезпечувати один чи більше з таких типів безпеки: запобігання, стримування, виявлення, зменшення, відновлення, виправлення, моніторинг та обізнаність. Яка з цих властивостей найкраща, залежить від конкретних обставин та від призначення кожного засобу, в багатьох випадках засоби безпеки забезпечують більше одного типу безпеки, що, знову ж таки, забезпечує додаткові переваги. За можливості, треба надавати перевагу тим засобам, які мають багато переваг, ніж ті, що їх стільки не мають.

Безпека повинна завжди показувати розумний баланс щодо ефектів, згаданих вище. Якщо занадто великий акцент робиться на типі засобу безпеки, малоймовірно, що загальна безпека буде ефективною. Наприклад, якщо більшість засобів стримування використовують без адекватних засобів виявлення, щоб визначити, коли стримування не спрацювало, загальна безпека не буде ефективною.

Перед реалізацією запропоновані засоби захисту треба порівняти з наявними засобами, щоб оцінити, що треба розширяти чи оновлювати. Якщо так, то це може бути дешевше, ніж запровадження нових засобів захисту.

Під час вибору засобів захисту важливо зважувати на вартість реалізації засобів захисту відносно вартості цінностей, що захищаються, та строки повернення інвестицій, пов'язаних зі зниженням ризику. Вартість реалізації та обслуговування засобу може бути набагато вищою, ніж вартість самого засобу, тому це треба враховувати під час вибору.

Технічні обмеження, а саме: вимоги продуктивності, керованості (вимоги обслуговування діяльності) та питань сумісності можуть заважати використанню деяких засобів безпеки. В цих випадках керівники системи та безпеки мають працювати разом для прийняття оптимальних рішень. Може трапитися випадок, коли засіб захисту буде знижувати продуктивність. Знову таки, керівник системи та керівник безпеки разом повинні прийняти рішення, що дозволить забезпечити необхідну продуктивність за умови гарантованої достатньої безпеки.

Такі аспекти, як законодавство про безпеку приватного життя та право можуть вимагати, щоб були наявні певні засоби захисту, тому використовується визначення незмінних базових елементів.

13.7 Розроблення базової безпеки організації

Коли організація вирішує запровадити базову безпеку до всієї організації чи до її частин, треба розглянути такі питання.

Які частини організації чи систем можуть бути захищені певним базовим рівнем, а які потребують іншого, і чи може той самий базовий рівень запроваджуватись для цілої організації?

На який рівень безпеки має бути орієнтована базова безпека (чи різні базові безпеки)?

Як можуть бути визначені засоби захисту, що формують іншу базову безпеку (за потреби)? На рис. 13.3 зображено різні способи застосування базової безпеки.

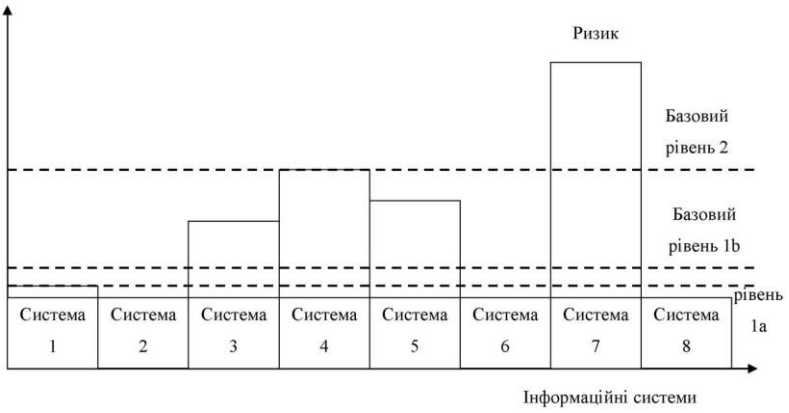


Рисунок 13.3 – Різні базові рівні

Перевага застосування різних базових рівнів в одній організації – це те, що більшість систем буде захищена належним чином, тобто застосовується не надмірно малий та не надмірно великий захист (наприклад, для інформаційних технологій з базовим рівнем 1 – системи 1, 2, 6, 8 та інформаційних технологій з базовим рівнем 2 – це системи 3, 4 та 5, як зазначено на рис. 13.3). Якщо інформаційні системи з різними вимогами безпеки є «насправді різними» (в тому сенсі, що більшість засобів безпеки, які потрібні для безпеки інформаційних технологій, різні), тоді для організації рекомендовано використовувати різні бази. Якщо вимоги до безпеки фундаментально відрізняються, рішення про використання базового підходу має бути переглянуто.

З іншого боку, якщо єдина відмінність між різними базовими рівнями – це та, що виникає потреба у деяких додаткових засобах захисту для формування вищих базових рівнів, тоді, можливо, не варто запроваджувати декілька різних базових рівнів. Якщо запроваджений тільки один базовий рівень, накладні видатки організації можуть бути значно зменшені, і кожен в організації зможе покладатися на наявність однакового рівня безпеки.

Рівень базової безпеки, на який треба орієнтуватися, звичайно, залежить від рішення, скільки рівнів базової безпеки можна логічно запровадити: один чи більше. Якщо вибрані різні базові рівні, ці рівні можуть бути встановлені достатньо точно до вимог безпеки інформаційних технологій систем, які потрібно захищати. Загалом, жоден базовий рівень не повинен бути спрямований на безпеку нижче найнижчих вимог до безпеки інформаційних технологій систем, які треба захищати (наприклад, нижче вимог інформаційних технологій системи 2 на рис. 13.3). Доцільно орієнтуватись на рівень, що є достатнім для більшості (базовий рівень 1a на рис. 13.3) чи всіх (базовий рівень 1b) інформаційних технологій систем, призначених для захисту. Часто доцільно орієнтуватись на найвищий рівень безпеки інформаційних систем для забезпечення безпеки їх базовими засобами, оскільки це, зазвичай, не дуже дорого, але забезпечує достатню безпеку для всіх задіяних інформаційних технологій систем. Необхідно уважно розглянути запроваджені інформаційні технології систем для прийняття остаточного рішення, які інформаційні технології системи будуть захищатись тим же базовим рівнем. Деякі інформаційні технології системи багато в чому схожі за сутністю та (або) за вимогами до безпеки – в цьому випадку є корисно захищати їх тим же самим базовим рівнем. З іншого боку, якщо декілька інформаційних технологій повністю відрізняються в своїх вимогах до безпеки, дуже часто найпростіше розглядати їх окремо.

Те ж саме і у випадку, якщо організація вирішує реалізовувати однаковий базовий рівень по всій організації. Ця базова безпека може бути орієнтована на три різні рівні:

– низький рівень, долучаючи специфічні засоби безпеки, щоб убезпечити всі інформаційні технології системи з вищими вимогами;

– середній рівень, долучаючи специфічні засоби безпеки, щоб убезпечити всі інформаційні технології системи з вищими вимогами;

– високий рівень, що є достатнім для безпеки всіх інформаційних технологій систем, передбачених базовою безпекою.

Як описано вище, середній та високий рівні базової безпеки можуть бути зручними для багатьох організацій, щоб досягти достатнього захисту, надійної безпеки по всій організації та зниження організаційних видатків. У підсумку, рішення треба приймати відповідно до політики безпеки організації та вимог інформаційних технологій систем, що розглядаються.

Запитання для самоконтролю

1. Яку має перевагу проведення детального аналізу ризику?
2. Коли повинні призначатися специфічні засоби захисту на основі детального аналізу ризиків?
3. Коли може бути досягнуто базову безпеку для інформаційної системи?
4. Що завжди потребує процес вибору засобів безпеки?
5. Поясніть на який рівень безпеки має орієнтуватися базова безпека?
6. Що треба визначити після оцінювання умов навколишнього середовища та компонентів інформаційної системи?
7. Які дії можуть бути корисними для визначення наявних чи планованих засобів безпеки?
8. Що містить реагування на порушення?
9. Які засоби захисту в сфері персоналу?
10. Які засоби захисту в сфері фізичної безпеки?
11. Які питання треба розглянути, коли організація вирішує запровадити базову безпеку до всієї організації чи до її частин?

ГЛАВА 14
ПРОЦЕДУРНИЙ РІВЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

14.1 Основні класи заходів процедурного рівня

Ми починаємо розгляд заходів безпеки, які орієнтовані на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, і вони ж виявляються головною загрозою, тому «людський чинник» заслуговує на особливу увагу.

В українських компаніях накопичений багатий досвід регламентування й реалізації процедурних (організаційних) заходів, однак справа в тому, що вони прийшли з «докомп'ютерного» минулого, тому потребують переоцінювання.

Варто усвідомити той ступінь залежності від комп'ютерної обробки даних, у який потрапило сучасне суспільство. Без усякого перебільшення можна сказати про необхідність інформаційної цивільної оборони. Спокійно, без перебільшення, потрібно пояснювати суспільству не тільки переваги, але й небезпеки, пов'язані з використанням інформаційних технологій. Акцент варто робити не на військовій або кримінальній стороні справи, а на цивільних аспектах, пов'язаних з підтримкою нормального функціонування апаратного й програмного забезпечення, тобто концентруватися на питаннях доступності й цілісності даних.

На процедурному рівні можна виділити такі класи заходів:

- керування персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

14.2 Керування персоналом

Керування персоналом починається з прийому нового співробітника на роботу й навіть раніше – зі складання посадових інструкцій. Уже на даному етапі бажано залучити до роботи фахівця з інформаційної безпеки для визначення комп'ютерних привілеїв, асоційованих з посадою. Існує два загальних принципи, які варто мати на увазі:

- розподіл обов'язків;
- мінімізація привілеїв.

Принцип розподілу обов'язків пропонує так розподіляти ролі й відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, небажана ситуація, коли великі платежі від імені організації виконує одна людина. Надійніше доручити одному співробітникові оформлення заявок на подібні платежі, а іншому – завіряти

ці заявки. Інший приклад – процедурні обмеження дій суперкористувача. Можна штучно «відокремити» пароль суперкористувача, повідомивши першу його частину одному співробітникові, а другу – іншому. Тоді критично важливі дії з адміністрування ІС вони зможуть виконати тільки вдвох, що знижує ймовірність помилок і зловживань.

Принцип мінімізації привілеїв пропонує виділяти користувачам тільки ті права доступу, які необхідні їм для виконання службових обов'язків. Призначення цього принципу очевидно – зменшити збиток від випадкових або навмисних некоректних дій.

Попереднє складання опису посади дозволяє оцінити її критичність і спланувати процедуру перевірки й відбору кандидатів. Чим відповідальніша посада, тим ретельніше потрібно перевіряти кандидатів: навести про них довідки, можливо, поговорити з колишніми товаришами по службі й т. д. Подібна процедура може бути тривалою й дорогою, тому немає сенсу додатково ускладнювати її. У той же час, нерозумно й зовсім відмовлятися від попередньої перевірки, щоб випадково не прийняти на роботу людину з карним минулим або психічним захворюванням.

Коли кандидат визначений, він, імовірно, повинен пройти навчання; принаймні, його варто докладно ознайомити зі службовими обов'язками, а також з нормами й процедурами інформаційної безпеки. Бажано, щоб заходи безпеки були ним засвоєні до вступу на посаду й до введення його системного рахунку з вхідним ім'ям, паролем та привілеями.

З моменту введення системного рахунку починається його адміністрування, а також протоколювання й аналіз дій користувача. Поступово змінюється оточення, у якому працює користувач, його службові обов'язки й т. п. Все це потребує відповідної зміни привілеїв. Технічно складними є тимчасові переміщення користувача, виконання ним обов'язків замість співробітника, що пішов у відпустку, і інші обставини, коли спочатку потрібно надати повноваження, а через деякий час обмежити. У такі періоди профіль активності користувача різко змінюється, що створює труднощі при виявленні підозрілих ситуацій. Певної акуратності варто дотримуватися й при видачі нових постійних повноважень, не забуваючи ліквідувати старі права доступу.

Ліквідація системного рахунку користувача, особливо у випадку конфлікту між співробітником та організацією, повинна вироблятися максимально оперативно (в ідеалі – одночасно з повідомленням про покарання або звільнення). Можливе й фізичне обмеження доступу до робочого місця. Зрозуміло, якщо співробітник звільняється, у нього потрібно прийняти все його комп'ютерне господарство й, зокрема, криптографічні ключі, якщо використовувалися засоби шифрування.

До керівництва співробітниками додається адміністрування осіб, що працюють за контрактом (наприклад, фахівців фірми-постачальника, що допомагають запустити нову систему). Відповідно до принципу мінімізації привілеїв, їм потрібно виділити рівно стільки прав, скільки необхідно, і

забрати ці права відразу після закінчення контракту. Проблема, однак, полягає в тому, що на початковому етапі впровадження «зовнішні» співробітники будуть адмініструвати «місцевих», а не навпаки. Тут на перший план виходить кваліфікація персоналу організації, його здатність швидко навчатися, а також оперативне проведення навчальних курсів. Важливі й принципи вибору ділових партнерів.

Іноді зовнішні організації приймають на обслуговування й адміністрування відповідальні компоненти комп'ютерної системи, наприклад, мережеве устаткування. Нерідко адміністрування виконується у віддаленому режимі. Загалом кажучи, це створює в системі додаткові уразливі місця, які необхідно компенсувати посиленим контролем засобів вилученого доступу або навчанням власних співробітників.

Ми бачимо, що проблема навчання – одна з основних з точки зору інформаційної безпеки. Якщо співробітник не знайомий з політикою безпеки своєї організації, він не може прагнути до досягнення сформульованих у ній цілей. Не знаючи заходів безпеки, він не зможе їх дотримуватися. Навпаки, якщо співробітник знає, що його дії протоколюються, він, можливо, утримається від порушень.

14.3 Фізичний захист

Безпека інформаційної системи залежить від оточення, у якому вона функціонує. Необхідно вжити заходів для захисту будинків і прилеглої території, підтримувальної інфраструктури, обчислювальної техніки, носіїв даних.

Основний принцип фізичного захисту, дотримання якого варто постійно контролювати, формулюється як «безперервність захисту в просторі й часі». Раніше ми розглядали поняття вікна небезпеки. Для фізичного захисту таких вікон бути не повинно.

Ми коротко розглянемо такі напрямки фізичного захисту:

- фізичне керування доступом;
- протипожежні заходи;
- захист підтримувальної інфраструктури;
- захист від перехоплення даних;
- захист мобільних систем.

Засоби фізичного керування доступом дозволяють контролювати та, за необхідності, обмежувати вхід та вихід співробітників і відвідувачів. Контролюватися може весь будинок організації, а також окремі приміщення, наприклад, ті, де розташовані сервери, комунікаційна апаратура й т. п.

При проектуванні й реалізації заходів фізичного керування доступом доцільно застосовувати об'єктний підхід. По-перше, визначається периметр безпеки, що обмежує контрольовану територію. На цьому рівні деталізації важливо продумати зовнішній інтерфейс організації – порядок

входу/виходу штатних співробітників і відвідувачів, внесення/винесення техніки. Усе, що не входить у зовнішній інтерфейс, повинно бути інкапсульовано, тобто захищене від несанкціонованих проникнень.

По-друге, виробляється декомпозиція контрольованої території, виділяються (під) об'єкти й зв'язки (проходи) між ними. За такої, більш глибокої деталізації варто виділити серед підоб'єктів найбільш критичні з погляду безпеки й забезпечити до них підвищену увагу. Декомпозиція повинна бути семантично виправданою, що забезпечує розмежування таких різнорідних сутностей, як устаткування різних власників або персонал, що працює з даними різного ступеня критичності. Важливо зробити так, щоб відвідувачі, за можливості, не мали безпосереднього доступу до комп'ютерів або, у крайньому випадку, подбати про те, щоб від вікон і дверей не проглядалися екрани моніторів і принтери. Необхідно, щоб відвідувачів за зовнішнім виглядом можна було відрізнити від співробітників. Якщо відмінність полягає в тому, що відвідувачам видаються ідентифікаційні картки, а співробітники ходять «без розпізнавальних знаків», зловмисникові досить зняти картку, щоб його вважали «своїм». Очевидно, що відповідні картки потрібно видавати всім.

Засоби фізичного керування доступом відомі давно. Це охорона, двері з замками, перегородки, телекамери, датчики руху й багато чого іншого. Для вибору оптимального (за критерієм вартість/ефективність) засобу доцільно провести аналіз ризиків (до цього ми ще повернемося). Крім того, є сенс періодично відслідковувати появу технічних новинок у даній сфері, намагаючись максимально автоматизувати фізичний захист.

Професія пожежника – одна з найдавніших, але пожежі, як і раніше, трапляються й завдають великої шкоди. Ми не збираємося цитувати параграфи протипожежних інструкцій або винаходити нові методи боротьби з вогнем – на це є професіонали. Відзначимо лише необхідність встановлення протипожежної сигналізації й автоматичних засобів пожежогасіння. Звернемо також увагу на те, що захисні заходи можуть створювати нові слабкі місця. Якщо на роботу взяли нового охоронця, це імовірно, поліпшує фізичне керування доступом. Якщо ж він ночами палить і п'є, то через підвищену пожежонебезпеку подібний засіб захисту може лише нашкодити.

До підтримувальної інфраструктури можна віднести системи електро-, водо- і теплопостачання, кондиціонери й засоби комунікацій. У принципі, до них можна застосувати ті ж вимоги цілісності й доступності, що й до інформаційних систем. Для забезпечення цілісності потрібно захищати устаткування від крадіжок та ушкоджень. Для підтримки доступності варто вибирати устаткування з максимальним терміном роботи на відмову, дублювати відповідальні вузли й завжди мати під рукою запчастини.

Окрему проблему становлять аварії водопроводу. Вони відбуваються нечасто, але можуть завдати величезної шкоди. При розміщенні комп'ютерів необхідно взяти до уваги розташування водопровідних і

каналізаційних труб, намагатися триматися від них подалі. Співробітники повинні знати, куди варто звертатися при виявленні протікань.

Перехоплення даних (про що ми вже писали) може здійснюватися різними способами. Зловмисник може підглядати за екраном монітора, читати пакети, передані по мережі, робити аналіз побічних електромагнітних випромінювань і наведень (ПЕМІН) і т. д. Залишається сподіватися на повселюдне використання криптографії (що, втім, поєднане у нас в країні з безліччю технічних і законодавчих проблем), намагатися максимально розширити контрольовану територію, розмістившись у тихому особнячку, віддалік від інших будинків, намагатися тримати під контролем лінії зв'язку (наприклад, помістити їх у надувну оболонку з виявленням проколювання), але найрозумніше, імовірно, – намагатися усвідомити, що для комерційних систем забезпечення конфіденційності є все-таки не головним завданням.

Мобільні й портативні комп'ютери – привабливий об'єкт крадіжки. Їх часто залишають без нагляду, в автомобілі або на роботі, і викрасти такий комп'ютер зовсім нескладно. Раз у раз засоби масової інформації повідомляють про те, що який-небудь офіцер англійської розвідки або американський військовий втратив у такий спосіб рухомое майно. Ми наполегливо рекомендуємо шифрувати дані на жорстких дисках таких комп'ютерів.

Загалом кажучи, при виборі засобів фізичного захисту варто робити аналіз ризиків. Так, ухвалюючи рішення щодо закупівлі джерела безперебійного живлення, необхідно врахувати якість електроживлення в будинку, займаному організацією (втім, майже напевно воно виявиться поганим), характер і тривалість збоїв електроживлення, вартість доступних джерел і можливі втрати від аварій (поломка техніки, припинення роботи організації й т. п.).У той же час, у багатьох випадках рішення очевидні. Засоби протипожежної безпеки обов'язкові для всіх організацій. Вартість реалізації багатьох засобів (наприклад, установлення звичайного замка на двері серверної кімнати) або мала, або хоч і помітна, але все-таки значно менша, ніж можливий збиток. Зокрема, має сенс регулярно копіювати великі бази даних.

14.4 Підтримка працездатності

Далі розглянемо ряд рутинних заходів, спрямованих на підтримку працездатності інформаційних систем. Саме тут чатує найбільша небезпека. Ненавмисні помилки системних адміністраторів і користувачів можуть призвести до ушкодження апаратури, руйнування програм і даних; у найкращому випадку вони створюють пролом у захисті, який уможливлює реалізацію загроз.

Недооцінювання факторів безпеки в повсякденній роботі – ахіллесова п'ята багатьох організацій. Коштовні засоби безпеки втрачають сенс, якщо

вони погано документовані, конфліктують з іншим програмним забезпеченням, а пароль системного адміністратора не змінювався з моменту встановлення.

Можна виділити такі напрямки повсякденної діяльності:

- підтримка користувачів;
- підтримка програмного забезпечення;
- конфігураційне керування;
- резервне копіювання;
- керування носіями;
- документування;
- регламентні роботи.

Підтримка користувачів має на увазі, насамперед, консультування й надання допомоги при вирішенні різного роду проблем. Іноді в організаціях створюють для цієї мети спеціальний «довідковий стіл», але частіше від користувачів відкараскується системний адміністратор. Дуже важливо з переліку питань уміти виявляти проблеми, пов'язані з інформаційною безпекою. Так, багато труднощів користувачів, що працюють на персональних комп'ютерах, може бути наслідком зараження вірусами. Доцільно фіксувати питання користувачів, щоб виявляти їхні типові помилки й випускати пам'ятки з рекомендаціями для найпоширеніших ситуацій.

Підтримка програмного забезпечення – один з найважливіших засобів забезпечення цілісності інформації. Насамперед, необхідно стежити за тим, яке програмне забезпечення встановлене на комп'ютерах. Якщо користувачі будуть установлювати програми за своїм розсудом, це може призвести до зараження вірусами, а також до появи утиліт, що діють в обхід захисних засобів. Цілком імовірно також, що «самодіяльність» користувачів поступово призведе до хаосу на їхніх комп'ютерах, а виправляти ситуацію доведеться системному адміністратору.

Другий аспект підтримки програмного забезпечення – контроль за відсутністю неавторизованої зміни програм і прав доступу до них. Сюди ж можна віднести підтримку еталонних копій програмних систем. Звичайно контроль досягається комбінуванням засобів фізичного й логічного керування доступом, а також використанням утиліт перевірки й забезпечення цілісності.

Конфігураційне керування дозволяє контролювати й фіксувати зміни, внесені в програмну конфігурацію. Насамперед, необхідно застрахуватися від випадкових або непродуманих модифікацій, вміти, як мінімум, повертатися до попередньої, такої, що працює, версії. Фіксація змін дозволить легко відновити поточну версію після аварії.

Кращий спосіб зменшити кількість помилок у рутинній роботі – максимально автоматизувати її. Мають рацію ті «ледачі» програмісти й системні адміністратори, які, оглянувши поглядом море одноманітних завдань, говорять: «Я нізащо не буду робити цього; я напишу програму, що

зробить усе за мене». Автоматизація й безпека залежать одна від одної; той, хто піклується в першу чергу про полегшення свого завдання, насправді оптимальним чином формує режим інформаційної безпеки.

Резервне копіювання необхідне для відновлення програм і даних після аварій. І тут доцільно автоматизувати роботу, сформувавши, як мінімум, комп'ютерний розклад створення повних й інкрементальних копій, а як максимум – скористатись відповідними програмними продуктами. Потрібно також налагодити розміщення копій у безпечному місці, захищеному від несанкціонованого доступу, пожеж, протікань, тобто від усього, що може привести до крадіжки або ушкодження носіїв. Доцільно мати кілька екземплярів резервних копій, і частину з них зберігати за межами території організації, захищаючись у такий спосіб від великих аварій й аналогічних інцидентів.

