

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кавун С. В.
Носов В. В.
Манжай О. В.

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник

Частина 2

Харків. Вид. ХНЕУ, 2008

УДК 32.973я73 р.
ББК 004.056(075.8)
К12

Рецензенти: докт. техн. наук, професор кафедри спеціалізованих комп'ютерних систем Української державної академії залізничного транспорту *Лістровий С. В.*; докт. техн. наук, професор кафедри штучного інтелекту Харківського національного університету радіоелектроніки *Філатов В. О.*; докт. техн. наук, професор кафедри інформаційної безпеки Харківського національного університету внутрішніх справ *Захаров І. П.*

Затверджено на засіданні вченої ради Харківського національного економічного університету.

Протокол №6 від 29.12.2008 р.

**Рекомендовано Міністерством освіти і науки України
як навчальний посібник для студентів вищих навчальних закладів
(лист №1.4/18-Г-1068 від 14.05.2008 р.)**

Кавун С. В.

К12 Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с. (Укр. мов.)

Подано теоретичний і практичний матеріал із сучасних проблем інформаційної безпеки, який містить методичні, наукові та практичні рішення з підвищення рівня знань студентів у сфері інформаційної безпеки.

Рекомендовано для аспірантів, науковців і студентів в економічній, технічній та виробничій сферах, а також фахівців із систем інформаційної безпеки, які спеціалізуються у сфері використання й упровадження інформаційних технологій у різних сферах діяльності.

ISBN 978-966-676-281-1
ISBN 978-966-676-323-8

УДК 32.973я73 р.
ББК 004.056(075.8)

© Харківський національний економічний університет, 2008
© Кавун С. В.
Носов В. В.
Манжай О. В.

2008

Вступ

Життя людей за всіх часів було небезпечним. З моменту народження людину підстерігають численні небезпеки її існування й благополуччя: голод, хвороби, хижі тварини, природні стихії, техногенні катастрофи.

Люди не залишалися байдужими до існуючих і можливих небезпек. Потреба в безпеці належить до числа базисних мотиваційних механізмів людської життєдіяльності, як у будь-яких інших живих істот. Еволюція людської історії виявила ряд закономірностей, що характеризують функцію безпеки:

соціальний прогрес не усуває й не скасовує небезпеки існуванню особистості, суспільства, держави;

у міру диференціації суспільства й ускладнення його організації розширюється й спектр соціальних небезпек;

системи безпеки є невід'ємним атрибутом складних соціальних систем і організацій;

недооцінка або ігнорування проблем ІБ на всіх рівнях соціальної організації не тільки обертається тими або іншими втратами, але, в остаточному підсумку, неминуче веде до зниження життєздатності (конкурентоспроможності) і навіть загибелі відповідних її елементів (суб'єктів).

Безпека – складне соціальне явище, багатопланове й багатогранне у своїх структурних складових і проявах, що відбиває суперечливі інтереси у відносинах різних соціальних суб'єктів. Нерідко одні з них прагнуть забезпечити свою безпеку за рахунок інших або не зважають на інтереси безпеки інших людей, груп, народів. Мислять застарілими категоріями й егоїстичними цінностями, які ігнорують ту основну закономірність, що безпека в епоху наростаючої глобалізації – неподільна. Звідси – обумовленість проблематики безпеки суб'єктивними позиціями, неоднозначними оцінками, фрагментарними судженнями. У методологічному плані важливо мати цілісне подання про безпеку як соціальному явищі.

Буквально дослівно безпека означає відсутність небезпеки. Подібне подання ще називають безпекою у вузькому значенні цього слова. У практичному плані таке значення має досить умовний характер, оскільки в реальному житті ситуації з повною відсутністю загроз зустрічаються досить рідко.

З погляду заходів протидії загрозам багатьом соціальним об'єктам безпека демонструє складний, багатокomпонентний склад і припускає системну організацію. Так само характеризується вона в Концепції національної безпеки: "Основу системи забезпечення національної безпеки становлять органи, сили й засоби забезпечення національної безпеки, що здійснюють заходи політичного, правового, організаційного, економічного, військового й іншого характеру, спрямовані на забезпечення безпеки особистості, суспільства й держави". Немає жодної конкретизації цих органів, сил і засобів, а також ув'язування їхніх функцій із загрозами національної безпеки, синхронізації з напрямками й завданнями забезпечення певних видів безпеки. Якщо з військовими загрозами більш менш все зрозуміло, і їх протидії служать Збройні сили й інші війська, сили й засоби військової організації держави, то щодо інших загроз такої зрозумілості немає. Багато що треба домислювати, припускати, вгадувати. Які сили й засоби, наприклад, задіюються державою й суспільством для забезпечення економічної безпеки країни й вітчизняного бізнесу?

Системи безпеки створюються й у рамках окремих організацій, підприємств, фірм. Система безпеки фірми становить, як вважають деякі автори, "організовану сукупність спеціальних структур, засобів, методів і заходів, що забезпечують безпеку підприємницької діяльності від внутрішніх і зовнішніх загроз". На погляд авторів цього підручника, із системи не можна виключати керівників фірми й персонал, що реалізує функції, повноваження й обов'язки забезпечення безпеки.

У частині I наведені матеріали першого модуля "Основи ІБ", що включає тему 1 "Загальні принципи безпеки інформаційних технологій", тему 2 "Канали витоку інформації", тему 3 "Організація інформаційної безпеки на підприємстві".

Частина II навчального посібника містить матеріали другого модуля "Особливості застосування ІБ у бізнесі" з теми 4 "Організація інформаційної безпеки комп'ютерних мереж" та теми 5 "Правові основи ІБ" і є логічним завершенням всього матеріалу з дисципліни "Інформаційна безпека".

4. ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ ✓

4.1. Стандарти ІЕБ ✓

- 4.1.1. Основні положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку) ◆
- 4.1.2. Основні положення "Загальних критеріїв" ◆
- 4.1.3. Базова технічна модель ІТ-безпеки у відповідності з NIST Special Publication 800-33 ◆
- 4.1.4. Оцінка безпеки ІС ◆
- 4.1.5. Стандарт ISO ◆
- 4.1.5. Механізми безпеки ◆
- 4.1.6. Стандарти ЕСМА ◆
- 4.1.7. Система стандартів Міністерства оборони США в області комп'ютерної безпеки ◆

4.2. Ідентифікація та автентифікація КС ✓

4.3. Методи та засоби ІЕБ в КС ✓

- 4.3.1. Криптографічні методи захисту інформації ◆
- 4.3.2. Етапи розробки систем захисту ◆
- 4.3.3. Критерії і особливості проектування оптимальної СЗІ ◆
- 4.3.4. Технічне завдання на розробку СЗІ і план захисту інформації ◆
- 4.3.5. Визначення якості реалізованої системи захисту ◆

Модуль 2. Особливості застосування ІБ у бізнесі

4. Організація інформаційної безпеки комп'ютерних мереж

4.1. Стандарти ІЕБ

В Україні нормативно-правову базу (дод. 3) щодо захисту інформації в КС від несанкціонованого доступу (НСД) складають відкриті документи [14 – 16, 23 – 30], які, на думку вітчизняних фахівців у цій сфері [8, 13, 17, 27, 33, 44, 53, 58], повною мірою не відображають сучасну трансформацію поглядів на процеси обробки інформації та новітні підходи до вирішення проблеми забезпечення ІБ. Новий погляд на проб-лему безпеки інформаційних технологій був закріплений у міжнародному стандарті ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій" [64 – 65]. Для розуміння основних положень цих документів необхідно розглянути елементи теорії захисту інформації в КС.

Розглядаючи питання безпеки інформації в КС, перш за все, вводять абстрактну модель комп'ютерної системи (дод. А, Б, Д, Е), і далі говорять про наявність деяких "бажаних" станів даних систем (дод. В).

Ці бажані стани описують (у термінах моделі власне комп'ютерної системи) ступінь "захищеності" системи. Властивість "захищеності" принципово не відрізняється від будь-яких інших властивостей технічної системи, наприклад, описуваних поняттям "надійної роботи", і є для системи зовнішньою, апіорно заданою.

Поняття "захищеність" взаємопов'язане з поняттями "джерело загрози" (позначення зовнішньої причини для виведення системи із стану "захищеності"), "загроза" (поняття, що знеособлює причину виведення системи із захищеного стану через дії джерела загрози) і "вразливість" (позначення властивості елемента системи, за допомогою якого реалізується загроза).

Інтегральною характеристикою, що описує властивості системи, яка потребує захисту, є ПБ – якісний (або якісно-кількісний) опис властивостей захищеності, виражений у термінах, що описують систему.

У теорії комп'ютерної безпеки практично завжди розглядається модель довільної КС у вигляді кінцевої множини елементів. Існує два підходи до розподілу зазначеної множини:

1. На дві підмножини:

множина об'єктів;

множина суб'єктів (дод. Ж).

Даний розподіл заснований на властивості елемента "бути активним" або "одержувати керування" (застосовуються також терміни "використовувати ресурси" або "користуватися обчислювальною потужністю"). Воно історично склалося на основі моделі обчислювальної системи, що належить фон Нейману, згідно з якою послідовність виконуваних інструкцій (програма, відповідна поняттю "суб'єкт") знаходиться в єдиному середовищі з даними (відповідними поняттю "об'єкт").

Властивості суб'єктів:

людина-користувач сприймає об'єкти та одержує інформацію про стан КС через суб'єкти, якими вона керує і які відображають інформацію в придатному для сприйняття людиною вигляді;

загрози компонентам КС виходять від суб'єктів як активної компоненти інформації, що породжує потоки і змінює стан об'єктів у КС;

суб'єкти можуть впливати один на одного через змінювані ними об'єкти, пов'язані з іншими суб'єктами, породжуючи зрештою в системі суб'єкти (або стани системи), які становлять загрозу для безпеки інформації або для працездатності самої системи.

2. На дві підмножини:

множина пасивних об'єктів, над якою виконуються операції;

множина активних об'єктів, які виконують або ініціюють ці операції:

об'єкти-користувачі;

об'єкти-процеси.

Термін "суб'єкт", що вживається відповідно до першого підходу, є суперпозицією об'єкта-користувача і об'єкта-процесу другого підходу.

Згідно з другим підходом, усі об'єкти можуть знаходитися в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Наприклад, пасивний об'єкт переходить у стан об'єкта-користувача, коли фізична особа "входить" у систему. Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою отримання певного виду доступу) призводить до появи потоку інформації між об'єктами та/або зміни стану системи.

Цей другий підхід використовується у вітчизняних документах із захисту інформації в КС від НСД.

В обох підходах ПБ пов'язана з поняттям "доступ". *Доступ* – це категорія, що описує процес виконання операцій суб'єктів над об'єктами (об'єктів-користувачів і об'єктів-процесів над пасивними об'єктами). Наприклад, ПБ для суб'єктно-об'єктної моделі включає опис:

множини можливих операцій над об'єктами;

для кожної пари "суб'єкт-об'єкт" призначення множини дозволених операцій, що є підмножиною всієї безлічі можливих операцій. Операції пов'язані з цільовою функцією системи, що захищається (тобто з категорією, що описує призначення системи й вирішувані завдання).

ПБ описує в загальному випадку нестационарний стан захищеності. Система, що захищається, може змінюватися, доповнюватися новими компонентами (суб'єктами, об'єктами, операціями суб'єктів над об'єктами), відповідно, і ПБ повинна бути підтримана в часі, що досягається *керуванням безпекою*.

Не стаціонарність КС, що захищається, а також питання реалізації ПБ в конкретних конструкціях системи, яка захищається, зумовлюють необхідність розгляду завдання *гарантування заданої ПБ*.

Резюмуючи, можна сказати, що теорія комп'ютерної безпеки вирішує чотири класи взаємопов'язаних завдання [45]:

1. Формулювання і вивчення ПБ.
2. Реалізація політик безпеки.
3. Гарантування заданої ПБ.
4. Керування безпекою.

Типовий життєвий цикл КС складається з наступних стадій:

1. Проектування КС і проектування ПБ.
2. Моделювання ПБ і аналіз коректності ПБ, що включає встановлення ступеня її адекватності цільовій функції КС.
3. Реалізація ПБ і механізмів її гарантування, а також процедур і механізмів керування безпекою.
4. Експлуатація захищеної системи.

З метою формування єдиного та формалізованого підходу до захисту інформації в КС, як було вже зазначено, були розроблені стандарти безпеки або критерії оцінки захищеності, які включають якісні та кількісні показники захищеності.

Стандарти безпеки ефективно сприяють вирішенню наступних проблем у сфері ІБ:

обґрунтоване формування цілей і структуризація завдань у процесі проектування захищених інформаційних систем;

забезпечення об'єктивності оцінок захищеності ІС і технологій;

створення методологічних і методичних підстав для взаємодії між основними учасниками сфери ІБ: виробниками, споживачами, експертами (рис. 4.1);

формування базису для формалізації описів цілей, завдань, вимог до захищених систем і самих систем у сфері захищених інформаційних технологій;

створення технологій кваліфікаційного аналізу і синтезу захищених інформаційних систем (дод. І);

розробка технологій перевірки захищеності систем, а також атестації та сертифікації як окремих елементів систем, так і захищених систем у цілому (дод. К).



Рис. 4.1. Необхідність взаємодії між основними учасниками у сфері ТЗІ

На сьогодні існує цілий ряд стандартів безпеки. У цьому напрямку ведуться інтенсивні дослідження, тому існуючі стандарти поповнюються й модифікуються, а також з'являються цілком нові стандарти, які враховують досвід раніше створених. Доречно також зазначити, що такого роду стандарти наповнюються великою кількістю окремих методик. Перелік найбільш відомих стандартів наведено у табл. 4.1.

Перелік найбільш відомих стандартів

Найменування стандарту	Позначення, країна	Коротка характеристика
Критерії безпеки КС Міністерства оборони США ("Оранжева книга")	TCSEC, США	Були розроблені Міністерством оборони США в 1983 р. з метою визначення вимог безпеки для КС, що висуваються до апаратного, програмного й спеціального забезпечення, а також з метою вироблення методології аналізу ПБ для інформаційних систем військового призначення. Публікація "Оранжевої книги" стала важливим етапом у роботах за стандартами безпеки, оскільки дала основу для нових розробок
Європейські критерії безпеки інформаційних технологій ("Європейські критерії")	ITSEC, Великобританія, Франція, Нідерланди, Німеччина	Були розроблені країнами Європи вслід за виходом "Оранжевої книги". У цих критеріях усі засоби захисту інформації розглядаються на трьох рівнях: з погляду цілей, з погляду функцій захисту і з погляду механізмів, що реалізують захист
ГОСТ Р ИСО/МЭК 15408-2002 (імплементовані "Загальні критерії")	Росія	Починаючи з 1992 р. було опубліковано ряд документів з питань захисту інформації від несанкціонованого доступу. Спочатку була розроблена "Концепція захисту засобів обчислювальної техніки від НСД до інформації", що стала ідейною основою для розробки решти документів

Найменування стандарту	Позначення, країна	Коротка характеристика
Федеральні критерії безпеки інформаційних технологій ("Федеральні критерії")	FSTITS, США	Розроблялися як складова національного стандарту з обробки інформації. Документ став узагальненням досліджень 80–90-х рр. у сфері ІБ. Ці критерії стали базою для розробки й сертифікації компонентів інформаційних технологій з погляду підтримання безпеки
Канадські критерії безпеки комп'ютерних систем ("Канадські критерії")	CSSCCSE, Канада	"Канадські критерії" розроблялися як основа для оцінки ефективності засобів підтримання безпеки КС з метою вироблення шкали критеріїв оцінки безпеки систем, створення основи для розробки специфікацій безпечних КС, розробки пропозицій із стандартизації опису характеристик безпечних систем
Загальні критерії безпеки інформаційних технологій ("Загальні критерії", "Єдині критерії")	CCITSE, ISO/IEC 15408, США, Великобританія, Франція, Канада, Нідерланди	Роботи за цим проектом були розпочаті в 1993 р. Основною метою було усунення концептуальних і технічних відмінностей між Європейськими, Федеральними і Канадськими критеріями. Загальні критерії розроблялися з орієнтацією на інтереси виробників, споживачів і експертів стосовно кваліфікації рівня безпеки

Найменування стандарту	Позначення, країна	Коротка характеристика
Критерії оцінки захищеності інформації в КС від НСД ("Критерії ДСТС ЗІ СБУ" (Держспецзв'язку))	Україна	Були введені в 1999 р. Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем і захисту інформації СБУ як національний стандарт. За своєю структурою нагадують "Канадські критерії"

Далі розкриємо основні та істотні в контексті даних питань, положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку) і "Загальних критеріїв".

4.1.1. Основні положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку)

"Критерії ДСТС ЗІ СБУ" (Держспецзв'язку) розглядають чотири типи загроз:

- загрози конфіденційності інформації;
- загрози цілісності інформації;
- загрози порушення працездатності ІС;
- загрози аудиту (спостереженості) системи.

У стандарті використовується поняття об'єкта інформаційного обміну, що відрізняється від інших. Сутність КС розглядається як сукупність об'єктів, а їх взаємодія описується трійкою:

- об'єкт-користувач;
- об'єкт-процес, що діє від імені користувача;
- об'єкт як пасивний елемент.

Такий підхід дозволяє за ситуації, коли один користувач запускає багато процесів, використовувати для опису цієї ситуації один об'єкт-користувач і безліч асоційованих з ним об'єктів-процесів. При цьому ПБ розрахована на одного користувача, що здійснює доступ до об'єктів за допомогою декількох процесів.

Загальна оцінка рівня безпеки системи складається з потужності функціональних вимог комплексу засобів захисту (КЗЗ) і рівня вимог адекватності їх реалізації (рис. 4.2).



Рис. 4.2. Складові загальної оцінки рівня безпеки системи

Для забезпечення максимального ступеня абстрагованості та інваріантності щодо ПБ і методів її реалізації у стандарті використовується поняття "Атрибути доступу", що позначає сукупність атрибутів безпеки, які асоціюються з користувачем, процесом або об'єктом. Як атрибут доступу користувача, процесу або об'єкта можуть виступати відповідний унікальний ідентифікатор, мітка безпеки або цілісності, криптографічний ключ, таблиця прав доступу або інші атрибути відповідно до реалізованої в комп'ютерній системі ПБ.

Функціональні можливості використовуваних засобів захисту характеризуються окремими показниками забезпечуваного рівня безпеки стосовно однієї з чотирьох загроз. Рівень адекватності реалізації (гарантій) ПБ має один узагальнений параметр (Г-1...Г-7).

Стисло розглянемо ранжування вимог "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку).

На рис. 4.3 показані окремі показники критеріїв конфіденційності.

Критерії конфіденційності

Рівень	Найменування	Пов'яз. рів.
КД-1	Мінімальна довірча конфіденційність	НИ-1
КД-2	Базова довірча конфіденційність	
КД-3	Повна довірча конфіденційність	
КД-4	Абсолютна довірча конфіденційність	
КА-1	Мінімальна адміністративна конфіденційність	НО-1,НИ-1
КА-2	Базова адміністративна конфіденційність	
КА-3	Повна адміністративна конфіденційність	
КА-4	Абсолютна адміністративна конфіденційність	
КК-1	Виявлення прихованих каналів	КО-1, Г-3
КК-2	Контроль прихованих каналів	КО-1, НР-1,Г-3
КК-3	Перекриття прихованих каналів	КО-1, Г-3
КВ-1	Мінімальна конфіденційність при обміні	-
КВ-2	Базова конфіденційність при обміні	НО-1
КВ-3	Повна конфіденційність при обміні	НО-1, НВ-1
КВ-4	Абсолютна конфіденційність при обміні	НО-1, НВ-1, НР-1, Г-3
КО-1	Повторне використання об'єктів	-

Рис. 4.3. Показники критеріїв конфіденційності

Особливістю функціональних критеріїв є те, що деякі їх рівні залежать від інших, і для того, щоб задовольнити вимоги цих рівнів, необхідно дотримуватись не тільки наведених у них вимог, але й вимог, пов'язаних розділів інших функціональних критеріїв і критеріїв гарантій у рамках зазначених рівнів.

Критерії конфіденційності регламентують захист ресурсів КС від несанкціонованого доступу шляхом реалізації відповідних послуг. Стисло охарактеризуємо ці послуги.

Довірча конфіденційність (КД-1...КД-4) дозволяє авторизованим користувачам керувати потоками інформації від об'єктів, що належать їх доменам, до інших користувачів системи. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибіркової керування.

Адміністративна конфіденційність (НО-1...НО-4) дозволяє адміністраторам або спеціально авторизованим користувачам керувати потоками інформації від об'єктів до користувачів системи. Ранжування

вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибіркової керування.

Повторне використання об'єктів (КО-1) дозволяє зробити безпечним використання розділюваних об'єктів, одночасно або послідовно доступних декільком процесам. Контроль повинен запобігати збереженню в розділюваних об'єктах залишкової інформації після завершення їх використання одним процесом і перед наданням доступу до них іншому процесу.

Аналіз прихованих каналів (КК-1...КК-3) дозволяє виявити й виключити присутність у системі потоків інформації, які не можуть контролюватися іншими засобами захисту. Ранжування вимог проводиться залежно від ступеня аналізу наявності прихованих каналів і можливостей щодо їх контролю й перекриття.

Конфіденційність при обміні (КВ-1...КВ-4) дозволяє забезпечити захист від несанкціонованого ознайомлення з об'єктами при їх переміщенні через незахищене середовище. Ранжування вимог проводиться залежно від ступеня захисту й вибіркової керування.

Критерії цілісності визначають можливості комп'ютерної системи щодо забезпечення власної цілісності та цілісності оброблюваної інформації, що в ній зберігається. Критерії цілісності передбачають наступні послуги: довірча та адміністративна цілісність, відкат, цілісність при обміні. На рис. 4.4 показані окремі показники критеріїв цілісності.

Критерії цілісності			
Рівень	Найменування	Пов'яз. рів.	
ЦД-1	Мінімальна довірча цілісність	НИ-1	Розділ ДОВІРЧА ЦІЛІСНІСТЬ АДМІНІСТ- РАТИВНА ЦІЛІСНІСТЬ ПРИ ОБМІНІ ВІДКАТ
ЦД-2	Базова довірча цілісність		
ЦД-3	Повна довірча цілісність		
ЦД-4	Абсолютна довірча цілісність		
ЦА-1	Мінімальна адміністративна цілісність	НО-1,НИ-1	
ЦА-2	Базова адміністративна цілісність		
ЦА-3	Повна адміністративна цілісність		
ЦА-4	Абсолютна адміністративна цілісність		
ЦВ-1	Мінімальна цілісність при обміні	-	
ЦВ-2	Базова цілісність при обміні	НО-1	
ЦВ-3	Повна цілісність при обміні	НО-1, НВ-1	
ЦО-1	Обмежений відкат	НИ-1	
ЦО-2	Повний відкат		

Рис. 4.4. Показники критеріїв цілісності

Довірча цілісність (ЦД-1...ЦД-4) дозволяє користувачу керувати потоками інформації від інших користувачів до об'єктів, що належать його домену. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибіркості керування.

Адміністративна конфіденційність (ЦА-1...ЦА-4) дозволяє адміністраторам або спеціально авторизованим користувачам керувати потоками інформації від користувачів системи до об'єктів. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибіркості керування.

Відкат (ЦО-1...ЦО-2) забезпечує можливість відміни послідовності здійснених дій і повернення об'єктів комп'ютерної системи до початкового стану. Ранжування критеріїв цього розділу проводиться залежно від множини операцій, які можуть бути відмінені.

Цілісність при обміні (ЦВ-1...ЦВ-3) дозволяє забезпечити захист від несанкціонованої модифікації об'єктів під час їх переміщення через незахищене середовище. Ранжування вимог проводиться залежно від ступеня захисту і вибіркості керування.

Критерії доступності регламентують роботу засобів, що забезпечують доступність комп'ютерної системи в цілому, окремих її функцій або ресурсів протягом певного інтервалу часу для авторизованих користувачів, а також гарантувати функціонування КС у разі відмови її окремих компонентів. Як заходи забезпечення доступності розглядаються контроль щодо використання ресурсів системи, забезпечення стійкості системи до відмов, забезпечення живучості й відновлення системи в умовах виходу з ладу її компонентів. На рис. 4.5 показані окремі показники критеріїв доступності.