Час від часу в тестових цілях варто перевіряти можливість відновлення інформації з копій.

Управляти носіями необхідно для забезпечення фізичного захисту й обліку дисків, стрічок, друкованих видач і т. п. Керування носіями повинне забезпечувати конфіденційність, цілісність і доступність інформації, що зберігається за межами комп'ютерних системах. Під фізичним захистом тут розуміється не тільки відбиття спроб несанкціонованого доступу, але й запобігання шкідливим впливам навколишнього середовища (спеки, холоду, вологи, магнетизму). Керування носіями повинно охоплювати весь життєвий цикл – від закупівлі до виведення з експлуатації. Документування – невід'ємна частина інформаційної безпеки. У вигляді документів оформляється майже все – від політики безпеки до журналу обліку носіїв. Важливо, щоб документація була актуальною, відбивала саме поточний стан справ, причому в несуперечливому вигляді.

До зберігання одних документів (які містять у собі, наприклад, аналіз уразливих місць системи й загроз) можна застосувати вимоги забезпечення конфіденційності, до інших, таких як план відновлення після аварій, – вимоги цілісності й доступності (у критичній ситуації план необхідно знайти й прочитати).

Регламентні роботи – дуже серйозна загроза безпеки. Співробітник, що здійснює регламентні роботи, одержує винятковий доступ до системи, і на практиці дуже важко проконтролювати, які саме дії він робить. Тут на перший план виходить ступінь довіри до тих, хто виконує таку роботу.

14.5 Реагування на порушення режиму безпеки

Програма безпеки, прийнята організацією, повинна передбачати набір оперативних заходів, спрямованих на виявлення й нейтралізацію порушень режиму інформаційної безпеки. Важливо, щоб у подібних випадках послідовність дій була спланована заздалегідь, оскільки потрібно вживати заходів термінових й скоординованих.

Реакція на порушення режиму безпеки переслідує три головні цілі:

- локалізація інциденту й зменшення нанесеної шкоди;
- виявлення порушника;
- попередження повторних порушень.

В організації повинна бути людина, яка буде на зв'язку 24 години на добу, яка б відповідала за реакцію на порушення. Усі повинні знати координати цієї людини й звертатися до неї за перших ознак небезпеки.

Важливість швидкої й скоординованої реакції можна продемонструвати на такому прикладі. Нехай локальна мережа підприємства складається з двох сегментів, адміністрованих різними людьми. Далі, нехай один із сегментів буде заражений вірусом. Майже напевно через кілька хвилин (або, у крайньому випадку, кілька десятків хвилин) вірус поширюється й на інший сегмент. Виходить, заходів потрібно вжити негайно. «Вичищати» вірус необхідно одночасно в обох сегментах; у іншому випадку сегмент, відновлений першим, заразиться від іншого, а потім вірус повернеться й у другий сегмент.

Нерідко вимога локалізації інциденту й зменшення нанесеної шкоди вступає в конфлікт із бажанням виявити порушника. У політиці безпеки організації пріоритети повинні бути розставлені заздалегідь. Оскільки, як показує практика, виявити зловмисника дуже складно, на наш погляд, у першу чергу варто піклуватися про зменшення збитку.

Щоб знайти порушника, потрібно заздалегідь з'ясувати контактні координати постачальника мережевих послуг і домовитися з ним про саму можливість і порядок виконання відповідних дій.

Щоб запобігти повторним порушенням, необхідно аналізувати кожен інцидент, виявляти причини, накопичувати відомості. Які джерела шкідливого ПЗ? Які користувачі мають звичку вибирати легкі паролі? На подібні питання й повинні дати відповідь результати аналізу.

Необхідно відслідковувати появу нових уразливих місць та якнайшвидше ліквідовувати асоційовані з ними вікна небезпеки. Хтось в організації повинен відслідковувати цей процес, уживати короткострокових заходів і коригувати програму безпеки для вживання довгострокових заходів.

14.6 Планування відновлювальних робіт

Жодна організація не застрахована від серйозних аварій, викликаних природними катаклізмами, діями зловмисника, недбалістю або некомпетентністю. У той же час, у кожній організації є функції, які керівництво вважає критично важливими, вони повинні виконуватися, незважаючи ні на що. Планування відновлювальних робіт дозволяє підготуватися до аварій, зменшити збиток від них і зберегти здатність до функціонування хоча б у мінімальному обсязі.

Відзначимо, що заходи інформаційної безпеки можна розділити на три групи, залежно від того, спрямовані вони на попередження, виявлення чи ліквідацію наслідків атак. Більшість засобів носить попереджувальний характер. Оперативний аналіз реєстраційної інформації й деякі аспекти реагування на порушення (так званого активного аудиту) слугують для виявлення й відбиття атак. Планування відновлювальних робіт, мабуть, можна віднести до останньої з трьох перерахованих груп.

Процес планування відновлювальних робіт можна розділити на такі етапи:

- виявлення критично важливих функцій організації, встановлення пріоритетів;
- ідентифікація ресурсів, необхідних для виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відновлювальних робіт;
- підготовка до реалізації обраної стратегії;
- перевірка стратегії.

Плануючи відновлювальні роботи, варто усвідомлювати те, що повністю зберегти функціонування організації не завжди можливо. Необхідно виявити критично важливі функції, без яких організація втрачає свою цілісність, і навіть серед критичних функцій розставити пріоритети, щоб якнайшвидше й з мінімальними витратами відновити роботу після аварії.

Ідентифікуючи ресурси, необхідні для виконання критично важливих функцій, варто пам’ятати, що багато хто з них має некомп’ютерний характер. На даному етапі бажано залучати до роботи фахівців різного профілю, здатних у сукупності охопити всі аспекти проблеми. Критичні ресурси звичайно відносять до однієї з нижченаведених категорій:

- персонал;
- інформаційна інфраструктура;
- фізична інфраструктура.

Формуючи списки відповідальних фахівців, варто враховувати, що деякі з них можуть безпосередньо постраждати від аварії (наприклад, від пожежі), хтось може перебувати в стані стресу, частина співробітників, можливо, не будуть мати змоги потрапити на роботу (наприклад, у випадку масових заворушень). Бажано мати невеликий резерв фахівців або заздалегідь визначити канали, по яких можна на деякий час залучити додатковий персонал.

Інформаційна інфраструктура містить у собі такі елементи:

- комп’ютери;
- програми й дані;
- інформаційні сервіси зовнішніх організацій;
- документацію.

Потрібно підготуватися до того, що на «запасному аеродромі», куди організація буде евакуйована після аварії, апаратна платформа може відрізнятися від вихідної. Відповідно, варто продумати заходи підтримки сумісності щодо програм і даних.

Серед зовнішніх інформаційних сервісів для комерційних організацій, імовірно, найважливіше отримати оперативну інформацію й зв'язок з державними службами, що курирують даний сектор економіки.

Документація важлива хоча б тому, що не вся інформація, з якою працює організація, подана в електронному вигляді. Швидше за все, план відновлювальних робіт надрукований на папері.

До фізичної інфраструктури належать будинки, інженерні комунікації, засоби зв'язку, оргтехніка й багато іншого. Комп'ютерна техніка не може працювати в поганих умовах, без стабільного електроживлення й т. п.

Аналізуючи критичні ресурси, доцільно врахувати часовий профіль їхнього використання. Більшість ресурсів потрібна постійно, але потреба може виникати тільки в певні періоди (наприклад, наприкінці місяця або року при складанні звіту).

При визначенні переліку можливих аварій потрібно спробувати розробити їхні сценарії. Як будуть розвиватися події? Якими можуть виявитися масштаби нещастя? Що відбудеться з критичними ресурсами? Наприклад, чи зможуть співробітники потрапити на роботу? Чи будуть виведені з ладу комп'ютери? Чи можливі випадки саботажу? Чи буде працювати зв'язок? Чи постраждає будинок організації? Чи можна буде знайти й прочитати необхідні папери?

Стратегія відновлювальних робіт повинна базуватися на наявних ресурсах і бути не занадто накладною для організації. При розробці стратегії доцільно провести аналіз ризиків, яким піддаються критичні функції, і спробувати обрати найбільш економічне рішення.

Стратегія повинна передбачати не тільки роботу за тимчасовою схемою, але й повернення до нормального функціонування.

Підготовка до реалізації обраної стратегії полягає у виробленні плану дій в екстрених ситуаціях і після їхнього закінчення, а також у забезпеченні деякої надмірності критичних ресурсів. Останнє можливо й без великої витрати засобів, якщо укласти з однією або декількома організаціями угоди про взаємну підтримку у випадку аварій – ті, хто не постраждав, надають частину своїх ресурсів у тимчасове користування менш щасливим партнерам.

Надмірність забезпечується також заходами резервного копіювання, зберігання копій у декількох місцях, поданням інформації в різних виглядах (на папері й у файлах) і т. д.

Має сенс укласти угоду з постачальниками інформаційних послуг про першочергове обслуговування в критичних ситуаціях або укласти угоди з декількома постачальниками. Правда, ці заходи можуть зажадати певних витрат.

Перевірка стратегії виробляється шляхом аналізу підготовленого плану, прийнятих і намічених заходів.

Запитання для самоперевірки

1. Процедурний рівень інформаційної безпеки.
2. Основні класи заходів процедурного рівня.
3. Керування персоналом.
4. Фізичний захист. Основні принципи фізичного захисту.
5. Підтримка працездатності.
6. Реагування на порушення режиму безпеки.
7. Планування відновлювальних робіт.
8. Основні принципи керування персоналом.
9. Основні етапи планування відновлювальних робіт.
10. Основні напрямки фізичного захисту.
11. Який підхід застосовують при проектуванні й реалізації заходів фізичного керування доступом?
12. Засоби фізичного керування доступом.
13. Основні напрямки повсякденної діяльності.
14. Головні цілі, які переслідує реакція на порушення режиму безпеки.
15. Регламентні роботи.
16. Елементи інформаційної інфраструктури.

ГЛАВА 15
ПРОГРАМНО-ТЕХНІЧНЙ ЗАХИСТ

15.1 Основні програмно-технічні заходи щодо рівня інформаційної безпеки

Програмно-технічні заходи, тобто заходи, спрямовані на контроль комп'ютерних сутностей – устаткування, програм й/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки. Нагадаємо, що збиток наносять, в основному, дії легальних користувачів, стосовно яких процедурні регулятори малоефективні. Головні вороги – некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

Комп'ютери допомогли автоматизувати багато сфер людської діяльності. Цілком природним є бажання покласти на них і забезпечення власної безпеки. Навіть фізичний захист все частіше доручають не охоронцям, а інтегрованим комп'ютерним системам, що дозволяє одночасно відслідковувати переміщення співробітників і в організації, і в інформаційному просторі.

Це друга причина, що пояснює важливість програмно-технічних заходів.

Треба, однак, ураховувати, що швидкий розвиток інформаційних технологій не тільки надає оборонцям нові можливості, але й об'єктивно ускладнює забезпечення надійного захисту, якщо опиратися винятково на заходи програмно-технічного рівня. Причин тут декілька:

- підвищення швидкодії мікросхем, розвиток архітектур з високим ступенем паралелізму дозволяє методом грубої сили долати бар'єри (насамперед криптографічні), які раніше здавалися неприступними;
- розвиток мереж і мережевих технологій, збільшення кількості зв'язків між інформаційними системами, ріст пропускної спроможності каналів розширюють коло зловмисників, що мають технічну можливість організовувати атаки;
- поява нових інформаційних сервісів призводить і до утворення нових уразливих місць як «усередині» сервісів, так і на їхніх з'єднаннях;
- конкуренція серед виробників програмного забезпечення змушує скорочувати строки розробки, що призводить до зниження якості тестування й випуску продуктів з дефектами захисту;
- парадигма постійного нарощування, нав'язування споживачам потужності апаратного й програмного забезпечення не дозволяє довго залишатися в межах надійних, апробованих конфігурацій й, крім того, вступає в конфлікт із бюджетними обмеженнями, через що знижується частка асигнувань на безпеку.

Перераховані міркування підкреслюють важливість комплексного підходу до інформаційної безпеки, а також необхідність гнучкої позиції при виборі й супроводі програмно-технічних регуляторів.

Центральним для програмно-технічного рівня є поняття сервісу безпеки.

Дотримуючись об'єктно-орієнтованого підходу, при розгляді інформаційної системи з одиничним рівнем деталізації ми побачимо сукупність надаваних нею інформаційних сервісів. Назвемо їх основними. Щоб вони могли функціонувати й мали необхідні властивості, необхідно кілька рівнів додаткових (допоміжних) сервісів – від СУБД і моніторів транзакцій до ядра операційної системи й устаткування.

До допоміжного відносять сервіси безпеки (ми вже зіштовхувалися з ними при розгляді стандартів і специфікацій у сфері ІБ); з-поміж них нас у першу чергу будуть цікавити універсальні, високорівневі, що допускають використання різних основних й допоміжних сервісів. Далі ми розглянемо такі сервіси:

- ідентифікація й аутентифікація;
- керування доступом;
- протоколювання й аудит;
- шифрування;
- контроль цілісності;
- екранування;
- аналіз захищеності;
- забезпечення відмовостійкості;
- забезпечення безпечного відновлення;
- тунелювання;
- керування.

Будуть описані вимоги до сервісів безпеки, їхня функціональність, можливі методи реалізації й місце в загальній архітектурі.

Якщо зіставити наведений перелік сервісів із класами функціональних вимог «Загальних критеріїв», то впадає в око їхня істотна розбіжність. Ми не будемо розглядати питання, пов'язані з приватністю. На наш погляд, сервіс безпеки, хоча б частково, повинен перебувати в розпорядженні того, кого він захищає. У випадку ж з приватністю це не так: критично важливі компоненти зосереджені не на клієнтській, а на серверній стороні, так що приватність, власне кажучи, виявляється властивістю пропонованої інформаційної послуги (у найпростішому випадку, приватність досягається шляхом збереження конфіденційності серверної реєстраційної інформації й захистом від перехоплення даних, для чого досить перерахованих сервісів безпеки).

З іншого боку, наш перелік є ширшим, ніж у «Загальних критеріях», оскільки в нього входять: екранування, аналіз захищеності й тунелювання. Ці сервіси мають важливе значення самі по собі й, крім того, можуть

комбінуватися з іншими сервісами для одержання таких необхідних захисних засобів, як, наприклад, віртуальні приватні мережі.

Сукупність перерахованих вище сервісів безпеки ми будемо називати повним набором. Уважається, що його, у принципі, досить для побудови надійного захисту на програмно-технічному рівні, щоправда, при дотриманні цілого ряду додаткових умов (відсутність уразливих місць, безпечне адміністрування й т. д.).

Для проведення класифікації сервісів безпеки й визначення їхнього місця в загальній архітектурі заходи безпеки можна розділити на види:

- превентивні, такі, що перешкоджають порушенням ІБ;
- заходи виявлення порушень;
- локалізувальні, такі, що звужують зону впливу порушень;
- заходи виявлення порушника;
- заходи відновлення режиму безпеки.

Більшість сервісів безпеки потрапляє в число превентивних, і це, безумовно, правильно. Аудит і контроль цілісності здатні допомогти у виявленні порушень; активний аудит, крім того, дозволяє запрограмувати реакцію на порушення з метою локалізації й/або простежування. Спрямованість сервісів відмовостійкості й безпечного відновлення очевидна. Нарешті, керування відіграє інфраструктурну роль, обслуговуючи всі аспекти ІС.

15.2 Особливості сучасних інформаційних систем, істотні з погляду безпеки

Інформаційна система типової сучасної організації є досить складним утворенням, побудованим у багаторівневій архітектурі клієнт/сервер, що користується численними зовнішніми сервісами й, у свою чергу, надає власні сервіси зовні. Навіть порівняно невеликі магазини, що забезпечують розрахунок з покупцями за допомогою пластикових карт (і, звичайно, що мають зовнішній Web-сервер), залежать від своїх інформаційних систем й, зокрема, від захищеності всіх компонентів систем і комунікацій між ними.

З погляду безпеки найбільш істотними вважаються такі аспекти сучасних ІС:

- корпоративна мережа має декілька територіально рознесених частин (оскільки організація розташовується на декількох виробничих майданчиках), зв’язки між якими перебувають у компетенції зовнішнього постачальника мережевих послуг та контролюються організацією;
- корпоративна мережа має одне або кілька підключень до Internet;
- на кожному з виробничих майданчиків можуть перебувати критично важливі сервери, у доступі до яких мають потребу співробітники, що працюють на інших майданчиках, мобільні користувачі й, можливо, співробітники інших організацій;
- для доступу користувачів можуть застосовуватися не тільки

комп’ютери, але й пристрої, які використовуються користувачами, зокрема, бездротовий зв’язок;

- протягом одного сеансу роботи користувачу доводиться звертатися до декількох інформаційних сервісів, що спираються на різні апаратно-програмні платформи;
- щодо доступності інформаційних сервісів висуваються жорсткі вимоги, які уособлюються в необхідності цілодобового функціонування з максимальним часом простою приблизно в декілька хвилин;
- інформаційна система є мережею з активними агентами, тобто в процесі роботи такі програмні компоненти, як апплети або сервлети, передаються з однієї машини на іншу й виконуються в цільовому середовищі, підтримуючи зв’язок з вилученими компонентами;
- не всі системи користувачів контролюються мережевими й/або системними адміністраторами організації;
- програмне забезпечення, особливо отримане по мережі, не може вважатися надійним, у ньому можуть бути помилки, що створюють проблеми в захисті;
- конфігурація інформаційної системи постійно змінюється на рівнях адміністративних даних, програм й апаратури (змінюється склад користувачів, їхні привілеї й версії програм, з’являються нові сервіси, нова апаратура й т. п.).

Варто враховувати ще два моменти. По-перше, для кожного сервісу основні межі ІБ (доступність, цілісність, конфіденційність) трактуються по-своєму. Цілісність, із погляду системи керування базами даних і з погляду поштового сервера, – речі принципово різні. Безглуздо говорити про безпеку локальної або іншої мережі взагалі, якщо мережа містить у собі різнорідні компоненти. Варто аналізувати захищеність сервісів, що функціонують у мережі. Для різних сервісів і захист будують по-різному. По-друге, основна загроза інформаційної безпеки організацій, як і раніше, виходить не від зовнішніх зловмисників, а від власних співробітників.

У силу викладених причин далі будуть розглядатися розподілені, різнорідні, багатосервісні, еволюціонувальні системи. Відповідно, нас буде цікавити рішення, орієнтоване на подібні конфігурації.

15.3 Архітектура безпеки

Сервіси безпеки, якими б потужними вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки перевірена архітектура здатна зробити ефективним об’єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися й протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота й зручність використання.

Теоретичною основою вирішення проблеми архітектурної безпеки є фундаментальне твердження, яке ми вже наводили, розглядаючи інтерпретацію «Оранжевої книги» для мережевих конфігурацій.

«Нехай кожен суб'єкт (тобто процес, що діє від імені якого-небудь користувача) укладений всередині одного компонента й може здійснювати безпосередній доступ до об'єктів тільки в межах цього компонента. Далі нехай кожен компонент містить свій монітор обігів, що відслідковує всі локальні спроби доступу, і всі монітори проводять у життя погоджену політику безпеки. Нехай, нарешті, комунікаційні канали, що зв'язують компоненти, зберігають конфіденційність і цілісність передавальної інформації. Тоді сукупність усіх моніторів утворить єдиний монітор обігів для всієї мережевої конфігурації».

Звернемо увагу на три принципи, які містяться в наведеному твердженні:

- необхідність розробки й впровадження в життя єдиної політики безпеки;
- необхідність забезпечення конфіденційності й цілісності при мережевих взаємодіях;
- необхідність формування складових сервісів за змістовним принципом, щоб кожен отриманий у такий спосіб компонент мав повний набір захисних засобів і із зовнішньої точки зору являв собою єдине ціле (не повинно бути інформаційних потоків, що йдуть до незахищених сервісів).

Якщо який-небудь (складовий) сервіс не має повного набору захисних засобів (склад повного набору описаний вище), необхідне залучення додаткових сервісів, які ми будемо називати екранованими. Екрановані сервіси встановлюються на шляхах доступу до не досить захищених елементів; у принципі, один такий сервіс може екранувати (захищати) велику кількість елементів.

Із практичної точки зору найбільш важливими є такі принципи архітектурної безпеки:

- безперервність захисту в просторі й часі, неможливість оминути захисні засоби;
- наслідування визнаним стандартам, використання апробованих рішень;
- ієрархічна організація ІС із невеликою кількістю сутностей на кожному рівні;
- посилення найслабшої ланки;
- неможливість переходу в небезпечний стан;
- мінімізація привілеїв;
- поділ обов'язків;
- системність оборони;
- розмаїтість захисних засобів;
- простота й керованість інформаційної системи.

Пояснимо зміст перерахованих принципів.

Якщо у зловмисника або незадоволеного користувача з'явиться можливість оминути захисні засоби, він, зрозуміло, так і зробить. Визначені вище екрановані сервіси повинні унеможливити подібні дії.

Наслідування визнаним стандартам і використання апробованих рішень підвищує надійність ІС і зменшує ймовірність потрапляння в тупикову ситуацію, коли забезпечення безпеки зажадає непомірно великих витрат і принципових модифікацій.

Ієрархічна організація ІС із невеликою кількістю сутностей на кожному рівні необхідна з технологічних міркувань. При порушенні даного принципу система стане некерованою й, отже, забезпечити її безпеку буде неможливо.

Надійність будь-якої оборони визначається найслабшою ланкою. Зловмисник не буде боротися проти сили, він віддасть перевагу легкій перемозі над слабкістю. (Зазвичай, найслабшою ланкою виявляється не комп'ютер або програма, а людина, і тоді проблема забезпечення інформаційної безпеки набуває нетехнічного характеру).

Принцип неможливості переходу в небезпечний стан означає, що за будь-яких обставин, у тому числі позаштатних, захисний засіб або повністю виконує свої функції, або повністю блокує доступ. Образно кажучи, якщо механізм звідного моста ламається, міст залишають піднятим, перешкоджаючи проходу ворога.

Стосовно програмно-технічного рівня принцип мінімізації привілеїв пропонує виділяти користувачам й адміністраторам тільки ті права доступу, які необхідні їм для виконання службових обов'язків. Цей принцип дозволяє зменшити збиток від випадкових або навмисних некоректних дій користувачів й адміністраторів.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, щоб одна людина не могла порушити критично важливий для організації процес або створити пролом у захисті за замовленням зловмисників. Зокрема, дотримання даного принципу особливо важливо, щоб запобігти зловмисним або некваліфікованим діям системного адміністратора.

Принцип ешелонованості оборони пропонує не покладатися на один захисний рубіж, яким би надійним він не здавався. Після засобів фізичного захисту повинні слідувати програмно-технічні засоби, за ідентифікацією й аутентифікацією – керування доступом й, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна, принаймні, затримати зловмисника, а завдяки наявності такого рубежу, як протоколювання й аудит, його дії не залишаться непоміченими.

Принцип розмаїтості захисних засобів припускає створення різних за своїм характером оборонних рубежів, щоб від потенційного зловмисника вимагалося б оволодіння різноманітними й, по можливості, несумісними між собою навичками.

Для забезпечення високої доступності (безперервності функціонування) необхідно дотримуватися таких принципів архітектурної безпеки:

- внесення в конфігурацію тієї або іншої форми надмірності (резервне устаткування, запасні канали зв'язку й т. п.);
- наявність засобів виявлення позаштатних ситуацій;
- наявність засобів реконфігурування для відновлення ізоляції й/або заміни компонентів, що відмовили або піддалися атаці на доступність;
- розосередженість мережевого керування, відсутність єдиної точки відмови;
- виділення підмереж та ізоляція груп користувачів один від одного. Даний захід, що є узагальненням поділу процесів на рівні операційної системи, обмежує зону поразки при можливих порушеннях інформаційної безпеки.

Ще один важливий архітектурний принцип – мінімізація обсягу захисних засобів, що їх виносять на клієнтські системи. Причин тому декілька:

– для доступу в корпоративну мережу можуть використовуватися споживчі пристрої з обмеженою функціональністю;

– конфігурацію клієнтських систем важко або неможливо контролювати.

До необхідного мінімуму варто віднести реалізацію сервісів безпеки на мережевому й транспортному рівнях і підтримку механізмів аутентифікації, стійких до мережевих загроз.

Запитання для самоперевірки

1. Основні програмно-технічні заходи.
2. Основні поняття програмно-технічного рівня інформаційної безпеки.
3. Основні і допоміжні сервіси безпеки.
4. Класифікація сервісів безпеки.
5. Для чого використовується протоколювання і аудит?
6. Назвіть найбільш істотні, з погляду безпеки, особливості сучасних українських ІС.
7. Основні принципи архітектурної безпеки.
8. Для чого використовується екранування?
9. Дайте означення поняття принципу ешелонованості.
10. Для чого використовується контроль цілісності?
11. Дайте означення поняття принципу неможливості переходу в небезпечний етап.
12. Принципи поділу обов'язків.
13. Принципи розмаїтості захисних засобів.

ГЛАВА 16
ПРОТОКОЛЮВАННЯ Й АУДИТ, ШИФРУВАННЯ, КОНТРОЛЬ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

16.1 Протоколювання й аудит. Основні поняття

Під протоколюванням розуміють збирання та зберігання інформації про події, що відбуваються в інформаційній системі. У кожного сервісу свій набір можливих подій, але в кожному разі їх можна розділити на зовнішні (викликані діями інших сервісів), внутрішні (викликані діями самого сервісу) і клієнтські (викликані діями користувачів й адміністраторів).

Аудит – це аналіз накопиченої інформації, проведений оперативно, у реальному часі або періодично (наприклад, раз на день). Оперативний аудит з автоматичним реагуванням на виявлені позаштатні ситуації називається активним.

Реалізація протоколювання й аудиту вирішує такі завдання:

- забезпечення підзвітності користувачів й адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень інформаційної безпеки;
- надання інформації для виявлення й аналізу проблем.

Протоколювання вимагає для своєї реалізації здорового глузду. Які події реєструвати? З яким ступенем деталізації? На подібні питання неможливо дати універсальні відповіді. Необхідно стежити за тим, щоб, з одного боку, вирішувалися перераховані вище завдання, а, з іншого, витрата ресурсів залишилася в межах припустимого. Занадто велике або докладне протоколювання не тільки знижує продуктивність сервісів (що негативно позначається на доступності), але й ускладнює аудит, тобто не збільшує, а зменшує інформаційну безпеку.

Розумний підхід до згаданих питань стосовно операційних систем пропонується в «Оранжевій книзі», де виділені такі події:

- вхід у систему (успішний чи ні);
- вихід із системи;
- звертання до вилученої системи;
- операції з файлами (відкрити, закрити, перейменувати, видалити);
- зміна привілеїв або інших атрибутів безпеки (режиму доступу, рівня благонадійності користувача й т. п.).

При протоколюванні події рекомендується записувати, принаймні, нижчевказану інформацію:

- дата й час події;
- унікальний ідентифікатор користувача – ініціатора дії;
- тип події;
- результат дії (успіх або невдача);

- джерело запиту (наприклад, ім’я термінала);
- імена порушених об’єктів (наприклад, відкритих або видалених файлів);
- опис змін, внесених у бази даних захисту (наприклад, нова мітка безпеки об’єкта).

Ще одне важливе поняття, що фігурує в «Оранжевій книзі», вибіркове протоколювання як відносно користувачів (уважно стежити тільки за підозрілими), так і відносно подій.

Характерна риса протоколювання й аудиту – залежність від інших засобів безпеки. Ідентифікація й аутентифікація слугують відправною точкою підзвітності користувачів, логічне керування доступом захищає конфіденційність і цілісність реєстраційної інформації. Можливо, для захисту залучаються й криптографічні методи.

Повертаючись до цілей протоколювання й аудиту, відзначимо, що забезпечення підзвітності важливо, в першу чергу, як стримувальний засіб. Якщо користувачі й адміністратори знають, що всі їхні дії фіксуються, вони, можливо, утримаються від незаконних операцій. Очевидно, якщо є підстави підозрювати якого-небудь користувача в нечесності, можна реєструвати всі його дії, аж до кожного натискання клавіші. При цьому забезпечується не тільки можливість розслідування випадків порушення режиму безпеки, але й виявлення некоректних змін (якщо в протоколі присутні дані до й після модифікації). Тим самим захищається цілісність інформації.

Реконструкція послідовності подій дозволяє виявити слабкість у захисті сервісів, знайти винуватця вторгнення, оцінити масштаби заподіяного збитку й повернутися до нормальної роботи.

Виявлення спроб порушень інформаційної безпеки – функція активного аудиту, про яку піде мова в наступному розділі. Звичайний аудит дозволяє виявити подібні спроби з запізненням, але й це виявляється корисним. У свій час вияв німецьких хакерів, що діяли за замовленням КДБ, почався з виявлення підозрілої розбіжності в кілька центів у щоденному звіті великого обчислювального центру.

Виявлення й аналіз проблем можуть допомогти поліпшити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переконфігурувати або переналаштувати систему, знову виміряти продуктивність і т. д.

Непросто здійснити організацію погодженого протоколювання й аудиту в розподіленій різнорідній системі. По-перше, деякі компоненти, важливі для безпеки (наприклад, маршрутизатори), можуть не мати своїх ресурсів протоколювання; у такому випадку їх потрібно екранувати іншими сервісами, які візьмуть протоколювання на себе. По-друге, необхідно погоджувати між собою події в різних сервісах.

16.2 Активний аудит. Основні поняття

Під підозрілою активністю розуміється поводження користувача або компонента інформаційної системи, що є злочинним (відповідно до заздалегідь визначеної політики безпеки) або нетиповим (відповідно до прийнятих критеріїв).

Завдання активного аудиту – оперативно виявляти підозрілу активність і надавати засоби для автоматичного реагування на неї.

Активність, що не відповідає політиці безпеки, доцільно розділити на атаки, спрямовані на незаконне одержання повноважень, і на дії, виконувані в межах наявних повноважень, але з порушенням політики безпеки.

Атаки порушують будь-яку осмислену політику безпеки. Іншими словами, активність атакуючого є руйнівною незалежно від політики. Отже, для опису й виявлення атак можна застосовувати такі універсальні методи, інваріантні щодо політики безпеки, як сигнатури і їхнє виявлення у вхідному потоці подій за допомогою апарата експертних систем.

Сигнатура атаки – це сукупність умов, при виконанні яких атака вважається дієвою, яка викликає заздалегідь зрозумілу реакцію. Найпростіший приклад сигнатури – «зафіксовані три послідовні невдалі спроби входу в систему з одного термінала», приклад асоційованої реакції – блокування термінала до з’ясування ситуації.

Дії, які виконуються в межах наявних повноважень, але порушують політику безпеки, ми будемо називати зловживанням повноваженнями. Зловживання повноваженнями можливі через неадекватність засобів розмежування доступу обраній політиці безпеки. Найпростішим прикладом зловживань є неетичне поводження суперкористувача, що переглядає особисті файли інших користувачів. Аналізуючи реєстраційну інформацію, можна виявити подібні події й повідомити про них адміністратора безпеки, хоча для цього необхідні відповідні засоби вираження політики безпеки.

Виділення зловживань повноваженнями в окрему групу неправомірних дій, що є засобами активного аудиту, не є загальноприйнятим, однак, на наш погляд, подібний підхід має право на існування й ми будемо його дотримуватися, хоча найбільш радикальним рішенням був би розвиток засобів розмежування доступу (див. «Можливий підхід до керування доступом у розподіленому об’єктному середовищі»).

Нетипова поведінка виявляється статистичними методами. У найпростішому випадку застосовують систему порогів, перевищення яких є підозрілим. (Втім, «граничний» метод можна трактувати і як виокремлений випадок сигнатури атаки, і як тривіальний спосіб вираження політики безпеки.) У більш розвинених системах порівнюються довгострокові характеристики роботи (названі довгостроковим профілем) з

короткостроковими профілями. (Тут можна побачити аналогію біометричної аутентифікації за поведінковими характеристиками.)

Стосовно засобів активного аудиту розрізняють помилки першого й другого роду: пропуск атак і фіктивні тривоги, відповідно. Небажаність помилок першого роду очевидна; помилки другого роду не менш неприємні, оскільки відволікають адміністратора безпеки від дійсно важливих справ, побічно сприяючи пропускання атак.

Переваги сигнатурного методу – висока продуктивність, невелика кількість помилок другого роду, обґрунтованість рішень. Основний недолік – невміння виявляти невідомі атаки й варіації відомих атак.

Основні переваги статистичного підходу – універсальність й обґрунтованість рішень, потенційна здатність виявляти невідомі атаки, тобто, мінімізація кількості помилок першого роду. Мінуси полягають у відносно високій частці помилок другого роду, поганій роботі у випадку, коли неправомірне поводження є типовим, коли типова поведінка плавно змінюється від легальної до неправомірної, а також у випадках, коли типового поводження немає (як показує статистика, таких користувачів приблизно 5–10%).

Засоби активного аудиту можуть розташовуватися на всіх лініях оборони інформаційної системи. На межі контрольованої зони вони можуть виявляти підозрілу активність у точках підключення до зовнішніх мереж (не тільки спроби нелегального проникнення, але й дії з «промацування» сервісів безпеки). У корпоративній мережі, у межах інформаційних сервісів і сервісів безпеки, активний аудит у змозі виявити й припинити підозрілу активність зовнішніх і внутрішніх користувачів, виявити проблеми в роботі сервісів, викликані як порушеннями безпеки, так й апаратно-програмними помилками. Важливо відзначити, що активний аудит, у принципі, здатний забезпечити захист від атак на доступність.

На жаль, формулювання «у принципі, здатний забезпечити захист» не випадкове. Активний аудит розвивається більше десяти років і перші результати здавалися досить багатообіцяючими. Досить швидко вдалося реалізувати розпізнавання простих типових атак, однак потім була виявлена безліч проблем, пов’язаних з виявленням заздалегідь невідомих атак, атак розподілених, розтягнутих у часі й т. п. Було б наївно очікувати повного вирішення подібних проблем найближчим часом. (Оперативне поповнення бази сигнатур атак не є, звичайно, таким рішенням.) Проте і на нинішній стадії розвитку активний аудит корисний як один з рубежів (точніше, як набір прошарків) ешелонованої оборони.

16.3 Функціональні компоненти й архітектура

У складі засобів активного аудиту можна виділити такі функціональні компоненти:

- компоненти генерації реєстраційної інформації. Вони перебувають на стику між засобами активного аудиту й контрольованих об’єктів;

- компоненти зберігання згенерованої реєстраційної інформації;

- компоненти витягування реєстраційної інформації (сенсори). Звичайно розрізняють мережні й хостові сенсори, маючи на увазі під першими виділені комп’ютери, мережеві карти яких установлені в режим прослуховування, а під другими – програми, що читають реєстраційні журнали операційної системи. На наш погляд, з розвитком комутаційних технологій це розходження поступово стирається, тому що мережеві сенсори доводиться встановлювати в активному мережному устаткуванні й, по суті, вони стають частиною мережевої ОС;

- компоненти перегляду реєстраційної інформації можуть допомогти при ухваленні рішення про реагування на підозрілу активність;

- компоненти аналізу інформації, що надійшла від сенсорів. Відповідно до наведеного визначення засобів активного аудиту виділяють пороговий аналізатор, аналізатор порушень політики безпеки, експертну систему, яка виявляє сигнатури атак, а також статистичний аналізатор, що виявляє нетипове поводження;

- компоненти зберігання інформації, які беруть участь в аналізі. Таке зберігання необхідно, наприклад, для виявлення атак, тривалих у часі;

- компоненти прийняття рішень і реагування («вирішувачі»). «Вирішувач» може одержувати інформацію не тільки від локальних, але й від зовнішніх аналізаторів, проводячи так званий кореляційний аналіз розподілених подій;

- компоненти зберігання інформації про контрольовані об’єкти. Тут можуть зберігатися як пасивні дані, так і методи, необхідні, наприклад, для витягування з об’єкта реєстраційної інформації або для реагування;

- компоненти, які відіграють роль організувальної оболонки для менеджерів активного аудиту, названі моніторами й об’єднувальними аналізаторами, «вирішувачі», сховище описів об’єктів й інтерфейсні компоненти. У число останніх входять компоненти інтерфейсу з іншими моніторами, як рівноправними, так і тими, які входять в ієрархію. Такі інтерфейси необхідні, наприклад, для виявлення розподілених, широкомасштабних атак;

- компоненти інтерфейсу з адміністратором безпеки.

Засоби активного аудиту будуються в архітектурі менеджер/агент. Основними агентськими компонентами є сенсори. Аналіз та прийняття рішень – функції менеджерів. Очевидно, між менеджерами й агентами повинні бути сформовані довірені канали.

Підкреслимо важливість інтерфейсних компонентів. Вони корисні як із внутрішньої для засобів активного аудиту точки зору (забезпечують розширюваність, підключення компонентів різних виробників), так і з зовнішньої точки зору. Між менеджерами (між компонентами аналізу й «вирішувачами») можуть існувати горизонтальні зв’язки, необхідні для

аналізу розподіленої активності. Можливо також формування ієрархій засобів активного аудиту з винесенням на верхні рівні інформації про найбільш масштабну й небезпечну активність.

Звернемо також увагу на архітектурну спорідненість засобів активного аудиту й керування, що є наслідком спільності виконуваних функцій. Продумані інтерфейсні компоненти можуть істотно полегшити спільну роботу цих засобів.

16.4 Шифрування

Ми починаємо розгляд криптографічних сервісів безпеки, точніше, виклад елементарних відомостей, що допомагають скласти загальне уявлення про комп'ютерну криптографію та її місце в загальній архітектурі інформаційних систем.

Криптографія необхідна для реалізації, принаймні, трьох сервісів безпеки:

- шифрування;
- контроль цілісності;
- аутентифікація (цей сервіс був розглянутий нами раніше).

Шифрування – найбільш потужний засіб забезпечення конфіденційності. У багатьох відносинах воно займає центральне місце серед програмно-технічних регуляторів безпеки, бувши основою реалізації багатьох з них, і в той же час останнім (а часом і єдиним) захисним рубежем. Наприклад, для портативних комп'ютерів тільки шифрування дозволяє забезпечити конфіденційність даних навіть у випадку крадіжки.

У більшості випадків і шифрування, і контроль цілісності відіграють глибоко інфраструктурну роль, залишаючись прозорими й для додатків, і для користувачів. Типове місце цих сервісів безпеки – на мережевому й транспортному рівнях реалізації стека мережевих протоколів.

Розрізняють два основних методи шифрування: симетричний й асиметричний. У першому з них той самий ключ (що зберігається в секреті) використовується як для шифрування, так і для розшифрування даних. Розроблені досить ефективні (швидкі й надійні) методи симетричного шифрування.

Рисунок 16.1 ілюструє використання симетричного шифрування. Для визначеності ми будемо вести мову про захист повідомлень, хоча події можуть розвиватися не тільки в просторі, але й у часі, коли зашифровуються й розшифровуються нікуди не переміщені файли.

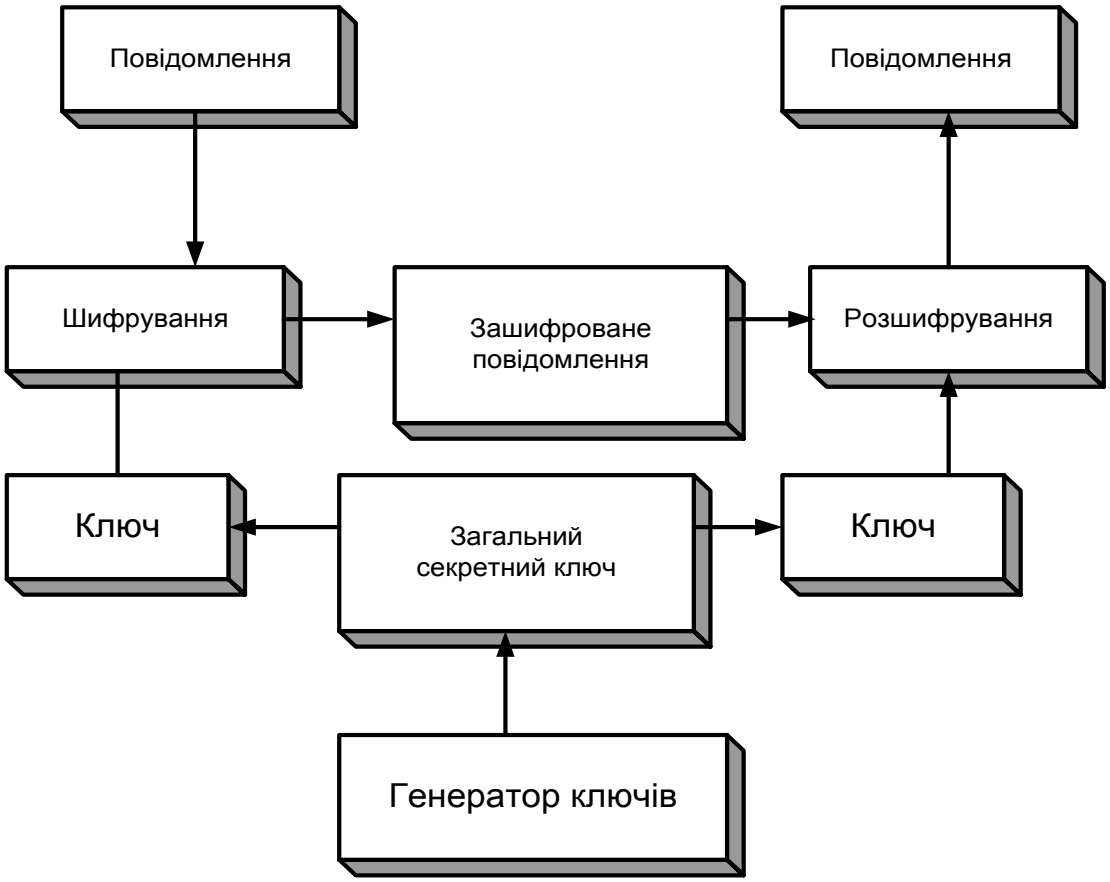


Рисунок 16.1 – Використання симетричного методу шифрування

Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомим і відправнику, і одержувачу. З одного боку, це створює нову проблему поширення ключів. З іншого боку, одержувач на підставі наявності зашифрованого й розшифрованого повідомлення не може довести, що він одержав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати самостійно.

В асиметричних методах використовуються два ключі. Один з них, несекретний (він може розміщуватися разом з іншими відкритими відомостями про користувача), застосовується для шифрування, інший (секретний, відомий тільки одержувачу) – для розшифрування. Найпопулярнішим серед асиметричних є метод RSA (Райвест, Шамір, Алліман), заснований на операціях з більшими (скажемо, 100-значними) простими числами і їхніми добутками.

Проілюструємо використання асиметричного шифрування (рис. 16.2).

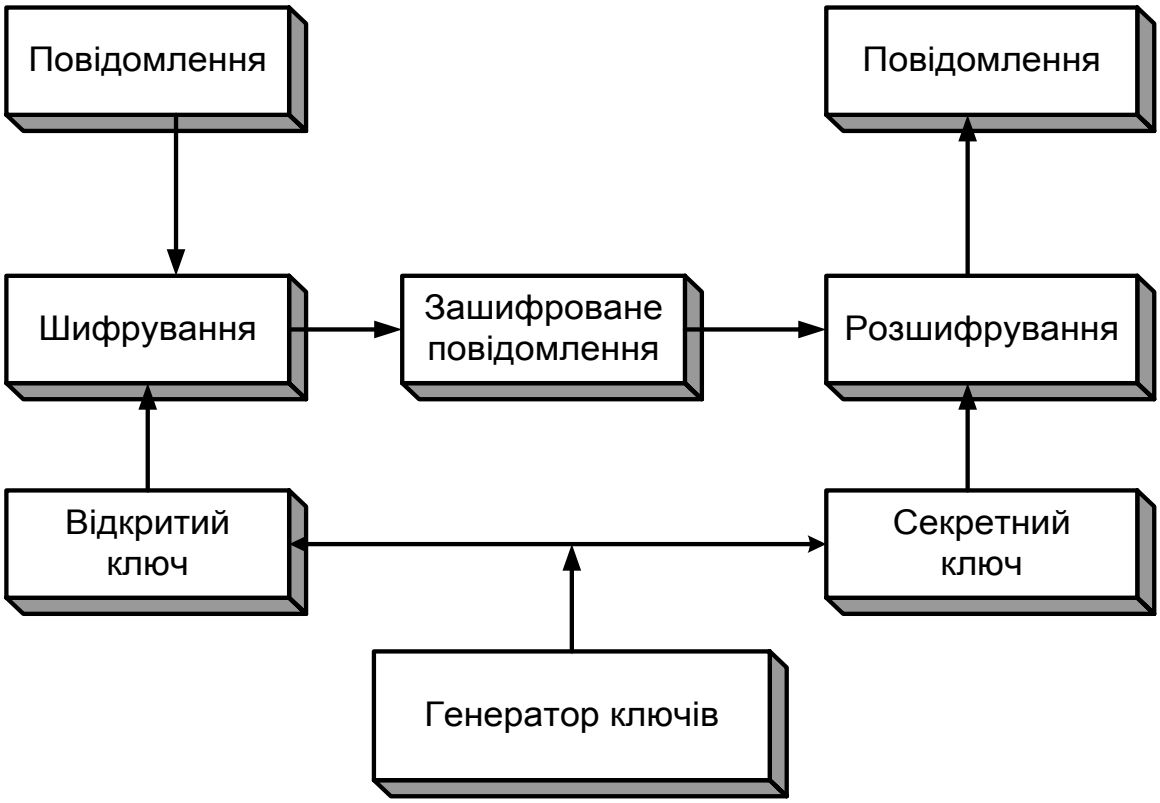


Рисунок 16.2 – Використання асиметричного методу шифрування

Істотним недоліком асиметричних методів шифрування є їхня низька швидкодія, тому дані методи доводиться поєднувати з симетричними (асиметричні методи на 3–4 порядки повільніші). Так, для вирішення завдання ефективного шифрування з передачею секретного ключа, використаного відправником, повідомлення спочатку симетрично зашифровують випадковим ключем, потім цей ключ зашифровують відкритим асиметричним ключем одержувача, після чого повідомлення й ключ відправляються по мережі.

Рисунок 16.3 ілюструє ефективне шифрування, реалізоване шляхом поєднання симетричного й асиметричного методів.

На рисунку16.4 показано розшифрування ефективно зашифрованого повідомлення.

Відзначимо, що асиметричні методи дозволили вирішити важливе завдання спільного вироблення секретних ключів (це істотно, якщо сторони не довіряють одна одній), що обслуговують сеанс взаємодії, при споконвічній відсутності загальних секретів. Для цього використовується алгоритм Діффі-Хеллмана.