Критерії доступності

Рівень	Найменування	Пов'яз. рів.
ДР-1	Квоти	НО-1
ДР-2	Припинення захоплення ресурсів	
ДР-3	Пріоритетність використання ресурсів	
ДС-1	Стійкість при обмежених відмовах	НО-1
ДС-2	Стійкість з погіршенням характеристик обслуговування	
ДС-3	Стійкість без погіршення характеристик обслуговування	
ДЗ-1	Модернізація	НО-1
ДЗ-2	Обмежена гаряча заміна	НО-1, ДС-1
ДЗ-3	Гаряча заміна будь-якого компоненту	
ДВ-1	Ручне відновлення	НО-1
ДВ-2	Автоматизоване відновлення	
ДВ-3	Вибіркове відновлення	

**Розділ
Викорис-
тання
ресурсів**

**Стій-
кість до
відмов**

**Гаряча
заміна**

**Віднов-
лення
після збоїв**

Рис. 4.5. Показники критеріїв доступності

Використання ресурсів (ДР-1...ДР-3) дозволяє користувачам керувати використанням КС. Вимоги ранжирують залежно від контрольованих ресурсів і можливостей керувати ними.

Стійкість до відмов (ДС-1...ДС-3) дозволяє забезпечувати працездатність системи і доступність її ресурсів у разі виходу з ладу окремих компонентів. Вимоги ранжирують залежно від кількості несправностей, за наявності яких зберігається працездатність системи, і від множини ресурсів, доступних в умовах виходу з ладу компонентів системи.

Гаряча заміна (ДЗ-1...ДЗ-3) характеризує можливості зберігати працездатність і доступність ресурсів системи у процесі заміни її компонентів, що відмовили. Вимоги ранжирують залежно від повноти реалізації.

Відновлення після збоїв (ДВ-1...ДВ-3) дозволяє повернути КС в безпечний стан після відмов або збоїв. Вимоги ранжирують залежно від ступеня автоматизації процесу відновлення.

Критерії спостереженості регламентують роботу засобів, що дозволяють встановити відповідальність користувачів за події в системі. Спостереженість забезпечується наступними засобами (послугами): реєстрація (аудит); ідентифікація й автентифікація; достовірний канал; розмежування обов'язків; цілісність КЗЗ; самотестування; ідентифікація і автентифікація при обміні; автентифікація відправника; автентифікація

одержувача. На рис. 4.6 відображені окремі показники критеріїв спостереженості.

Критерії спостереженості			Розділ
Рівень	Найменування	Пов'яз. рів.	
НР-1	Зовнішній аналіз	НИ-1	Реєстрація
НР-2	Захищений журнал	НИ-1, НО-1	
НР-3	Сигналізація про небезпеку		
НР-4	Детальна реєстрація		
НР-5	Аналіз у реальному часі		
НИ-1	Зовнішня ідентифікація та автентифікація	-	Ідентифікація і автентифікація
НИ-2	Одиночна ідентифікація та автентифікація	НК-1	
НИ-3	Множинна ідентифікація та автентифікація		
НК-1	Однонаправлений достовірний канал	-	Достовірний канал
НК-2	Двонаправлений достовірний канал	-	
НО-1	Виділення адміністратора	НИ-1	Розмежування обов'язків
НО-2	Розмежування обов'язків адміністраторів		
НО-3	Розмежування обов'язків на підставі привілеїв		
НЦ-1	КСЗ з контролем цілісності	НР-1, НО-1	Цілісність КСЗ
НЦ-2	КСЗ з гарантованою цілісністю	-	
НЦ-3	КСЗ з функціями диспетчера доступу		
НТ-1	Самотестування за запитом	НО-1	Самотестування
НТ-2	Самотестування при старті		
НТ-3	Самотестування у реальному часі		
НВ-1	Автентифікація за запитом	-	Ідентифікація і автентифікація при обміні
НВ-2	Автентифікація джерела даних		
НВ-3	Автентифікація з підтвердженням		
НА-1	Базова автентифікація відправника	НИ-1	Автентифікація відправника
НА-2	Автентифікація відправника з підтвердженням		
НП-1	Базова автентифікація одержувача	НИ-1	Автентифікація одержувача
НП-2	Автентифікація одержувача з підтвердженням		

Рис. 4.6. Показники критеріїв спостереженості

Реєстрація (НР-1...НР-5) дозволяє виявити потенційно небезпечні дії користувачів. Вимоги ранжирують залежно від ступеня їх деталізації, складності процесу аналізу подій і можливості виявляти потенційні загрози безпеки.

Ідентифікація та автентифікація (НИ-1...НИ-3) дозволяє КЗЗ перевірити достовірність користувачів, що намагаються отримати доступ до системи та її ресурсів. Ранжування вимог здійснюється залежно від функціональності можливостей її механізмів ідентифікації й автентифікації.

Достовірний канал (НК-1...НК-3) забезпечує можливість безпосередньої конфіденційної взаємодії між користувачем і КЗЗ. Вимоги ранжируються залежно від гнучкості механізмів, що забезпечують пряму взаємодію з КЗЗ, і можливостями користувача ініціювати взаємодію з КЗЗ.

Розмежування обов'язків (НО-1...НО-3) дозволяє зменшити потенційний збиток від дій користувачів (з наміром і без) і обмежити авторитарність керування. Вимоги ранжирують залежно від вибіркової керування можливостями користувачів і адміністраторів.

Цілісність комплексу засобів захисту (НЦ-1...НЦ-3) дозволяє визначати міру здатності КЗЗ захищати себе і гарантувати свою здатність керувати захищеними об'єктами. Вимоги ранжирують залежно від повноти вимог до політики цілісності КЗЗ, функціональності КЗЗ і ступеня контролю на доступ.

Самотестування (НТ-1...НТ-3) дозволяє перевірити КЗЗ і гарантувати коректність функціонування і цілісність певної сукупності функцій КС. Вимоги ранжируються залежно від можливості виконання тестів у процесі запуску або штатного функціонування.

Ідентифікація і автентифікація при обміні (НВ-1...НВ-3) дозволяє забезпечити взаємну достовірність між двома КЗЗ перед їх взаємодією. Вимоги ранжируються залежно від повноти реалізації.

Автентифікація відправника (НА-1,НА-2) дозволяє забезпечити неможливість відмови певного користувача від факту отримання об'єкта. Вимоги ранжируються залежно від можливості підтвердження результатів перевірки незалежною третьою стороною.

Автентифікація одержувача (НП-1,НП-2) дозволяє забезпечити неможливість відмови користувача від авторства створення й відправки об'єкта. Вимоги ранжируються залежно від можливості підтвердження результатів перевірки незалежною третьою стороною.

Критерії гарантій регламентують вимоги до процесу розробки та реалізації КЗЗ, що дозволяють визначити адекватність реалізації ПБ і відображають ступінь довіри до комплексу засобів захисту. Критерії гарантій охоплюють усі стадії та аспекти створення й експлуатації системи і включають розділи, що належать до:

- 1) архітектури КЗЗ;
- 2) середовища розробки:
процесу розробки;

- керування конфігурацією;
- 3) послідовності розробки:
 - розробки функціональних специфікацій:
 - ПБ;
 - моделі ПБ;
 - проекту архітектури;
 - детального проекту;
 - його реалізації;
- 4) середовища функціонування;
- 5) документації:
 - керівництва з безпеки для користувача;
 - керівництва адміністратора безпеки;
- 6) випробування комплексу засобів захисту.

Вимоги до *архітектури* забезпечують гарантії спроможності КЗЗ реалізувати ПБ.

Вимоги до *середовища розробки* забезпечують гарантії повної керованості розробником процесами розробки й супроводу оцінюваної КС.

Вимоги до *послідовності розробки* (процесу проектування) забезпечують гарантії існування точного опису КС на кожній стадії проектування й точної відповідності реалізації КС з початковими вимогами до ПБ.

Вимоги до *середовища функціонування* забезпечують гарантії відсутності несанкціонованих модифікацій КС під час постачання замовнику, а також інсталяції та ініціалізації замовником КС так, як це передбачається розробником.

Вимоги до *документації* визначають обов'язкову наявність у вигляді окремих документів або розділів інших документів, опис послуг безпеки (функціональності), що реалізуються КЗЗ, керівництво адміністратора щодо послуг безпеки, керівництво користувача щодо послуг безпеки.

Вимоги до *випробування КЗЗ* регламентують порядок аргументування, доказу й перевірки стійкості КЗЗ до атак.

Передбачено сім рівнів гарантій (Г1...Г7). Із зростанням номера рівня відбувається конкретизація, доповнення й посилення вимог без зміни їх структури. Рівень гарантій (адекватності) реалізації ПБ характеризує якість усієї системи в цілому.

Порядок оцінки КС на предмет відповідності даним критеріям визначається відповідними нормативними документами Держспецзв'язку (ДСТС ЗІ СБУ). Експертна комісія, яка проводить оцінку КС, визначає кількість і рівень реалізованих у КС послуг безпеки і ступінь дотримання вимог гарантій.

Результатом оцінки є рейтинг (функціональний профіль захищеності), який складається з ряду (переліку) літерно-числових комбінацій, що позначають рівні реалізованих послуг, у поєднанні з рівнем гарантій.

Нормативні документи Держспецзв'язку (ДСТС ЗІ СБУ) [24] вводять *функціональні профілі захищеності*, що є переліком мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи КС, щоб задовольняти певні вимоги до захищеності оброблюваної інформації. *Стандартні функціональні профілі* формуються на основі існуючих вимог до захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти загрозам і забезпечити виконання цих вимог.

Опис профіля складається з трьох частин:

- 1) літерно-числового ідентифікатора;
- 2) знака рівності;
- 3) переліку рівнів послуг у фігурних дужках.

Ідентифікатор у свою чергу включає:

- позначення класу КС (1, 2 або 3);
- літерну частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д);
- номер профілю;
- необов'язкове літерне позначення версії.

Усі частини ідентифікатора відокремлюються одна від одної крапкою.

Наприклад, 2.К.4 — функціональний профіль номер чотири, що відображає вимоги до КС класу 2, основна вимога щодо захисту оброблюваної інформації – забезпечення конфіденційності.

Наведемо приклад стандартного профілю захищеності КЗЗ обчислювальної системи у складі КС класу 3 з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації:

3.КЦД.1 = { КД-2, КО-1, КВ-1,

ЦД-1, ЦО-1, ЦВ-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,
ЦД-1, ЦА-2, ЦО-1, ЦВ-2,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

3.КЦД.3 = { КД-2, КА-2, КО-1, КК-1, КВ-3,
ЦД-1, ЦА-3, ЦО-2, ЦВ-2,
ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2 }

3.КЦД.4 = { КД-3, КА-3, КО-1, КК-1, КВ-3,
ЦД-1, ЦА-3, ЦО-2, ЦВ-2,
ДР-3, ДС-2, ДЗ-2, ДВ-2,
НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }

3.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, КВ-4,
ЦД-4, ЦА-4, ЦО-2, ЦВ-3,
ДР-3, ДС-3, ДЗ-3, ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НА-1, НП-1, НВ-2, НА-1, НП-1 }

Відповідно, нормативні документи Держспецзв'язку (ДСТС ЗІ СБУ) [24; 28 – 30] визначають вимоги до профілів захищеності КЗЗ, що входять до складу КС різних класів і призначень (наприклад, КС, які призначені для автоматизації банківської діяльності або органів державної влади).

4.1.2. Основні положення "Загальних критеріїв"

"Загальні критерії" як об'єкт безпеки розглядають не КС, а ІТ-систему і ІТ-продукт, які є похідними від поняття "інформаційна технологія" (ІТ). Під інформаційною технологією розуміють цілеспрямовану організовану сукупність інформаційних процесів, реалізованих з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування [46]. Відповідно розглядають і безпеку інформаційних технологій (ІТ-безпека).

У "Загальних критеріях" ключовими поняттями є: Protection Profile – *профіль захисту*, Security Target – *мета безпеки або проект захисту* і

Target of Evaluation – *об'єкт оцінки*. Під об'єктом оцінки розуміється ІТ-продукт.

Профіль захисту – це незалежна від реалізації структура для визначення й обґрунтування вимог безпеки, що є незмінним і повним набором завдань безпеки, функціональних вимог і вимог адекватності. Профіль захисту розробляється для нових продуктів і систем.

Проект захисту – це структура, що залежить від реалізації і є повним набором завдань безпеки, функціональних вимог і вимог адекватності, узагальнених специфікацій і обґрунтувань. Вимоги безпеки, що містяться у проекті захисту, визначаються за допомогою посилань на відповідні профілі захисту і вимоги "Загальних критеріїв". На основі проекту захисту здійснюється оцінка конкретного ІТ-продукту.

"Загальні критерії" є стандартом, що визначає структуру й зміст двох документів – профілю захисту і проекту захисту, – і містять енциклопедію вимог, які обираються і упаковуються у профіль захисту і проект захисту. З одного боку, профіль захисту може розглядатися як детальне визначення вимог безпеки і вимог адекватності, які споживачі хочуть бачити в ІТ-продукті. З іншого – проект захисту може розглядатися як опис у термінах вимог безпеки того, що постачальник пропонує в ІТ-продукті (рис. 4.7).

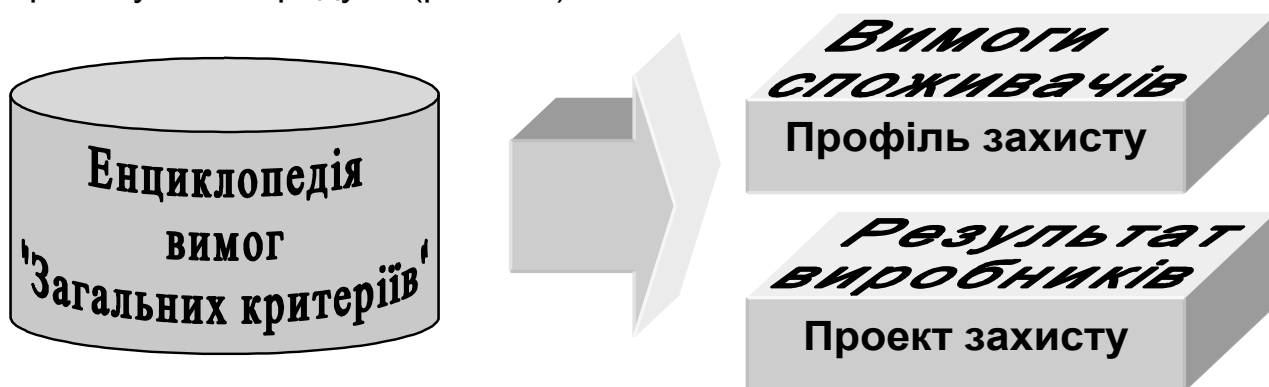


Рис. 4.7. Роль "Загальних критеріїв" у виробленні профілю і проекту захисту

У проекті захисту передбачається можливість включення функціональних вимог і вимог адекватності "Загальних критеріїв", що не містяться у вимогах.

Кваліфікаційний аналіз ІТ-продукту може проводитися паралельно з його розробкою або після її завершення. Для оцінки ІТ-продукту необхідно мати:

проект захисту, що описує функції безпеки ІТ-продукту і вимог безпеки в термінах прийнятого профілю захисту;
сукупність необхідних відомостей про ІТ-продукт;
власне ІТ-продукт, предмет оцінки безпеки.

Процес кваліфікаційного аналізу включає три стадії.

1. Аналіз профілю захисту на предмет його повноти, несуперечності, можливості його реалізації та використання як сукупності вимог для аналізованого продукту.

2. Аналіз проекту захисту на предмет його відповідності вимогам профілю захисту, а також повноти, несуперечності, можливості його реалізації й використання як опису ІТ-продукту.

3. Аналіз ІТ-продукту на предмет відповідності проекту захисту.

Схему оцінки безпеки ІТ-продукту на основі "Загальних критеріїв" можна подати у вигляді, поданому на рис. 4.8.

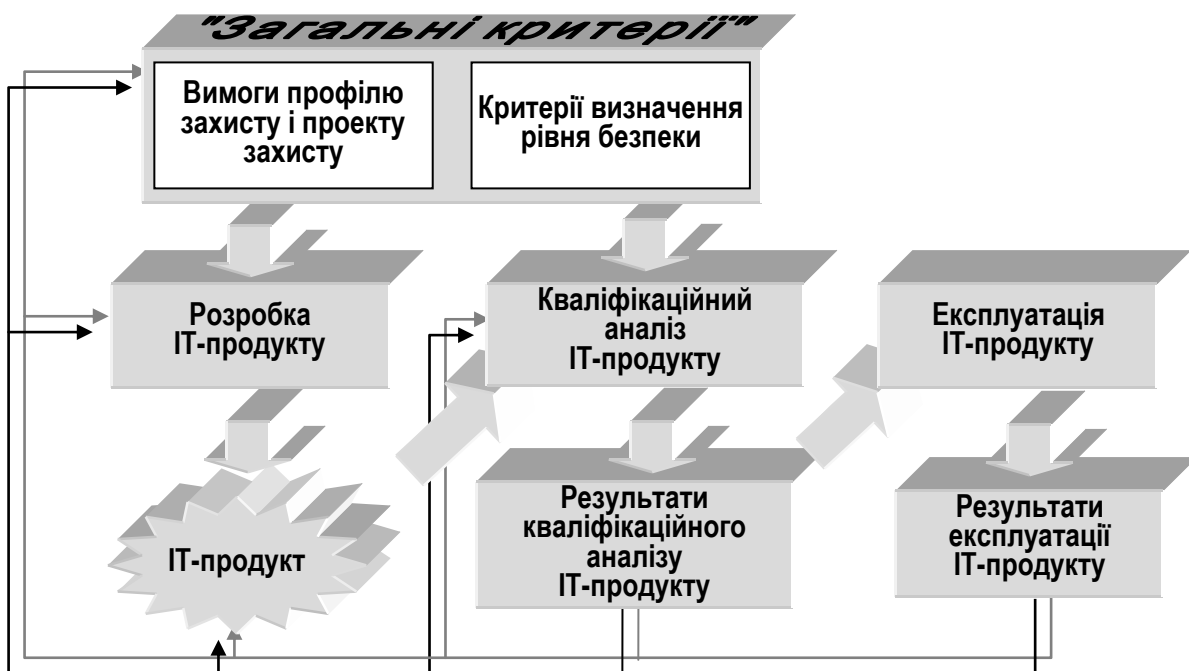


Рис. 4.8. Схема оцінки безпеки ІТ-продукту на основі "Загальних критеріїв"

Результатом кваліфікаційного аналізу є висновок про те, що проаналізований ІТ-продукт відповідає представленому проекту захисту. Висновок складається з декількох звітів, які відрізняються рівнем деталізації і врахування думок експертів щодо кваліфікації ІТ-продукту на підставі "Загальних критеріїв". Ці звіти можуть бути включені в каталог оцінених виробів, щоб вони стали доступними широкому колу виробників і споживачів ІТ-продукту.

Застосування передбаченої "Загальними критеріями" технології сертифікації призводить до підвищення якості роботи виробників у процесі проектування й розробки ІТ-продуктів, а також до підвищення безпеки їх експлуатації. Окрім цього, у продуктах, що пройшли кваліфікацію рівня безпеки, зменшується ймовірність появи помилок і уразливостей.

Структура й розділи профілю захисту та проекту захисту показані на рис. 4.9. Як видно з наведених тут структури профілю захисту та проекту захисту, ці документи регламентують взаємодію споживачів, виробників та експертів з кваліфікації у процесі створення ІТ-продукту. Фактично положення цих документів визначають технологію розробки захищених систем.

Найважливішим елементом цієї технології є вимоги безпеки. Розглянемо таксономію цих вимог. Вимоги безпеки поділені на дві категорії: *функціональні вимоги* і *вимоги адекватності*.

Функціональні вимоги регламентують порядок функціонування забезпечувальних компонентів ІТ-продукту і визначають можливості засобів захисту. Адекватність є характеристикою ІТ-продукту, яка відображає ефективність підтримання заявленого рівня безпеки, а також ступінь коректності реалізації засобів захисту. Адекватність ґрунтується на ін-формації про процеси проектування, створення й експлуатації ІТ-продукту. Вимоги адекватності регламентують технологію та процес створення ІТ-продукту, а також необхідність проведення аналізу слабких місць захисту.

Функціональні вимоги поділені на *класи*. Члени класу розрізняються за обсягом охоплення цілей безпеки. Членами класу є *сімейства*. Сімейство – група наборів вимог безпеки, які забезпечують виконання певної частини завдань безпеки, але можуть відрізнятися один від одного в акцентах або жорсткості. Членами сімейства є *компоненти*. Компонент описує найменший з можливих для обрання набір вимог безпеки, які можуть бути включені у профіль і проект захисту. Компоненти побудовані з *елементів*. Елемент – найнижчий і неподільний рівень вимог безпеки. Ієрархія поділу показана на рис. 4.10.

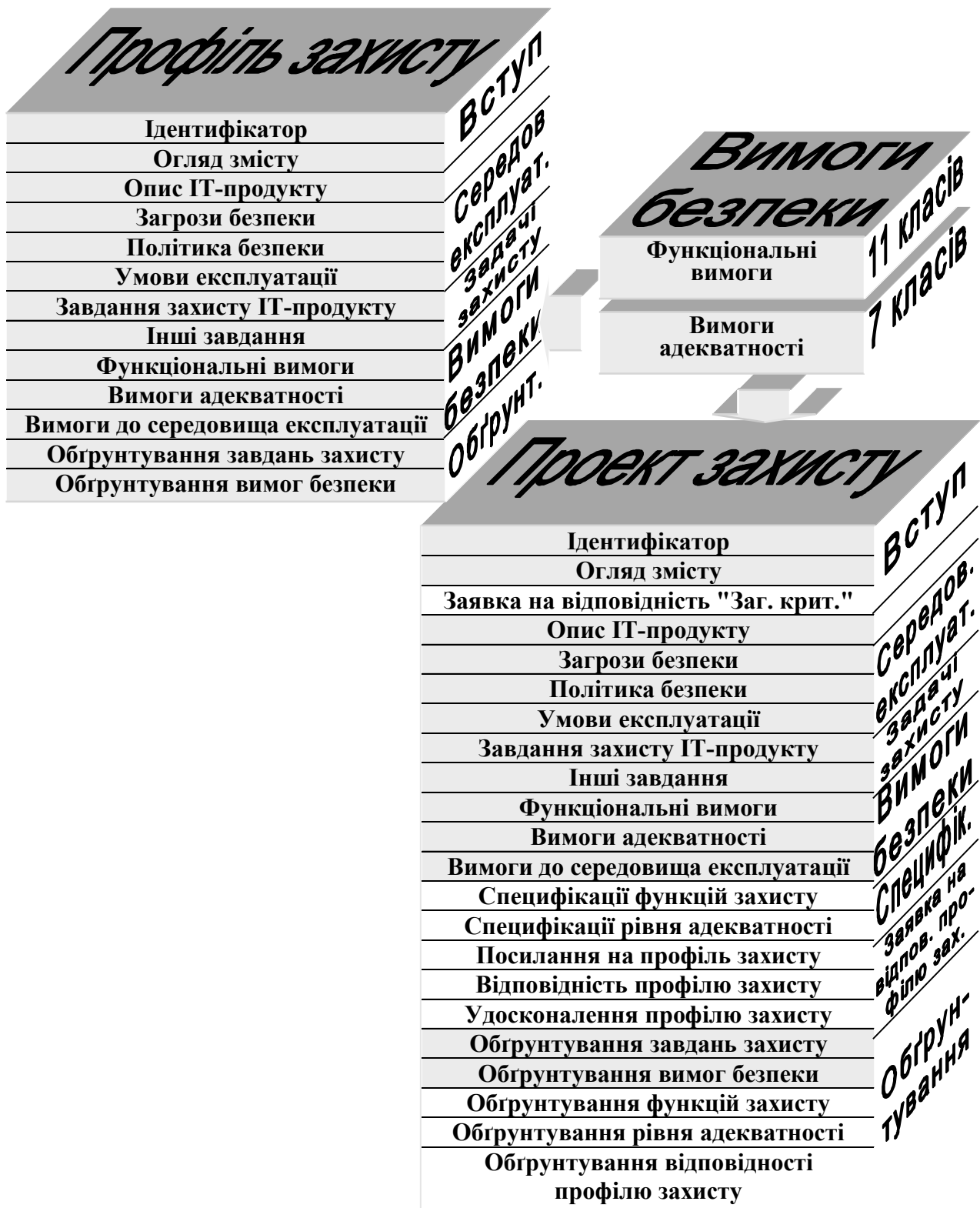


Рис. 4.9. Структура профілю захисту та проекту захисту

Функціональні вимоги

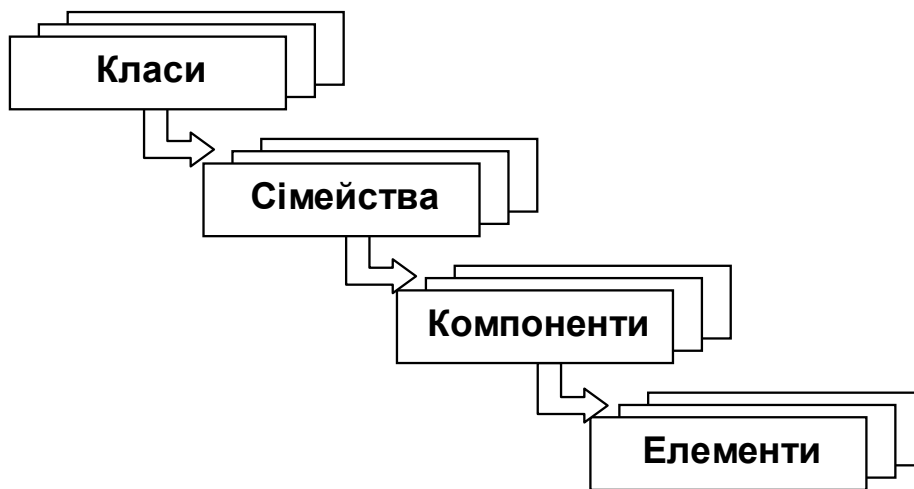


Рис. 4.10. Структура функціональних вимог

Компоненти у сімействі можуть перебувати як в *ієрархічному* зв'язку (коли необхідне посилення вимог), так і без такого (коли має місце якісно нова вимога). Між компонентами можуть існувати *залежності*. Залежності виникають, коли одного компонента недостатньо для досягнення мети безпеки, що зумовлює необхідність використання також іншого компонента. Залежності можуть існувати між функціональними компонентами, компонентами аудиту, а також між тими та іншими. Щоб гарантувати закінченість вимог до об'єкта оцінки, залежності повинні бути враховані під час включення компонентів у профіль захисту і проект захисту. Компоненти можуть бути перетворені за допомогою дозволених дій, щоб забезпечити виконання певної ПБ або протистояти певній загрозі. Не всі дії допустимі на всіх компонентах. Кожен компонент ідентифікує і визначає:

а) дозволені дії або обставини, за яких певна дія може бути застосована до цього компонента;

б) результати застосування дії.