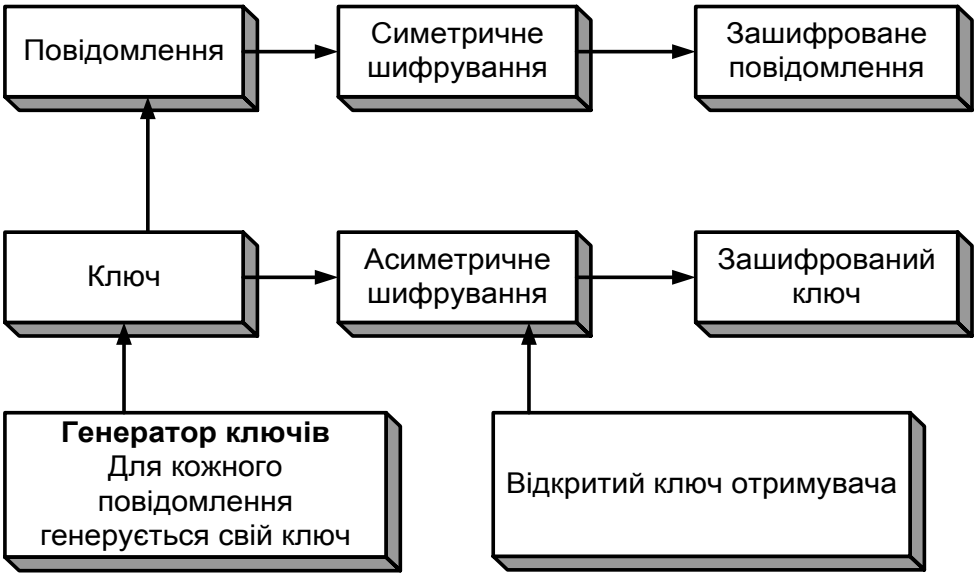


Рисунок 16.3 – Ефективне шифрування повідомлення

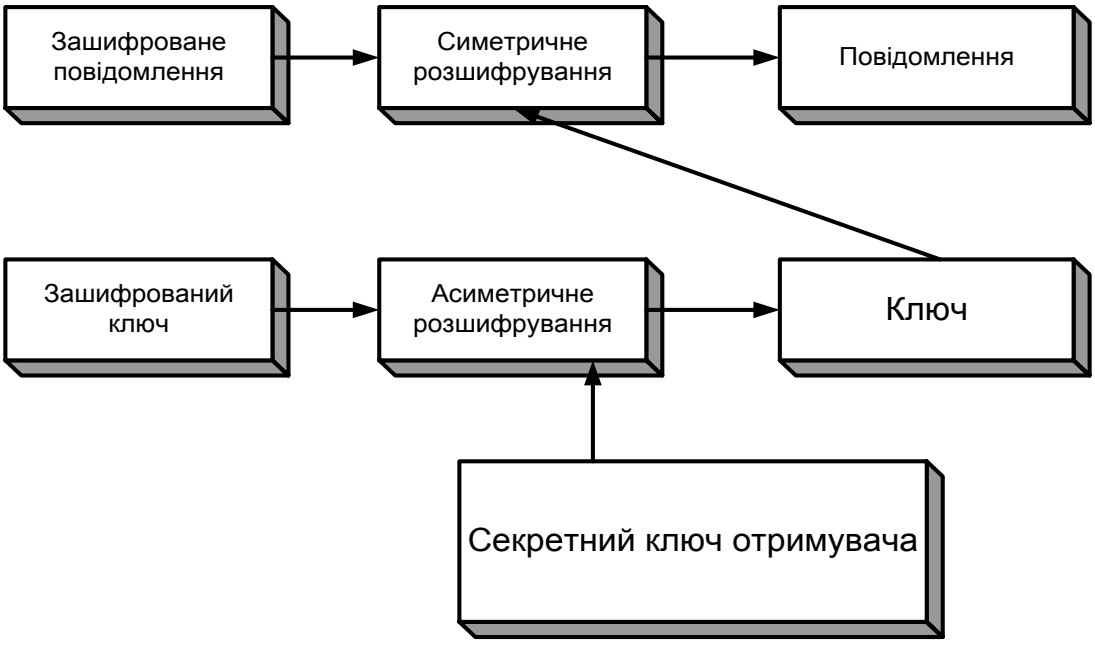


Рисунок 16.4 – Розшифрування ефективно зашифрованого повідомлення

Дещо розповсюдився різновид симетричного шифрування, заснований на використанні складених ключів. Ідея полягає в тому, що секретний ключ ділиться на дві частини, що зберігаються окремо. Кожна частина сама по собі не дозволяє виконати розшифрування. Якщо в правоохоронних органів з'являються підозри щодо особи, яка використовує деякий ключ, вони можуть у встановленому порядку одержати половинки ключа й далі діяти звичайним для симетричного розшифрування чином.

Порядок роботи зі складеними ключами – вдалий приклад проходження принципу поділу обов'язків. Він дозволяє поєднувати права на різного роду таємниці (персональну, комерційну) з можливістю ефективно стежити за порушниками закону, хоча, звичайно, тут дуже багато тонкощів і технічного, і юридичного плану.

Багато криптографічних алгоритмів як один з параметрів потребують псевдовипадкового значення, у випадку передбачення якого в алгоритмі з'являється уразливість (подібне уразливе місце було виявлено в деяких варіантах Web-навігаторів). Генерація псевдовипадкових послідовностей – важливий аспект криптографії.

16.5 Контроль цілісності

Криптографічні методи дозволяють надійно контролювати цілісність як окремих порцій даних, так і їхніх наборів (таких як потік повідомлень); визначати дійсність джерела даних; гарантувати неможливість відмовитися від зроблених дій («безвідмовність»).

В основі криптографічного контролю цілісності лежать два поняття:

- хеш-функція;
- електронний цифровий підпис (ЕЦП).

Хеш-функція – це складнообернене перетворення даних (однобічна функція, реалізована, як правило, засобами симетричного шифрування зі зв'язуванням блоків). Результат шифрування останнього блоку (що залежить від усіх попередніх) і слугує результатом хеш-функції. Нехай є дані, цілісність яких потрібно перевірити, хеш-функція й раніше обчислений результат її застосування до вихідних даних (так званий дайджест). Позначимо хеш-функцію через h, вихідні дані – через T, перевірні дані – через T. Контроль цілісності даних зводиться до перевірки рівності $h(T') = h(T)$. Якщо вона виконана, вважається, що $T = T$. Збіг дайджестів для різних даних називається колізією. У принципі, колізії, звичайно, можливі, оскільки потужність сукупності дайджестів є меншою, ніж потужність безлічі хешованих даних, однак те, що h є функція однобічна, означає, що за прийнятний час спеціально організувати колізію неможливо.

Розглянемо тепер застосування асиметричного шифрування для вироблення й перевірки електронного цифрового підпису. Нехай $E(T)$ позначає результат шифрування тексту T за допомогою відкритого ключа, а $D(T)$ – результат розшифрування тексту T (як правило, шифрованого) за допомогою секретного ключа. Щоб асиметричний метод міг застосовуватися для реалізації ЕЦП, необхідно виконання тотожності

$$E(D(T)) = D(E(T)) = T.$$

На рисунку 16.5 показана процедура вироблення електронного цифрового підпису, що полягає в шифруванні перетворенням *D* дайджесту *h(T).*

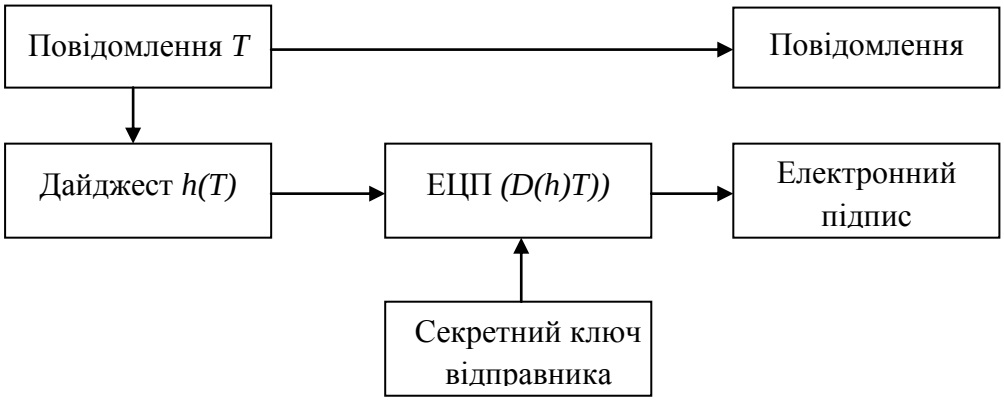


Рисунок 16.5 – Вироблення електронного цифрового підпису

Перевірка ЕЦП може бути реалізована так, як показано на рис. 16.6.

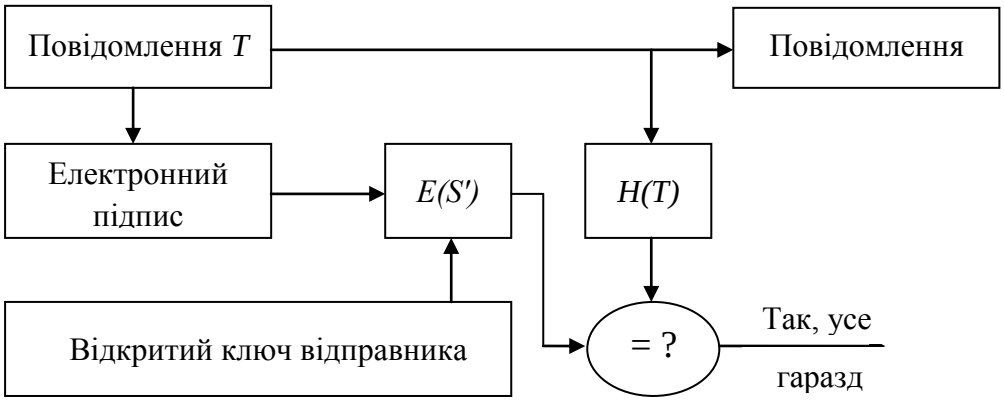


Рисунок 16.6 – Перевірка електронного цифрового підпису

З рівності

$$E(S') = h(T')$$

витікає, що $S' = D(h(T))$ (для доведення досить застосувати до обох частин перетворення D і викреслити в лівій частині тотожне перетворення $D(E)$). Таким чином, електронний цифровий підпис захищає цілісність повідомлення й засвідчує особистість відправника, тобто захищає цілісність джерела даних та є основою безвідмовності.

16.6 Цифрові сертифікати

При використанні асиметричних методів шифрування (і, зокрема, електронного цифрового підпису) необхідно мати гарантію дійсності пари (ім’я користувача, відкритий ключ користувача). Для вирішення цього

завдання в специфікаціях X.509 уводяться поняття цифрового сертифіката й засвідчувального центру.

Засвідчувальний центр – це компонент глобальної служби каталогів, відповідальний за керування криптографічними ключами користувачів. Відкриті ключі й інша інформація про користувачів зберігаються засвідчувальними центрами, у вигляді цифрових сертифікатів, що мають таку структуру:

- порядковий номер сертифіката;
- ідентифікатор алгоритму електронного підпису;
- ім’я засвідчувального центру;
- строк придатності;
- ім’я власника сертифіката (ім’я користувача, якому належить сертифікат);
- відкриті ключі власника сертифіката (ключів може бути декілька);
- ідентифікатори алгоритмів, асоційованих з відкритими ключами власника сертифіката;
- електронний цифровий підпис (ЕЦП), згенерований з використанням секретного ключа засвідчувального центру (підписується результат хешування всієї інформації, що зберігається в сертифікаті).

Цифрові сертифікати мають такі властивості:

- будь-який користувач, що знає відкритий ключ засвідчувального центру, може взнати відкриті ключі інших клієнтів центру й перевірити цілісність сертифіката;
- ніхто, крім засвідчувального центру, не може модифікувати інформацію про користувача без порушення цілісності сертифіката.

У специфікаціях X.509 не описується конкретна процедура генерації криптографічних ключів і керування ними, однак даються деякі загальні рекомендації. Зокрема, обумовлюється, що пари ключів можуть породжуватися кожним з нижченаведених способів:

- ключі може генерувати сам користувач. У такому випадку секретний ключ не потрапляє в руки третіх осіб, однак потрібно вирішувати завдання безпечного зв’язку із засвідчувальним центром;
- ключі генерує довірена особа. У такому випадку доводиться вирішувати завдання безпечної доставки секретного ключа власникові й надання довірених даних для створення сертифіката;
- ключі генеруються засвідчувальним центром. У такому випадку залишається тільки завдання безпечної передачі ключів власникові.

Цифрові сертифікати у форматі X.509 версії 3 стали не тільки форматним, але й фактичним стандартом, підтримуваним численними засвідчувальними центрами.

Запитання для самоперевірки

1. Протоколювання й аудит. Основні поняття.
2. Які завдання вирішує реалізація протоколювання й аудиту?
3. Чому протоколювання не може забезпечити невідмовність?
4. Яку інформацію рекомендується записувати при протокольованій події?
5. Активний аудит. Основні поняття.
6. Функціональні компоненти й архітектура.
7. Шифрування.
8. Для чого необхідна криптографія?
9. Симетричний метод шифрування.
10. Асиметричний метод шифрування.
11. Контроль цілісності.
12. Що таке хеш-функція?
13. Цифрові сертифікати.
14. Сигнатурний метод виявлення атак.
15. Статистичний метод виявлення атак.
16. Граничний метод виявлення атак.
17. Структура цифрових сертифікатів.
18. Властивості цифрових сертифікатів.

ГЛАВА 17
ЕКРАНУВАННЯ ТА АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

17.1 Екранування. Основні поняття

Формальна постановка завдання екранування полягає в нижчевикладеному. Нехай є дві сукупності інформаційних систем. Екран – це засіб розмежування доступу клієнтів з однієї сукупності до серверів з іншої сукупності. Екран здійснює свої функції, контролюючи всі інформаційні потоки між двома сукупностями систем (рис. 17.1). Контроль потоків полягає в їхній фільтрації, можливо, з виконанням деяких перетворень.

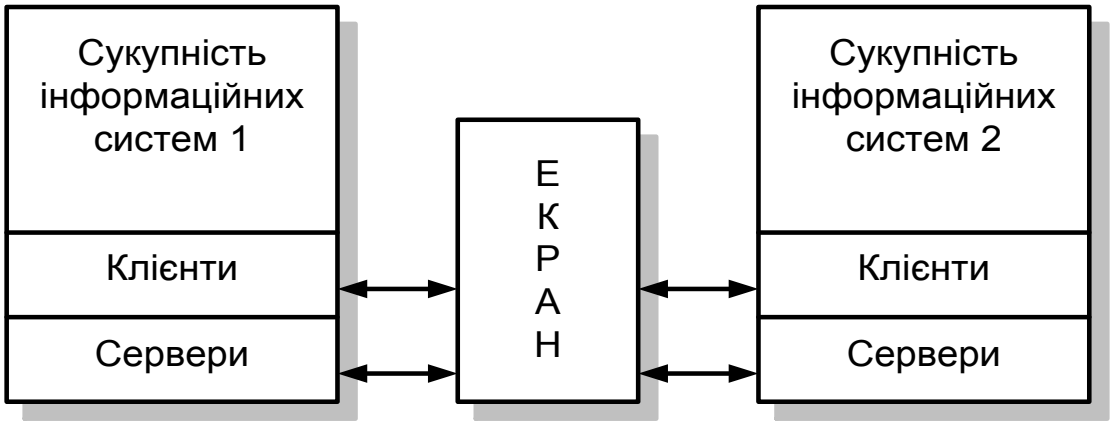


Рисунок 17.1 – Екран як засіб розмежування доступу

На наступному рівні деталізації екран (напівпроникну мембрану) зручно подати як послідовність фільтрів. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може й відразу «перекинути» за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата й повернення результату відправникові (рис. 17.2)

Крім функцій розмежування доступу екрани здійснюють протоколювання обміну інформацією.

Звичайно, екран не є симетричним, для нього визначені поняття «усередині» й «зовні». При цьому завдання екранування формулюється як захист внутрішньої області від потенційно ворожої зовнішньої. Так, міжмережеві екрани (МЕ) (запропонований авторами переклад англійського терміна firewall) найчастіше встановлюють для захисту корпоративної мережі організації, що має вихід в Internet (див. наступний розділ).

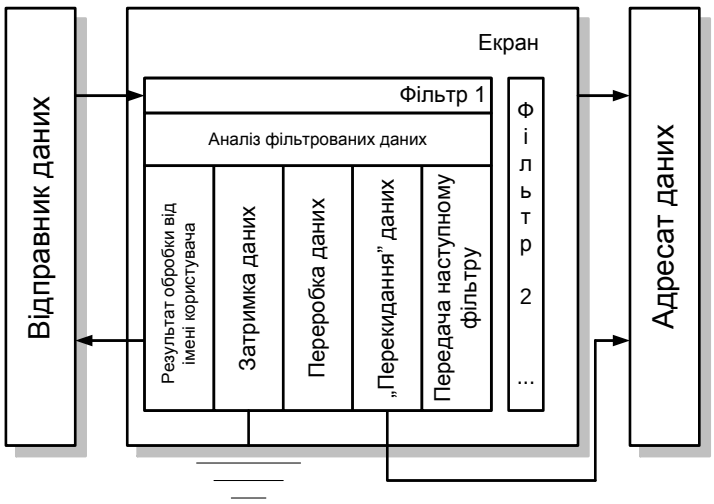


Рисунок 17.2 – Екран як послідовність фільтрів

Екранування допомагає підтримувати доступність сервісів внутрішньої області, зменшуючи або взагалі ліквідуючи навантаження, викликане зовнішньою активністю. Зменшується уразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен перебороти екран, де захисні механізми сконфігуровані особливо ретельно. Крім того, екранувальна система, на відміну від універсальної, може будуватися більш просто й, отже, більш безпечним чином.

Екранування дає можливість контролювати також інформаційні потоки, спрямовані в зовнішню область, що сприяє підтримці режиму конфіденційності в ІС організації.

Підкреслимо, що екранування може використовуватися як сервіс безпеки не тільки в мережевому, але й у будь-якому іншому середовищі, де відбувається обмін повідомленнями. Найважливіший приклад подібного середовища – об'єктно-орієнтовані програмні системи, коли для активізації методів об'єктів виконується (принаймні, у концептуальному плані) передача повідомлень. Ймовірно, що в майбутніх об'єктно-орієнтованих середовищах екранування стане одним з найважливіших інструментів розмежування доступу до об'єктів.

Екранування може бути частковим, захищаючи певні інформаційні сервіси. Екранування електронної пошти описано в статті «Контроль над корпоративною електронною поштою: система «Дозор-Джет»» (Jet Info, 2002, 5).

Обмежувальний інтерфейс також можна розглядати як різновид екранування. На невидимий об'єкт важко нападати, особливо за допомогою фіксованого набору засобів. У цьому сенсі Web-інтерфейс має природний захист, особливо в тому випадку, коли гіпертекстові документи формуються динамічно. Кожен користувач бачить лише те, що йому належить бачити. Можна провести аналогію між динамічно формованими

гіпертекстовими документами й поданнями в реляційних базах даних, з тим істотним застереженням, що у випадку Web можливості істотно ширші.

Екранувальна роль Web-сервісу наочно проявляється й тоді, коли цей сервіс здійснює посередницькі (точніше, інтегрувальні) функції при доступі до інших ресурсів, наприклад до таблиць бази даних. Тут не тільки контролюються потоки запитів, але й приховується реальна організація даних.

17.2 Архітектурні аспекти

Боротися з загрозами, притаманними мережевому середовищу, засобами універсальних операційних систем не є можливим. Універсальна ОС – це величезна програма, що, напевно, містить, крім явних помилок, деякі особливості, які можуть бути використані для нелегального одержання привілеїв. Сучасна технологія програмування не дозволяє зробити надто великі програми безпечними. Крім того, адміністратор, що має справу зі складною системою, далеко не завжди в змозі врахувати всі наслідки вироблених змін. Нарешті, в універсальній багатокористувальній системі проломи у безпеці постійно створюються самими користувачами (слабкі й/або рідко змінювані паролі, невдало встановлені права доступу, залишений без догляду термінал і т. п.). Єдиний перспективний шлях пов’язаний з розробкою спеціалізованих сервісів безпеки, які в силу своєї простоти допускають формальну або неформальну верифікацію. Міжмережевий екран саме і є таким засобом, що допускає подальшу декомпозицію, пов’язану з обслуговуванням різних мережевих протоколів.

Міжмережевий екран розташовується між захищуваною (внутрішньою) мережею й зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, у другому – про внутрішній. Залежно від точки зору, зовнішній міжмережевий екран можна вважати першою або останньою (але ніяк не єдиною) лінією оборони. Першою – якщо дивитися на світ очима зовнішнього зловмисника. Останньою – якщо прагнути захищеності всіх компонентів корпоративної мережі й припиненню неправомірних дій внутрішніх користувачів.

Міжмережевий екран – ідеальне місце для вбудовування засобів активного аудиту. З одного боку, і на першому, і на останньому захисних рубежах виявлення підозрілої активності по-своєму важливо. З іншого боку, МЕ здатний реалізувати будь-яку потужну реакцію на підозрілу активність, аж до розриву зв’язку з зовнішнім середовищем. Щоправда, потрібно усвідомлювати те, що з’єднання двох сервісів безпеки в принципі може створити пролом, що сприяє атакам на доступність.

На міжмережевий екран доцільно покласти ідентифікацію/ аутентифікацію зовнішніх користувачів, що мають потребу у доступі до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

У силу принципів ешелонованості оборони для захисту зовнішніх підключень звичайно використовується двокомпонентне екранування (рис. 17.3). Первинна фільтрація (наприклад, блокування пакетів керівного протоколу SNMP, небезпечного атаками на доступність, або пакетів з певними IP-адресами, внесеними в «чорний список») здійснюється граничним маршрутизатором (див. також наступний розділ), за яким розташовується так звана демілітаризована зона (мережа з помірною довірою безпеки, куди виносяться зовнішні інформаційні сервіси організації – Web, електронна пошта й т. п.) і основний МЕ, що захищає внутрішню частину корпоративної мережі.

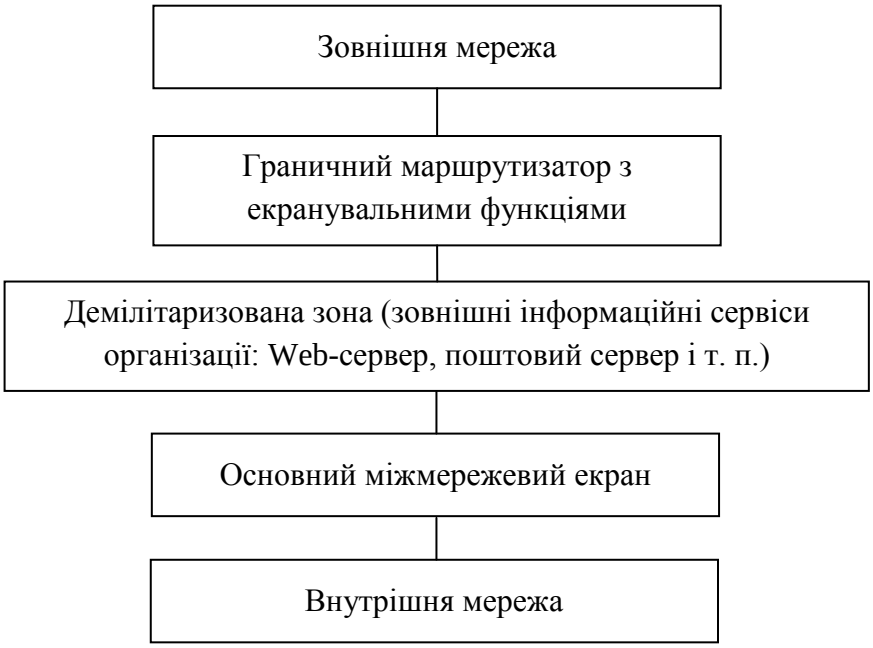


Рисунок 17.3 – Двокомпонентне екранування з демілітаризованою зоною

Теоретично міжмережевий екран (особливо внутрішній) повинен бути багатопротокольним, однак на практиці домінування сім'ї протоколів TCP/IP настільки велике, що підтримка інших протоколів уявляється надмірністю, шкідливою для безпеки (чим сервіс складніший, тим він більш уразливий).