До дозволених дій відносяться: *призначення, вибір і обробка*.

Призначення дозволяє заповнити специфікацію ідентифікованого параметра під час використання компонента. Параметр може бути ознакою або правилом, яке конкретизує вимогу до певної величини або діапазону величин. Наприклад, елемент функціонального компонента може заявляти, що дана дія повинна бути виконана неодноразово. У

цьому випадку призначення забезпечує число або діапазон чисел, які повинні використовуватися в параметрі.

Вибір – це дія вибору одного або більшої кількості пунктів із списку, щоб конкретизувати можливості елемента.

Таксономію класів функціональних вимог "Загальних критеріїв" наведено на рис. 4.11.



Рис. 4.11. Таксономія класів функціональних вимог "Загальних критеріїв"

Обробка дозволяє включити додаткові деталі в елемент і передбачає засновану на цілях безпеки інтерпретацію вимоги, правила, константи або умови. Обробка повинна тільки обмежити набір можливих прийнятних функцій або механізмів, щоб здійснити вимоги, але не збільшувати їх. Обробка не дозволяє створювати нові вимоги або видаляти вже існуючі й не впливає на список залежностей, пов'язаних із компонентом.

Назви функціональних класів мають наступне значення:

- 1) *Аудит безпеки (FAU: Security audit)*. Аудит системи безпеки – це розпізнавання, реєстрація, зберігання й аналіз інформації, що належить до системи безпеки.

- 2) *Зв'язок (FCO: Communication)*. Виконання вимог цього класу гарантує, що передавач інформації не зможе відмовитися від надсилання повідомлення, а приймач – від його отримання.
- 3) *Криптографічна підтримка (FCS: Cryptographic support)*. Клас містить сімейства вимог щодо керування криптографічними ключами і операціями.
- 4) *Захист даних користувача (FDP: User data protection)*. Клас визначає вимоги безпеки, що відносяться до захисту даних користувача під час вводу, виводу і зберігання інформації.
- 5) *Ідентифікація та автентифікація (FIA: Identification and authentication)*. Вимоги цього класу стосуються процедур визначення й верифікації користувачів, їх повноважень у системі, а також правильної прив'язки атрибутів безпеки до кожного користувача.
- 6) *Керування безпекою (FMT: Security management)*. Клас містить вимоги щодо керування атрибутами і даними функцій безпеки, а також ролями безпеки.
- 7) *Секретність (FPR: Privacy)*. Реалізація вимог даного класу забезпечить захист користувача від розкриття й зловживань його повноваженнями іншими користувачами.
- 8) *Безпека захисту (FPT: Protection of the TSF)*. Клас містить функціональні вимоги, що стосуються цілісності й керування механізмами безпеки системи незалежно від специфіки ПБ, що реалізовується.
- 9) *Використання ресурсів (FRU: Resource utilisation)*. Вимоги цього класу забезпечують доступність необхідних ресурсів (таких, як можливість обробки і/або зберігання), а також захист у разі блокування функціональних можливостей, викликаних відмовами системи.

Таксономію сімейств функціональних вимог для всіх класів "Загальних критеріїв" подано на рис. 4.12.

- 10) *Доступ до системи (FTA: TOE access)*. Клас визначає функціональні вимоги контролю за встановленим сеансом роботи користувача незалежно від вимог щодо ідентифікації та автентифікації.
- 11) *Надійний маршрут/канал (FTP: Trusted path/channels)*. Клас забезпечує вимоги:
 - надійного комунікаційного маршруту між користувачами і функціями безпеки системи;
 - надійного каналу зв'язку між функціями безпеки системи.

Розділ стандарту, що описує **вимоги адекватності**, включає (рис. 4.13):
критерії для оцінки профілю й проекту захисту;
класи, сімейства та компоненти адекватності ІТ-продукту;
рівні адекватності ІТ-продукту.

Аудит безпеки	Автоматичне реагування на вторгнення в систему	FAU	Неможливість для джерела відмовитися від факту передачі інформації	FCO	
	Реєстрація і облік подій		Неможливість для приймача відмовитися від факту отримання інформації		
	Аналіз аудиту безпеки		Захист даних користувача		
	Контроль доступу до протоколу аудиту		Політика керування доступом	FDP	
	Відбір подій для реєстрації й обліку		Засоби керування доступом		
	Виділення ресурсів під протокол аудиту	Експорт даних			
Криптографічна підтримка	Керування криптографічними ключами	FCS	Політика керування зв'язком		
	Криптографічні операції		Засоби керування зв'язком		
Ідентифікація та автентифікація	Реакція на невдалі спроби автентифікації	FIA	Імпорт даних		FDP
	Набір атрибутів безпеки користувачів		Захист даних при передачі внутрішніми каналами		
	Генерація і перевірка ключів і паролів		Знищення залишкової інформації		
	Автентифікація користувачів		Відкат		
	Ідентифікація користувачів		Автентифікація даних		
	Відповідність атрибутів безпеки користувачів і суб'єктів, що представляють їх в системі		Цілісність даних у процесі зберігання		
Керування безпекою	Керування функціями безпеки ІТ-продукту	FMT	Захист даних при передачі зовнішніми каналами	FDP	
	Керування атрибутами безпеки		Захист даних при передачі внутрішніми каналами		
	Керування даними функцій безпеки		Безпека захисту		
	Анулювання		Тестування апаратно-програмної платформи		
	Закінчення атрибуту безпеки		Захист від збоїв		
	Функції управління безпекою		Забезпечення взаємодії засобів захисту		
Секретність	Анонімність сеансів роботи з системою	FPR	Забезпечення конфіденційності при взаємодії засобів захисту		FPT
	Використання псевдонімів		Забезпечення цілісності при взаємодії засобів захисту		
	Невиведення характеристик користувачів		Захист інформаційного обміну між засобами захисту		
	Спостереженість сеансів роботи із системою		Фізичний захист		
Використання ресурсів	Відмовостійкість	FRU	Безпека відновлення після збоїв	FPT	
	Обслуговування на основі пріоритетів		Відгук атрибутів безпеки		
	Розподіл ресурсів		Розпізнавання повторних передач інформації та імітації подій		
Доступ до системи	Обмеження на використання користувачами атрибутів і суб'єктів		FTA		
	Обмеження числа одночасних сеансів	"Застарівання" атрибутів безпеки			
	Блокування сеансу роботи	Розподіл по доменах			
	Оголошення, попередження, запрошення й підказки	Забезпечення синхронізації			
	Протокол сеансів користувачів	Відлік часу			
	Керування параметрами сеансів	Модифікація ПО засобів захисту			
	Обмеження на сеанси роботи	Розподіл інформації			
		Реплікація інформації			
		Керування безпекою			
		Керівництво безпекою			
		Самотестування			
		Захист засобів управління безпекою			
		Надійний маршрут/канал	FTP		
		Надійний маршрут між користувачами і функціями безпеки системи			
		Надійний канал зв'язку між функціями безпеки системи			

Рис. 4.12. Таксономія сімейств функціональних вимог для всіх класів "Загальних критеріїв"

Вимоги адекватності

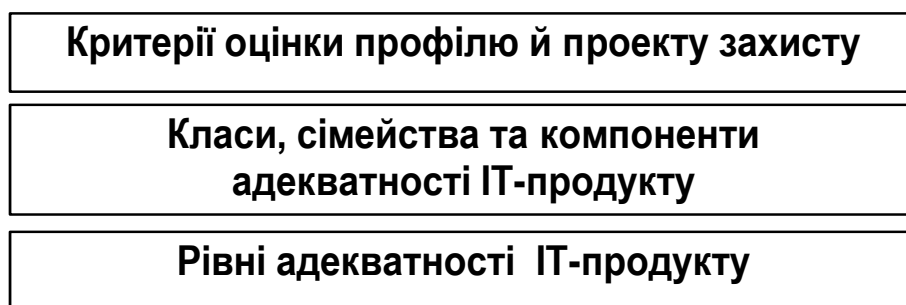


Рис. 4.13. Структура опису стандартом вимог адекватності

Критерії оцінки профілю захисту та проекту захисту складаються з двох класів *API* і *ASE*, кожен із яких оцінює відповідно профіль захисту і проект захисту (рис. 4.14). Класи, у свою чергу складаються із сімейств, що відображають структуру й основний зміст відповідних документів.



Рис. 4.14. Класи та сімейства критеріїв оцінки профілю захисту і проекту захисту

Мета оцінки профілю й проекту захисту полягає в тому, щоб показати, що ці документи є повними, послідовними, технічно грамотними й прийнятними для використання за призначенням. Профіль захисту, що задовольняє цим критеріям, може мати право на включення в перелік зумовлених профілів захисту.

Згідно з концепцією "Загальних критеріїв" необхідно визначити міру адекватності, засновану на оцінці ІТ-продукту. Стандарт пропонує визначення адекватності, засноване на активному дослідженні ІТ-продукту експертами з посиленням уваги на можливостях, глибині та строгості методів оцінки. Передбачається, що високий ступінь

адекватності досягається шляхом застосування великих зусиль під час проведення оцінки.

Структура вимог адекватності подібна до структури функціональних вимог. На відміну від функціональних вимог усі сімейства вимог адекватності є лінійно ієрархічними.

Таксономія вимог адекватності подана на рис. 4.15.



Рис. 4.15. Таксономія вимог адекватності

Пояснимо класи вимог адекватності.

- 1) *Керування конфігурацією (ACM: Configuration management)* забезпечує збереження цілісності ІТ-продукту та його відповідності вимогам дисципліни і керування під час уточнення й модифікації ІТ-продукту. Запобігає несанкціонованим змінам, додаванням або видаленням в ІТ-продукті, гарантуючи таким чином відповідність тих ІТ-продукту і документації, які використовуються для оцінки, з тими, які підготовлені для поширення.
- 2) *Постачання і функціонування (ADO: Delivery and operation)*. Клас адекватності визначає вимоги до заходів, процедур і стандартів, що стосуються надійного постачання, інсталяції та експлуатаційного використання ІТ-продукту, які гарантують, що

рівень безпеки, запропонований ІТ-продуктом, не скомпрометований у процесі переміщення, інсталяції, запуску і функціонування.

- 3) *Розробка (ADV: Development)*. Цей клас вимог адекватності охоплює собою вимоги до покрокового уточнення функцій безпеки, виходячи з узагальненої специфікації ІТ-продукту в проекті захисту зверху вниз до фактичної реалізації. Кожне з результуючих представлень функцій безпеки забезпечує інформацією, яка допомагає експерту під час сертифікації визначити, чи задоволені функціональні вимоги ІТ-продукту.
- 4) *Керівні документи (AGD: Guidance documents)*. Клас адекватності визначає вимоги до зрозумілості та повноти експлуатаційної документації, поданої розробником. Якість документації для кінцевих користувачів і для адміністраторів є значущим чинником безпечного функціонування ІТ-продукту.
- 5) *Життєвий цикл (ALC: Life cycle support)*. Цей клас точно визначає модель життєвого циклу для всіх кроків розробки ІТ-продукту, зокрема процедур і політики усунення недоліків, правильного використання інструментів і методів, а також заходів безпеки, вживаних для захисту середовища розробки.
- 6) *Випробування (ATE: Tests)*. Даний клас адекватності встановлює вимоги до випробувань, які демонструють, що функції безпеки задовольняють функціональним вимогам безпеки ІТ-продукту.
- 7) *Оцінка вразливості (AVA: Vulnerability assessment)*. Цей клас визначає вимоги, направлені на ідентифікацію вразливих місць ІТ-продукту, зумовлені як побудовою, так і функціонуванням, неправомірним використанням або неправильною конфігурацією ІТ-продукту.

Ранжування вимог адекватності подане у вигляді впорядкованих списків. "Загальні критерії" пропонують сім стандартних рівнів адекватності (*EAL – Evaluation Assurance Level*), кожен із яких визначає ступінь відповідності ІТ-продукту кожній вимозі адекватності (адекватність зростає від першого рівня до сьомого). Назви рівнів відображають можливості засобів контролю і верифікації, що застосовується в ході розробки й аналізу ІТ-продукту. Кожен із рівнів містить повний набір вимог адекватності й визначає масштаб адекватності у стандарті. На рис. 4.16 показані назви рівнів адекватності.

Рівень 1 – найнижчий рівень адекватності, для якого оцінка є значущою і економічно виправданою. Цей рівень призначений для виявлення очевидних помилок при мінімальних витратах. Компоненти рівня забезпечують мінімальний рівень адекватності шляхом аналізу функцій безпеки. Аналіз проводиться за наслідками незалежного тестування кожної з функцій безпеки.

<i>Рівні адекватності (EAL)</i>	
Застосування функціонального тестування	EAL1
Застосування структурного тестування	EAL2
Застосування методик тестування і контролю	EAL3
Застосування методик розробки, тестування і аналізу	EAL4
Застосування напівформальних методів розробки і тестування	EAL5
Застосування напівформальних методів верифікації в процесі розробки і тестування	EAL6
Застосування формальних методів верифікації в процесі розробки і тестування	EAL7

Рис. 4.16. Сім стандартних рівнів адекватності

Стисло охарактеризуємо рівні адекватності.

Рівень 2 – структурно перевірений проект. Застосовується, коли розробників або користувачів задовольняє помірно низький рівень гарантованої безпеки за відсутності повного звіту про розробку. Компоненти цього рівня забезпечують адекватність шляхом аналізу функцій безпеки і *проекту високого рівня підсистем* ІТ-продукту. Аналіз, підтриманий незалежним тестуванням кожної з функцій безпеки, актом тестування розробником "чорної скриньки" і свідоцтвом пошуку розробником чітких вразливих місць (наприклад, у загальнодоступній сфері).

Рівень 3 – методично перевірений проект, що є протестованим, дозволяє добросовісному розробнику одержати максимальну адекватність безпеки на стадії розробки проекту без істотної зміни звичайних методів розробки. Тому рівень застосовується, коли

розробники або користувачі вимагають помірного рівня адекватності безпеки, повного дослідження виробу й процесу розробки без істотних технічних витрат.

Компоненти цього рівня забезпечують адекватність шляхом аналізу функцій безпеки і проекту високого рівня підсистем ІТ-продукту. Аналіз, підтриманий незалежним тестуванням функцій безпеки, актом тестування розробником "сірої скриньки", незалежним підтвердженням вибіркового результату тестування розробником і свідченням пошуку розробником чітких вразливих місць. Рівень також забезпечує додаткову адекватність шляхом включення засобів контролю навколишнього середовища розробки і керування конфігурацією ІТ-продукту.

Рівень 4 – методично розроблений і перевірений проект, дозволяє розробнику одержувати максимальну адекватність безпеки у випадках проектування, заснованого на визнаних комерційних методах розробки. Є найвищим економічно доцільним рівнем для орієнтування на існуючі типи виробів. Тому рівень застосовується, коли розробники або користувачі вимагають помірно високого рівня адекватності безпеки у звичайних товарних виробках і готові зазнати певних технічних витрат для додаткового забезпечення.

Компоненти четвертого рівня забезпечують адекватність шляхом аналізу функцій безпеки, проекту високого рівня підсистем, *проекту низького рівня модулів ІТ-продукту і піднабору виконання*. Аналіз підтриманий незалежним тестуванням функцій безпеки, актом тестування розробником "сірої скриньки", незалежним підтвердженням вибіркового результату тестування розробником, свідченням пошуку розробником чітких вразливих місць і незалежним пошуком чітких вразливих місць. Використовуються також засоби контролю навколишнього середовища розробки й додаткових засобів керування конфігурацією ІТ-продукту, включаючи засоби автоматизації цього процесу.

Рівень 5 – напівформально розроблений і перевірений проект, дозволяє розробнику одержати максимальну адекватність безпеки під час проектування, заснованого на суворих комерційних методах розробки і підтриманих помірним використанням спеціальних технічних методів забезпечення. Тому рівень застосовується, коли розробники або користувачі вимагають високого рівня адекватності безпеки і ретельного

підходу до розробки без істотних додаткових витрат, що відносяться до технічних методів забезпечення.

Компоненти п'ятого рівня забезпечують адекватність шляхом аналізу функцій безпеки, проекту високого рівня підсистем, проекту низького рівня модулів ІТ-продукту і *всіх напрямків* функціонування. Додаткова адекватність одержана за рахунок формальної моделі і напівформального представлення функціональної специфікації, проекту високого рівня й напівформальної демонстрації відповідності між ними. Аналіз підтриманий незалежним тестуванням функцій безпеки, актом тестування розробником "сірої скриньки", незалежним підтвердженням вибіркового результату тестування розробником, свідченням пошуку розробником чітких вразливих місць і незалежним пошуком вразливих місць. Результати такого пошуку гарантують відносний ступінь опору несанкціонованому доступу. Аналіз також включає *пошук таємних каналів і підтриманий вимогою модульного проекту ІТ-продукту*. Рівень також забезпечує адекватність за допомогою засобів контролю навколишнього середовища розробки і усебічного керування конфігурацією ІТ-продукту, включаючи автоматизацію.

Рівень 6 – напівформально верифікований і перевірений проект, дозволяє розробникам одержувати високу адекватність за рахунок застосування технічних методів забезпечення ІТ-продукту в умовах складного навколишнього середовища. Тому застосовується під час розробці спеціальних виробів для використання в ситуаціях високого ризику, де цінність активів, які захищаються, виправдовує додаткові витрати. Компоненти рівня забезпечують адекватність шляхом аналізу функцій безпеки, проекту високого рівня підсистем, проекту низького рівня модулів ІТ-продукту і структурованого представлення функціонування. Додаткова адекватність досягається за рахунок побудови формальної моделі, напів формального представлення функціональної специфікації, проекту високого рівня і проекту низького рівня, а також напівформальної демонстрації відповідності між ними. Аналіз, підтриманий незалежним тестуванням функцій безпеки, актом тестування розробником "сірої скриньки", незалежним підтвердженням вибіркового результату тестування розробником, свідченням пошуку розробником чітких вразливих місць і незалежним пошуком вразливих місць. Результати такого пошуку гарантують високий ступінь опору несанкціонованому доступу. Аналіз також включає систематичний пошук

таємних каналів і підтриманий вимогою модульного та *ієрархічного* проекту ІТ-продукту. Рівень також забезпечує адекватність за рахунок структурованого процесу розробки, засобів контролю навколишнього середовища розробки і усебічного керування конфігурацією ІТ-продукту, включаючи повну автоматизацію.

Рівень 7 – формально верифікований і перевірений проект, є досяжною верхньою межею оцінки адекватності для фактично корисних виробів і розглядається тільки для експериментального застосування до всіх виробів, окрім концептуально простих і добре зрозумілих. Тому рівень застосовується при розробці спеціальних виробів для застосування в ситуаціях надзвичайно високого ризику і/або там, де висока цінність активів виправдовує вищі витрати. Практичне застосування рівня в даний час обмежене виробами із зосередженими функціональними можливостями забезпечення, які піддаються формальному аналізу.

Компоненти сьомого рівня забезпечують адекватність шляхом аналізу функцій безпеки, проекту високого рівня підсистем, проекту низького рівня модулів ІТ-продукту і структурованого представлення функціонування. Додаткова адекватність забезпечується за рахунок формальної моделі, *формального представлення функціональної специфікації та проекту високого рівня*, напівформального представлення проекту низького рівня, формальної та напівформальної демонстрації відповідності між ними. Аналіз, підтриманий незалежним тестуванням функцій безпеки, актом тестування розробником "*білої скриньки*", незалежним підтвердженням **усіх** результатів тестування розробником, свідченням пошуку розробником чітких уразливостей і незалежним пошуком вразливих місць. Результати такого пошуку гарантують високий опір несанкціонованому доступу. Аналіз також включає систематичний пошук прихованих каналів і підтриманий вимогою модульного, ієрархічного і *простого* проекту ІТ-продукту. Рівень також забезпечує адекватність за рахунок структурованого процесу розробки засобів контролю навколишнього середовища, розробки та всебічного керування конфігурацією ІТ-продукту, включаючи повну автоматизацію.

Американським національним інститутом стандартів і технологій (NIST) на базі "Загальних критеріїв" була розроблена *Базова технічна*

модель ІТ-безпеки [47], яка наочно показує зв'язок компонентів безпеки ІТ-продукту. Познайомимося докладніше з цією моделлю.

4.1.3. Базова технічна модель ІТ-безпеки у відповідності з NIST Special Publication 800-33

Відповідно до цієї моделі *головна мета безпеки інформаційних технологій (Security Goal)* – це надання можливості організації виконувати свої функції, враховуючи можливі ІТ-ризики для організації, її партнерів і споживачів.

Мета ІТ-безпеки досягається за допомогою вирішення п'яти завдань безпеки (*Security Objectives*), які відповідають чотирьом основним загрозам безпеки (доступності, конфіденційності, цілісності, спостереженості) і гарантіям реалізації ІТ-безпеки. Тракткування цих завдань таке:

1) *Забезпечення доступності (Availability) (тільки ресурсів, призначених для використання)*. Авторизовані користувачі мають доступ до відповідних ресурсів нормально працюючої системи. Це завдання спрямоване на запобігання зумисному або незумисному неавторизованому видаленню даних, випадкам необґрунтованої відмови в доступі до ресурсу, спробам використання системи або даних у несанкціонованих цілях.

2) *Забезпечення цілісності (Integrity) (системи і даних)*. Цілісність має два аспекти:

цілісність даних – дані не можуть бути несанкціоновано модифіковані під час їх зберігання, передачі та обробки;

цілісність системи – функціонування системи без втручання в її роботу і несанкціонованих маніпуляцій.

3) *Забезпечення конфіденційності (Confidentiality) (даних і системної інформації)*. Конфіденційна інформація не може бути доступна для неавторизованого користувача під час її зберігання, обробки й передачі.

4) *Забезпечення спостереженості (Accountability)*. Здатність вибіркового спостереження (фіксації) за діями об'єктів і суб'єктів в ІТ-системі. Спостереженість – це організаційна вимога ПБ, що досягається за допомогою механізмів причетності, примушення,

локалізації несправностей, виявлення і запобігання вторгненням, відновлення юридичними заходами.

5) *Забезпечення гарантій (Assurance) (адекватна реалізація попередніх чотирьох завдань)*. Досягнення стану, коли є підстави вірити, що механізми безпеки реалізовані й працюють відповідно до розробленого проекту ІТ-системи. Перші чотири завдання безпеки (цілісність, доступність, конфіденційність і спостереженість) адекватно реалізовані, якщо:

функціональні вимоги правильно сформульовані й коректно реалізовані;

забезпечено достатній захист від зумисних помилок користувачів або помилок програмного забезпечення;

забезпечено достатню стійкість від зумисного проникнення й використання манівців.

Забезпечення гарантій є найбільш узагальненим завданням, без вирішення якого робота над іншими чотирма не має сенсу.

Усі завдання залежать одне від одного і не можуть бути вирішені окремо (рис. 4.17).

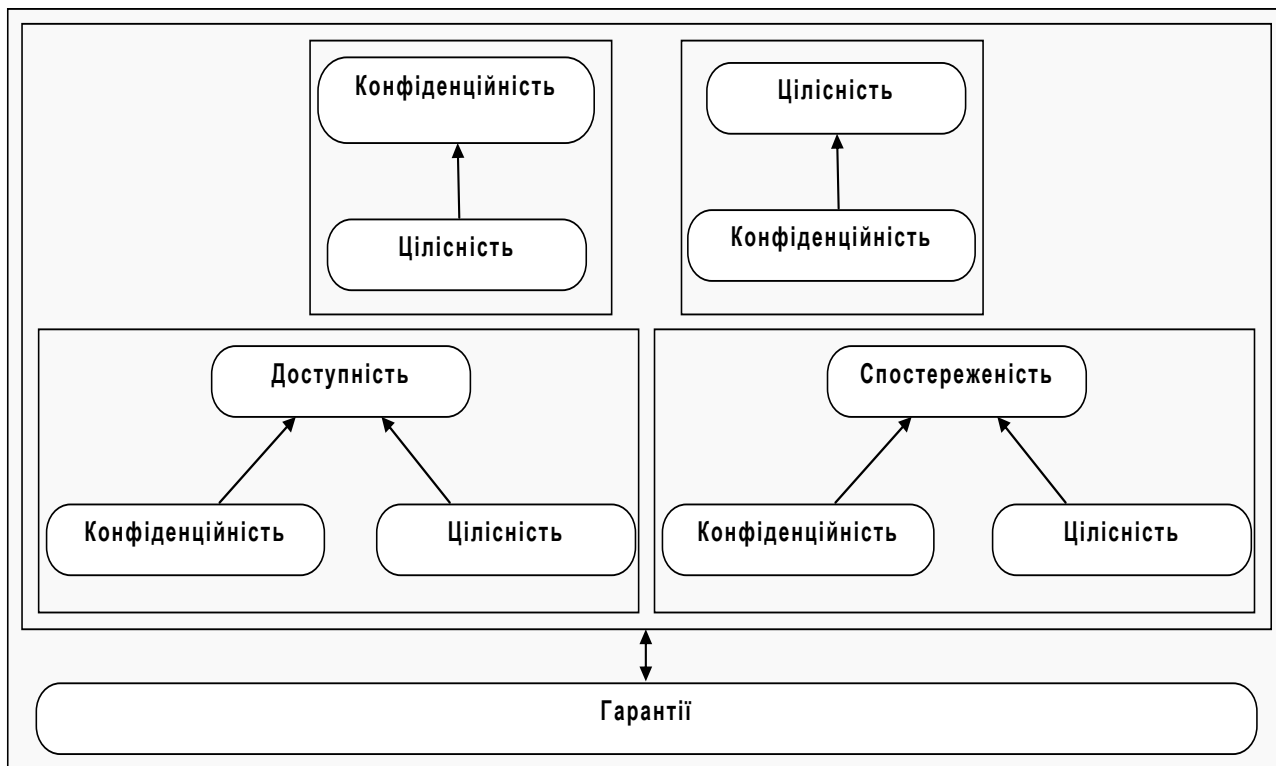


Рис. 4.17. П'ять завдань безпеки (Security Objectives)

Порушення цілісності може спричинити некоректну роботу механізмів конфіденційності, і навпаки, порушення конфіденційності (наприклад, розкриття пароля адміністратора) може призвести до виникнення можливості обходу механізмів цілісності.

Залежність доступності та спостереженості від конфіденційності та цілісності можна пояснити, наприклад, так:

порушення конфіденційності певної інформації (наприклад, пароліної інформації) може призвести до можливості обминання механізмів доступності та спостереженості;

порушення цілісності системи може призвести до компрометації механізмів доступності та спостереженості.

У конкретних системах ці завдання можуть мати різний ступінь і якість організації.

Вирішення завдань захисту покладається на **послуги безпеки**, які можуть бути віднесені до одного з наступних класів.

- 1) *Забезпечення (Support)*. Послуги є загальними і лежать в основі реалізації решти послуг безпеки.
- 2) *Запобігання (Prevent)*. Послуги спрямовані на запобігання порушенням безпеки.
- 3) *Виявлення й відновлення (Detection and Recover)*. Послуги спрямовані на виявлення порушень безпеки і повернення системи у безпечний стан.

На рис. 4.18 показано модель взаємодії названих послуг безпеки в ІТ-системі.

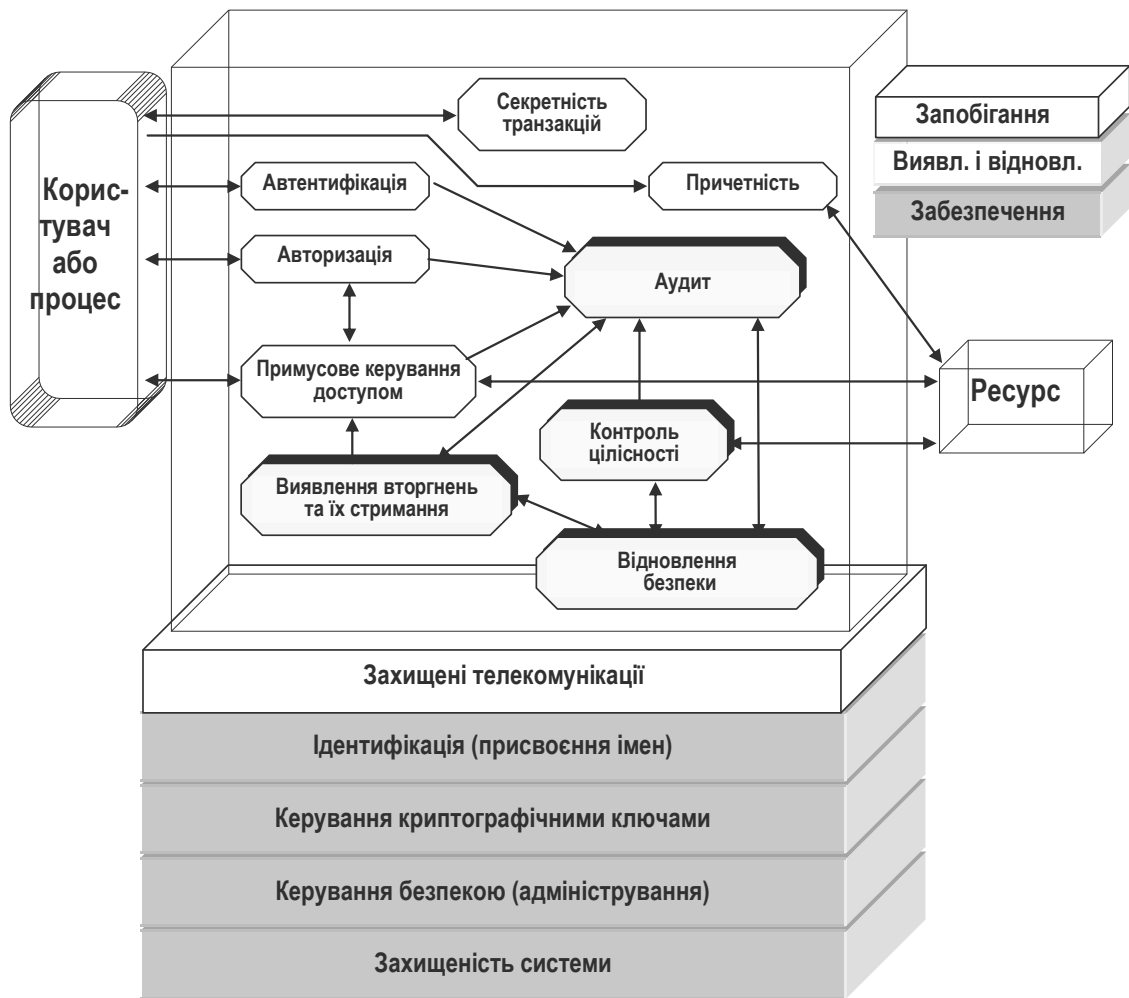


Рис. 4.18. **Модель взаємодії послуг безпеки в ІТ-системі**

До послуг *забезпечення* відносяться:

Ідентифікація (присвоєння імен) (Identification (and naming)).

Необхідна умова для реалізації більшості послуг безпеки. Забезпечує можливість присвоєння унікального ідентифікатора користувачам, процесам, інформаційним та іншим ресурсам.

Керування криптографічними ключами (Cryptographic key management). Послуга обов'язкова у випадках використання криптографічних функцій для безпечного керування ключами.

Керування безпекою (адміністрування) (Security administration).

Керування процесом налаштування параметрів інсталяції, експлуатації програмного й апаратного забезпечення послуг безпеки, а також облік змін в умовах експлуатації.

Захищеність системи (System protections).

Сукупність властивостей системи, які дозволяють довіряти технічній реалізації системи. Розглядається якість реалізованих засобів захисту, процедури їх

розробки, способи досягнення й вирішення технічних завдань. Прикладами засобів захищеності системи є захист залишкової інформації (захист від повторного використання), мінімізація повноважень, розподіл процесів, модульність і можливість порівняння розробки, мінімізація кола обізнаних осіб і т. д.

До послуг *запобігання* належать:

Захищені телекомунікації (Protected communications).

Забезпечення в розподілених *системах* цілісності, конфіденційності та доступності інформації під час її передачі каналами зв'язку. Різні механізми безпеки забезпечують приховування смислового змісту повідомлень, захист від знищення, підстановки, модифікації, повторної передачі даних та інших видів зловмисних дій.

Автентифікація (Authentication). Перевірка достовірності суб'єктів.

Авторизація (Authorization). Надання (наділення) суб'єктів певними (специфікованими) повноваженнями щодо виконання ними дій у даній системі.

Примусове керування доступом (Access control enforcement).

Забезпечення використання ресурсів відповідно до встановленої ПБ (правил розмежування доступу).

Причетність (Non-repudiation). Забезпечення неможливості відмови одержувача від факту отримання інформації й відправника від авторства створення й відправки інформації.

Секретність транзакцій (Transaction privacy). Забезпечення конфіденційності транзакцій, що виконуються користувачами в ІТ-системі.

До послуг *виявлення й відновлення* належать:

Аудит (Audit). Реєстрація подій, що впливають на безпеку системи, з метою надання інформації для подальшого відновлення безпеки системи.

Виявлення вторгнень та їх утримання (Intrusion detection and containment). Виявлення спроб порушень безпеки і по можливості протидії цим діям або, як мінімум, їх реєстрації.

Контроль цілісності (Proof of Wholeness). Своєчасне виявлення порушень цілісності елементів системи, від яких залежить її безпека.

Відновлення безпеки (Restore 'secure' state). Реакція системи на порушення з метою відновлення безпеки. Послуга реалізується через виконання таких дій, як негайне роз'єднання або припинення роботи, відмова суб'єкт в доступі, тимчасове позбавлення суб'єкта прав, занесення суб'єкта в "чорний список" і т. п.

На рис. 4.19 показано необхідні набори послуг для вирішення завдань доступності та цілісності, на рис. 4.20 – конфіденційності, на рис. 4.21 – спостереженості, і на рис. 4.22 – гарантій. Проте, як було зазначено вище, вирішення окремого завдання неможливе без вирішення всіх інших (рис. 4.19).

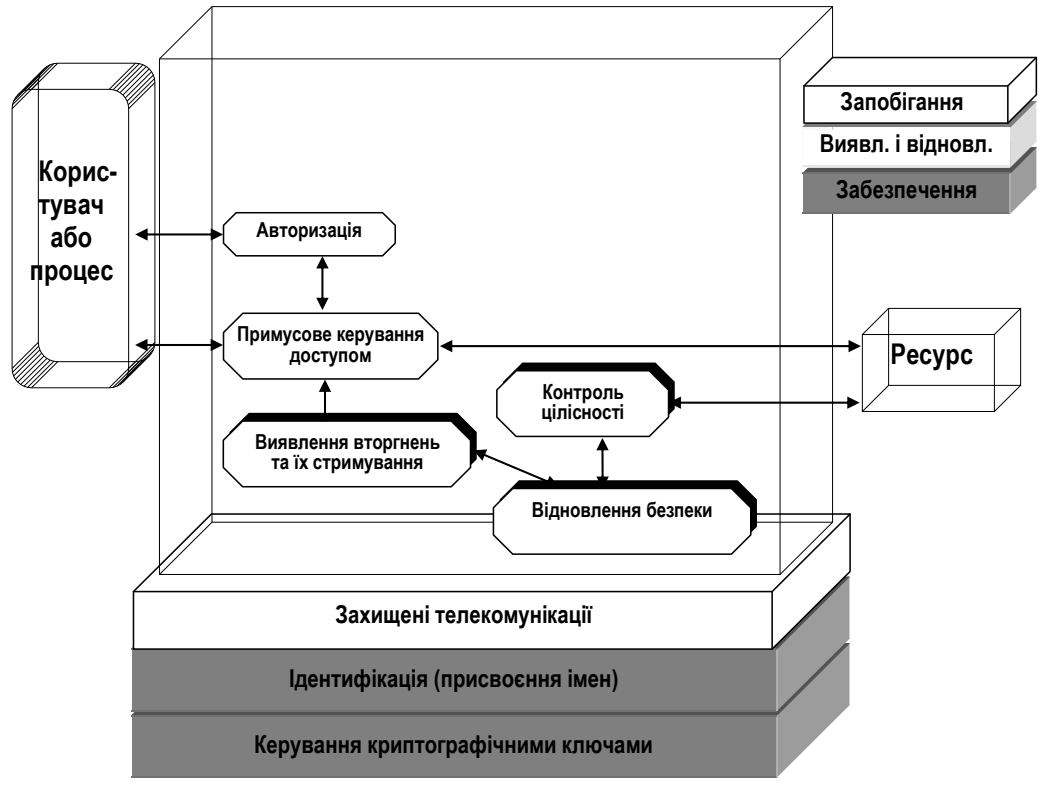


Рис. 4.19. Необхідні набори послуг для вирішення завдань доступності та цілісності

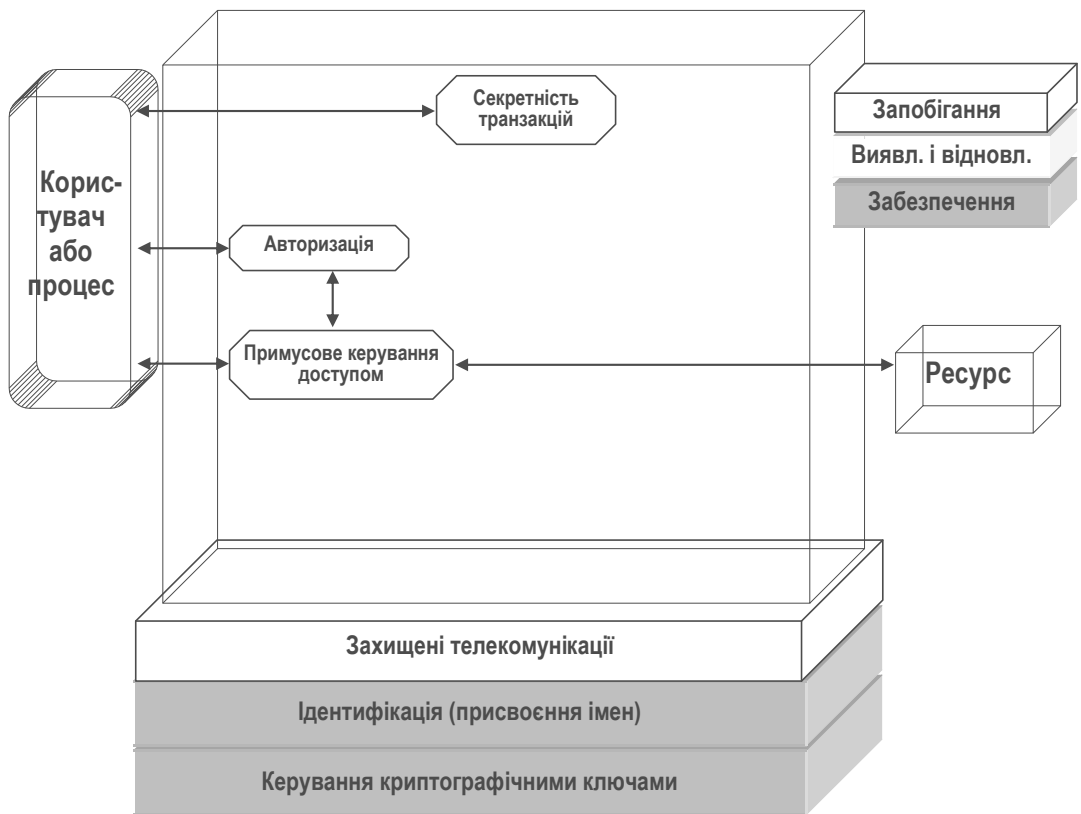


Рис. 4.20. **Необхідні набори послуг для вирішення завдань конфіденційності**

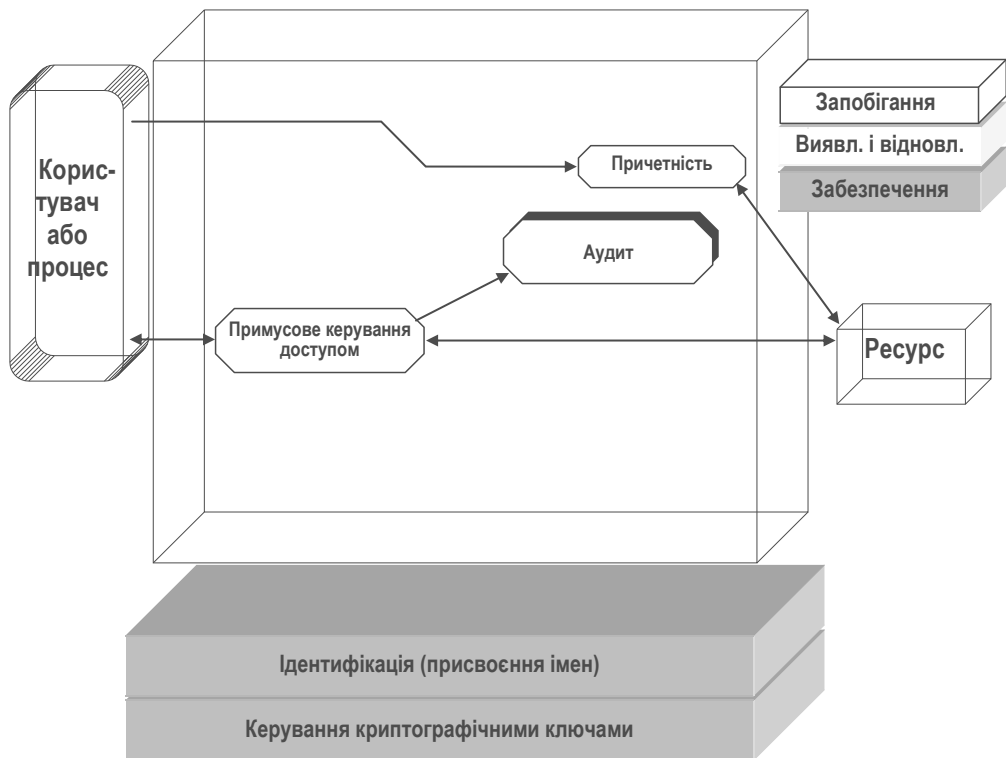


Рис. 4.21. **Необхідні набори послуг для вирішення завдань спостереженості**

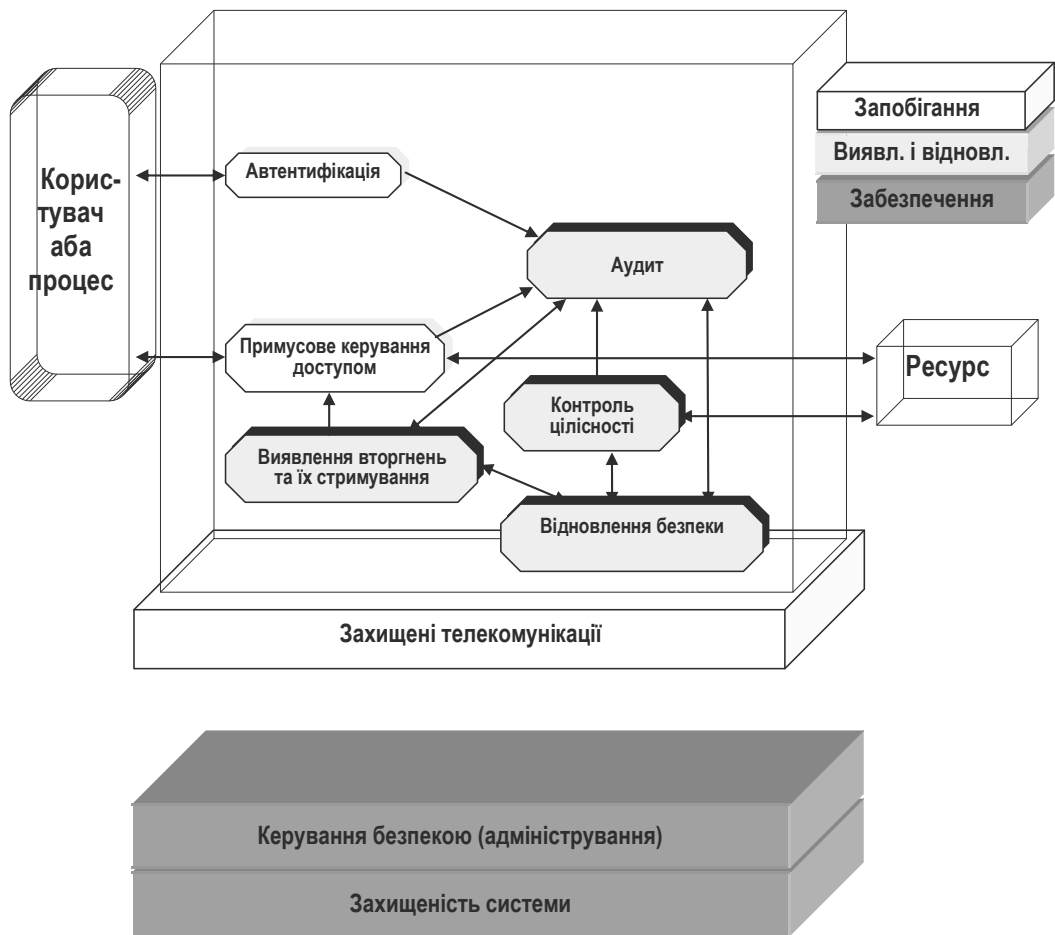


Рис. 4.22. Необхідні набори послуг для вирішення завдань гарантій



Рис. 4.23. Технічна модель ІТ-безпеки за "Загальними критеріями"

Запропонована технічна модель ІТ-безпеки, в якій сформульовано основні завдання безпеки й послуги їх забезпечення, дозволяє далі використовувати "Загальні критерії" для висунення функціональних вимог і вимог адекватності до профілю й проекту захисту ІТ-системи (рис. 4.23).