Загалом кажучи, і зовнішній, і внутрішній міжмережеві екрани можуть стати вузьким місцем, оскільки обсяг мережевого трафіка має тенденцію до швидкого зростання. Один з підходів до вирішення цієї проблеми припускає розбиття МЕ на кілька апаратних частин й організацію спеціалізованих серверів-посередників. Основний міжмережевий екран може проводити грубу класифікацію вхідного трафіка за видами і передоручати фільтрацію відповідним посередникам (наприклад,

посередникові, що аналізує HTTP-трафік). Вихідний трафік спочатку обробляється сервером-посередником, що може виконувати й такі функціонально корисні дії, як кешування сторінок зовнішніх Web-серверів, що знижує навантаження на мережу взагалі й основний МЕ зокрема.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є скоріше винятком, ніж правилом. З іншого боку, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожний з яких підключений до Internet. У цьому випадку кожне підключення повинне захищатися своїм екраном. Можна вважати, що корпоративний зовнішній міжмережевий екран є складовим, і потрібно вирішувати завдання узгодженого адміністрування (керування й аудиту) всіх компонентів.

Протилежністю складовим корпоративним МЕ (або їхнім компонентам) є персональні міжмережеві екрани й персональні екранувальні пристрої. Перші є програмними продуктами, які встановлюються на персональні комп'ютери й захищають тільки їх. Другі реалізуються на окремих пристроях і захищають таку невелику локальну мережу, як мережа домашнього офісу.

При розгортанні міжмережевих екранів варто дотримуватися розглянутих нами раніше принципів архітектурної безпеки, у першу чергу подбавши про простоту й керованість, про ешелонованість оборони, а також про неможливість переходу в небезпечний стан. Крім того, варто брати до уваги не тільки зовнішні, але й внутрішні загрози.

17.3 Класифікація міжмережевих екранів

При розгляді будь-якого питання, що стосується мережевих технологій, основою слугує семирівнева еталонна модель ISO/OSI. Міжмережеві екрани також доцільно класифікувати за рівнем фільтрації – канальним, мережевим, транспортним або прикладним. Відповідно, можна говорити про екранувальні концентратори (мости, комутатори) (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

Фільтрація інформаційних потоків здійснюється міжмережевими екранами на основі набору правил, що є вираженням мережевих аспектів політики безпеки організації. У цих правилах, крім інформації, яка зберігається у фільтрованих потоках, можуть фігурувати дані, отримані з оточення, наприклад, поточний час, кількість активних з'єднань, порт, через який надійшов мережевий запит, і т. д. Таким чином, у міжмережевих екранах використовується дуже потужний логічний підхід до розмежування доступу.

Можливості міжмережевого екрана безпосередньо визначаються тим, яка інформація може використовуватися в правилах фільтрації і якою може

бути потужність наборів правил. Загалом кажучи, чим вищим є рівень моделі ISO/OSI, на якому функціонує МЕ, тим більш змістовна інформація йому доступна й, отже, тим тонше й надійніше він може бути сконфігурованим.

Екранувальні маршрутизатори (і концентратори) мають справу з окремими пакетами даних, тому іноді їх називають пакетними фільтрами. Рішення про те, пропустити чи затримати дані, приймаються для кожного пакета незалежно, на підставі аналізу адрес й інших полів заголовків мережевого (канального) і, можливо, транспортного рівнів. Ще один важливий компонент аналізованої інформації – порт, через який надійшов пакет.

Екранувальні концентратори є засобом не стільки розмежування доступу, скільки оптимізації роботи локальної мережі за рахунок організації так званих віртуальних локальних мереж. Останні можна вважати важливим результатом застосування внутрішнього міжмережевого екранування.

Сучасні маршрутизатори дозволяють зв’язувати з кожним портом кілька десятків правил і фільтрувати пакети як на вході, так і на виході. У принципі, як пакетний фільтр може використовуватися й універсальний комп’ютер, обладнаний декількома мережевими картами.

Основні переваги екранувальних маршрутизаторів – доступна ціна (на межі мереж маршрутизатор потрібний практично завжди, питання лише в тому, як задіяти його екранувальні можливості) і прозорість для більш високих рівнів моделі OSI. Основний недолік – обмеженість аналізованої інформації та, як наслідок, відносна слабкість забезпечуваного захисту.

Транспортне екранування дозволяє контролювати процес встановлення віртуальних з’єднань і передачу інформації з них. З погляду реалізації екранувальний транспорт являє собою досить просту, а виходить, надійну програму.

Порівняно з пакетними фільтрами транспортне екранування має більшу кількість інформації, тому відповідний міжмережевий екран може здійснювати більш тонкий контроль за віртуальними з’єднаннями (наприклад, він здатний відслідковувати кількість передаваної інформації й розривати з’єднання після перевищення певного порогу, перешкоджаючи тим самим несанкціонованому експорту інформації). Аналогічно, можливе накопичення більш змістовної реєстраційної інформації. Головний недолік – звуження сфери застосування, оскільки поза контролем залишаються датаграмні протоколи. Звичайно, транспортне екранування застосовують у поєднанні з іншими підходами, як важливий додатковий елемент.

Міжмережевий екран, що функціонує на прикладному рівні, здатний забезпечити найбільш надійний захист. Як правило, подібний МЕ являє собою універсальний комп’ютер, на якому функціонують екранувальні агенти, інтерпретуючи протоколи прикладного рівня (HTTP, FTP, SMTP, telnet і т. д.) у тому ступені, який необхідний для забезпечення безпеки.

При використанні прикладних МЕ, крім фільтрації, реалізується ще один найважливіший аспект екранування. Суб'єкти з зовнішньої мережі бачать тільки шлюзовий комп'ютер; відповідно, їм доступна тільки та інформація про внутрішню мережу, яку він уважає за потрібне експортувати. Прикладний МЕ насправді екранує, тобто закриває, внутрішню мережу від зовнішнього світу. У той же час, суб'єктам внутрішньої мережі здається, що вони напряму спілкуються з об'єктами зовнішнього світу. Недолік прикладних МЕ – відсутність повної прозорості, що потребує спеціальних дій для підтримки кожного прикладного протоколу.

Якщо організація має у своєму розпорядженні вихідні тексти прикладного МЕ й спроможна ці тексти модифікувати, перед нею відкриваються надзвичайно широкі можливості з налаштування екрана з урахуванням власних потреб. Справа в тому, що при розробці систем клієнт/сервер у багатоланковій архітектурі з'являються специфічні прикладні протоколи, які потребують захисту не менше стандартних. Підхід, заснований на використанні екранувальних агентів, дозволяє побудувати такий захист, не знижуючи безпеку й ефективність інших додатків і не ускладнюючи структуру зв'язків у міжмережевому екрані.

Комплексні міжмережеві екрани, що охоплюють рівні від мережевого до прикладного, поєднують у собі кращі властивості «однорівневих» МЕ різних видів. Захисні функції виконуються комплексними МЕ прозорим для додатків чином, не вимагаючи внесення будь-яких змін ні в існуюче програмне забезпечення, ні в дії, що стали для користувачів звичними.

Комплексність МЕ може досягатися різними способами: «знизу догори», від мережевого рівня через накопичення контексту до прикладного рівня, або «зверху вниз», за допомогою доповнення прикладного МЕ механізмами транспортного й мережевого рівнів.

Крім виразних можливостей і припустимої кількості правил, якість міжмережевого екрана визначається ще двома дуже важливими характеристиками – простотою використання й власною захищеністю. У плані простоти використання першорядне значення мають наочний інтерфейс при визначенні правил фільтрації й можливість централізованого адміністрування складених конфігурацій. У свою чергу, в останньому аспекті хотілося б виділити засоби централізованого завантаження правил фільтрації й перевірки набору правил на несуперечність. Важливо і централізоване збирання та аналіз реєстраційної інформації, а також одержання сигналів про спроби виконання дій, заборонених політикою безпеки.

Власна захищеність міжмережевого екрана забезпечується тими ж засобами, що й захищеність універсальних систем. Мається на увазі фізичний захист, ідентифікація й аутентифікація, розмежування доступу, контроль цілісності, протоколювання й аудит. При виконанні централізованого адміністрування варто також подбати про захист

інформації від пасивного й активного прослуховування мережі, тобто забезпечити її (інформації) цілісність і конфіденційність. Надто важливо оперативне накладення латок, що ліквідують виявлені уразливі місця МЕ.

Хотілося б підкреслити, що природа екранування як сервісу безпеки дуже глибока. Крім блокування потоків даних, що порушують політику безпеки, міжмережевий екран може приховувати інформацію про захищувані мережі, що, тим самим, перешкоджає діям потенційних зловмисників. Потужним методом приховування інформації є трансляція «внутрішніх» мережевих адрес, що попутно вирішує проблему розширення адресного простору, виділеного організації.

Відзначимо також додаткові можливості міжмережевих екранів:

- контроль інформаційного наповнення (антивірусний контроль «на ходу», верифікація Java-апплетів, виявлення ключових слів в електронних повідомленнях і т. п.);
- виконання функцій ПЗ проміжного шару.

Особливо важливим є останній з перерахованих аспектів. ПЗ проміжного шару, як і традиційні міжмережеві екрани прикладного рівня, приховує інформацію про надавані послуги. За рахунок цього воно може виконувати такі функції, як маршрутизація запитів і балансування навантаження. Вважається цілком природним, щоб ці можливості були реалізовані в межах міжмережевого екрана. Це істотно спрощує дії з забезпечення високої доступності експортованих сервісів і дозволяє здійснювати перемикання на резервні потужності прозорим для зовнішніх користувачів чином. У результаті до послуг, які традиційно надаються міжмережевими екранами, додається підтримка високої доступності мережевих сервісів.

17.4 Аналіз захищеності

Сервіс аналізу захищеності призначений для виявлення уразливих місць з метою їхньої оперативної ліквідації. Сам по собі цей сервіс ні від чого не захищає, але допомагає виявити (і усунути) прогалини в захисті раніше, ніж їх зможе використати зловмисник. У першу чергу маються на увазі не архітектурні (їх ліквідувати складно), а «оперативні» проломи, що з’явилися в результаті помилок адміністрування або через неуважність до відновлення версій програмного забезпечення.

Системи аналізу захищеності (названі також сканерами захищеності), як і розглянуті вище засоби активного аудиту, засновані на накопиченні й використанні знань. У цьому випадку маються на увазі знання про прогалини в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати.

Відповідно, ядром таких систем є база уразливих місць, що визначає доступний діапазон можливостей і потребує практично постійної актуалізації.

У принципі, можуть виявлятися проломи найрізноманітнішої природи: наявність шкідливого ПЗ (зокрема, вірусів), слабкі паролі користувачів, невдало сконфігуровані операційні системи, небезпечні мережеві сервіси, невстановлені латки, уразливості в додатках і т. д. Однак найбільш ефективними є мережеві сканери (очевидно, у силу домінування сімейства протоколів TCP/IP), а також антивірусні засоби. Антивірусний захист ми зараховуємо до засобів аналізу захищеності, не вважаючи її окремим сервісом безпеки.

Сканери можуть виявляти уразливі місця як шляхом пасивного аналізу, тобто вивчення конфігураційних файлів, задіяних портів і т. п., так і шляхом імітації дій атакуючого. Деякі знайдені уразливі місця можуть усуватися автоматично (наприклад, лікування заражених файлів), про інші повідомляється адміністраторові.

Системи аналізу захищеності містять у собі традиційний «технологічний цукор»: автовиявленням компонентів аналізованої ІС з графічним інтерфейсом, який допомагає ефективно працювати з протоколом сканування.

Контроль, забезпечуваний системами аналізу захищеності, носить реактивний, запізнілий характер, він не захищає від нових атак, однак варто пам’ятати, що оборона повинна бути ешелонованою, і як один з рубежів, контроль захищеності цілком адекватний. Відзначимо також, що переважна більшість атак носить рутинний характер; вони можливі тільки тому, що відомі проломи в захисті роками залишаються неусунутими.

Запитання для самоперевірки

1. Екранування. Основні поняття.
2. Які функції виконує екран?
3. Функції міжмережевого екрана.
4. Принципи архітектурної безпеки, які застосовуються до міжмережевих екранів.
5. Комплексне екранування.
6. Архітектурні аспекти.
7. Класифікація міжмережевих екранів.
8. Додаткові можливості міжмережевих екранів.
9. Аналіз захищеності.
10. Екран як засіб розмежування доступу.
11. Екран як послідовність фільтрів.
12. Двокомпонентне екранування демілітаризованою зоною.

ГЛАВА 18
КЕРУВАННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

18.1 Керування безпекою інформаційних технологій

Планування і загальний огляд процесів планування і керування

Планування і керування захистом інформаційних технологій – загальний процес встановлення і підтримування програми безпеки інформаційних технологій в організації. На рисунку 18.1 відображено основні елементи цього процесу.

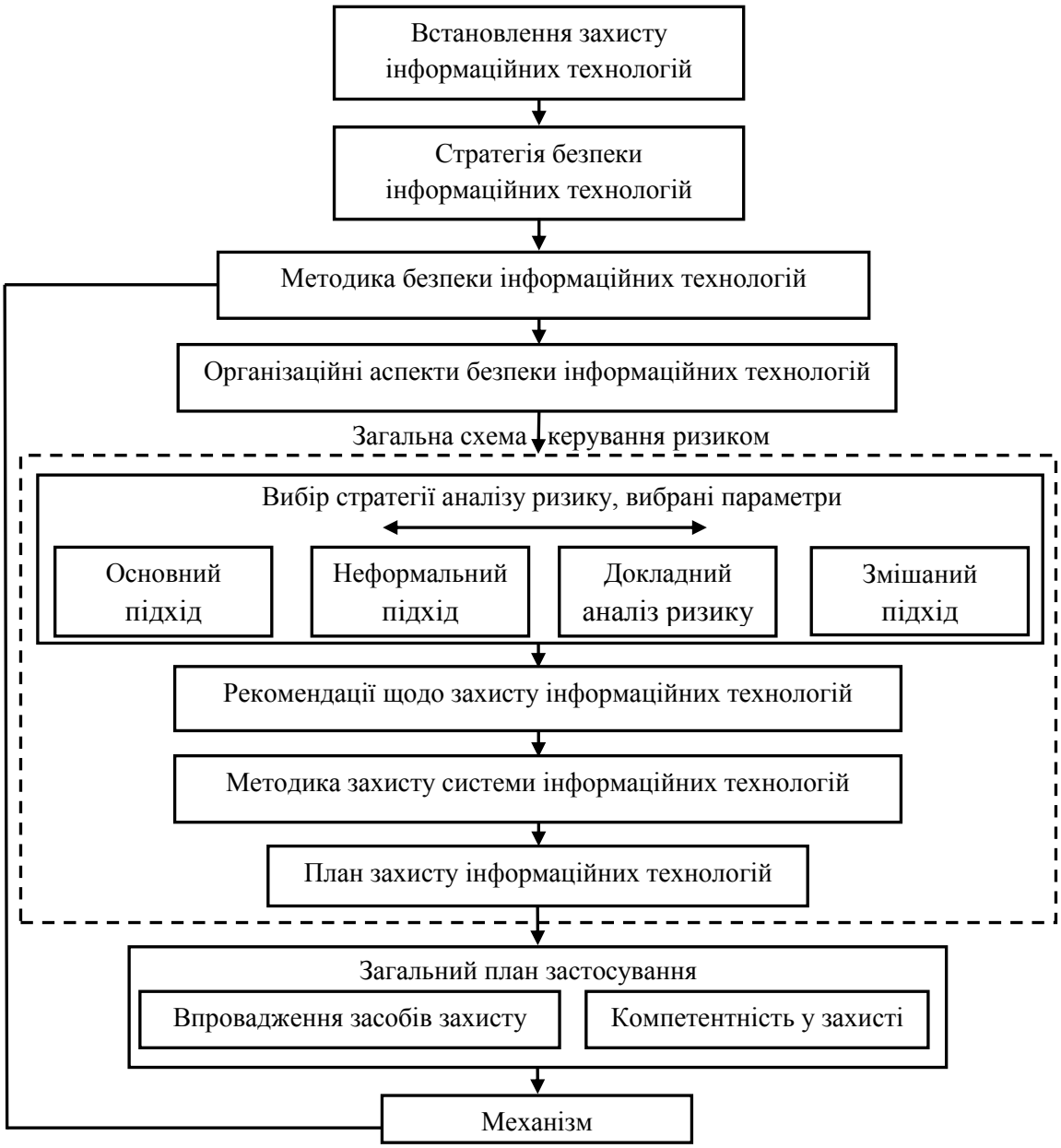


Рисунок 18.1 – Загальна схема керування безпекою інформаційних технологій

Відмінність типів керування, розмірів і структур організацій зумовлює орієнтацію процесу на середовище. Важливо, що всі аспекти та функції, які зображені на рис. 18.1, пристосовані до типу, розміру і структури організації та способу ведення діяльності. Безумовно, ці елементи керування є лише частиною діяльності організації.

Відправною точкою є встановлення чітких цілей захисту інформаційних технологій організації. Вони виходять з цілей вищого рівня (наприклад, з цілей ділової активності) і, в свою чергу, визначають стратегію безпеки інформаційних технологій організації і корпоративну методику безпеки інформаційних технологій. Отже, частиною методики безпеки інформаційних технологій є створення відповідної структури організації, яка буде гарантувати досягнення певної мети.

Загальна схема керування ризиком

Керування ризиком складається з чотирьох різних дій:

– визначення загальної стратегії керування ризиком згідно з корпоративною методологією керування безпекою інформаційних технологій;

– вибір засобів захисту для конкретної системи інформаційних технологій згідно з аналізом ризику або відповідно до концепції керування ризиком;

– розробка методик захисту системи інформаційних технологій, виходячи з рекомендацій безпеки, та, в разі потреби, модифікація методологій захисту інформаційних технологій (і відповідних відомчих методик захисту інформаційних технологій);

– розробка проектів безпеки інформаційних технологій щодо застосування засобів захисту на основі схвалених методик захисту системи інформаційних технологій.

Загальний план застосування

Застосування необхідних засобів захисту для кожної системи інформаційних технологій має відповідати проектам безпеки інформаційних технологій. Поліпшення загальної компетентності в захисті інформаційних технологій, чим часто нехтують, є важливим аспектом ефективності засобів захисту. Рисунок 18.1 показує, що ці два завдання, а саме: застосування засобів захисту і програми компетентності в захисті – треба розв’язувати паралельно, оскільки звична поведінка конкретного користувача не може бути раптово змінена і для освоєння потрібен певний час.

Загальний огляд функцій механізму доопрацювання

Механізм доопрацювання охоплює:

– обслуговування засобів захисту для забезпечення їхньої безперервної й ефективної роботи;

– перевірку засобів захисту, яка гарантує, що вони задовольняють обумовлені методики і проекти;

– контроль активів, загроз, уразливості і засобів захисту щодо відхилень, щоб виявити зміни, які впливають на ризики;

– відстежування кожного інциденту, щоб гарантувати відповідну реакцію на небажані події.

Механізм доопрацювання – тривалий процес, який повинен містити переоцінювання рішень, прийнятих раніше.

Інтеграція захисту інформаційних технологій

Усі дії щодо захисту інформаційних технологій будуть більш ефективними, якщо їх застосовують одночасно в усій організації і з самого початку кожного життєвого циклу системи інформаційних технологій. Процес захисту інформаційних технологій – це важливий окремий цикл діяльності, який повинен бути інтегрований в усі стадії життєвого циклу системи інформаційних технологій. Захист найефективніший, якщо його інтегрують у нові системи з самого початку, успадковані системи та їхня діяльність мають користь від інтеграції захисту протягом усього періоду.

Життєвий цикл системи інформаційних технологій може бути поділений на три базові стадії. Кожна з цих стадій стосується безпеки інформаційних технологій таким чином:

– проектування: захист інформаційних технологій треба враховувати протягом усього процесу проектування та прийняття рішень щодо діяльності організації;

– комплектація: вимоги захисту інформаційних технологій потрібно інтегрувати в процеси проектування, розробки, придбання, оновлювання або в інші конструктивні зміни системи. Інтегрування вимог захисту в ці процеси гарантує оптимальність вартісно-ефективних показників засобів захисту, задіяних у системі, а також їхню своєчасність і відсутність наслідків;

– дії: захист інформаційних технологій необхідно інтегрувати в оперативне середовище. Система інформаційних технологій, яку використовують для виконання визначеної функції, звичайно зазнає ряд оновлень, які охоплюють закупівлю нових апаратних компонентів, зміни або доповнення програмного забезпечення. Крім того, часто змінюється оперативне середовище. Зміни в оточенні (середовищі) можуть створювати нові вразливості системи, які треба аналізувати, оцінювати і відповідно коригувати або сприймати. Також є важливим призначення або зняття захищеності системи.

Убезпечування інформаційних технологій – безперервний процес з багатьма зворотними зв’язками всередині і між стадіями життєвого циклу системи інформаційних технологій. Повний зворотний зв’язок був показаний на рисунок 18.1. У більшості випадків зворотний зв’язок пронизує всю основну діяльність процесу захисту інформаційних технологій. Це забезпечує безперервний потік інформації щодо виявлення уразливості, загроз і засобів захисту системи інформаційних технологій

протягом усіх трьох стадій життєвого циклу системи інформаційних технологій.

Також варто зазначити, що кожна зі сфер діяльності організації може визначити унікальні вимоги щодо захисту інформаційних технологій. Ці сфери повинні взаємно зміцнювати одна одну і весь процес захисту інформаційних технологій, спільно використовуючи інформацію про стан безпеки, що, в свою чергу, може впливати на процес прийняття управлінських рішень.

18.2 Методика безпеки інформаційних технологій

Цілі (які повинні бути досягнуті), стратегії (як досягнути цих цілей) і методики (правила для досягнення цілей) можна визначити для кожного рівня організації і для кожного ділового підрозділу чи відділу. Для досягнення ефективної безпеки інформаційних технологій необхідно впорядкувати різні цілі, стратегії і методики для кожного організаційного рівня і ділового підрозділу. Узгодженість між відповідними документами, незважаючи на вплив різних точок зору, дуже важлива, оскільки більшість загроз (таких як злом системи, знищення файлів і пожежі) – загальні проблеми ділової активності.