Наведена на рис. 4.22 технологія проектування може бути використана для розробки проекту (плану) системи захисту інформації, що знижує за обраним критерієм ризику для інформаційних ресурсів, які потребують захисту відповідно до виявленої множини загроз.

4.1.4. Оцінка безпеки ІС

В умовах використання ІТ під безпекою розуміється стан захищеності ІС від внутрішніх і зовнішніх загроз.

Показник захищеності ІС – характеристика засобів системи, що впливає на захищеність і яка описує певну групу вимог, що варіюються за рівнем і глибиною залежно від класу захищеності.

Для оцінки реального стану безпеки ІС можуть застосовуватися різні критерії. Аналіз вітчизняного й закордонного досвіду показав спільність підходу до визначення стану безпеки ІС у різних країнах. Для надання користувачеві можливості оцінки вводиться деяка система показників і задається ієрархія класів безпеки. Кожному класу відповідає певна сукупність обов'язкових функцій. Ступінь реалізації обраних критеріїв показує поточний стан безпеки. Наступні дії зводяться до порівняння реальних загроз із реальним станом безпеки.

Якщо реальний стан перебиває загрози повною мірою, система безпеки вважається надійною й не вимагає додаткових заходів. Таку систему можна віднести до класу систем з повним перекриттям загроз і каналів витоку інформації. Інакше система безпеки має потребу в додаткових заходах захисту.

Розглянемо коротко підходи до оцінки безпеки ІС у США й у Росії. Питаннями стандартизації й розробки нормативних вимог на захист інформації в США займається Національний центр комп'ютерної безпеки міністерства оборони США (NCSC – National Computer Security Center). Центр ще в 1983 р. видав критерії оцінки безпеки КС (TCSEC – Trusted Computer System Evaluation Criteria). Цей документ називається Жовтогарячою книгою. В 1985 р. вона була затверджена як урядовий

стандарт. Жовтогаряча книга містить основні вимоги й специфікує класи для оцінки рівня безпеки комп'ютерних систем. Використовуючи ці критерії NCSC: тестує ефективність механізмів контролю безпеки комп'ютерних систем. Критерії, перераховані в Жовтогарячій книзі, роблять ІБ величиною, що допускає її вимір і дозволяють оцінити рівень безпеки тієї або іншої системи. Можливості аналізу ступеня безпеки ІС привели до міжнародного визнання федерального стандарту США. NCSC вважає безпечною систему, що за допомогою спеціальних механізмів захисту контролює доступ інформації таким чином, що тільки відповідні повноваження, що мають особи або процеси, які виконуються від їх імені, можуть одержати доступ на читання, запис, створення або видалення інформації.

У Жовтогарячій книзі наводяться наступні рівні безпеки систем:

вищий клас, позначається як А;

проміжний клас – В;

низький рівень безпеки – С;

клас систем, не минулі випробування – Д. Клас Д привласнюється тим системам, які не пройшли випробування на більше високий рівень захищеності, а також системам, що використовують для захисту лише окремі заходи або функції (підсистеми безпеки).

Клас С розбивається на два підкласи (за зростаючими вимогами до захисту). Тому що С1 повинен забезпечувати вибірний захист, засоби безпеки систем класу С1 повинні задовольняти вимогам вибірного керування доступом, забезпечуючи поділ користувачів і даних. Для кожного об'єкта й суб'єкта задається перелік припустимих типів доступу (читання, запис, друк й т. д.) суб'єкта до об'єкта. У системах цього класу обов'язкова ідентифікація (присвоєння кожному суб'єктові персонального ідентифікатора) і автентифікація (установлення дійсності) суб'єкта доступу, а також підтримка з боку встаткування.

Клас С2 повинен забезпечувати керований доступ, а також ряди додаткових вимог. Зокрема, у системах цього класу обов'язкове ведення системного журналу, у якому повинні відзначатися події, пов'язані з безпекою системи. Сам журнал повинен бути захищений від доступу будь-яких користувачів, за винятком співробітників безпеки.

У системах класу В, що містить три підкласи, повинен бути повністю контрольований доступ. Повинен виконуватися ряд вимог, головним із яких є наявність гарно розробленої й документованої

формальної моделі ПБ, що вимагає дії вибірного й повноважного керування доступом до всіх об'єктів системи. Уводиться вимога керування інформаційними потоками відповідно до ПБ. ПБ – становить собою набір законів, правил і практичного досвіду, на основі яких будуються керування, захист і розподіл конфіденційної інформації.

Аналіз класів безпеки показує, що, чим він вище, тим більш тверді вимоги висуваються до системи.

Розроблені також основні вимоги до проектної документації.

Щодо стандартизації апаратних засобів ІС і телекомунікаційних мереж у США розроблені правила стандарту TEMPEST (Transient Electromagnetic Pulse Emanations Standard). Цей стандарт передбачає застосування спеціальних заходів захисту апаратури від паразитних випромінювань електромагнітної енергії, перехоплення якої може призвести до оволодіння охоронюваними відомостями. Стандарт TEMPEST забезпечує радіус контрольованої зони перехоплення порядку одного метра.

Це досягається спеціальними системотехнічними, конструктивними й програмно-апаратними рішеннями.

Керівні документи (до деякої міри аналогічні розробленим NCSC) в області захисту інформації розроблені Державною технічною комісією при Президенті. Вимоги цих документів обов'язкові для виконання тільки в державному секторі або комерційних організаціях, які обробляють інформацію, що містить державну таємницю. Для інших комерційних структур документи носять рекомендаційний характер.

В одному з документів, що має назву "Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем і вимоги щодо захисту інформації", наведена класифікація автоматизованих систем на класи за умовами їх функціонування з метою розробки й застосування обґрунтованих заходів щодо досягнення необхідного рівня безпеки. Установлюються дев'ять класів захищеності, кожен із яких характеризується певною мінімальною сукупністю вимог із захисту. Захисні заходи охоплюють підсистеми:

- керування доступом;
- реєстрації й обліку (ведення журналів і статистики);
- криптографічну (використання різних механізмів шифрування);
- забезпечення цілісності;
- законодавчих заходів;

фізичних заходів.

Досить важливе використання документа "Засобу обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Показники захищеності". У ньому визначені сім класів захищеності СВТ від несанкціонованого доступу до інформації. Найнижчий клас сьомий, найвищий - перший. Кожен клас успадковує вимоги захищеності від попереднього. Методики оцінки безпеки ІС як у США, так і в Росії дозволяють оцінити реальну безпеку інформаційної системи з віднесенням її до певного класу захищеності. Клас захищеності ІС – певна сукупність вимог із захисту засобів ІС від НСД до інформації.

Аналіз міжнародних стандартів з питань захисту інформації в КС

Усі стандарти й керівні документи можна поділити на дві групи:

- визначальні переліки обов'язкових послуг і механізмів безпеки;
- визначальні критерії оцінки захищеності систем.

Перша група включає стандарти, розроблені ISO і ECMA й призначені, в основному, для обліку вимог безпеки при розробці інших стандартів взаємодії відкритих і розподілених систем.

4.1.5. Стандарт ISO

Для забезпечення безпеки розподілених систем Міжнародна організація стандартів ISO (International Standard Organization) розробила доповнення до базової еталонної моделі взаємодії відкритих систем і випустила в 1988 році стандарт ISO 7498-2 Security Architecture (*Архітектура безпеки*).

Цей стандарт визначає загрози безпеки й установлює *вимоги до безпеки в середовищі взаємодії відкритих систем*.

Архітектура безпеки охоплює *загальний опис засобів захисту даних і методів*, пов'язаних з їх роботою. Захист передбачає:

- ідентифікацію абонентів;
- запобігання читання повідомлень будь-якими особами;
- захист трафіка від його аналізу сторонніми;
- виявлення перекручувань блоків даних;
- виявлення змін потоків повідомлень;
- керування методами кодування інформації (криптографії).

Однією з найважливіших складової архітектури безпеки є **ПБ**, тобто сукупність законів, правил і вимог, що регламентують діяльність організації з керування, захисту й розподілу “чутливої” інформації.

Реалізація формальної моделі ПБ будується з використанням так званої Довірчої обчислювальної бази (Trusted Computing Base-TCB), що включає загальні механізми внутрішнього захисту системи (апаратні, мікропрограмні й програмні), комбінація яких забезпечує реалізацію вимог ПБ, утворить базове середовище захисту й підтримує користувальницькі служби, необхідні в захищених КС.

**Вимоги стандарту ISO за номенклатурою послуг,
наданих системою безпеки**

Система безпеки відповідно до стандарту ISO повинна забезпечувати наступні послуги безпеки (табл. 4.2):

Таблиця 4.2

Розподіл послуг безпеки за рівнями еталонної моделі ISO

Послуги безпеки	Рівні еталонної моделі (OSI)						
	1	2	3	4	5	6	7
Автентифікація однорангового об'єкта			*	*			*
Автентифікація джерела даних			*	*			*
Контроль доступу			*	*			*
Конфіденційність з'єднання	*	*	*	*		*	*
Конфіденційність без установлення з'єднання		*	*	*		*	*
Конфіденційність виділеного поля						*	*
Конфіденційність трафіка		*	*				*
Цілісність з'єднання з відновленням				*			*
Цілісність з'єднання без відновлення			*	*			*
Цілісність виділеного поля із установленням з'єднання							*
Цілісність блоку даних без установлення з'єднання			*	*			*
Цілісність виділеного поля без							*

установлення з'єднання							
Доказ джерела							*
Доказ доставки							*

1. Автентифікація однорангового об'єкта – відбувається при встановленні з'єднання або під час обміну даними для підтвердження того, що одноранговий об'єкт є тим, за кого себе видає.

2. Автентифікація джерела даних. Ця послуга підтверджує, що джерелом блоку даних є саме той, хто очікувався. Дана послуга не запобігає дублюванню або модифікації блоків даних [11].

3. Контроль доступу, що запобігає несанкціонованому використанню ресурсів, доступних через середовище OSI. Не всі ресурси повинні бути ресурсами OSI. Контроль доступу може застосовуватися до деяких видів доступу (читання/запис даних, активізація інформаційних ресурсів, виконання операцій над ресурсами), або до всіх видів доступу до ресурсу [5].

4. Конфіденційність з'єднання, що забезпечує конфіденційність усіх даних користувача цього з'єднання.

5. Конфіденційність у режимі без установлення з'єднання, що забезпечує конфіденційність всіх даних користувача в окремому сервісному блоці даних.

6. Конфіденційність виділеного поля забезпечує конфіденційність певного поля в блоці даних з'єднання або сервісний блок даних у випадку режиму без установлення з'єднання.

7. Конфіденційність трафіка – запобігає одержанню інформації шляхом спостереження трафіка.

8. Цілісність з'єднання з відновленням – забезпечує цілісність всіх даних користувача цього з'єднання й дозволяє виявити модифікацію, підстановку або вилучення будь-яких даних або цілого сервісного блоку даних із можливим наступним відновленням.

9. Цілісність з'єднання без відновлення забезпечує ті ж можливості, що й попередня послуга, але без відновлення [15].

10. Цілісність виділеного поля в режимі із установленням з'єднання забезпечує цілісність виділеного поля даних користувача у всьому потоці сервісних блоків даних, переданих через це з'єднання, і виявить модифікацію, підстановку або вилучення цього поля.

11. Цілісність блоку даних у режимі без установлення з'єднання забезпечує цілісність окремого сервісного блоку даних і дозволяє виявити його модифікацію.

12. Цілісність виділеного поля в режимі без установлення з'єднання – дозволяє виявити модифікацію виділеного поля в окремому сервісному блоці даних.

13. Доказ джерела – полягає в наданні одержувачеві даних доказів (у вигляді даних) із запобіганням будь-якої спроби відправника заперечувати в результаті факт передачі [9].

14. Доказ доставки – полягає в наданні відправникові даних доказів (у вигляді даних) із запобіганням будь-якої спроби одержувача заперечувати згодом факт одержання даних.

4.1.6. Механізми безпеки

Механізми безпеки призначені для реалізації послуг безпеки. Виділяють наступні механізми безпеки:

механізми шифрування (забезпечують послуги конфіденційності, а також є елементами ряду інших механізмів);

механізми цифрового підпису (забезпечують послуги впізнавання й доказу);

механізми контролю доступу (реалізують послугу контролю доступу, забезпечують надання об'єктам відповідних прав доступу до ресурсів);

механізми цілісності даних (підтримують послуги цілісності й частково послуги доказу);

механізми обмінної автентифікації (послуга автентифікації однорангового об'єкта) [35];

механізми підстановки графіка (підтримують послуги конфіденційності графіка й запобігають аналізу трафіка);

механізми керування маршрутизацією (використовуються послугами конфіденційності) [44];

механізми арбітражу (для підтвердження деяких характеристик даних, переданих між об'єктами).

Керування безпекою

Керування безпекою в середовищі OSI включає ті функції, які не стосуються самої взаємодії систем, але які необхідні для підтримки безпеки їх взаємодії.

Функції безпеки можуть бути розділені на три більші групи:

- керування безпекою системи;
- керування послугами безпеки;
- керування механізмами безпеки.

Керування безпекою системи розглядає питання керування безпекою всього середовища OSI і включає функції:

- підтримки цілісності методики безпеки;
- взаємозв'язку з іншими функціями керування OSI і керування послугами й механізмами безпеки;
- керування механізмом подій безпеки, механізмом контролю безпеки й механізмом відновлення безпеки.

Механізм подій безпеки – включає фіксацію спроб порушення безпеки системи, а також може включати фіксацію нормальних подій, таких, як підключення об'єкта й т. п. Під керуванням цим механізмом розуміється встановлення граничних значень для включення сигналізації про події безпеки й повідомлення об'єктів про дані події.

Механізм контролю безпеки – передбачає перегляд і вивчення системних журналів, а також спостереження за функціонуванням системи з метою визначення достатності засобів її контролю на відповідність прийнятій методиці безпеки й процедурам обробки даних, виявлення порушень безпеки й виробіток рекомендацій з вивчення засобів контролю й процедур безпеки. Керування даним механізмом включає вибір подій безпеки, що заносяться в журнал безпеки, включення й відключення реєстрації подій безпеки й підготовка звітів про безпеку системи.

Механізм відновлення безпеки реалізує процедури відновлення на основі правил методики безпеки. Керування ним полягає у встановленні правил, що визначають дії системи при порушеннях безпеки, а також у повідомленні об'єктів про порушення в системі й втручанні адміністратора.

Керування послугами безпеки – реалізує керування окремими послугами безпеки (визначення й призначення необхідної послуги безпеки, визначення правил вибору конкретного механізму безпеки для необхідної послуги, узгодження параметрів механізмів безпеки, а також

виклик певних механізмів безпеки за допомогою функції керування механізмом безпеки).

Керування механізмом безпеки полягає в керуванні окремими механізмами безпеки.

Керування ключами має на увазі генерацію ключів з періодичністю, обумовленою необхідним рівнем безпеки, і їхнє поширення на об'єкти в реальних відкритих системах безпечним способом.

Керування шифруванням може включати взаємодія з керуванням ключами, визначення криптографічних параметрів і криптографічну синхронізацію.

Керування цифровими підписами й керування цілісністю даних пов'язані з керуванням ключами й визначають вибір криптографічних параметрів і алгоритмів, використання протоколу між взаємодіючими об'єктами й, можливо, третім об'єктом (арбітром).

Керування контролем доступу може включати поширення атрибутів безпеки (включаючи паролі) й підтримка списків контролю доступу або мандатів.

Керування впізнаванням визначає поширення паролів і ключів (використовуючи керування ключами) на об'єкти, що здійснюють упізнавання, і може включати використання протоколу між взаємодіючими об'єктами й об'єктами, що надають послуги впізнавання.

Керування підстановкою може визначати правила, використовувані, наприклад, для визначення частоти генерації фіктивних блоків даних і їх характеристик.

Керування маршрутизацією включає визначення каналів і підмереж, що вважаються безпечними щодо одного із критеріїв безпеки.

Керування арбітражем може включати поширення інформації про арбітрів і використання протоколу між арбітром і взаємодіючими об'єктами.

Архітектура безпеки включає необхідні технічні й програмні засоби, аналіз характеристик їхньої роботи.

Реалізація всіх вимог архітектури безпеки, відповідних стандарту ISO, досить важка. На сьогоднішній день систем безпеки, повністю відповідних ISO немає. Дані стандарти фактично є *мірою відповідності* реальних систем еталону.

4.1.7. Стандарти ЕСМА

Стандарти ЕСМА розроблені 9-ю Технічною групою 32-го Технічного комітету (TG9/TC32) ЕСМА (European Computer Manufacturers Association – Асоціація європейських виробників комп'ютерів).

Основний стандарт, що одержав назву TR/46 (Technical Report), був опублікований у липні 1988 року. У ньому приводиться деяка абстрактна модель, усередині якої визначаються стандарти безпечної взаємодії розподілених систем. Основними висновками цього документа є:

стандарти безпеки не повинні залежати від обраної ПБ;

підсистема безпеки у відкритих системах повинна розпізнавати різні області захисту, представлені різними адміністраторами.

Пізніше був розроблений стандарт ЕСМА-13 8 "Security in Open Systems – Data Elements and Service Definitions", що визначає послуги безпеки, що використовують у подальшій стандартизації. Цей стандарт призначений для розроблювачів стандартів прикладних служб. Цей стандарт показує, як додати засоби безпеки в розроблювальні додатки відповідно до загальної моделі і як досягти взаємодії (interoperability) з іншими додатками.

На рис. 4.23 подано схему захисту в розподіленій системі. Вона складається із трьох кілець захисту.

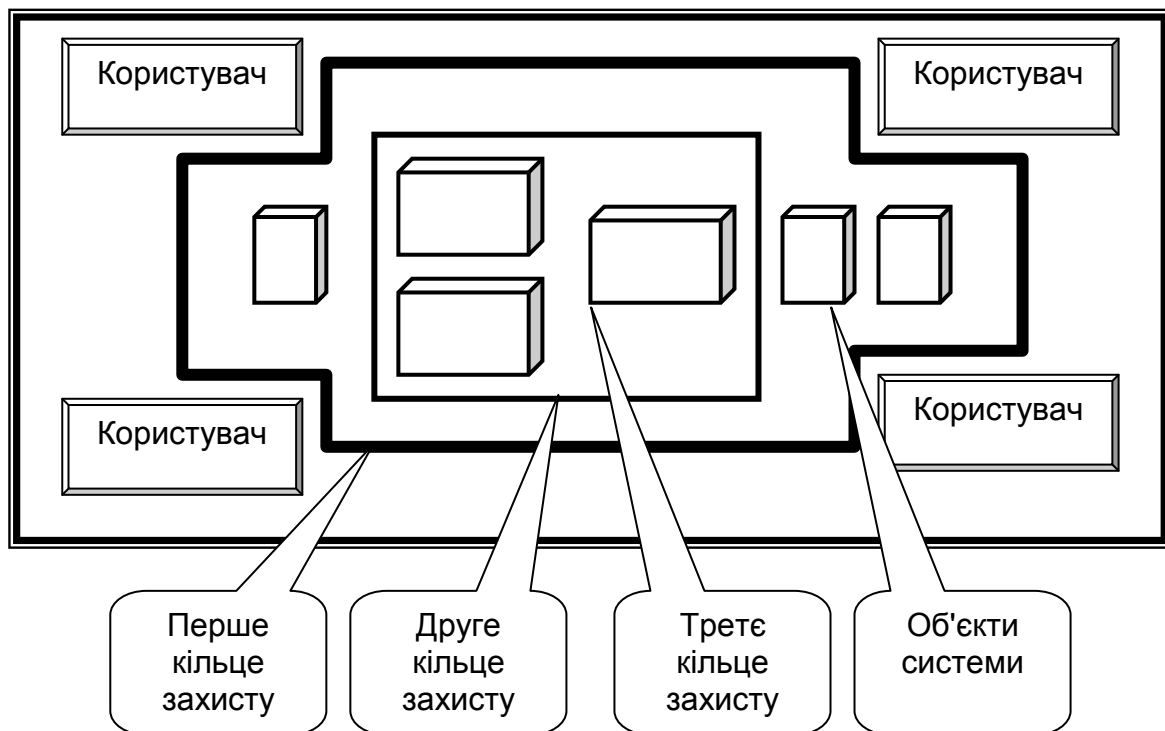


Рис. 4.23. Компоненти моделі ЕСМА

Перше кільце відокремлює користувачів від розподіленої системи. Сама розподілена система перебуває усередині першого кільця захисту й складається з об'єктів, які є суб'єктами керування безпекою.

Друге кільце безпеки оточує кожен із об'єктів, що входять до складу розподіленої системи. Це означає, що всі взаємодії об'єктів контролюються. Всі взаємодії об'єктів, що вимагають послуг безпеки, здійснюються через інфраструктуру безпеки, у якій ці об'єкти перебувають.

Третє кільце безпеки оточує внутрішні складові кожного об'єкта (дані й здатність обчислень). Модель дозволяє об'єктам мати своє внутрішнє керування доступом, забезпечуючи об'єкти необхідною інформацією й додатковими послугами. У безпеку, забезпечувану сама по собі об'єктом, інфраструктура не втручається, за винятком вимог творця об'єктів.

Ключова концепція моделі безпеки для відкритих розподілених систем полягає у використанні інформації про повноваження (security information). Інформація про повноваження генерується певними службами безпеки у відповідь на автентифіковані запити до них і потім використовується іншими службами безпеки для дозволу або заборони певних дій.

Інформація про повноваження є засіб, за допомогою якого відомості про повноваження (security knowledge) поширюються усередині розподіленої системи. Це означає, що ця інформація повинна бути надійною, а також її можна легко передавати будь-якому, навіть незахищеному об'єкту.

Інформація про повноваження, передана в розподіленій системі впакована й захищена від небажаного використання. Після одержання вона перевіряється одержувачем (звичайно, однією із служб безпеки) і потім використовується для визначення прав доступу. У цьому випадку інформація про повноваження використана для поширення довіри й привілеїв у розподіленій системі.

У рамках стандарту розроблений єдиний формат для передачі інформації про повноваження усередині розподіленої системи. Він називається **сертифікатом атрибутів привілеїв** (Privileged Attributes Certificate) – набір атрибутів привілеїв і інформації, що управляє їх використанням, що перебувають під криптографічним захистом.

Атрибути привілеїв (Privileged Attributes) – атрибути, пов'язані з об'єктом захисту, які використовуються разом із керуючими атрибутами при доступі до об'єкта, визначають права доступу суб'єкта стосовно цього об'єкта.

Керуючі атрибути (Control Attributes) – атрибути, пов'язані з об'єктом захисту й використовувани разом з атрибутами привілеїв для керування доступом до цього об'єкта.

Інформація про повноваження кодується як набір атрибутів безпеки, що збігаються з атрибутами, використовуваними в стандарті ISO "Information Processing Systems Open Systems Interconnection The Directory". Сам PAC захищений від зміни й незаконного використання.

Класи служб економічної безпеки (ЕБ), які передбачені в моделі ЕСМА, подані на рис. 4.24.

Клас служб **інформації про повноваження (Security Information Class)** створює інформацію про повноваження, використовувани усередині розподіленої системи. Він містить у собі служби автентифікації, атрибутів і обміну між областями безпеки.

Основне призначення *служби автентифікації* полягає в одержанні від користувача деяких "розпізнавальних знаків" (credentials), їх перевірці й видачі мандата (certified identity). Більшість механізмів автентифікації призначені для користувачів, однак вони можуть бути застосовані й до об'єктів. Для рішення проблеми автентифікації об'єктів і користувачів використовується концепція "поручителя об'єкта". Як поручитель для об'єкта виступає інфраструктура, що породжує об'єкт і виділяє ресурси для його існування. Для користувача в моделі передбачений "поручитель суб'єкта", функцією якого є з одного боку, взаємодія з користувачем з метою одержання його "розпізнавальних знаків" (пароль, біометричні ознаки й ін.), а, з іншого – взаємодія із службою автентифікації відповідним чином. *Служба автентифікації з "поручителем суб'єкта" утворить зовнішнє кільце захисту.*

Служба атрибутів призначена для читання мандата або установки привілеїв, що перевіряються, та деяких дій і повернення безлічі перевірених привілеїв. У моделі враховано, що синтаксис атрибутів може бути різним у різних частинах розподіленої системи. Ця служба також виконує перетворення подання PAC для різних середовищ (але не для різних областей). У різних областях безпеки (security domains) можуть бути реалізовані різні ПБ, а також області можуть управлятися

різними адміністраторами безпеки. Різні області безпеки будуть мати різні повноваження для підпису PAC, а також, можливе, розходження в синтаксисі й семантиці. Призначення *служби обміну між областями ЕБ* – перетворення формату PAC при переході з однієї області в іншу.

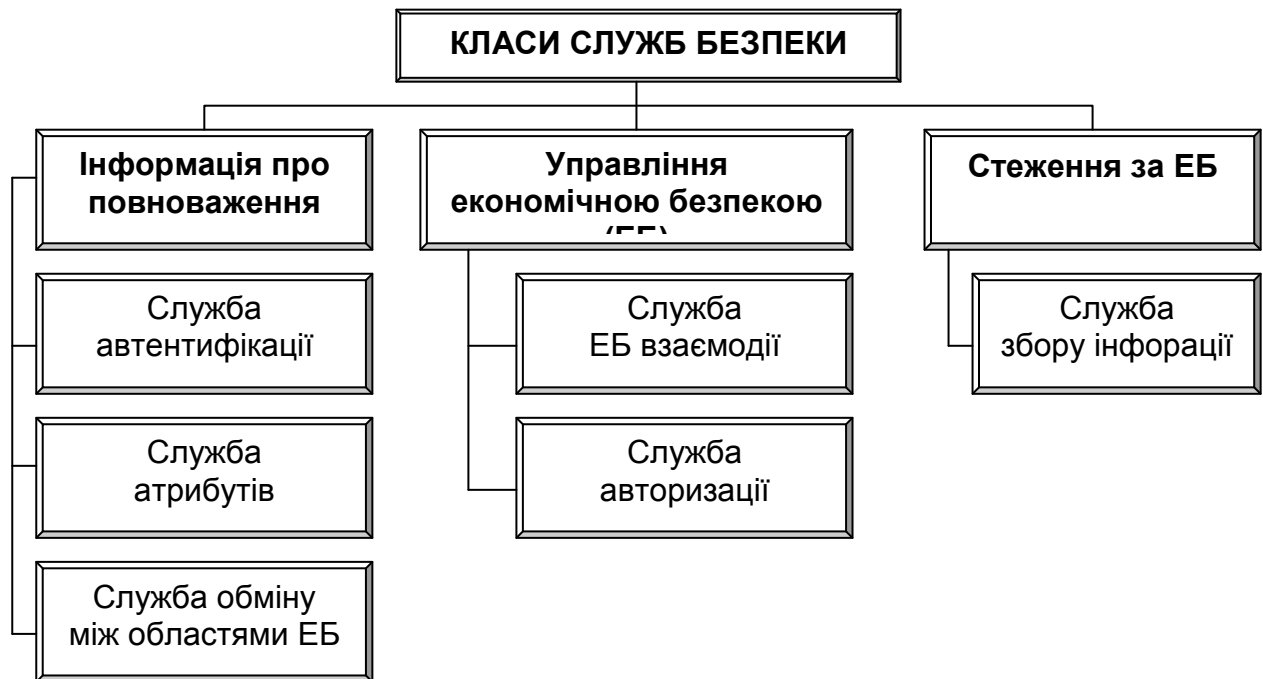


Рис. 4.24. Класи служб економічної безпеки

Клас **служб керування** (Security Control Class) забезпечує внутрішнє керування розподіленою системою. Він читає, перевіряє й інтерпретує інформацію про повноваження для керування діяльністю сутностей у розподілених системах.

Служба ЕБ взаємодії (Secure Assosiation Service) створена для забезпечення безпечного зв'язку, включаючи всю необхідну комунікаційну безпеку між двома будь-якими об'єктами системи незалежно від того, у якій області безпеки вони перебувають. Складова частина цієї служби перебуває на кожному кінці об'єднання. Передбачається, що взаємодія об'єктів неможлива без звертання до цієї служби.

Призначення *служби авторизації* – ухвалювати рішення щодо керування доступом. Вона зчитує атрибути привілеїв ініціатора, що управляють атрибутами мети, опису операції й іншу необхідну інформацію. Служба повертає результат рішення: "ТАК", "НІ" або "ПОМИЛКА". *Служби безпечної взаємодії й авторизації утворюють кільце безпеки навколо кожного об'єкта.*

Клас **служб спостереження за ЕБ** (Security Monitoring Class) забезпечує внутрішнє спостереження й керування безпекою в розподіленій системі в цілому. Він представлений тільки однією службою – службою збору інформації про безпеку системи (Security Audit Information Collection Service).

Служба збору інформації про безпеку системи призначена не тільки для збору деякої інформації, але також і для її обробки й аналізу та керування відновленням безпеки.

Модель безпеки, що відповідає стандарту TG9/TC32, передбачає мінімальні обмеження для розроблювача прикладних систем.

Головна особливість моделі полягає в тому, що ця модель незалежна від будь-якої ПБ або механізму керування доступом. Так, наприклад, вона підтримує вибірну політику (списки доступу) або повноважну політику безпеки.

Логічний сервіс моделі може бути реалізований різними шляхами: у вигляді окремих прикладних додатків на окремих комп'ютерах або у вигляді єдиної операційної системи на кожному з комп'ютерів.

Взаємодії між службами не обмежують розроблювача прикладних систем, що дозволяє йому самостійно вирішувати яким чином маніпулювати передачею інформації про привілеї для досягнення максимальної зручності для користувача.

Аналіз стандартів і керівництв другої групи показав спільність ідеї, що лежить в основі підходу до оцінки безпеки (ступеня захищеності) комп'ютерних систем. Суть її полягає в наступному. Для надання користувачам можливості обґрунтованого вибору систем обробки даних з погляду їх безпеки вводиться деяка система їхньої класифікації. Задається ієрархія функціональних класів безпеки. Кожному класу відповідає певна сукупність обов'язкових функцій безпеки. Конкретна комп'ютерна система ставиться до деякого класу безпеки, якщо в ній реалізовані всі відповідні йому функції безпеки і якщо вона не може бути віднесена до більш високого класу безпеки.

4.1.8. Система стандартів Міністерства оборони США в області комп'ютерної безпеки

У період з 1983 по 1988 рік у США Міністерством оборони (Department of Defense, DoD) і Національним комітетом з комп'ютерної безпеки (National Committee of Computer Security, NCSC) була розроблена система стандартів в області комп'ютерної безпеки. Вона включає наступні документи:

1. Комп'ютерні критерії оцінки систем (5200.28 STD) (Жовтогаряча книга).

2. Індустріальне керівництво захисту для охорони секретної інформації (5220.22 м) (Жовта книга).

3. Керівні принципи керування паролями (CSC-STD-002-85) (Зелена книга).

4. Критерії оцінки в певних середовищах (CSC-STD-003-85) (Жовта книга).

5. Керівництво в довірених системах (NCSC-TG-001, Версія-2) (Коричнева книга).

6. Довірена оцінка виробу (програми). Керівництво для продавців NCSC-TG-002, Версія -1 (Синя книга).

7. Глосарій комп'ютерних термінів захисту (NCSC-TG-004, Версія-1) (Голуба книга).

8. Довірена мережна інтерпретація (NCSC-TG-005, Версія-1) (Червона книга).

У документі виділені загальні вимоги щодо забезпечення безпеки оброблюваної інформації, потім визначений перелік показників (показники захищеності), що характеризують реалізацію загальних вимог. Сукупність цих показників визначає рівень безпеки розглянутої системи.

Документ визначає шість основних вимог безпеки. Чотири з них ставляться до керування доступом до інформації (ПБ, маркування, ідентифікація й облік), а два до надаваних гарантій (упевненість у системі й безперервність захисту).

Ці основні вимоги конкретизуються в показниках захищеності. У документі докладно описуються вимоги до реалізації кожного показника захищеності для відповідного класу.

Клас захищеності привласнюється системі при проходженні нею сертифікації. Під час сертифікації фахівці NCSC на підставі представлених вихідних текстів програм і документації на систему оцінюють рівень реалізації тієї або іншої можливості системи щодо захисту інформації.

Слід зазначити, що сертифікації підлягає вся система в цілому, а клас захищеності привласнюється тільки в тому випадку, коли "найслабкіший" показник задовольняє вимоги класу захищеності.

Нижче в порядку зростання переваги з погляду безпеки наведені наступні класи комп'ютерних систем (табл. 4.3).

Клас D: мінімальна захищеність. У клас D включаються ті системи, які не пройшли випробувань на більш високий рівень захищеності, а також системи, що використовують для захисту лише окремі функції (під-системи) безпеки.

Таблиця 4.3

Показники захищеності "Жовтогарячої книги"

№ з/п	Найменування показника	Клас захищеності					
		C1	C2	B1	B2	B3	A1
SECURITY POLICY							
1	Discretionary Access Control	+	+	+	=	=	=
2	Mandatory Access Control	-	-	+	+	=	--
3	Labels	-	-	+	+	=	=
4	Labels Integrity	-	-	+	=	=	=
5	Working Labels	-	-	-	+	=	=
6	Label Frequency	-	-	+	=	=	=
7	Object Reuse	-	+	=	+	=	=
8	Resource Encapsulation	-	+	=	-	-	-
9	Exported Machine Readable Output	-	-	+	=	=	=
10	Exported Human -Readable Labels	-	-	+	=	=	=
ACCOUNTABILITY							
11	Identification & Authentication	+	+	=	=	=	=
12	Audit	-	+	+	+	+	=
13	Trusted Path	-	-	-	+	=	=
ASSURANCE							
14	Design Specification & Verification	-	-	+	+	+	+
15	System Architecture	+	=	=	+	+	=
16	System Integrity	+	=	=	=	=	=
17	Security Testing	+	+	+	+	+	=
18	Trusted Recovery	-	-	-	-	+	=
19	Configuration Management	-	-	-	+	+	+
20	Trusted Facility Management	-	-	-	+	+	=
21	Trusted Distribution	-	-	-	-	+	=
22	Covert Channel Analysis	-	-	-	+	=	+
DOCUMENTATION							
23	Security Features User's Guide	+	=	=	=	=	=
24	Trusted Facility Manual	+	+	+	+	+	=
25	Test Documentation	+	=	=	+	=	+
26	Design Documentation	+	=	+	+	=	+

Клас С1: вибірний захист. Засоби захисту систем класу С1 задовольняють вимоги вибіркової політики керування доступом, забезпечуючи поділ користувачів і даних. Вибірною політикою керування доступом полягає в тому, що для кожного об'єкта й суб'єкта в системі чітко й недвозначно задається перелік припустимих типів доступу (читання, запис і ін.) суб'єкта до об'єкта. У системах цього класу обов'язкові ідентифікація й автентифікація суб'єкта доступу, а також підтримка з боку встаткування.

Клас С2: керований доступ. До вимог класу С1 додаються вимоги унікальної ідентифікації суб'єкта доступу, захисту за замовчуванням і реєстрацією подій. Унікальна ідентифікація означає, що будь-який користувач системи повинен мати унікальне ім'я. Захист за замовчуванням припускає призначення повноважень доступу користувача за принципом "усе, що не дозволено, те заборонено". Всі ті ресурси, які чітко не дозволені користувачеві, вважаються недоступними.

У системах цього класу обов'язкове ведення системного журналу, у якому повинні зазначатися події, пов'язані з безпекою системи. Дані журналу повинні бути захищені від доступу будь-яких користувачів, за винятком адміністратора системи.

Системи класу В. Системи класу В характеризуються реалізацією в них повноважної моделі керування доступом, при якій кожен суб'єкт і об'єкт системи забезпечується мітками конфіденційності й рішення на доступ суб'єкта до об'єкта приймається за певним правилом на основі зіставлення інформації, що містяться в обох мітках. При цьому встаткування повинне забезпечити цілісність міток безпеки й використання їх при розмежуванні доступу. У системах цього класу повинна бути реалізована концепція монітора посилань.

Клас В1: міточний захист. Мітки безпеки повинні бути привласнені всім суб'єктам і об'єктам системи, які можуть містити конфіденційну інформацію. При цьому повинна контролюватися відповідність міток на даних, експортованих із системи із пристроями, на які здійснюється вивід. Мітка безпеки на дані, що вводяться, запитується у користувача.

Клас В2: структурований захист. Додатково до вимог класу В1 висувається вимога наявності певної й документованої формальної моделі ПБ, що вимагає дії вибіркового й повноважного керування доступом до всіх об'єктів системи. Система повинна бути чітко поділена на

критичні й некритичні до захисту елементи. Також висуваються додаткові вимоги із захисту механізмів автентифікації. Інтерфейс із ТСВ повинен бути добре документований.

Клас В3: області безпеки. В системах цього класу в устаткуванні повинна бути реалізована концепція монітора посилань (reference monitor). Усі взаємодії суб'єктів з об'єктами повинні контролюватися монітором посилань. Із системи захисту повинен бути виключений код, що не потрібен для забезпечення підтримки ПБ. Механізми реєстрації подій безпеки повинні також повідомляти адміністратора й користувача про порушення безпеки.

Клас А1: верифікована розробка. Системи цього класу відрізняються від класу В3 тим, що для перевірки специфікацій застосовуються формальні методи.

Аналіз класів захищеності показує, що чим вище клас захищеності системи, тим жорсткіші вимоги щодо довіри системи. Це виражається не тільки в розширеному тестуванні можливостей системи й поданні розширеної документації, але й у використанні формальних методів перевірки правильності специфікацій програм і верифікації текстів програм.

Для цілей криптографічного захисту широко використовується стандарт DES, затверджений у США Національним інститутом стандартів і технологій (National Institute of Standards and Technologies – NIST).

Умовні позначення

"-" – немає вимог до даного класу,

"+" – нові або додаткові вимоги;

"=" – вимоги збігаються з вимогами до попереднього класу

4.2. Ідентифікація та автентифікація КС

З метою забезпечення можливості розмежування доступу до ресурсів АІС і можливості реєстрації подій такого доступу кожен суб'єкт (користувач, процес) і об'єкт (ресурс) автоматизованої системи, що захищається, повинен бути однозначно ідентифікований. Для цього в системі повинні зберігатися спеціальні ознаки кожного суб'єкта й об'єкта, за якими їх можна було б однозначно впізнати.

Ідентифікація – це, з одного боку, присвоєння індивідуальних імен, номерів чи спеціальних ідентифікаторів суб'єктам і об'єктам системи, з іншого – це їх розпізнавання (упізнання) за привласненим їм унікальним ідентифікатором. Наявність ідентифікатора дозволяє спростити процедуру виділення конкретного суб'єкта (визначений об'єкт) з безлічі однотипних суб'єктів (об'єктів). Найчастіше як ідентифікатори застосовуються умовні позначки у вигляді набору символів.

Автентифікація – це перевірка (підтвердження) дійсності ідентифікації суб'єкта чи об'єкта системи. Мета автентифікації суб'єкта – переконатися в тому, що він є саме тим, ким представився (ідентифікувався). Мета автентифікації об'єкта – переконатися, що це саме той об'єкт, який потрібний.

Автентифікація користувачів здійснюється зазвичай шляхом перевірки знання ними паролів (спеціальних секретних послідовностей символів), володіння якими-небудь спеціальними пристроями (картками, ключовими вставками і т. п.) з унікальними ознаками чи шляхом перевірки унікальних фізичних характеристик і параметрів (відбитків пальців, особливостей райдужної оболонки ока, форми п'ясті рук і т. п.) самих користувачів за допомогою спеціальних біометричних пристроїв.

При цьому до паролю висувають дві конфліктуючі вимоги: він повинен бути досить складним для розкриття і в той же час добре запам'ятовуватися. До цих вимог слід додати кілька рекомендацій з вибору пароля:

1. Пароль повинен включати не менше 6 – 7 символно-цифрових знаків. При цьому доцільно використовувати цифри і арабські, і римські, літери – і великі, і малі.

2. Пароль не повинен включати однакові цифри, літери, їх комбінації, що повторюються.

3. Як пароль не можна використовувати дату поточного дня, своє прізвище, ім'я, назви мультфільмів, книжок, фільмів, міст, ім'я літературних героїв, особисту інформацію: ім'я чоловіка, телефонний номер, номер автомобіля, кличку собаки, хобі, номер службового кабінету і т. ін.

4. Не використовуйте послідовність клавіш на клавіатурі.

5. Обирайте пароль, що не має ніякого смислового навантаження для вас.

Засоби ідентифікації й автентифікації повинні бути стійкими до мережних загроз та забезпечувати концепцію єдиного входу в мережу.

Уведення значень користувачем свого ідентифікатора і пароля здійснюється найчастіше з клавіатури. Але можуть використовуватися й інші типи ідентифікаторів – магнітні картки, радіочастотні безконтактні картки, смарт-карти, електронні таблетки Touch Memory.

Використання біометричних засобів дозволяє здійснювати ідентифікацію й автентифікацію людини одночасно. Біометричні методи (наприклад, сканування відбитків пальців) характеризуються, з одного боку, високим рівнем вірогідності впізнавання користувачів, а з іншого – можливістю помилок розпізнавання першого й другого роду (пропуск чи помилкова тривога) і більш високою вартістю реалізуючих їх систем.

Створення системи захисту інформації в корпоративній мережі ІС породжує цілий комплекс проблем. У комплексі корпоративна система захисту інформації повинна вирішувати наступні завдання:

- 1) забезпечення конфіденційності інформації;
- 2) захист від перекручування;
- 3) сегментування (поділ на частини) й забезпечення індивідуальності ПБ для різних сегментів системи;
- 4) автентифікація користувачів – процес достовірної ідентифікації ототожнення користувача, процесу або пристрою, логічних і фізичних об'єктів мережі для різних рівнів мережного керування;
- 5) протоколювання подій, дистанційний аудит, захист реєстраційних протоколів і ін.

Побудова системи інформаційної безпеки мережі ґрунтується на семирівневій моделі декомпозиції системного керування OSI/ISO. Відповідно до стандартів Міжнародної організації зі стандартизації (ISO), що розробляє стандарти взаємодії відкритих систем (OSI), виділяють сім рівнів мережної архітектури, що забезпечує передачу й обробку інформації в мережі. Така семирівнева модель забезпечує повний набір функцій, реалізований відкритою за стандартами ISO архітектурою мережі. Сім рівнів мережного керування включають: фізичний, каналний, мережний, транспортний, сеансовий, представницькі, прикладний рівні.

На *фізичному рівні*, що становить середовище поширення даних (кабель, оптоволокно, радіоканал, каналостворююче устаткування), застосовують зазвичай засоби шифрування або приховання сигналу.

Вони малозастосовні в комерційних відкритих мережах, тому що є більш надійне шифрування.

На *каналному рівні*, відповідальному за організацію взаємодії двох суміжних вузлів (двокрапкові ланки), можуть бути використані засоби шифрування й достовірної ідентифікації користувача. Однак використання й тих і інших засобів на цьому рівні може виявитися надлишковим. Не обов'язково робити шифрування на кожній двокрапковій ланці між двома вузлами.

Мережний рівень вирішує завдання поширення й маршрутизації пакетів інформації з мережі в цілому. Цей рівень критичний щодо реалізації засобів криптозахисту. Поняття пакета існує на цьому рівні. На більш високих рівнях є поняття повідомлення. Повідомлення може містити контекст або формуватися на прикладному рівні, захист якого ускладнений із погляду керування мережею. Мережний рівень може бути базовим для реалізації засобів захисту цього й нижчеподаних рівнів керування. До них належать: *транспортний* (управляє передачею інформації), *сеансовий* (забезпечує синхронізацію діалогу), *рівень подань* (визначає єдиний спосіб подання інформації зрозумілий користувачам і комп'ютерам), *прикладний* (забезпечує різні форми взаємодії прикладних процесів). Однак захист на мережному рівні не достатній, тому що невідомо, що за інформація впакована в пакети, не видно користувачів і процесів, що породжують цю інформацію. Ряд завдань захисту інформації лежить вище мережного рівня: шифрування й забезпечення вірогідності впізнавання (автентифікація) повідомлень (а не пакетів), обробка протоколу із забезпеченням його захисту, контроль доступу й дотримання повноважень, протоколювання подій. Керування рівнями вище мережного складне і різноманітне, тому розглянути можливі стратегії захисту інформації для них важко. Рішення може бути знайдене на шляху до пошуку єдиної технологічної бази, що володіє максимальною спільністю й поширеністю, для захисту інформації й мережної інтеграції розподілених користувальницьких додатків. Як засоби захисту інформації транспортного, сеансового й рівня подань (всі три перерахованих рівні називають *middleware*, використовується програмне забезпечення, наприклад, Teknekron Information Bus (TIB). Засоби захисту прикладного рівня в даному пункті не розглядаються. Використання єдиної, універсальної технології захисту інформації в мережах забезпечується програмним середовищем інтеграції додатків.

Це середовище забезпечує розвинене протоколювання подій, відстеження переміщення повідомлень по мережі, поділ повноважень користувачів, підтримку засобів шифрування й цифрового підпису й багато чого іншого. Програмно-технічні рішення в області платформ і протоколів захисту інформації в мережах можуть бути:

для технології "клієнт-сервер" найпоширенішим є варіант Unix (сервер) і Windows (клієнт);

ОС Unix містить вбудовану підтримку протоколів TCP/IP (Transport Control Protocol / Internet Protocol – транспортний протокол з контролем). Це один з важливих факторів технологічності інтеграції систем на основі цього протоколу й цієї операційної системи.

протокол TCP/IP має високу сумісність як із різними за фізичною природою, швидкісними характеристиками каналами, так і із широким колом апаратних платформ. Про користь протоколу TCP/IP говорить наявність найбільш розвинених технологій криптозахисту на мережному рівні. Завдання забезпечення безпеки в TCP/ IP-мережах вирішуються з будь-яким необхідним рівнем надійності.

Таким чином, архітектурну концепцію системи захисту інформації в мережах можна представити у вигляді трьох шарів: засобу захисту мережного рівня, middleware-системи й засоби захисту, пропоновані прикладними системами.

4.3. Методи та засоби ІЕБ в КС

Створення систем інформаційної безпеки (СІБ) в ІС і ІТ ґрунтується на наступних принципах:

Системний підхід до побудови системи захисту, що означає оптимальне поєднання взаємозалежних організаційних, програмних, апаратних, фізичних і інших властивостей, підтверджених практикою створення вітчизняних і закордонних систем захисту й застосовуваних на всіх етапах технологічного циклу обробки інформації.

Принцип безперервного розвитку системи. Цей принцип, що є одним із основних для комп'ютерних інформаційних систем, ще більш актуальний для СІБ. Способи реалізації загроз інформації в ІТ безупинно вдосконалюються, а тому забезпечення безпеки ІС не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні й реалізації найбільш раціональних методів, способів і

шляхів удосконалювання СІБ, безперервному контролю, виявленні її вузьких і слабких місць, потенційних каналів витоку інформації й нових способів несанкціонованого доступу.

Поділ і мінімізація повноважень з доступу до оброблюваної інформації й процедур обробки, тобто надання як користувачам, так і самим працівникам ІС мінімуму суворо певних повноважень, достатніх для виконання ними своїх службових обов'язків.

Повнота контролю й реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача й протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності при виникненні в системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів і обслуговуючого персоналу.

Забезпечення контролю за функціонуванням системи захисту, тобто створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення будь-яких засобів боротьби зі шкідливими програмами.

Забезпечення економічної доцільності використання системи захисту, що виражається в перевищенні можливого збитку ІС і ІТ від реалізації загроз над вартістю розробки й експлуатації СІБ.

У результаті вирішення проблем безпеки інформації сучасні ІС і ІТ повинні мати наступні основні ознаки:

- наявність інформації різного ступеня конфіденційності;
- забезпечення криптографічного захисту інформації різного ступеня конфіденційності при передачі даних;
- ієрархічність повноважень суб'єктів доступу до програм до компонентів ІС і ІТ (до файлів-серверів, каналів зв'язку й т. п.);
- обов'язковим керуванням потоками інформації як у локальних мережах, так і при передачі каналами зв'язку на далекі відстані;
- наявність механізму реєстрації й обліку спроб несанкціонованого доступу, подій в ІС і документів, виведених на друк;
- обов'язковість забезпечення цілісності ПЗ й інформації в ІТ;
- обов'язковість обліку магнітних носіїв;

наявність фізичної охорони засобів обчислювальної техніки й магнітних носіїв;

наявність спеціальної служби ІБ системи.