Взаємозв'язки методик

Методика безпеки інформаційних технологій може бути внесена до корпоративного технологічного й методологічного керування, і все це разом формує основу для загальних стратегічних положень в інформаційних технологіях. Ці положення повинні містити певні вагомі твердження на користь захисту, особливо якщо є необхідність узгодження захисту і стратегії. Рисунок 18.2 показує залежність між різними методиками. Незалежно від документації та адміністративної структури, використованої організації, дуже важливо, щоб різні положення описаних методик, для підтримки узгодженості, були однаково спрямовані.

Інші методики захисту інформаційних технологій необхідні для певних систем і служб або для групи систем інформаційних технологій і служб. Їх, зазвичай, описують як методики захисту систем інформаційних технологій. Це важливий аспект керування, оскільки їхній контекст і межі чітко визначені та обґрунтовані діловими і технологічними підставами.

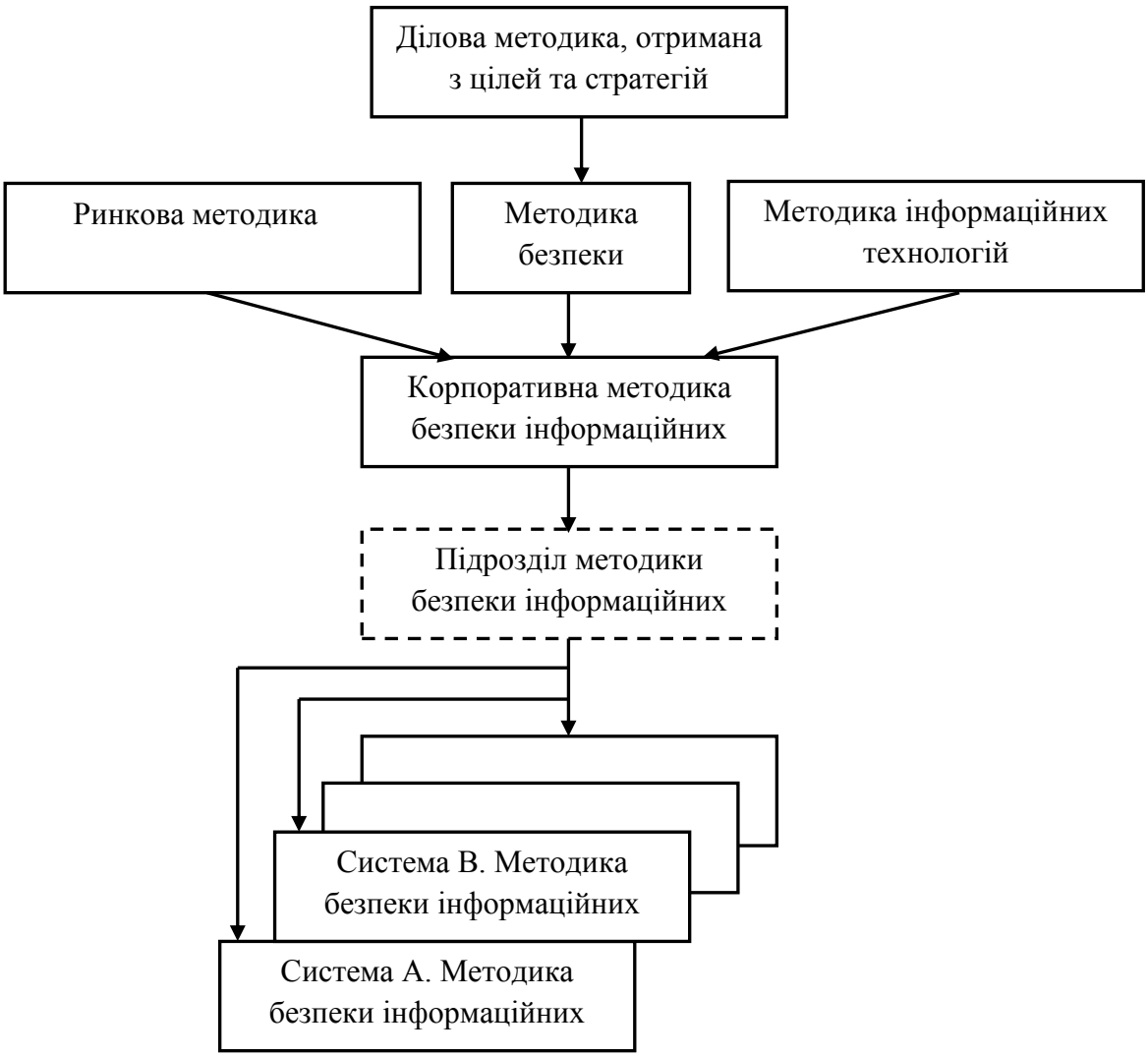


Рисунок 18.2 – Залежності між різними методиками

Елементи методики безпеки інформаційних технологій

Методика безпеки повинна охоплювати, принаймні, такі розділи:

– вимоги безпеки інформаційних технологій (умови конфіденційності, цілісності, доступності, обліковості, достовірності і надійності, особливо з урахуванням уявлень власників активів);

– інфраструктура організації і розподіл обов'язків;

– інтеграція захисту в розробці і реалізації системи;

– директиви і процедури;

– визначання класів для класифікації інформації;

– стратегії керування ризиком;

– планування непередбачуваних обставин;

– підготовка персоналу (особлива увага повинна приділятися службовцям відповідних посад, наприклад, технічному персоналу й адміністраторам системи);

– компетентність і навчання;

– юридичні і регуляторні зобов'язання;

– зовнішнє керування й інформаційна взаємодія;
– реакція на інциденти.

18.3 Організаційні аспекти безпеки інформаційних технологій

Функції та обов'язки

Безпека інформаційних технологій є міжгалузевою темою і стосується кожного проекту інформаційних технологій, системи і всіх користувачів інформаційних технологій в організації. Відповідний розподіл посад і розмежування обов'язків гарантують, що всі важливі завдання будуть успішно й ефективно виконані.

Цієї мети досягають за допомогою різних організаційних заходів залежно від розміру та структури організації. У кожній конкретній організації мають існувати такі структури:

– рада з безпеки інформаційних технологій, яка підсумовує міжгалузеві досягнення та затверджує директиви і стандарти;

– контролер (головний) безпеки інформаційних технологій, який діє як центральна ланка всіх аспектів безпеки інформаційних технологій в організації.

Як рада з безпеки інформаційних технологій, так і контролер безпеки інформаційних технологій повинні мати добре визначені та однозначні обов'язки і мати достатній вплив, щоб гарантувати прив'язку до методології безпеки інформаційних технологій. Організація повинна забезпечити надійний зв'язок між контролером безпеки інформаційних технологій, радою з безпеки інформаційних технологій і представниками інших підрозділів в організації, а також визначити повноваження й відповідальність контролера безпеки інформаційних технологій. Ці обов'язки повинні бути схвалені радою з безпеки інформаційних технологій. Перелік цих обов'язків може бути доповнений шляхом зовнішніх консультацій. Детальніше див. далі (контролер безпеки інформаційних технологій).

Рисунок 18.3 показує типовий приклад зв'язків між контролером безпеки інформаційних технологій, радою з безпеки інформаційних технологій і представниками таких підрозділів в організації, як інші відділи безпеки, товариства користувачів і персонал інформаційних технологій. Ці стосунки можуть полягати як у безпосередньому керуванні, так і у функціонуванні.

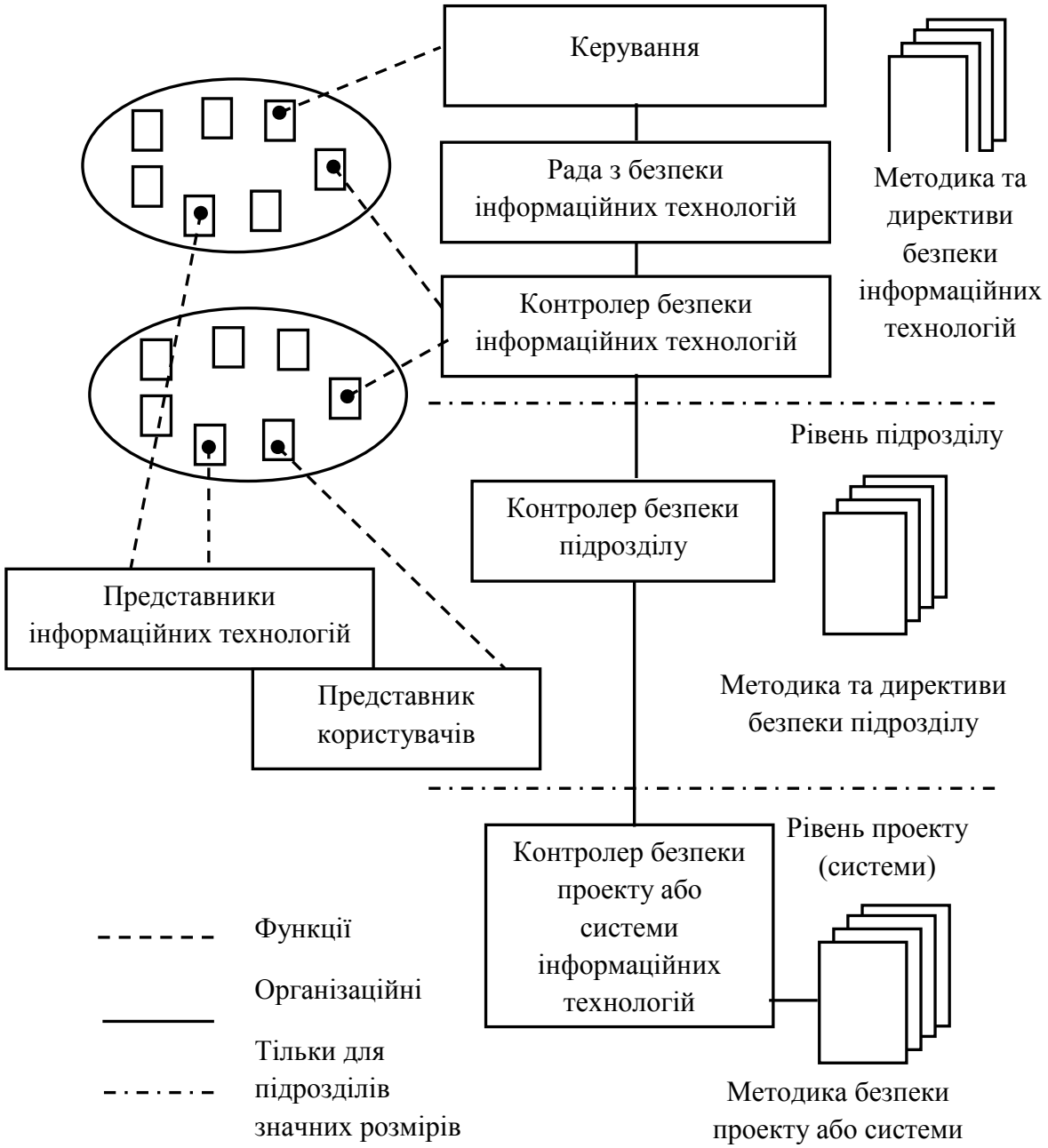


Рисунок 18.3 – Приклад організації безпеки інформаційних технологій

Наприклад, для організації безпеки інформаційних технологій, зображеної на рис. 18.3, використовуються три організаційних рівні. Їх можна легко пристосувати до будь-якої організації, додаючи або вилучаючи відповідні рівні згідно з потребами організації. Невеликі й середні організації можуть мати контролера безпеки інформаційних технологій, чиї обов’язки охоплюють всі питання, пов’язані з безпекою. Коли функції тісно залежать одна від одної, важливо забезпечити відповідні перевірки й утримання рівноваги, щоб уникнути концентрації дуже великої кількості обов’язків у однієї особи, без можливості впливу на неї або контролю за нею.

Рада з безпеки інформаційних технологій

Така рада складається з персоналу необхідного рівня кваліфікації для визначання вимог, розробки методик, складання програми захисту, аналізу здобутків та видачі вказівок (завдань, рекомендацій) контролеру безпеки інформаційних технологій. Для цього може використовуватися вже існуюча рада, або має бути створена окрема рада з безпеки інформаційних технологій. Ця рада може створюватися в існуючій структурі. В обов'язки ради з безпеки інформаційних технологій входить:

– повідомлення керівного комітету інформаційних технологій про стратегічні плани безпеки;

– розробка корпоративної методики безпеки інформаційних технологій в межах підтримки всієї стратегії інформаційних технологій і затвердження її керівним комітетом інформаційних технологій;

– перенесення методик безпеки інформаційних технологій у програму безпеки інформаційних технологій;

– контроль застосування програми захисту до інформаційних технологій;

– контроль ефективності методик безпеки інформаційних технологій;

– підтримування компетентності щодо проблем безпеки інформаційних технологій;

– надання консультацій з питань персоналу, фінансів, інформації, знань, іншого, необхідними для підтримування процесів проектування та застосування програми захисту інформаційних технологій.

Для максимальної ефективності роботи в раду повинні входити спеціалісти з базовою підготовкою з захисту і технічних аспектів системи інформаційних технологій, а також представники постачальників послуг і користувачів системи. Знання і кваліфікація в усіх цих галузях необхідні для розробки практичних методик безпеки інформаційних технологій.

Контролер безпеки інформаційних технологій

Оскільки відповідальність за безпеку інформаційних технологій розподілена, то існує ризик, що в результаті ніхто не буде відчувати відповідальності взагалі. Щоб уникнути цього, повинен бути призначений відповідальний за всі питання безпеки інформаційних технологій. Контролер безпеки інформаційних технологій повинен діяти як центральна ланка щодо всіх аспектів безпеки інформаційних технологій в організації. Для цього може бути задіяна вже наявна посада, з додатковими обов'язками, або, що найчастіше доцільно, необхідна окрема посада. Треба надавати перевагу особі, що вже має базовий рівень підготовки з питань захисту інформаційних технологій.

Головні обов'язки контролера безпеки інформаційних технологій:

– нагляд за реалізацією програми захисту інформаційних технологій;

– зв'язок і звітування перед органом з безпеки інформаційних технологій;

– підтримка корпоративних методик захисту інформаційних технологій і директив;

– координація розслідувань інцидентів;

– керування ходом проведення програми компетентності безпеки на рівні корпорації;

– визначення компетенції системних контролерів безпеки проекту (і, за наявності, відповідних контролерів безпеки підрозділів інформаційних технологій).

Контролер безпеки проекту інформаційних технологій і контролер безпеки системи інформаційних технологій

Індивідуальні проекти або системи повинні мати відповідального за захист, якого називають контролером безпеки інформаційних технологій. У деяких випадках це може бути посада за сумісництвом. Обов'язок керування цими контролерами входить до компетенції контролера безпеки інформаційних технологій (або, де можливо, контролера підрозділу безпеки інформаційних технологій). Контролер безпеки в цьому випадку діє як головна ланка всіх аспектів захисту проекту, системи або групи систем. Головні обов'язки цих посадовців:

– зв'язок та підзвітність корпоративному контролеру безпеки (або, де можливо, контролеру підрозділу безпеки інформаційних технологій);

– ініціювання і підтримка проекту або методики захисту системи інформаційних технологій;

– розробка і реалізація проекту безпеки;

– щоденний контроль реалізації та використання захисних засобів інформаційних технологій;

– ініціювання і допомога в запобіганні інцидентам.

Відповідальність

Відповідальність є необхідною для забезпечення ефективного захисту в інформаційних технологіях, якщо керування на різних рівнях забезпечується зусиллями конкретних осіб. Бізнесова відповідальність охоплює і цілі безпеки інформаційних технологій, а саме:

– розуміння глобальних потреб організації;

– розуміння необхідності захисту інформаційних технологій в організації;

– пояснення зобов'язань щодо захисту інформаційних технологій;

– готовність приділяти увагу потребам захисту інформаційних технологій;

– готовність розподіляти ресурси для захисту інформаційних технологій;

– обізнаність на найвищому рівні, що таке засоби захисту інформаційних технологій або їхні складові (межі, обсяг).

Цілі безпеки інформаційних технологій повинні бути оголошені для всієї організації. Кожний службовець чи субпідрядник повинен знати свої

функції та обов’язки, їхній вплив на захист інформаційних технологій і активно брати участь у досягненні цих цілей.

Послідовний підхід

Послідовний підхід до захисту інформаційних технологій треба застосовувати до процесів проектування, експлуатації й оновлення. Захист повинен бути невід’ємним складником протягом усього життєвого циклу інформації і системи інформаційних технологій від проектування до знищення.

Організаційна структура, показана на рис. 18.3, може підтримувати узгоджений підхід до захисту інформаційних технологій у межах організації. Це, однак, потребує прив’язки до стандартів, охоплюючи міжнародні, національні, регіональні, промислові і корпоративні стандарти або правила, які вибирають і застосовують згідно з потребами захисту інформаційних технологій організації. Технічні стандарти повинні бути доповнені правилами і рекомендаціями щодо їх впровадження, використання і керування ними.

Переваги використання стандартів такі:

– інтегрованість захисту;

– здатність до взаємодії;

– послідовність;

– мобільність;

– економність розмірів (шкали затрат);

– взаємодія між організаціями.

18.4 Рекомендації щодо захисту інформаційних технологій

Будь-який з підходів повинен надати мінімальний набір рекомендацій для доведення ризику до допустимого рівня. Ці рекомендації повинні бути схвалені адміністрацією та охоплювати:

– критерії для визначення допустимих рівнів ризиків для систем розглянутих інформаційних технологій;

– вибір засобів захисту, які доводять ризики до припустимого рівня;

– переваги, отримані внаслідок застосування цих засобів захисту, і значне зниження ризиків;

– приймання ризиків, що залишаються після застосування всіх засобів захисту.

Вибір засобів захисту

Є декілька типів засобів захисту: ті, які попереджають, зменшують, контролюють, виявляють або виправляють небажані інциденти, і ті, які відновлюють засоби захисту після небажаних інцидентів. Запобігання може охоплювати засоби, які стримують небажані дії і забезпечують краще розуміння захисту. Основні сфери, де можна застосовувати відповідні захисні засоби, і деякі приклади для кожної сфери такі:

– апаратні засоби (резервне копіювання, ключі);

– програмне забезпечення (електронні підписи, реєстрація, антивірусні засоби);

– зв’язок (мережеві пристрої захисту (firewall), кодування інформації);

– фізичне оточення (захисні споруди, контрольні пункти);

– персонал (компетентність персоналу, процедури для швидкого анулювання доступу службовця);

– адміністрування (повноваження, розподіл апаратних засобів, ліцензоване керування).

Засоби захисту не є незалежними один від одного, і їх часто використовують спільно. Процес вибору повинен враховувати залежність засобів захисту. У процесі вибору засобів захисту треба також перевіряти, чи не залишилися прогалини. Такі прогалини роблять можливим обхід наявних засобів захисту і дають змогу випадковим загрозам викликати пошкодження.

Для нових систем або для тих, де зроблені корінні зміни, вибір засобів захисту повинен враховувати структуру захисту. Структура захисту є частиною загальної структури системи і відображає наскільки задовольняються вимоги безпеки системи інформаційних технологій. Це також стосується і технічних засобів захисту, навіть коли розглядають нетехнічні аспекти.

Усі засоби захисту потребують уваги, щоб гарантувати ефективне використання. Багато засобів захисту для досягнення ефективності потребують підтримки керівництвом. Ці чинники треба враховувати протягом всього процесу вибору засобів захисту.

Дуже важливо, щоб використання засобів захисту було ефективним і не викликало зайвого втручання користувача або органу керування. Якщо засоби захисту спричиняють істотні зміни, то їх застосування потрібно враховувати в програмі компетентності захисту, а також у керуванні змінами і налаштуванням системи.

Врахування ризику

Після застосування вибраних засобів захисту завжди буде існувати залишковий ризик. Це пов’язано з принциповою неможливістю побудови абсолютно захищеної системи, а також з тим, що деякі активи, можливо, залишаються навмисно незахищеними (наприклад, через низький ризик або високі витрати на засоби захисту порівняно з розрахунковою вартістю активів, які треба захищати).

Перший крок процесу врахування ризику полягає в оцінцюванні вибраних засобів захисту, в ідентифікації і визначенні всіх залишкових ризиків. Наступний крок повинен кваліфікувати залишкові ризики як такі, що «можуть бути допущеними», і такі, що «не можуть бути допущеними» організацією.

Очевидно, що неприйнятні ризики не можна допускати і тому не обхідні додаткові засоби захисту, що обмежують ураження або наслідки ризиків. У кожному з цих випадків необхідно прийняти відповідне рішення.

Або ризик треба оцінювати як допустимий, або необхідні додаткові витрати на засоби захисту, які понизять ризик до припустимого рівня.

18.5 Алгоритм керування інформаційною безпекою

Міжнародний стандарт ISO/IEC 17799:2005 (BS 7799-1:2002) «Керування інформаційною безпекою – Інформаційні технології» («Information Technology – Information Securtiy Management») є найбільш відомим та використовуваним стандартом у сфері захисту інформації. Алгоритм застосування стандарту ISO/IEC 17799:2005 наведено на рисунку 18.4.

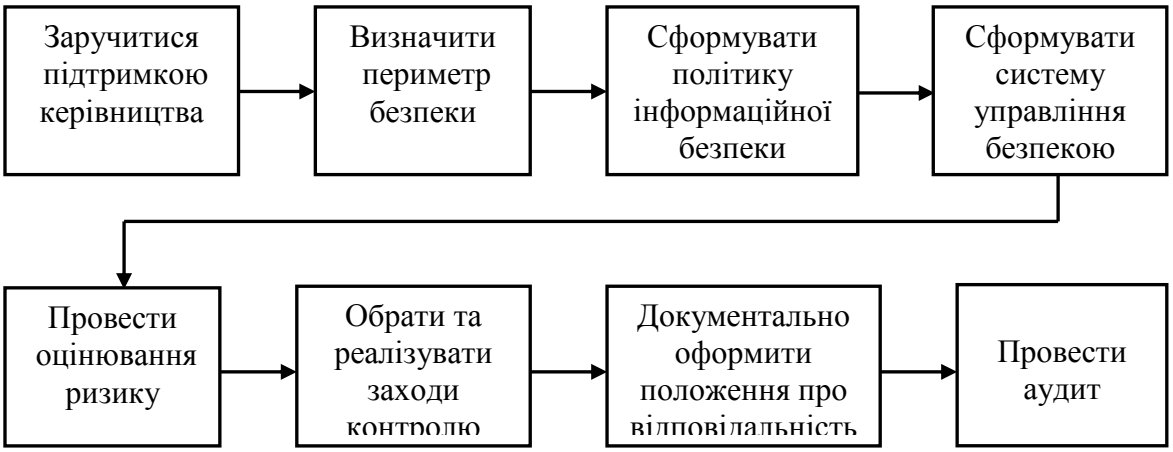


Рисунок 18.4 – Алгоритм застосування стандарту ISO/IEC 17799:2005

Стандарт розроблено на основі першої частини британського стандарту BS 17799-1:2002 «Практичні рекомендації з керування інформаційною безпекою» («Information Securtiy Management – Part 1: Code of Practice for Information Securtiy Management»), він належить до нового покоління стандартів інформаційної безпеки. Поточна версія стандарту ISO/IEC 17799:2005 (BS 7799-1:2002) розглядає нижченаведені питання забезпечення інформаційної безпеки організації (рис. 18.5):

- необхідність забезпечення інформаційної безпеки;
- терміни та визначення інформаційної безпеки;
- політику інформаційної безпеки;
- організацію інформаційної безпеки;
- класифікацію та управління інформаційними ресурсами;
- питання безпеки, пов’язані з персоналом;
- фізична безпека;
- адміністрування безпеки інформаційних систем;
- керування доступом;
- вимоги до безпеки інформаційних систем у ході їхньої розробки, експлуатації і супроводу;

-управління бізнес-процесами організації з точки зору інформаційної безпеки;

-внутрішній аудит інформаційної безпеки;

-забезпечення безперервності бізнесу;

-відповідність вимогам.