Під час розгляду *структури СІБ* можливий традиційний підхід – виділення забезпечуючих підсистем.

СІБ, як і будь-яка ІС, повинна мати певні види власного програмного забезпечення, опираючись на які вона буде здатна виконати свою цільову функцію.

1. *Правове забезпечення* – сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, керівництв, вимоги яких є обов'язковими в рамках сфери їх діяльності в системі захисту інформації.

2. *Організаційне забезпечення*. Мається на увазі, що реалізація ІБ здійснюється певними структурними одиницями, такими, наприклад, як служба безпеки фірми і її складових структур: режим, охорона й ін.

3. *Інформаційне забезпечення*, що включає в себе відомості, показники, параметри, що лежать в основі рішення завдань, що забезпечують функціонування СІБ. Сюди можуть входити як показники доступу, обліку, зберігання, так і інформаційне забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби безпеки.

4. *Технічне (апаратне) забезпечення*. Передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності СІБ.

5. *Програмне забезпечення*. Маються на увазі різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінку наявності й небезпеки різних каналів витоку та способів несанкціонованого доступу до інформації.

6. *Математичне забезпечення*. Це – математичні методи, використовувані для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів, які мають зловмисники, зон і норм необхідного захисту.

7. *Лінгвістичне забезпечення*. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері забезпечення ІБ.

8. *Нормативно-методичне забезпечення*. Сюди входять норми й регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації; різного роду методики, що забезпечують діяльність

користувачів при виконанні своєї роботи в умовах твердих вимог дотримання конфіденційності. Нормативно-методичне забезпечення може бути злите із правовим.

Слід зазначити, що із всіх мір захисту в цей час провідну роль відіграють *організаційні заходи*. Тому виникає питання про організацію служби безпеки. Реалізація ПБ вимагає настроювання засобів захисту, керування системою захисту й здійснення контролю за функціонуванням ІС.

Як правило, завдання керування й контролю вирішуються адміністративною групою, склад і розмір якої залежать від конкретних умов. Дуже часто в цю групу входять адміністратор безпеки, менеджер безпеки й оператори.

Забезпечення й контроль безпеки становлять собою комбінацію технічних і адміністративних мір. За даними закордонних джерел у співробітників адміністративної групи зазвичай 1/3 часу займає технічна робота й близько 2/3 – адміністративна (розробка документів, пов'язаних із захистом ІС, процедур перевірки системи захисту й т. д.). Розумне поєднання цих заходів сприяє зменшенню ймовірності порушень ПБ.

Адміністративну групу іноді називають групою ІБ. Ця група може бути організаційно злита з підрозділом, що забезпечує внутрішньомашинне інформаційне забезпечення, тобто з адміністратором БД. Але частіше вона відособлена від усіх відділів або груп, що займаються керуванням самої ІС, програмуванням і іншими стосовними до системи, завданнями, щоб уникнути можливого зіткнення інтересів.

До обов'язків співробітників, що входять у цю групу, повинне бути включене не тільки виконання директив вищого керівництва, але й участь у вирішенні всіх питань, пов'язаних із процесом обробки інформації з погляду забезпечення його захисту. Всі їхні розпорядження, що стосуються цієї області, обов'язкові до виконання співробітниками всіх рівнів і організаційних ланок ІС і ІТ.

Нормативи й стандарти щодо захисту інформації накладають вимоги на побудову ряду компонентів, які традиційно входять у забезпечуючі підсистеми самих ІС, тобто можна говорити про наявність тенденції до злиття забезпечуючих підсистем ІС і СІБ.

Прикладом може служити використання ОС – основи системного ПЗ ІС. У різних країнах виконана безліч досліджень з аналізу й

класифікації вад захисту ІС. Виявлено, що основні недоліки захисту ІС зосереджені в ОС. Використання захищених ОС є однією з найважливіших умов побудови сучасних ІС.

Складено зведені таблиці характеристик і параметрів операційних систем, що пройшли оцінку відповідно до вимог Міністерства оборони США й Жовтогарячої книги. Особливо важливі вимоги до ОС, орієнтовані на роботу з локальними й глобальними мережами. Розвиток Internet зробив особливо значний вплив на розробку захищених ОС. Розвиток мережних технологій привело до появи великої кількості мережних компонентів. Системи, що пройшли сертифікацію без обліку вимог до мережного програмного забезпечення, у цей час часто використовуються в: мережному оточенні й навіть підключаються до Internet. Це приводить до появи вад, не виявлених при сертифікації захищених обчислювальних систем, що вимагає безперервної доробки ОС.

Найбільш захищеними вважалися ОС на базі UNIX, але й вони зажадали істотної переробки щодо захисту.

Зареєстровано численні атаки на популярну операційну систему Windows NT через її мережні компоненти, що привело до необхідності безперервної доробки й найпоширенішої в цей час ОС.

Зажадали вдосконалювання й існуючі стандарти й норми, що стосуються захисту інформації. Наприклад, у додавання до Жовтогарячої книги з'явилися спеціальні вимоги міністерства оборони США для мережних компонентів.

У найбільшій мережі світу Internet атаки на комп'ютерні системи прокочуються, як цунамі, не знаючи ні державних кордонів, ні расових або соціальних розходжень. Іде постійна боротьба інтелекту, а також організованості системних адміністраторів і винахідливості хакерів. Розроблена корпорацією Microsoft операційна система Windows NT як основу ІС одержує все більшого поширення. І, звичайно, хакери всього світу звернули на неї пильну увагу.

У міру появи повідомлень про уразливі місця в Windows NT корпорація Microsoft швидко створює спочатку латки (hotfixes), а потім пакети відновлення (service packs), що допомагають захистити операційну систему. У результаті Windows NT постійно змінюється в кращий бік. Зокрема, у ній з'являється усе більше можливостей для побудови мережі, дійсно захищеної від несанкціонованого доступу до інформації.

Методи й засоби забезпечення безпеки інформації в ІС схематично подані на рис. 4.25.

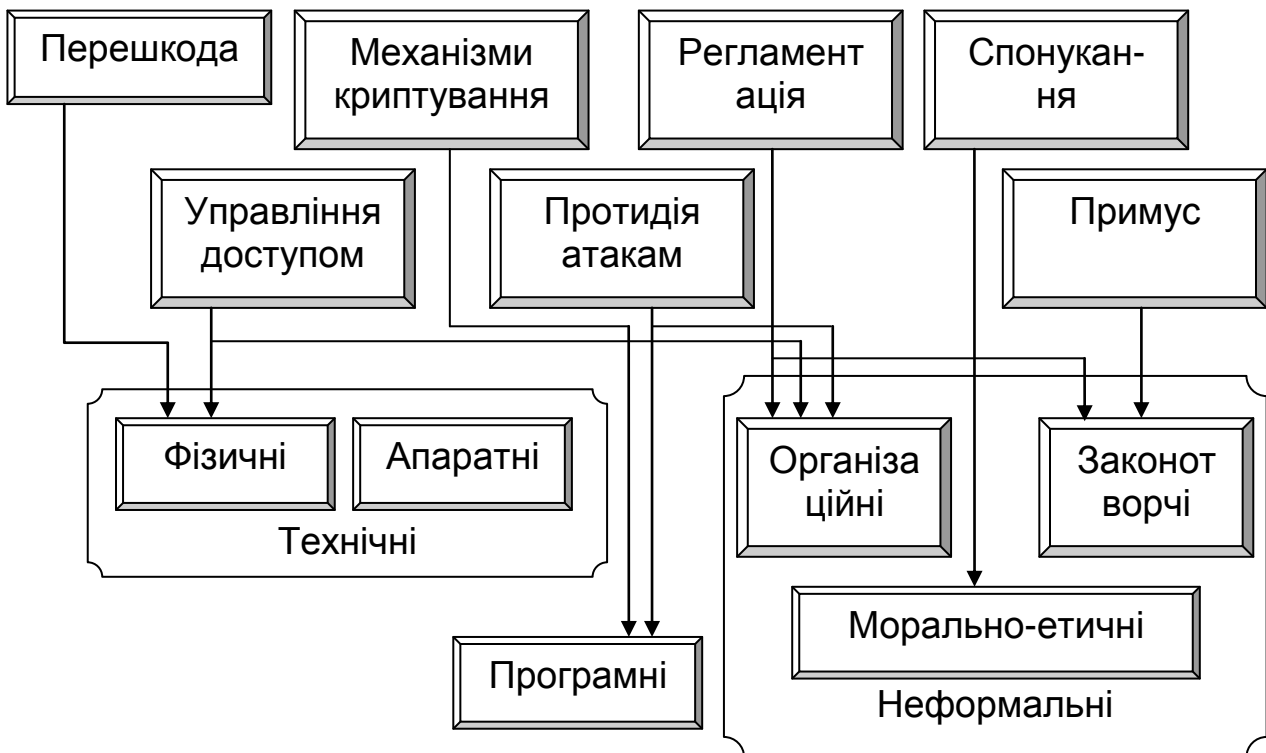


Рис. 4.25. **Методи та засоби забезпечення безпеки інформації**

Перешкода – метод фізичного перегородження шляхів зловмисникові для захисту інформації (до апаратури, носіям інформації й т. д.).

Керування доступом – методи захисту інформації регулюванням використання всіх ресурсів ІС і ІТ. Ці методи повинні протистояти всім можливим шляхам несанкціонованого доступу до інформації. Керування доступом включає наступні функції захисту:

ідентифікацію користувачів, персоналу й ресурсів системи (присвоєння кожному об'єкту персонального ідентифікатора);

упізнання (установлення дійсності) об'єкта або суб'єкта за пред'явленим ідентифікатором;

перевірку повноважень (перевірка відповідності дня тижня, часу доби, запитуваних ресурсів і процедур установленому регламенту);

дозвіл і створення умов роботи в межах установленого регламенту;

реєстрацію (протоколювання) звертань до захищених ресурсів;

реагування (сигналізація, відключення, затримка робіт, відмова в запиті й т. п.) при спробах несанкціонованих дій.

Механізми шифрування – криптографічне закриття інформації. Ці методи захисту усе ширше застосовуються як при обробці, так і при зберіганні інформації на магнітних носіях. Під час передачі інформації каналами зв'язку за великої відстані цей метод є єдино надійним.

Протидія атакам шкідливих програм припускає комплекс різноманітних заходів організаційного характеру й використання антивірусних програм. Цілі прийнятих заходів – це зменшення ймовірності інфікування АІС, виявлення фактів зараження системи; зменшення наслідків інформаційних інфекцій, локалізація або знищення вірусів; відновлення інформації в ІС. Оволодіння цим комплексом засобів вимагає знайомства зі спеціальною літературою [43].

Регламентація – створення таких умов автоматизованої обробки, зберігання й передачі захищеної інформації, при яких норми й стандарти із захисту виконуються найбільшою мірою.

Примус – метод захисту, при якому користувачі й персонал ІС змушені дотримуватися правил обробки, передачі й використання захищеної інформації, що під погрозою матеріальної, адміністративної або кримінальної відповідальності.

Спонування – метод захисту, що спонукує користувачів і персонал ІС не порушувати встановлені порядки за рахунок дотримання сформованих моральних і етичних норм.

Уся сукупність технічних засобів підрозділяється на апаратні й фізичні.

Апаратні засоби – пристрої, що вбудовуються безпосередньо в обчислювальну техніку, або пристрої, які сполучаються з нею за стандартним інтерфейсом.

Фізичні засоби включають різні інженерні пристрої й прилади, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту й здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій. Приклади фізичних засобів: замки на дверях, ґрати на вікнах, засоби електронної охоронної сигналізації й т. п.

Програмні засоби – це спеціальні програми й програмні комплекси, призначені для захисту інформації в ІС. Як було зазначено вище багато хто з них злиті з ПЗ самої ІС. Із засобів ПЗ системи захисту виділимо ще програмні засоби, що реалізують механізми шифрування (криптографії).

Криптографія – це наука про забезпечення таємності й/або автентичності (дійсності) переданих повідомлень.

Організаційні засоби здійснюють регламентацію виробничої діяльності в ІС і взаємин виконавців на нормативно-правовій основі таким чином, що розголошення, витік і несанкціонований доступ до конфіденційної інформації стають неможливими або істотно ускладнюються за рахунок проведення організаційних заходів. Комплекс цих заходів реалізується групою інформаційної безпеки, але повинен перебувати під контролем першого керівника.

Законотворчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, обробки й передачі інформації обмеженого доступу й устанавлюються міри відповідальності за порушення цих правил.

Морально-етичні засоби захисту включають будь-які норми поведження, які традиційно склалися раніше, складаються в міру поширення ІС і ІТ у країні й у світі або спеціально розробляються. Морально-етичні норми можуть бути неписані (наприклад, чесність) або оформлені в який-небудь звід (устав) правил або приписань. Ці норми, як правило, не є законодавчо затвердженими, але оскільки їхнє недотримання приводить до зниження престижу організації, вони вважаються обов'язковими для виконання. Характерним прикладом таких приписань є Кодекс професійного поведження членів Асоціації користувачів ПК США.

4.3.1. Криптографічні методи захисту інформації

Готове до передачі інформаційне повідомлення спочатку відкрите й незахищене, зашифровується й тим самим перетворюється в шифрограму, тобто в закритий текст або графічне зображення документа. У такому вигляді повідомлення передається каналом зв'язку, навіть і не захищеним. Санкціонований користувач після одержання повідомлення дешифрує його (тобто розкриває) за засобами зворотного перетворення криптограми, внаслідок чого виходить вихідний, відкритий вид повідомлення, доступний для сприйняття санкціонованим користувачам.

Методу перетворення в криптографічній системі відповідає використання спеціального алгоритму. Дія такого алгоритму

запускається унікальним числом (послідовністю біт), зазвичай називаним ключем, що шифрує.

Для більшості систем схема генератора ключа може становити собою набір інструкцій і команд або вузол апаратури, або комп'ютерну програму, або все це разом, але в кожному разі процес шифрування (дешифрування) реалізується тільки цим спеціальним ключем. Щоб обмін зашифрованими даними проходив успішно, як відправникові, так і одержувачеві необхідно знати правильну ключову установку й зберігати її в таємниці.

Стійкість будь-якої системи закритого зв'язку визначається ступенем таємності використовуваного в ній ключа. Проте цей ключ повинен бути відомий іншим користувачам мережі, щоб вони могли вільно обмінюватися зашифрованими повідомленнями. У цьому змісті криптографічні системи також допомагають вирішити проблему автентифікації (встановлення дійсності) прийнятої інформації. Зломщик у випадку перехоплення повідомлення буде мати справу тільки із зашифрованим текстом, а правдивий одержувач, приймаючи повідомлення, закриті відомим йому й відправникові ключем, буде надійно захищений від можливої дезінформації.

Сучасна криптографія знає два типи криптографічних алгоритмів: класичні алгоритми, засновані на використанні закритих, секретних ключів, і нові алгоритми з відкритим ключем, у яких використовуються один відкритий і один закритий ключ (ці алгоритми називаються також асиметричними). Крім того, існує можливість шифрування інформації й більш простим способом – з використанням генератора псевдовипадкових чисел.

Використання генератора псевдовипадкових чисел полягає в генерації гами шифру за допомогою генератора псевдовипадкових чисел при певному ключі й накладенні отриманої гами на відкриті дані оборотним способом.

Надійність шифрування за допомогою генератора псевдовипадкових чисел залежить як від характеристик генератора, так і, причому більшою мірою, від алгоритму одержання гами.

Цей метод криптографічного захисту реалізується досить легко й забезпечує досить високу швидкість шифрування, однак недостатньо стійкий до дешифрування й тому не застосовуємо для таких серйозних інформаційних систем, якими є, наприклад, банківські системи.

Для класичної криптографії характерне використання однієї секретної одиниці – ключа, що дозволяє відправникові зашифрувати повідомлення, а одержувачеві розшифрувати його. У випадку шифрування даних, збережених на магнітному або іншому носіях інформації, ключ дозволяє зашифрувати інформацію за записом на носій і розшифрувати при читанні з нього.

Існує досить багато різних алгоритмів криптографічного захисту інформації. Серед них можна назвати алгоритми DES, Rainbow (США); FEAL-4 і FEAL-8 (Японія); B-Crypt (Великобританія); алгоритм шифрування за ДСТ 28147 - 89 (Росія) і ряд іншими, реалізованими закордонними й вітчизняними постачальниками програмних і апаратних засобів захисту. Розглянемо основні з них, найбільш широко застосовувані в закордонній і вітчизняній практиці. Алгоритм, викладений у стандарті DES (Data Encryption Standard), найпоширеніший і широко застосовується для шифрування даних у США. Цей алгоритм був розроблений фірмою IBM для власних цілей. Однак після перевірки Агентством національної безпеки США він був рекомендований до застосування як федеральний стандарт шифрування. Цей стандарт використовується багатьма недержавними фінансовими інститутами, у тому числі банками й службами обігу грошей. Лише деякі дані, методи захисту яких визначаються спеціальними актами, не захищаються стандартом DES.

Алгоритм DES не є закритим, і був опублікований для широкого ознайомлення, що дозволяє користувачам вільно застосовувати його для своїх цілей.

При шифруванні застосовується 64-розрядний ключ, але використовуються тільки 56 розрядів ключа, а інші вісім розрядів є контрольними.

Алгоритм DES досить надійний. Він має велику гнучкість при реалізації різних додатків обробки даних, тому що кожен блок даних шифрується незалежно від інших. Це дозволяє розшифровувати окремі блоки зашифрованих повідомлень або структури даних, а отже, відкриває можливість незалежної передачі блоків даних або довільного доступу до зашифрованих даних. Алгоритм може реалізовуватися як програмним, так і апаратним способами. Істотний недолік цього алгоритму – мала довжина ключа.

Алгоритм шифрування, обумовлений російським стандартом ДЕРЖСТАНДАРТ 28147-89, є єдиним алгоритмом криптографічного захисту даних.

Цей алгоритм може реалізовуватися як апаратним, так і програмним способами, задовольняє всім криптографічним вимогам, що склалися у світовій практиці, і, як наслідок, дозволяє здійснювати криптографічний захист будь-якої інформації, незалежно від ступеня її таємності. В алгоритмі ДЕРЖСТАНДАРТ 28147-89, на відміну від алгоритму DES, використовується 256-розрядний ключ, що представляється у вигляді восьми 32-розрядних чисел. Розшифровуються дані за допомогою того ж ключа, за допомогою якого вони були зашифровані. Алгоритм ДЕРЖ-СТАНДАРТ 28147-89 повністю задовольняє всім вимогам криптографії й має ті ж переваги, що й інші алгоритми (наприклад, DES), але позбавлений їх недоліків. Він дозволяє виявляти як випадкові, так і навмисні модифікації зашифрованої інформації. Основні недоліки цього алгоритму – більша складність його програмної реалізації й дуже низька швидкість роботи.

Найбільш перспективними системами криптографічного захисту даних сьогодні вважаються асиметричні криптосистеми, які називаються також системами з відкритим ключем. Їх суть полягає в тому, що ключ, використовуваний для зашифрування, відмінний від ключа розшифрування. При цьому ключ зашифрування не секретний і може бути відомий всім користувачам системи. Однак розшифрування за допомогою відомого ключа неможливе. Для розшифрування використовується спеціальний секретний ключ. Знання відкритого ключа не дозволяє визначити ключ секретний. Таким чином, розшифрувати повідомлення може тільки його одержувач, що володіє цим секретним ключем.

Суть криптографічних систем з відкритим ключем зводиться до того, що в них використовуються так звані необоротні функції (іноді їх називають одnobічними або односпрямованими), які характеризуються наступною властивістю: для даного вихідного значення за допомогою деякої відомої функції досить легко обчислити результат, але розрахувати за цим результатом вихідне значення надзвичайно складно. Відомо кілька криптосистем з відкритим ключем. Найбільш розроблена на сьогодні система RSA, запропонована ще в 1978 р. Алгоритм RSA названий за першими буквами прізвищ його авторів: Р. Л. Райвеста (R L.

Rivest), А. Шамира (A. Shamir) і Л. Адлемана (L. Adleman). RSA – це система колективного користування, у якій кожен з користувачів має свої ключі зашифрування й розшифрування даних, причому секретно тільки ключ розшифрування.

Фахівці вважають, що системи з відкритим ключем більше підходять для шифрування переданих даних, ніж для захисту даних, збережених на носіях інформації. Існує ще одна властивість застосування цього алгоритму – цифрові підписи, що підтверджують дійсність переданих документів і повідомлень.

Асиметричні криптосистеми найбільш перспективні, тому що для них не використовується передача ключів іншим користувачам і вони реалізуються як апаратним, так і програмним способами системи типу RSA, працюють приблизно в тисячу разів швидше ніж класичні, і вимагають довжини ключа близько 3000 біт. Тому всі їх переваги зводяться до низької швидкості роботи. Крім того, для ряду функцій знайдені алгоритми функцій, тобто доведено, що вони не є необоротними, використовуваних у системі RSA, але немає й суворого доказу необоротності використовуваних функцій. Останнім часом все частіше виникає питання про заміну в системах передачі й обробки інформації рукописного підпису, що підтверджує дійсність того або іншого документа, її електронним аналогом – електронним цифровим підписом (ЕЦП). Нею можуть скріплюватися будь-які електронні документи, починаючи з різних повідомлень і закінчуючи контрактами. ЕЦП може застосовуватися також для контролю доступу до особливо важливої інформації. ДО ЕЦП висуваються дві основні вимоги: висока складність фальсифікації й легкість перевірки.

Для реалізації ЕЦП можна використовувати як класичні криптографічні алгоритми, так і асиметричні, причому саме останні мають всі властивості, необхідні для ЕЦП.

Однак ЕЦП надзвичайно піддана дії узагальненого класу програм "троянський кінь" з навмисно закладеними в них потенційно небезпечними наслідками, що активізуються за певних умов. Наприклад, у момент зчитування файлу, у якому перебуває підготовлений до підпису документ, ці програми можуть змінити ім'я особи, що підписується, дату, які-небудь дані (наприклад, суму в платіжних документах) і т. п.

Тому при виборі системи ЕЦП перевага безумовно повинна бути віддана її апаратній реалізації, що забезпечує надійний захист інформації від НСД, виробіток криптографічних ключів і ЕЦП.

З викладеного випливає, що надійна криптографічна система повинна задовольняти ряд певних вимог:

процедури зашифрування й розшифрування повинні бути "прозорі" для користувача;

дешифрування закритої інформації повинне бути максимально ускладнено;

зміст переданої інформації не повинен позначатися на ефективності криптографічного алгоритму;

надійність криптозахисту не повинна залежати від змісту в секреті самого алгоритму шифрування (прикладом цього є як алгоритм DES, так і алгоритм ДЕРЖСТАНДАРТ 28147- 89).

Процеси захисту інформації, шифрування й дешифрування пов'язані з кодованими об'єктами й процесами, їхніми властивостями, особливостями переміщення. Такими об'єктами й процесами можуть бути матеріальні об'єкти, ресурси, товари, повідомлення, блоки інформації, транзакції (мінімальні взаємодії з базою даних по мережі). Кодування, крім цілей захисту, підвищуючи швидкість доступу до даних, дозволяє швидко визначати й виходити на будь-який вид товару й продукції, країну-виробника й т. д. У єдиний логічний ланцюжок пов'язуються операції, що належать до однієї угоди, але географічно розкидані по мережі.

Наприклад, штрихове кодування використовується як різновид автоматичної ідентифікації елементів матеріальних потоків, наприклад товарів, і застосовується для контролю за їх рухом у реальному часі. Досягається оперативність керування потоками матеріалів і продукції, підвищується ефективність керування підприємством. Штрихове кодування дозволяє не тільки захистити інформацію, але й забезпечує високу швидкість читання й запису кодів. Поряд зі штриховими кодами з метою захисту інформації використовують голографічні методи.

Методи захисту інформації з використанням голографії є актуальним напрямком, що розвивається. Голографія становить розділ науки й техніки, що займається вивченням і створенням способів, пристроїв для запису й обробки хвиль різної природи. Оптична голографія заснована на явищі інтерференції хвиль. Інтерференція

хвиль спостерігається при розподілі в просторі хвиль і повільному просторовому розподілі результуючої хвилі. Виникаюча при інтерференції хвиль картина містить інформацію про об'єкт. Якщо цю картину фіксувати на світлочутливій поверхні, то утвориться голограма. При опроміненні голограми або її ділянки опорною хвилею можна побачити об'ємне тривимірне зображення об'єкта. Голографія застосовна до хвиль будь-якої природи й у цей час знаходить все більше практичне застосування для ідентифікації продукції різного призначення.