Рисунок 18.5 – Основні сфери застосування стандарту ISO/IEC 17799:2005

Специфікація систем керування інформаційною безпекою визначає можливі функціональні специфікації системи управління інформаційною безпекою з точки зору їхньої перевірки на відповідність вимогам (рис. 18.6) .

Рисунок 18.6 – Склад робочої документації для сертифікації

Відповідно до положень стандарту регламентується процедура аудиту безпеки інформаційних систем (рис. 18.7).

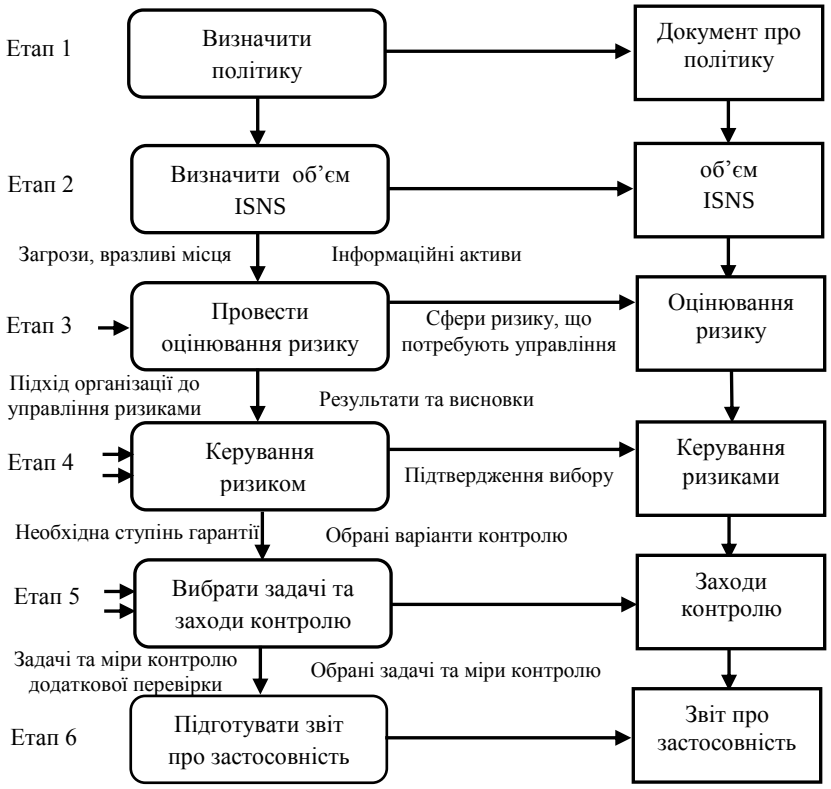


Рисунок 18.7 – Рекомендовані етапи перевірки режиму інформаційної безпеки

Правила з управління інформаційною безпекою розбиті на десять розділів:

– політика безпеки;
– організація безпеки;
– класифікація ресурсів і їхній контроль;
– безпека персоналу;
– фізична безпека;
– адміністрування інформаційних систем і мереж;
– управління доступом;
– розробка і супровід інформаційних систем;
– планування безперервної роботи організації;
– контроль виконання вимог політики безпеки.

Десять ключових механізмів керування інформаційною безпекою, що пропонуються в стандарті ISO 17799, вважаються особливо важливими. Ключові засоби контролю є або обов'язковими вимогами (наприклад, вимоги чинного законодавства), або вважаються основними структурними елементами інформаційної безпеки (наприклад, навчання правилам безпеки). Ці засоби актуальні для всіх організацій і є основою системи

керування інформаційною безпекою. Вони служать як основа для організації, що починає реалізацію засобів керування інформаційною безпекою. До ключових відносять такі засоби контролю:

– документ про політику інформаційної безпеки;

– розподіл обов'язків із забезпечення інформаційної безпеки;

– навчання і підготовка працівників до підтримування режиму інформаційної безпеки;

– повідомлення про випадки порушення безпеки;

– засоби безпеки від вірусів;

– планування безперервної роботи організації;

– контроль над копіюванням програмного забезпечення, захищеного законом про авторські права;

– захист документації і даних організації;

– контроль відповідності політики безпеки.

Стандарт ISO 17799 (BS 7799) дозволяє задати правила безпеки і визначити політику безпеки. Так, наприклад, в табл. 18.1 наведені контрольні запитання згідно з стандартом BS 7799-2, які дозволяють оцінити систему керування інформаційною безпекою та задати правила безпеки.

Додаткові рекомендації з вибору політики безпеки має керівництво Британського інституту стандартів (*www.bsi-glbal.com*) у вигляді серій:

- «Можливості сертифікації на відповідність вимог стандарту BS 7799-2»;

- «Керівництво з вибору засобів забезпечення інформаційної безпеки відповідно до BS 7799-2» тощо.

Аспекти керування і планування призначені для адміністраторів, до компетенції яких входить взаємодія з системами інформаційних технологій організації. Це адміністратори інформаційних технологій, які відповідальні за спостереження за процесами розробки, реалізації, випробовування, постачання або оперування системами інформаційних технологій, та адміністратори, відповідальні за ефективність використання систем інформаційних технологій.

Дії персоналу інформаційних технологій, який відповідає за впровадження, експлуатацію, застосування системи безпеки інформаційних технологій і ефективність використання систем інформаційних технологій описані в стандарті ДСТУ ISO/IEC TR 13335-2:2003.

Керування безпекою систем інформаційних технологій – це процес досягнення і забезпечення необхідних рівнів конфіденційності, цілісності, доступності, обліковості, достовірності та надійності.

Подані в ДСТУ рекомендації призначені для тих, хто пов'язаний з керуванням безпекою інформаційних технологій. Ці рекомендації можна використовувати для ідентифікації і керування усіма аспектами безпеки.

18.6 Методика захисту системи інформаційних технологій

Методики, які розробляються для захисту системи інформаційних технологій, повинні ґрунтуватись на методиці захисту системи. Ці методики захисту системи містять багато принципів і правил для убезпечування систем і служб. Методики повинні бути реалізовані у вигляді застосування відповідних засобів захисту систем і служб, щоб гарантувати, що досягнуто належний рівень захисту.

Методики захисту системи інформаційних технологій повинні бути затверджені вищим керівництвом як обов'язкові набори принципів і правил, щоб гарантувати використання фінансових та трудових ресурсів за призначенням.

Ключові моменти, які треба враховувати під час визначання кожної методики захисту системи інформаційних технологій, такі:

– визначення характеристик системи інформаційних технологій і її меж;

– визначення бізнесових цілей, яких буде досягнуто системою, оскільки вони можуть впливати на методику захисту системи, на вибір і застосування засобів захисту;

– визначення потенційно несприятливих уражень від:

• недоступності, відмови або знищення допоміжних чи основних активів, також інформації;

• несанкціонованої зміни інформації або програмного забезпечення;

• несанкціонованого розголошування даних з наслідками, що їх вимірюють кількісно, такими як прямі або непрямі фінансові втрати, а також з такими якісними наслідками, як втрата престижу, інформації, що викликає збитки або небезпеку, порушення особистої конфіденційності;

– рівень інвестування в інформаційні технології;

– існування істотних загроз системі інформаційних технологій та оброблюваній інформації;

– уразливість через слабкі місця, які дозволяють ідентифікованим загрозам впливати на системи інформаційних технологій;

– необхідність засобів захисту, адекватних ідентифікованим ризикам;

– витрати на захист в інформаційних технологіях, тобто витрати на захист активів інформаційних технологій (кошти, вкладені в захист інформаційних технологій, треба розглядати як частину капіталу власника системи інформаційних технологій);

– структура принципів вибору зовнішніх провайдерів (наприклад, обчислювальні центри, обслуговування інформаційних систем).

Захист інформаційних технологій вимагає планового підходу і не повинен розглядатися окремо. Це має бути головним питанням у процесі стратегічного планування для гарантування, що захист був запланований та інтегрований в систему з самого початку.

18.7 Впровадження засобів захисту інформаційних технологій

Після затвердження проекту безпеки інформаційних технологій необхідно його впровадити. Як правило, за це відповідає системний контролер безпеки інформаційних технологій. У процесі застосування засобів захисту досягнення цілей повинні гарантуватись такі аспекти:

– вартість засобів захисту повинна залишитись у прийнятих межах;

– засоби захисту використовують відповідно до вимог проекту безпеки;

– використання і керування засобами захисту повинно відповідати вимогам проекту безпеки інформаційних технологій.

Більшість технічних засобів захисту потребує експлуатаційного та адміністративного регламентування, їх не можна використовувати як звичайні технічні засоби. Відповідні інструкції повинні бути підтримані і впроваджені керівництвом.

Заходи безпеки охоплюють і навчання задіяного персоналу, компетентного у питаннях захисту, а саме:

– персоналу, відповідального за впровадження системи інформаційних технологій;

– персоналу, відповідального за експлуатацією системи інформаційних технологій;

– контролерів безпеки проекту і системи інформаційних технологій;

– персоналу, відповідального за керування безпекою, наприклад за контролювання доступу.

Після реалізації плану безпеки інформаційних технологій треба формально затвердити застосування засобів захисту, зазначених у проекті безпеки системи інформаційних технологій. Після затвердження дозвіл передають у систему інформаційних технологій або послуги вводять в дію. Процес затвердження в деяких комітетах проводять як акредитацію.

Будь-які істотні зміни в системі інформаційних технологій або послугах повинні викликати повторну перевірку, повторні випробовування і затвердження системи інформаційних технологій або послуг.

18.8 Механізм доопрацювання заходів захисту інформаційних технологій

Всі засоби захисту потрібно використовувати так, щоб вони функціонували і продовжували функціонувати передбачуваним і відповідним способом. Цей аспект безпеки є одним з найважливіших, однак йому часто приділяють мало уваги. Частіше система або служба вже існують, тому захист впроваджують пізніше і потім залишають без нагляду. Існує навіть тенденція ігнорувати засоби захисту, які були застосовані, а підтримці чи убезпечуванню приділяти незначну увагу. Більше того, втрату ефективності засобів захисту потрібно спрогнозувати у

планах, а не спостерігати вже як факт. Також необхідно перевіряти узгодженість захисту, контролювати робоче оточення, оглядати записи у журналі та обробляти інциденти для гарантії тривалості процесу убезпечування.

Обслуговування

Обслуговування засобів захисту, що охоплює також і керування, є важливою частиною програми безпеки організації. Всі рівні керівництва, відповідальні за обслуговування, мають гарантувати:

– виділення необхідних ресурсів організації для обслуговування засобів захисту;

– періодичну переатестацію засобів захисту для гарантування виконання ними своїх функцій;

– модернізацію засобів захисту у разі появи нових вимог;

– чітко визначену відповідальність за обслуговування засобів захисту;

– незмінність певного рівня ефективності наявних засобів захисту під час модифікації технічного й програмного забезпечення у разі розширення системи інформаційних технологій;

– запобігання новим загрозам або ураженням при модернізації технологій.

Якщо здійснено описані вище заходи з обслуговування, то засоби захисту продовжуватимуть виконувати своє призначення, що дає змогу уникати несприятливих і збиткових уражень.

Відповідність засобів захисту

Перевірка відповідності засобів захисту, тобто аудит чи ревізія захисту, є дуже важливим для гарантування відповідності й узгодженості з планом безпеки системи інформаційних технологій.

Щоб гарантувати, що рівень безпеки інформаційних технологій залишається ефективним, впроваджувані засоби захисту повинні завжди відповідали проекту чи плану захисту системи інформаційних технологій. Затвердження необхідно проводити на усіх етапах проходження проектів і систем інформаційних технологій, а саме:

– проектування і впровадження;

– життєвого циклу експлуатації;

– заміни або переміщення.

Перевіряють відповідність захисту за допомогою зовнішнього або внутрішнього персоналу (наприклад, аудиту), і це повинно значною мірою ґрунтуватись на використанні контрольних списків, що стосуються проекту або методики захисту системи інформаційних технологій.

Перевірку відповідності захисту треба планувати та об’єднувати з іншими запланованими заходами. Вибіркові перевірки особливо корисні для визначання чи відповідає виконавчий персонал і користувачі певним засобам захисту і процесам.

Перевірка забезпечить оцінювання коректності функціонування засобів захисту, правильність їхнього впровадження і використання. У разі

виявлення невідповідності безпеці засобів захисту повинен бути створений і реалізований план коригувальних дій з подальшим аналізом результатів.

Контроль

Контроль – вирішальна частина циклу захисту інформаційних технологій. Якщо він проводиться коректно, то це дає адміністрації чітке уявлення про те:

– що було досягнуто порівняно з поставленими цілями;

– чи переконливими є досягнення і які специфічні ініціативи впроваджено.

Всі зміни в активах, загрозах, уразливості засобів захисту потенційно можуть мати суттєвий вплив на ризики і раннє виявлення змін дозволяє здійснити запобіжні заходи.

Багато засобів захисту ведуть журнали з безпеки для фіксації важливих подій. Ці журнали треба, як мінімум, періодично переглядати і, якщо можливо, аналізувати за допомогою статистичних методів для раннього прогнозування тенденцій щодо змін і прогнозування повторів несприятливих подій. Використання журналів тільки для аналізу подій, що відбулися, веде до втрати потенційних можливостей засобів захисту. Контроль повинен також охоплювати процедури для звітності контролеру безпеки інформаційних технологій і для керування на постійній основі.

Обробка інцидентів

Практично неможливо уникнути небажаних інцидентів у захисті. Кожний інцидент потрібно досліджувати настільки глибоко, наскільки вагомий збиток він спричинив. Регулювання інциденту дає змогу відповідно реагувати на випадкові або навмисні збої нормального режиму роботи системи інформаційних технологій. Отже, проект звітності і розслідування інцидентів повинен бути придатним для всієї організації і сервісних служб системи інформаційних технологій. Після цього потрібно об’єднати міжорганізаційні плани звітності для глибшого розуміння місць виявлення інцидентів безпеки інформаційних технологій і пов’язаних з ними загроз, їх впливу на активи інформаційних технологій та ділову активність.

При розслідуванні інцидентів безпеки інформаційних технологій необхідно:

– з’ясувати чи було компетентним і ефективним реагування на інцидент;

– зробити висновки з інцидентів, щоб запобігти подібним несприятливим подіям.

На базі висновків з розслідування інцидентів готується план дій із наперед визначеними рішеннями, що. в свою чергу, дає змогу організації на прийнятних умовах припинити подальше пошкодження і, якщо можливо, продовжувати ділову активність із запасними засобами. План реагування на інциденти повинен містити вимоги хронологічного документування всіх подій і заходів (це повинно допомогти

ідентифікувати джерела інцидентів). Це є передумовою для досягнення іншої мети – зменшення ризику в майбутньому через вдосконалення засобів захисту. Інший позитивний наслідок інцидентів – збільшення готовності інвестувати в засоби захисту.

Важливо також проаналізувати здійснення й документування інциденту, керуючись такими питаннями:

– що сталося і коли саме?

– чи діяв персонал згідно з планом?

– чи вчасно необхідна інформація була в розпорядженні персоналу?

– що персонал запропонував робити інакше наступного разу?

Відповіді на ці питання допоможуть зрозуміти інцидент. Також це допоможе знизити ризик шляхом збільшення релевантності проектів і методик захисту інформаційних технологій (наприклад, вдосконалення засобів захисту, зменшення уразливості й адаптування програми компетентності в захисті).

Запитання для самоперевірки

1. Які питання забезпечення інформаційної безпеки організації розглядає стандарт ISO/IEC 17799:2005 (BS 7799-1:2002)?
2. Наведіть контрольні питання політики інформаційної безпеки.
3. Наведіть контрольні питання організації безпеки.
4. Наведіть контрольні питання з захисту доступу сторонніх організацій.
5. Наведіть контрольні питання класифікації і управління активами.
6. Наведіть контрольні питання класифікації інформації.
7. Наведіть контрольні питання реагування на інциденти безпеки.
8. Наведіть контрольні питання фізичного захисту і захисту середовища.
9. Наведіть контрольні питання з безпеки обладнання.
10. Наведіть контрольні питання загальних засобів безпеки.
11. Наведіть контрольні питання управління діяльністю.
12. Наведіть контрольні питання операційних процедур та відповідальність.
13. Наведіть контрольні питання планування потужності і приймання систем.
14. Наведіть контрольні питання з захисту від зловмисного коду.
15. Наведіть контрольні питання управління мережею.
16. Наведіть контрольні питання управління доступом.
17. Наведіть контрольні питання у правління доступом працівників.
18. Наведіть контрольні питання управління доступом у операційній системі.
19. Наведіть контрольні питання з маркування і безпеки носіїв інформації.

20. Наведіть контрольні питання з обміну інформацією і програмним забезпеченням.

21. Наведіть контрольні питання розробки і підтримання системи.

22. Наведіть контрольні питання аудиту політики інформаційної безпеки і технічної відповідності.

23. Наведіть контрольні питання рекомендацій з аудиту систем.

24. Наведіть контрольні питання з захисту системних файлів.

ПІСЛЯМОВА

Розповідати про інформаційну безпеку, як і про будь-яку справу, в якій необхідно використовувати поєднання знань та творчого підходу, можна дуже довго.

Тому автори щодо глибини висвітлення питань з інформаційної безпеки керувалися таким принципом: гарантованим створенням необхідного мінімуму знань щодо питань і використанням ситуацій та засобів, які найчастіше зустрічаються на практиці.

Формування і забезпечення функціонування ефективно діючої системи інформаційної безпеки в державі – складний і багатогранний процес, який потребує значних зусиль усіх гілок влади, вітчизняної науки, керівників усіх рівнів. Вирішення деяких проблем, очевидно, потребує суттєвого часу, але їхнє вирішення зумовлене необхідністю формування виваженої державної політики забезпечення інформаційної безпеки. Водночас інформаційна безпека, яка забезпечує охорону з боку держави, не повинна гальмувати процеси формування національного інформаційного простору, що відповідав би інформаційно-інтелектуальному потенціалові держави та не перешкоджав би входженню України у світовий інформаційний простір як суб'єкта рівноправних міжнародних відносин. Зважаючи на це, стратегічним завданням державної політики щодо інформаційної безпеки має стати формування систем на основі науково обґрунтованих політичних, соціальних, економічних критеріїв і світового досвіду правового регулювання та організації забезпечення її функціонування. Система інформаційної безпеки відомостей, які підлягають охороні з боку держави, повинна відповідати правовому режимові кожного виду відомостей, діяти безперервно на кожному етапі їхнього формування і поширення та бути адекватною загрозам, що діють в інформаційній сфері.

ЛІТЕРАТУРА

1. Чарльз Хант. Разведка на службе вашего предприятия / Чарльз Хант, Вахе Зартаньян. – Киев : «Укрзакордонвізасервіс», 1992. – 160 с.
2. Герасименко В. А. Защита информации в автоматизированых системах обработки данных : в 2-х кн. / Герасименко В. А. – М. : Энергоатомиздат, 1984.
3. Хофман Л. Д. Современные методы защиты информации / Хофман Л. Д. – М. : Сов.радио, 1980. – 126 с.
4. Гавриш В. С. Практическое пособие по защите коммерческой тайны / Гавриш В. С. – Симферополь : Таврида, 1994. – 108 с.
5. Палый А. И. Радиоэлектронная борьба / Палый А. И – М. : Воениздат, 1989. – 268 с.
6. ДСТУ 3396.0-96. Захист інформації. Основні положення.
7. ДСТУ 3396.1-96. Захист інформації. Порядок проведення роботи.
8. Апорович А. Ф. Проектирование радиотехнических систем / Апорович А. Ф. – Минск : Вышэйшая школа, 1988. – 221 с.
9. Обнаружение радиосигналов. [под ред. А. А. Колосова]. – М. : Радио и связь, 1989. – 288 с.
10. Шрюфер Е. Обробка сигналів, цифрова обробка дискретизованих смгналів : підручник / Шрюфер Е. ; за ред. В. П. Бабака. – К. : Либідь, 1992. – 296 с.
11. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатов – К. : Издательство Юниор, 2003. – 503 с.
12. Хорошко В. О. Комп'ютерна стеганографія : навчальний посібник / Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. – Вінниця : ВНТУ, 2017. – 155 с.
13. Хорошко В. О. Основи науково-дослідної роботи в галузі інформа-ційної безпеки : навч. пос. / Хорошко В. О., Орєхова І. І., Яремчук Ю. Є. – Київ : ДУІКТ, 2012. – 175 с.
14. Гулак Г. М. Основи криптографічного захисту інформації : підруч. / [Гулак Г. М., Мухачов В. А., Хорошко В. О., Яремчук Ю. Є.]. – Вінниця : ВНТУ, 2011. – 199 с.
15. Голубенко О. Л. Політика інформаційної безпеки : підручник / [Голубенко О. Л., Хорошко В. О., Яремчук Ю. Є. та ін.]. – Луганськ : вид-во СНУ ім. В. Даля, 2009. – 300 с.
16. Голубенко О. Л. Політика інформаційної безпеки. Практикум : навч. пос. / [Голубенко О. Л., Хорошко В. О., Петров О. С. та ін.]. – Луганськ : вид-во СНУ ім. В. Даля, 2010. – 208 с.
17. Хорошко В. О. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник / [Хорошко В. О., Азаров О. Д., Максименко Г. О., Яремчук Ю. Є.]. – Вінниця : ВНТУ, 2007. – 333 с.

18. Мастяниця Й. І. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання / Й. І. Мастяниця, О. В. Соснін, Л. Є. Шиманський – К. : Національний інститут стратегічних досліджень, 2000. – 98 с.

19. Василюк В. Я. Інформаційна безпека держави : курс лекцій / В. Я. Василюк, С. О. Климчук – К. : КНТ, Видавничий дім «Скіф», 2008. – 136 с.

20. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / Баранов О. А. – К. : Видавничий дім «СофтПрес», 2005. – 316 с.

21. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

22. Почепцов Г. Г. Информационные войны. Основы военно-коммуни-кативных исследований / Почепцов Г. Г. – М. : Рефл-бук, К. : Ваклер, 2000. – 576 с.

23. Расторгуев С. П. Информационная война / Расторгуев С. П. – М. : Радио и связь,1999. – 416 с.

24. Расторгуев С. П. Философия информационной войны / Расторгу-ев С. П. – М. : Московский психолого-социальный институт, 2003. – 486 с.

25. Соснін О. В. Про правові основи удосконалення системи державно-го управління інформаційними ресурсами / О. В. Соснін, Л. Є. Шимен-ський // Політологічний вісник : зб. наук. праць. – 2002. – № 10. – К. : Т-во «Знання України». – С. 212–219.

26. Баранов А. А. Концептуальные вопросы информационной безопас-ности Украины / Баранов А. А. // Безопасность информации. – 1995. – № 2. – С. 4–10.

27. Конеев И. Р. Информационная безопасность предприятия / И. Р. Ко-неев, А. В. Беляев – СПб. : БХВ–Петербург, 2003. – 688 с.

28. Браіловський М. М. Технічний захист інформації на об'єктах інформаційної діяльності / М. М. Браіловський. Головень С. М. – К. : ДУІКТ, 2007. – 178 с.

29. Петренко С. А. Политика информационной безопасности / С. А. Пет- ренко, В. А. Курбатов – М. : Компания Ай Ти, 2006. – 400 с.

30. Дзюбань О. П. Теоретичні основи національної безпеки України : навчальний посібник / О. П. Дзюбань, О. В. Соснін – К. : Освіта України, 2008. – 384 с.

31. Алексєєнко І. В. Національні держави в умовах глобалізації світу (політичні і правові аспекти). / Алексєєнко І. В. – К. : Аспект – поліграф, 2006. – 360 с.

32. Артюшин Л. М. Теоретичні аспекти стратегії воєнної безпеки сус-пільства і держави : монографія / Л. М. Артюшин, Г. Ф. Костенко. – Харків : НУВС, 2003. – 176 с.

33. Буттлер А. Национальные интересы, национальная и международная безопасность / А. Буттлер // Полис. – 2002. – № 4. – С. 146–158.
34. Буравльов Є. П. Глобалізація: проблеми безпеки / Буравльов Є. П. – К. : Ін-т проблем нац. безпеки, 2007. – 160 с.
35. Войтович Р. В. Вплив глобалізації на систему державного управ-ління: теоретико-методологічний аналіз / Войтович Р. В. – К. : Вид-во НАДУ, 2007. – 679 с.
36. Горбулін В. П. Системно-концептуальні засади стратегії національ-ної безпеки України / В. П. Горбулін, А. Б. Качинський. – К. : Євроатлан-тикінформ, 2007. – 592 с.
37. Даник Ю. Г. Національна безпека запобігання критичним ситуаціям / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін. – Житомир : Рута, 2006. – 387 с.
38. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест ; за ред. проф. В. О. Хорошка. – К. : ДУІКТ, 2008. – 186 с.
39. Ленков С. В. Методы и средства защиты информации : в 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008.
40. Основи інформаційної безпеки / [Андреєв В. І., Хорошко В. О., Чередниченко В. С., Шелест М. Є.]. – [2-е вид., доп. і перероб]. – К. : ДУІКТ, 2009. – 292 с.
41. Голубенко О. Л. Політика інформаційної безпеки / О. Л. Голубенко, В. О. Хорошко – Луганськ : СНУ ім. В. Даля, 2009. – 300 с.
42. Кобозева А. А. Аналіз захищеності інформаційних систем / А. А. Ко-бозева, І. О. Мачалін, В. О. Хорошко – К. : ДУІКТ, 2010. – 316 с.
43. Єжова Л. Ф. Управління інформаційною безпекою : в 2-х т. / [Єжо-ва Л. Ф., Корченко А. О., Мачалін І. О. та ін.]. – [2-е вид., доп. і перероб]. – К. : НАУ, 2012.
44. Бурячок В. Л. Технологія прийняття рішень у складних у складних соціотехнічних системах / В. Л. Бурячок, В. О. Хорошко. – К. : ДУІКТ, 2012. – 344 с.
45. Стратегія кібернетичної безпеки України, 2016 р.
46. Закон України «Про основи національної безпеки України», 2003 р.
47. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 1994 р.
48. Закон України «Про захист персональних даних», 2010 р.
49. Закон України «Про електронні документи та електронний документообіг», 2003 р.
50. Закон України «Про електронний цифровий підпис», 2003 р.

ПЕРЕЛІК СКОРОЧЕНЬ

АБС – автоматизована банківська система
АРМ – автоматизовані робочі місця
АСОД – автоматизовані системи обробки даних
АСУ – автоматизовані системи управління
ДЕ – дескриптори
ДЗ – джерело завади
ЕЦП – електронний цифровий підпис
ЕМЗ – електромагнітна завада
ЗІ – захист інформації
ІБ – інформаційна безпека
ІС – інформаційна система
КНОІ – канали несанкціонованого одержання інформації
МЕ – міжмережевий екран
НЕМЗ – ненавмисна електромагнітна завада
ОС – операційна система
ОЦКК – обчислювальний центр колективного користування
ПЕВМН – побічні електромагнітні віпромінювання і наведення
ПЗ – програмне забезпечення
ПЗ ПШ – програмне забезпечення проміжного шару
ПЗП – постійний запам’ятовувальний пристрій
ППЦІ – причини порушення цілісності інформації
ПРД – правила розмежування доступу
РЗ – рецептор завади
РКД – рольове керування доступом
СУБД – системи управління базами даних
ТЗ – технічний захист

ГЛОСАРІЙ

Активи – усе, що має цінність для організації – ресурси організації (матеріальні й нематеріальні цінності).

Аналіз ризику – процес визначання ймовірності ураження активів, наслідків уражень і ділянок, що потребують застосування засобів захисту.

Аудит – ревізія, що здійснюється уповноваженою особою з метою забезпечення незалежного оцінювання програмних продуктів і процесів, щоб оцінити їх відповідність вимогам.

Базові засоби керування – мінімально необхідна кількість засобів захисту, визначених для системи чи організації.

Базис – офіційно схвалена версія елемента конфігурації, незалежна від середовища, формально розроблена та виправлена впродовж заданого часу в рамках життєвого циклу елемента конфігурації.

Безпека – безпека інформації та даних у такий спосіб, щоб неуповноважена особа або організація не могли їх прочитати або змінити, але щоб це не перешкоджало доступові до них з боку уповноважених осіб чи організацій.

Безпека інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Безпека інформації в системі – діяльність, спрямована на запобігання несанкціонованих дій щодо інформації в системі.

Безпека в інформаційних технологіях – всі аспекти, пов’язані з визначенням, досягненням і забезпеченням конфіденційності, цілісності, доступності, обліковості, достовірності і надійності.

Блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Валідація (англ. *Validation*) – 1. Підтвердження того, що окремі вимоги щодо визначеного передбаченого використання виконуються і здійснюються шляхом перевірки та забезпечення об’єктивних доказів.

2. Процес підтвердження відповідності або надання законної сили.

Примітка 1. При проектуванні та розробленні окремих вимог валідація полягає у процесі перевірки продукту для встановлення відповідності потребам користувача.

Примітка 2. Валідація виконується, як правило, над кінцевим продуктом у заданих умовах функціонування. Потреба у ній може виникнути на більш ранніх етапах.

Примітка 3. Термін «валідований» використовується для надання відповідного статусу окремим вимогам щодо визначення передбаченого використання розділів.

Примітка 4. Багаторазова валідація може здійснюватись у разі наявності різних передбачених використань [ISO 8402, 2.18].

Верифікація – підтвердження виконання заданих вимог, що здійснюється шляхом перевірки та забезпечення об'єктивних доказів, також комплекс процедур перевірки точності і достовірності даних (інформації).

Примітка 1. При проектуванні та розробленні комплекс процедур верифікація полягає у процесі перевірки результатів певної діяльності для визначення відповідності вимогам, встановленим щодо цієї діяльності.

Примітка 2. Термін «верифікація» використовується для надання відповідного статусу інформації (даним).

Версія – примірник елемента, що підлягає ідентифікації.

Примітка. Модифікація версії програмного продукту, результатом якої є нова версія, потребує дії щодо керування конфігурацією.

Вилучення – припинення активної підтримки з боку організації, що здійснює експлуатацію та супровід, часткова чи повна заміна на нову систему або введення в дію оновленої системи.

Вірус інформаційної системи – це спеціально написана програма, котра може «приписувати» себе до інших програм (тобто «заражати» їх), розмножуватися і народжувати нові віруси для виконання різних небажаних дій в інформаційній системі.

Виток інформації – результат дій, внаслідок яких інформація в системі стає відомчою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниці) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з встановленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, внесенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

Власник інформації – фізична або юридична особа, якій належить право власності на інформацію.

Власник системи – фізична або юридична особа, якій належить право власності на систему.

Готовий для використання продукт – вже розроблений та доступний продукт, що може використовуватись у початковому вигляді («як є») або із модифікацією.

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Державна таємниця (далі також секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та

які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою.

Державний експерт з питань таємниці – посадова особа, уповноважена здійснювати відповідно до вимог Закону України «Про державну таємницю» віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, змін ступеня секретності цієї інформації до її розсекречування.

Достовірність – властивість, яка гарантує, що ідентифікатори предмета чи ресурсу задовольняють необхідні вимоги. Достовірність застосовують до об'єктів: споживачів, процесів, систем чи інформації.

Доступність (англ. Availability) — властивість інформаційного ресурсу, яка полягає в тому, що авторизований користувач та/або процес, який наділений відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (прийнятного) інтервалу часу.

Доступ до інформації в системі – отримання користувачем можливості оброблення інформації в системі

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

Доступ до державної таємниці – надання повноваженою посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Елемент конфігурації – об'єкт (сутність) в рамках конфігурації, який задовольняє функцію кінцевого користування і може бути однозначно ідентифікований з певної точки зору (у вказаному значенні, щодо певної базової точки).

Елемент, що не передається, – апаратні чи програмні продукти, які не потребують передачі згідно з контрактом, але які можуть застосовуватись під час розроблення програмного продукту.

Забезпечення якості – всі дії, що плануються та регулярно здійснюються в рамках системи якості і належним чином демонструються з метою забезпечення достатньої впевненості в тому, що об'єкт буде задовольняти вимоги щодо якості.

> **Примітка 1.** Забезпечення якості може мати як внутрішню, так і зовнішню мету:
>
> а) внутрішнє забезпечення якості. У межах організації забезпечення якості передбачає надання впевненості керівництву;
>
> б) зовнішнє забезпечення якості. При наявності відповідного контракту забезпечення якості передбачає надання впевненості клієнтові або іншим організаціям чи особам.

Примітка 2. Між деякими діями з керування якістю та забезпечення якості існує взаємозв'язок.

Примітка 3. Якщо вимоги щодо якості не відображають повністю потреби користувача, забезпечення якості може не передбачати достатньої впевненості.

Загроза – потенційна причина небажаного інциденту, що заподіює шкоду системі, організації чи тому й іншому.

Загроза для інформації – витік, можливість блокування або порушення цілісності інформації.

Примітка. Загроза для інформації може здійснюватися під час застосування технічних засобів чи технологій, недосконалих щодо захисту інформації.

Замовник – організація, що замовляє або отримує систему, програмний продукт чи послугу від постачальника.

Примітка. Термін «замовник» є синонімом покупця, клієнта, власника або користувача.

Замовлення – процес одержання системи, програмного продукту або програмної послуги.

Запит щодо пропозиції (тендер) – документ, що використовується замовником як засіб для оголошення своїх намірів потенційним учасникам тендеру щодо замовлення певної системи, програмного продукту чи програмної послуги.

Засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифа секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Засіб захисту – засіб, процедури чи механізми, що дають змогу зменшити ризик.

Залишковий ризик – ризик, що залишається після впровадження засобів захисту.

Звід відомостей, що становлять державну таємницю, – акт, в якому зведено перелік відомостей, які, згідно з рішеннями державних експертів з питань таємниць, становлять державну таємницю визначену Законом України «Про державну таємницю».

Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає.

Ідентифікація користувача – розпізнання користувача (за прізвищем і паролем) для виявлення повноважень-прав доступу до даних. Вибір режиму їх використання.

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами.

Інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Інформація – сукупність знань про фактичні дані і залежність між ними.

1) тільки однина, інформування;

2) відомості про які-небудь події, чиюсь діяльність і т. ін., повідомлення про щось;

3) сукупність відомостей (даних), які сприймаються з навколишнього середовища (вхідна інформація), видаються у навколишнє середовище (вихідна інформація) або зберігаються всередині нової системи (внутрішня інформація);

4) головний елемент будь-якої з функцій управління, вона повинна відображати реальний світ, процеси, явища, використовувати при цьому зрозумілу користувачеві мову, бути своєчасною, корисною та необхідною йому;

5) це знання, відомості, дані, отримані і накопичені у процесі розвитку науки і практичної діяльності людей, які можуть бути використані у суспільному виробництві і управлінні як фактор збільшення обсягу виробництва і підвищення його ефективності;

6) стосовно електронного документообігу, сукупність фактів, явищ, подій, які є цікавими, що підлягають обліку й обробці;

7) під інформацією, згідно з Законом України «Про інформацію» [3–2] розуміють будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

У розглянутих виразах завжди існують: джерело й споживач інформації. Як першим, так і другим можуть бути об’єкти науки, техніки, суспільства та природи, тварини, люди. У взаємодії між ними й народжується інформація. Залежно від галузі знань розрізняють наукову, технічну, комерційну й інші види інформації.

При першому підході у розгляді поняття «інформація» можна визначити існування двох типів інформації, а саме:

- *перший тип:* інформація технічна, яка передається по каналах зв’язку і відображається на екранах дисплеїв. Кількість такої інформації може бути точно обраховано і процеси, що проходять із такою інформацією, підпорядковуються фізичним законам;

- *другий тип:* інформація семантична, тобто смислова. Це та інформація, яка вміщується, наприклад, у літературному творі. При такому визначенні інформації припускаються різні кількісні оцінки і будуються математичні теорії. Але все зводиться до того, що оцінки тут вельми умовні і приблизні.

Другий підхід полягає в тому, що інформація – фізична величина, така ж, як температура, швидкість і в певних умовах інформація однаковим

чином описує як процеси, що проходять у природних фізичних системах, так і процеси, що проходять в системах штучно створених.

Третій підхід полягає у тому, що інформація єдина, але кількісні і якісні оцінки повинні бути однаковими. У цьому випадку, з одної сторони, можна обчислити цінність інформації, а з другої сторони, такі обчислення справедливі лише в обмеженому числі випадків, наприклад, цінність будь-якого винаходу неможливо підрахувати на момент появи винаходу.

Інформація, що становить банківську таємницю, – це вид таємної інформації, який охоплює відомості про операції, рахунки, вклади клієнтів та респондентів.

Інформація, що становить професійну таємницю, – це вид таємної інформації, який охоплює відомості, надані органові державної влади у зв'язку з виконанням покладених на нього функцій, якщо розголошення таких відомостей заборонено законом, що визначає статус відповідного органу державної влади, і ці відомості не належать до інших передбачених законом видів таємної інформації або інформації про особу.

Інформація, що становить службову таємницю, – це вид таємної інформації, який створюється під час поточної діяльності організацій і який охоплює відомості в сфері управління, внутрішньої та зовнішньої політики, економіки та фінансів, банківської діяльності, науки й техніки, зовнішніх відносин, охорони здоров'я, а також відомості у сфері оборони, державної політики, охорони правопорядку та в інших сферах державної діяльності, що не містять інших видів таємної інформації, розголошення якої може завдати шкоди інтересам держави та суспільства.

Інформація, що становить таємницю листування, телефонних розмов і телеграфної та іншої кореспонденції, – це вид таємної інформації, який охоплює відомості, яку передають засобами зв'язку за допомогою листування, телефонних розмов, телеграфної та іншої кореспонденції.

Інформація в сфері оборони – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойовій готовності Збройних сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно із законодавством України.

Інформація, що становить таємницю страхування, – це вид таємної інформації, який охоплює відомості про страхувальника та його майновий стан.

Інформація, що становить комерційну таємницю, – відомості науково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (у тому числі секрети виробництва (ноу-хау)), що мають дійсну або потенційну комерційну цінність у силу невідомості її третім особам, до якої немає вільного доступу на законній підставі та стосовно якої власником такої інформації введений режим комерційної таємниці.

Термін «ноу-хау» («know-how») вперше був застосований в американській судовій практиці в 1916 році у судовій праві «Дізенд проти Брауна» і з того часу застосовується у всьому світі, дослівний переклад терміна означає «знаю як» (скорочення від «знаю як зробити») і знайшов застосування в правовій літературі більшості держав світу та став звичайним в економічному обігу. Він відомий в комерційних і юридичних колах, але до теперішнього часу немає достатньо чіткого його визначення, щоб задовольнити усіх, вираз «ноу-хау» є професіоналізмом, побутовим жаргоном, що набув повсюдного поширення у зв'язку зі своєю виразністю.

Загальним для всіх термінів є те, що до «ноу-хау» відносять технічні прийоми і виробничу інформацію. «Ноу-хау» може виступати як інформація з обмеженим доступом, так і відкрита інформація.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційний процес – будь-який процес, у якому присутній хоча б один із елементів: передача інформації, її приймання, зберігання, обробка, видача користувачу.

Кваліфікація – процес демонстрації здатності об'єкта виконувати задані вимоги.

Кваліфікаційні вимоги – множина критеріїв чи вимог, які повинні задовольнятись для того, щоб програмний продукт можна було кваліфікувати як такий, що відповідає специфікаціям на нього і готовий для використання в його цільовому середовищі.

Кваліфікаційні випробування – випробування, які проводить розробник і засвідчує замовник (відповідним чином) для демонстрації того, що програмний продукт відповідає специфікаціям на нього і готовий для використання в його цільовому середовищі.

Керування ризиком – загальний процес визначання, регулювання і відокремлювання чи мінімізації сумнівних подій, що можуть впливати на ресурси системи інформаційних технологій.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Контракт – двостороння угода, якій, як правило, надано статус юридичної сили, або подібна внутрішня угода, виключно у межах організації, щодо надання програмних послуг або постачання, розробки, виробництва, експлуатації чи супроводу програмного продукту.

Конфіденційність – властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об'єктами чи процесами.

Користувач – особа або організація, що використовує діючу систему для виконання заданої функції.

Примітка. Користувач може виконувати інші ролі, наприклад, замовника, розробника, супроводжувача.

Криптографічний захист інформації – вид захисту інформації, який реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її спроможності, цілісності, авторства тощо.

Криптографічний ключ – послідовність символів, що забезпечує можливість шифрування – дешифрування.

Логічна бомба – здійснює таємну вставку в програму набору команд, яка спрацьовує лише один раз, але при визначених умовах.

Матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Модель життєвого циклу – концептуальна структура, що містить процеси, дії та завдання, які стосуються розробки, експлуатації та супроводу програмного продукту, і охоплює життєвий цикл системи, починаючи з визначення вимог до неї і закінчуючи припиненням її використання.

Модель загроз для інформації – формалізований опис методів та засобів здійснення загроз для інформації.

Моніторинг – перевірка стану діяльності постачальника та її результатів з боку замовника або третьої сторони.

Надійність – властивість незмінності визначених поведінки та результатів.

Несанкціоновані дії щодо інформації в системі – дії, що проводяться з порушеннями порядку доступу до цієї інформації, встановленого відповідно до законодавства.

Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, знищення, реєстрації, приймання, обробки, передачі, які здійснюються в системі за допомогою технічних та програмних засобів.

Обліковість – властивість, яка гарантує, що за діями об'єкта завжди можна однозначно визначити сам об'єкт.

Оцінювання – систематичне визначення ступеня відповідності об'єкта (сутності) заданим щодо нього критеріям.

Охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошення секретної інформації та втратам її матеріальних носіїв.

Перепустка – картка чи інший вид документа, виданий окремим особам, які працюють або яким в силу інших причин потрібен

санкціонований доступ в організацію або на режимну територію, зону, приміщення з метою спрощення допуску та упізнання осіб, в тому числі документи на транспортні засоби, видані для аналогічних цілей. Перепустками іноді називають посвідчення особи.

Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі внаслідок яких змінюється її зміст.

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробки інформації в системі та правила обробки цієї інформації.

Постачальник – організація, що укладає контракт із замовником на постачання системи, програмного продукту чи програмної послуги згідно з умовами контракту.

> **Примітка 1.** Термін «постачальник» є синонімом підрядника, виробни-ка, продавця або торгівця.
>
> **Примітка 2.** Замовник може визначити частину своєї організації як підрядника.

Програмна послуга – виконання діяльності, роботи або обов'язків, пов'язаних із програмним продуктом, наприклад, таких, як його розробка, супровід та експлуатація.

Програмний модуль – фрагмент коду, що може бути скомпільований окремо.

Програмний продукт – набір програм, процедур та, можливо, пов'язаної з ними документації та даних.

> **Примітка.** Термін «продукт» має інтерпретуватися як частина системи у загальновживаному значенні.

Програмно-апаратні засоби – поєднання апаратного пристрою та машинних інструкцій або комп'ютерних даних, що розміщуються як програмний засіб типу «тільки для читання» в апаратному пристрої. Програмний засіб не можна швидко змінювати програмним шляхом.

Процес – множина взаємопов'язаних дій, що перетворює входи на виходи.

> **Примітка.** Термін «дії» охоплює використання ресурсів [ISO 8402. 1.2.].

Редакція – окрема версія елемента конфігурації, що надається з певною метою (наприклад, тестова редакція).

Режим секретності – встановлений згідно з вимогами Закону України «Про державну таємницю» та інших нормативно-правових актів єдиного порядку забезпечення охорони державної таємниці.

Режимна зона – частина режимної території режимного об'єкта, що визначена для здійснення діяльності, пов'язаної з інформацією, що має гриф з обмеженим доступом.

Режимне приміщення – кімната, декілька кімнат із загальним для них входом (виходом), аудиторія, зал тощо, що визначені для здійснення діяльності, пов'язаної з інформацією з обмеженим доступом.

Розробник – організація, що провадить дії з розробки (включно з аналізом вимог, проектуванням, випробуваннями під час приймання) в межах життєвого циклу програмного забезпечення.

Розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Ризик – ймовірність того, що активи чи група активів уразливі до загрози, що може спричинювати їхнє ушкодження чи знищення.

Система – інтегрована структура, що складається з одного чи більшої кількості процесів, компонентів апаратного забезпечення, компонентів програмного забезпечення, засобів та персоналу, що забезпечує можливість задоволення встановленої потреби або цільової функції.

Стратегія захисту в інформаційних технологіях – правила, директиви і дії з керування захистом, які поширюються на активи, разом із критичною інформацією організації і її систем інформаційних технологій.

Ступінь секретності («особливої важливості», «цілком таємно», «таємно») – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Супроводжувач – організація, що здійснює діяльність із супроводу.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхми передачі, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Тестове покриття – ступінь, до якого набір тестових даних випробовує вимоги до системи або програмного продукту. (Міра, що характеризує здатність тестових даних випробовувати вимоги до системи або програмного продукту).

Тестопридатність – ступінь можливості розробки об’єктивного та здійсненого тесту для встановлення відповідності вимогам.

Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Троянський кінь – здійснює введення до чужої програми таких команд, які дозволяють здійснити інші, не плановані власником програми функції, але одночасно зберегти і попередню працездатність.

Угода – визначення термінів та умов, за яких будуть здійснюватися робочі відносини.

Ураження – результат небажаного інциденту.

Уразливість – сприйнятливість активів чи групи активів до загроз.

Формулювання роботи – документ, що використовується замовником як засіб опису та специфікації завдань, які потрібно виконати згідно з контрактом.

Цілісність – дивись цілісність даних і цілісність системи.

Цілісність даних – дані не можуть бути змінені чи зруйновані несанкціонованим способом.

Цілісність системи – властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних чи випадкових несанкціонованих втручань.

Черв'як інформаційної системи – це спеціальна самостійно розповсюджувальна програма, яка здійснює зміни даних або програм інформаційної системи, без права на це, шляхом передачі, впровадження або розповсюдження за допомогою мережі інформаційних систем.

Навчальне видання

Дудикевич Валерій Богданович
Хорошко Володимир Олексійович
Яремчук Юрій Євгенович

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Редактор В. Дружиніна

Оригінал-макет підготовлено Ю. Яремчуком

Підписано до друку 18.01.2018.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. 18,17.
Наклад 50 (1-й запуск 1-20) пр. Зам. № 2018-026.

Видавець та виготовлювач
інформаційний редакційно-видавничий центр.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
Тел. (0432) 65-18-06.
press.vntu.edu.ua;
E-mail: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.