Технологія застосування кодів у сучасних умовах переслідує цілі захисту інформації, скорочення трудовитрат і забезпечення швидкості її обробки, економії комп'ютерної пам'яті, формалізованого опису даних на основі їх систематизації й класифікації.

У сукупності кодування, шифрування й захист даних запобігають перекручуванню інформаційного відображення реальних виробничо-господарських процесів, руху матеріальних, фінансових і інших потоків, а отже сприяють обґрунтованості формування й прийняття управлінських рішень.

4.3.2. Етапи розробки систем захисту

При первісній розробці й реалізації системи захисту ІС, звичайно, виділяють три стадії.

Перша стадія – виробіток вимог включає:

виявлення й аналіз уразливих в ІС і ІТ елементів, які можуть піддатися загрозам;

виявлення або прогнозування загроз, яким можуть піддатися уразливі елементи ІС;

аналіз ризику.

Вартісне вираження ймовірної події, що веде до втрат, називають ризиком. Оцінки ступеня ризику у випадку здійснення того або іншого варіанта загроз, виконувані за спеціальними методиками, називають аналізом ризику.

На *другій стадії* – визначення способів захисту – приймаються рішення про те:

які загрози повинні бути усунуті і якою мірою;

які ресурси ІС повинні бути захищені й у якій мірі;

за допомогою яких засобів повинен бути реалізований захист;

яка повинна бути вартість реалізації захисту й витрати на експлуатацію ІС із урахуванням захисту від потенційних загроз.

Друга стадія передбачає розробку плану захисту й формування ПБ, що повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведження системи в різних ситуаціях.

План захисту містить наступні розділи (групи відомостей):

1. Поточний стан системи (як результат роботи першої стадії).
2. Рекомендації з реалізації системи захисту.
3. Відповідальність персоналу.
4. Порядок запровадження в дію засобів захисту.
5. Порядок перегляду плану й складу захисту.

ПБ становить деякий набір вимог, що пройшли відповідну перевірку, реалізованих за допомогою організаційних мір і програмно-технічних засобів та визначальну архітектуру системи захисту. Для конкретних організацій ПБ повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації й т. д.

Третя стадія – побудова системи ІБ, тобто реалізація механізмів захисту як комплексу процедур, і засобів забезпечення безпеки інформації. Наприкінці виробляється оцінка надійності системи захисту, тобто рівня забезпечуваної нею безпеки.

Функціонування системи ІБ спрямовано на реалізацію принципу безперервного розвитку. За необхідністю з певною періодичністю аналізувати поточний стан системи й вводити в дію нові засоби захисту. Щодо цього цікава практика захисту інформації в США.

Американський фахівець в області безпеки інформації А. Патток пропонує концепцію системного підходу до забезпечення захисту конфіденційної інформації, що одержала назву "метод OpSec" (Operation Security).

Суть методу полягає в тому в тім, щоб припинити, запобігти або обмежити витік тієї частини інформації, що дозволить конкурентові визначити, що здійснює або планує підприємство.

Процес організації захисту інформації з методу OpSec проводиться регулярно й щоразу поетапно.

Перший етап (аналіз об'єкта захисту) полягає у визначенні того, що потрібно захищати.

Аналіз проводиться за наступними напрямками:

визначається інформація, що має потребу в захисті;

виділяються найбільш важливі елементи (критичні) захищеної інформації;

визначається строк існування критичної інформації (час, не обходжений конкурентові для реалізації отриманої інформації);

визначаються ключові елементи інформації (індикатори), що відбивають характер охоронюваних відомостей;

класифікуються індикатори за функціональними зонами підприємства (виробничо-технологічні процеси, система матеріально-технічного забезпечення виробництва, підрозділу керування й т. д.).

Другий етап передбачає виявлення загроз:

визначається, кого може зацікавити захищена інформація;

оцінюються методи, використовувані конкурентами для одержання цієї інформації;

оцінюються ймовірні КВІ;

розробляється система заходів щодо припинення дій конкурента або будь-якого зломщика.

На *третьому етапі* проводиться аналіз ефективності прийнятих і постійно діючих підсистем забезпечення безпеки (фізична безпека документації, надійність персоналу, безпека використовуваних для передачі конфіденційної інформації ліній зв'язку й т. д.).

На *четвертому етапі* визначаються необхідні міри захисту. На підставі проведених на перших трьох етапах аналітичних досліджень виробляються необхідні додаткові заходи й засоби із забезпечення безпеки підприємства.

На *п'ятому етапі* керівниками фірми (організації) розглядаються подані пропозиції за всіма необхідними мірами безпеки й розрахунки їх вартості й ефективності.

Шостий етап полягає в реалізації вжитих додаткових заходів безпеки з урахуванням установлених пріоритетів.

Сьомий етап припускає контроль і доведення до персоналу фірми реалізованих заходів безпеки.

Слід зазначити, що розглянутий метод вимагає участі в його реалізації групи аналітиків із числа досвідчених фахівців як в області інформатики, так і в тих областях знань, які необхідні для проведення аналізу.

4.3.3. Критерії та особливості проектування оптимальної СЗІ

Маючи всі необхідні вхідні дані для моделі СЗІ, необхідно приступити до проектування оптимальної системи захисту інформації.

Метою побудови СЗІ є мінімізація інформаційних ризиків для об'єктів захисту. Як цільова функція захищеності, що характеризує ризик для інформаційних ресурсів, введемо *відносний потенційний збиток E* (2.1), що характеризує потенційний збиток від впливу сукупності виявлених джерел загроз, загроз і уразливостей об'єктів захисту з урахуванням витрат, пов'язаних з використанням СЗІ. Проте створення в ІС додаткової підсистеми, яка вирішує завдання захисту інформації, призводить до зниження її функціональності (обмеження функцій ІС, для яких неможливо або важко створити механізм захисту) і продуктивності (збільшення часу доступу до об'єктів захисту). Цю ситуацію можна наочно показати трикутником суперечностей трьох показників (рис. 4.26).

Захищеність ІС Z можна подати як функцію, залежну від відносного потенційного збитку при реалізації загроз, функціональності та продуктивності ІС:

$$Z = f(E, N_f, T_a), \quad (2.1)$$

де E – відносний потенційний збиток при реалізації загроз;

N_f – кількість функцій ІС, що характеризують функціональність ІС;

T_a – середній час доступу до об'єктів захисту ІС.

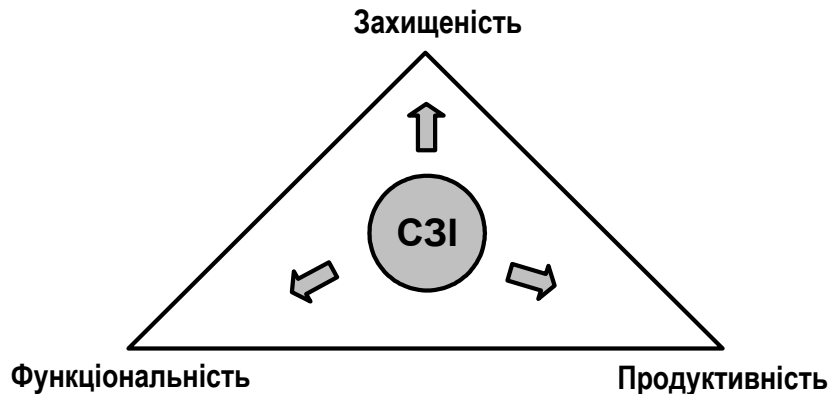


Рис. 4.26. Трикутник суперечностей

З урахуванням цього задача оптимізації полягає в забезпеченні максимального рівня захищеності при мінімальному відносному потенційному збитку, максимальній функціональності та продуктивності ІС (максимум функцій ІС і мінімум середнього часу доступу до об'єктів захисту ІС):

$$Z_{\max} \begin{cases} E \rightarrow \min \\ N_f \rightarrow \max \\ T_a \rightarrow \min \end{cases} \quad (2.2)$$

Така постановка свідчить про багатокритеріальний характер задачі проектування СЗІ, що природно ускладнює її розв'язання. Тому задачу доцільно звести до однокритеріальної шляхом введення обмежень. У результаті одержимо

$$Z_{\text{opt}} \begin{cases} E \rightarrow \min \\ N_f \geq N_{f0} \\ T_a \leq T_{a0} \end{cases} \quad (2.3)$$

де N_{f0} і T_{a0} – задані обмеження на функціональність та продуктивність ІС.

З практичної точки зору зручніше оперувати не необхідною функціональністю і продуктивністю, а зниженням функціональності (ΔN_f) і продуктивності (ΔT_a) від встановлення системи захисту. Тоді однокритеріальна задача оптимізації виглядатиме таким чином:

$$Z_{\text{opt}} \begin{cases} E \rightarrow \min \\ \Delta N_f \geq \Delta N_{f0} \\ \Delta T_a \leq \Delta T_{a0} \end{cases}, \quad (2.4)$$

де ΔN_{f0} і ΔT_{a0} – задані обмеження на зниження функціональності й продуктивності ІС.

Якщо розраховане значення відносного потенційного збитку E не задовольняє вимоги до ефективності СЗІ, то в допустимих межах можна змінювати задані обмеження на зниження функціональності та продуктивності, вирішуючи задачу оптимізації методом послідовного зниження обмежень. При цьому необхідно задати крок зниження функціональності та продуктивності.

У цьому випадку задача розв'язується шляхом реалізації ітераційної процедури відсіювання варіантів, що не задовольняють заданому відносному потенційному збитку, і шляхом зниження вимог до обмежень на функціональність і продуктивність.

Особливістю проектування СЗІ є те, що початкові дані, одержані на перших етапах побудови СЗІ, змінюються з часом функціонування ІС, що може бути пов'язано зі зміною умов і середовища функціонування, втратою або збільшенням вартості інформаційних ресурсів, знаходження зловмисниками помилок у реалізації методів і засобів захисту. Ці зміни повинні бути враховані у процесі функціонування СЗІ. Тому процедура проектування СЗІ також є ітераційною.

Послідовність завдань, які вирішуються під час проектування СЗІ, можна узагальнити таким чином.

- 1) Розрахунок параметрів N_f і T_a .
- 2) Призначення обмежень ΔN_{f0} і ΔT_{a0} .
- 3) Аналіз векторів S , A , V , R .

4) Формування декількох варіантів векторів C (варіантів $C3I$), які відрізняються вартістю реалізації.

5) Розрахунок результатів перетворень $S \xrightarrow{C} S^c$, $A \xrightarrow{C} A^c \xrightarrow{S^c} A^{cs}$ $V \xrightarrow{C} V^c \xrightarrow{A^{cs}} V^{csa}$ для всіх варіантів C .

6) Розрахунок E , ΔN_f і ΔT_a для всіх варіантів C .

7) Вибір системи захисту інформації з E , яка задовольняє умови $\Delta N_f \geq \Delta N_{f0}$, $\Delta T_a \leq \Delta T_{a0}$.

8) Якщо варіанти $C3I$ не задовольняють заданим обмеженням, то необхідним є проведення аналізу зміни E при встановленні приростів ΔN_{f0} і ΔT_{a0} методом послідовного зниження обмежень з оцінкою доцільності вибору $C3I$, що задовольняє новим обмеженням.

Під час формування $C3I$ необхідно враховувати, що будь-який механізм захисту повинен проектуватися з урахуванням його впливу в цілому на безпеку ІС і з урахуванням функцій інших механізмів захисту. Комплектування різнорідних механізмів захисту в єдину систему підвищує якість і ефективність функціонування $C3I$.

4.3.4. Технічне завдання на розробку $C3I$ і план захисту інформації

Відповідно до вітчизняних нормативних документів [23; 27] на етапі розробки проекту $C3I$ для автоматизованих систем (можна адаптувати й для узагальненої ІС) необхідно:

сформувати технічне завдання (ТЗ) на розробку $C3I$, відповідно до якого здійснюватиметься проведення *експертизи (атестації)* ІС на відповідність вимогам захищеності інформації;

розробити план захисту інформації, відповідно до якого функціонуватиме $C3I$.

Технічне завдання на розробку $C3I$ повинно містити наступні основні розділи [27]:

- 1) загальні відомості;
- 2) мета й призначення комплексної системи захисту інформації*;
- 3) загальна характеристика АС і умов її функціонування;

* У вітчизняних нормативних документах щодо захисту інформації в автоматизованих системах вживається термін "комплексна система захисту інформації (КСЗІ)", а не $C3I$. Однак, тлумачення поняття КСЗІ не відрізняється від аналогічного тлумачення поняття $C3I$, що викликає сумнів у доцільності його вживання.

- 4) вимоги до комплексної системи захисту інформації;
- 5) вимоги до складу проектної та експлуатаційної документації;
- 6) етапи виконання робіт;
- 7) порядок внесення змін і доповнень до ТЗ;
- 8) порядок проведення випробувань комплексної системи захисту інформації.

Основна інформація, необхідна для формування розділів ТЗ, була викладена вище, а з частиною, що залишилася, можна ознайомитися в джерелі [27].

План захисту інформації повинен складатися з наступних розділів [23]:

- 1) завдання захисту інформації в автоматизованій системі;
- 2) класифікація інформації, яка обробляється в АС;
- 3) опис компонентів АС й технології обробки інформації;
- 4) загрози для інформації в автоматизованій системі;
- 5) ПБ інформації в автоматизованій системі;
- 6) система документів для забезпечення захисту інформації в АС.

Як і для ТЗ необхідна інформація була викладена вище, а вимоги нормативного документа щодо змісту розділів плану захисту інформації наведено в роботі [23].

Роблячи підсумок етапу розробки проекту (плану) системи захисту інформації, що знижує за вибраним критерієм ризику для інформаційних ресурсів, які потребують захисту, відповідно до виявленої множини загроз, можна визначити перелік документів, які необхідно мати на виході (табл. 4.4).

Таблиця 4.4

Приклад переліку документів

№ з/п	Найменування документа	Примітка
1	<i>Технічне завдання на розробку СЗІ</i>	
2	<i>Проект (план) захисту інформації, що складається із сукупності документів і включає формалізовану модель СЗІ</i>	

Реалізація проекту (плану) захисту інформації

З метою реалізації, тобто впровадження розробленого проекту (плану) захисту інформації складається *календарний план захисту інформації*, який може мати наступні розділи [23]:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

До організаційних заходів щодо реалізації проекту (плану) захисту інформації можна віднести:

- розробку й впровадження положень та інструкцій щодо реалізації проекту захисту інформації;

- внесення відповідних змін і доповнень до діючих керівних документів організації;

- визначення і встановлення прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІзОД та ІПЗ;

- придбання необхідних нормативних документів і запланованих засобів забезпечення ТЗІ;

- встановлення порядку впровадження запланованих захищених засобів обробки інформації, програмних і технічних засобів ТЗІ, а також засобів контролю ТЗІ;

- визначення порядку взаємодії підрозділів організації в рамках плану захисту інформації;

- визначення порядку взаємодії із зовнішніми організаціями;

- встановлення порядку розгляду результатів виконання затверджених заходів і робіт із захисту інформації;

- визначення порядку проведення атестації СЗІ, її елементів і розробка програми атестаційних випробувань;

- забезпечення управління системою захисту інформації.

До контрольно-правових заходів щодо реалізації проекту (плану) захисту інформації можна віднести встановлення порядку і впровадження контролю за виконанням:

- персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
- заходів, розроблених за наслідками попередніх перевірок;
- тощо.

Профілактичні заходи, спрямовані на формування у персоналу

(користувачів) ІС мотивів поведінки, які спонукають їх до безумовного виконання в повному обсязі вимог режиму, правил проведення робіт тощо, а також на формування відповідного морально-етичного стану в колективі.

Інженерно-технічні заходи спрямовані на:

налагодження, випробування і введення в експлуатацію, супровід і технічне обслуговування апаратних і програмних засобів захисту інформації, що передбачені планом;

інженерне устаткування споруд і приміщень, у яких розміщуються засоби обробки інформації, зокрема в процесі капітального будівництва.

Планування роботи з кадрами включає заходи:

щодо підбору й навчання персоналу (користувачів) встановленим правилам безпеки інформації та методам захисту інформації;

підвищення їх кваліфікації.

Навчання повинно здійснюватися відповідно до затвердженої програми власними силами, із залученням фахівців зовнішніх організацій або на базі іншої організації.

У результаті, відповідно до п'ятого етапу побудови СЗІ, необхідно мати *календарний план захисту інформації* та реалізовану СЗІ.

4.3.5. Визначення якості реалізованої системи захисту

За результатами реалізації проекту (плану) СЗІ слід скласти в довільній формі *акт приймання робіт з ТЗІ*, який підписується виконавцями, представниками зацікавлених організацій (підрозділів), керівником підрозділу ТЗІ і затверджується керівником організації.

Для визначення повноти та якості робіт з ТЗІ слід провести атестацію об'єктів інформаційної діяльності. Під терміном *атестація СЗІ* розуміється дослідження ефективності системи технічного захисту інформації шляхом оцінювання відповідності фактичного (реалізованого) рівня захисту інформації вимогам нормативних документів.

Атестація є обов'язковою для ІС, у яких циркулює державна інформація, що потребує захисту, або інформація, захист якої гарантує держава. У цьому випадку атестацію проводить сама організація, що має відповідний *дозвіл на проведення робіт з технічного захисту*

інформації для власних потреб [53], або зовнішня організація, що має відповідну ліцензію на право діяльності у сфері ТЗІ.

Для інших ІС процедура атестації є доцільною з погляду неупередженої та об'єктивної оцінки реалізованого рівня інформаційної безпеки, яку можна провести своїми силами або із залученням на договірних засадах організацій, які надають послуги *аудиту інформаційної безпеки*.

Вітчизняну нормативну базу, яка регламентує процедуру оцінки якості та ефективності реалізованої СЗІ, складають документи [2; 54; 55], де використовуються два схожі терміни: *атестація й державна експертиза*. Термін "атестація" вживається в джерелі [55] для СЗІ, які передбачають захист інформації тільки від витоку технічними каналами, а термін "державна експертиза" вживається в роботі [54] щодо так званої *комплексної системи захисту інформації*, яка реалізується в автоматизованій (комп'ютерній) системі. При комплексному підході до побудови СЗІ необхідність такого розмежування термінів і систем захисту інформації не очевидна.

Види державної експертизи і порядок її організації та проведення проілюстровані на рис. 4.27, 4.28, а атестації – на рис. 4.29, 4.30.

Державна експертиза

Проводиться з метою оцінки захищеності інформації, яка обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, приміщеннях, інженерно-технічних спорудах і т. п., і підготовки обґрунтованих висновків для ухвалення відповідних рішень

Первинна

Основний вид експертизи, який передбачає виконання всіх необхідних заходів для підготовки й ухвалення рішення щодо об'єкта експертизи

Контрольна

Здійснюється іншим організатором: за ініціативою замовника, за наявності у нього обґрунтованих претензій до висновку первинної експертизи, або за ініціативою Держспецзв'язку (ДСТСЗІ СБУ) для перевірки висновків первинної експертизи

Рис. 4.27. Приклад державної експертизи

Таким чином, в результаті проведення державної експертизи СЗІ необхідно мати:

протокол виконання робіт відповідно до окремої методики експертизи комплексної системи (засобу) технічного захисту інформації;
експертний висновок, зареєстрований і затверджений експертною радою Держспецзв'язку (ДСТС ЗІ СБУ);
атестат відповідності, зареєстрований і виданий у Держспецзв'язку (ДСТС ЗІ СБУ).

У результаті проведення атестації СЗІ, де передбачається захист інформації тільки від витоків технічними каналами, необхідно мати:



Рис. 4.28. Порядок та проведення експертизи

Атестація

Оцінювання ефективності комплексу технічного захисту інформації, яка циркулюватиме на ОІД, від витoku технічними каналами на відповідність вимогам нормативних документів ТЗІ

Первинна

Здійснюється після (або під час) ухвалення рішення про проведення робіт із створення комплексу ТЗІ

Чергова

Термін проведення визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації

Позачергова

Проводять у разі змін умов функціонування ОІД, що призводить до змін інформаційних загроз, і за висновками органів, які контролюють стан ТЗІ

Рис. 4.29. Приклад атестації

акт атестації комплексу технічного захисту інформації з протоколами випробувань;

технічний паспорт на комплекс ТЗІ.

Зразки деяких документів наведено в дод. 7 – 9.



Рис. 4.30. Порядок організації та проведення атестації

По суті, при визначенні якості реалізованої СЗІ спочатку проводиться аналіз проекту (плану) СЗІ на його несуперечність, повноту, оптимальність і відповідність вибраній нормативній базі. Далі перевіряється якість реалізації положень проекту СЗІ.

Для недержавних організацій, що оперують тільки власною ІПЗ, для оцінки якості реалізованої СЗІ доцільним вбачається залучення організацій, які надають послуги аудиту інформаційної безпеки:

щодо захисту від НСД у рамках вимог "Загальних критеріїв";

щодо захисту від витоку технічними каналами – в рамках відкритих документів, які визначають вимоги до порядку захисту державної таємниці.

У результаті, після проведення робіт відповідно до шостого етапу побудови СЗІ, необхідно мати наступні документи (табл. 4.5).

Таблиця 4.5

Перелік необхідних документів відповідно до шостого етапу

№ з/п	Найменування документа	Примітка
1	<i>Акт приймання робіт з ТЗІ</i>	Внутрішній документ
2	<i>Протокол виконання робіт відповідно до окремої методики експертизи комплексної системи (засобу) технічного захисту інформації</i>	Підписаний експертами і затверджений організатором експертизи
3	<i>Експертний висновок</i>	Зареєстрований і затверджений експертною радою Держ-спецзв'язку
4	<i>Атестат відповідності</i>	Зареєстрований і виданий Держспецзв'язку
5	<i>Акт атестації комплексу технічного захисту інформації з протоколами випробувань</i>	Якщо не проводилася державна експертиза
6	<i>Технічний паспорт на комплекс ТЗІ</i>	Якщо не проводилася державна експертиза

Контроль функціонування й керування системою захисту

Створена СЗІ не є статичною системою, оскільки в процесі функціонування ІС відбувається зміна умов, середовища, складу загроз, ресурсів, які захищаються, і т. д. Управління системою захисту інформації полягає в адаптації в найкоротший строк її механізмів до поточних змін. У проекті СЗІ, який вже реалізовано й оцінено, передбачені механізми контролю та управління системою захисту інформації. Основним завданням цього етапу є проведення аналітичної оцінки поточного стану безпеки інформації за допомогою вже передбачених і реалізованих механізмів.

Нормативним документом [56] передбачається контроль Держспецзв'язку (ДСТС ЗІ СБУ) за функціонуванням системи захисту інформації, захист якої гарантується державою. На виконання цього припису Держспецзв'язку організовує і проводить контрольні-інспекційні перевірки з питань ТЗІ щодо суб'єктів системи ТЗІ. Види перевірок проілюстровані на рис. 4.31.

Порушення встановлених норм і вимог ТЗІ, виявлені під час проведення перевірок, поділяються на *три категорії порушень*:

- 1) створюється реальна можливість реалізації інформаційних загроз;
- 2) створюються передумови реалізації інформаційних загроз;
- 3) інші порушення.

За результатами комплексної перевірки комісією складається *акт перевірки стану і ефективності заходів з технічного захисту інформації*, а за результатами цільової та контрольної перевірки – *довідка*, і вживаються відповідні заходи впливу на суб'єктів системи ТЗІ України.

Контрольно-інспекційна робота з питань ТЗІ

Планування і проведення перевірок стану ТЗІ.
 Проведення аналізу і надання рекомендацій щодо вдосконалення заходів з ТЗІ.
 Проведення перевірок суб'єктів системи ТЗІ щодо виконання ними завдань або здійснення діяльності в цій галузі відповідно до дозволів і ліцензій

Перевірки

Комплексна

Вивчається й оцінюється стан ТЗІ

Цільова

Вивчаються окремі напрямки ТЗІ;
 перевіряється виконання рішень (розпоряджень, наказів, вказівок) органом державної влади з питань ТЗІ;
 виконання завдань або здійснення діяльності в області ТЗІ відповідно до дозволів і ліцензій

Контрольна

Перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки (контрольні перевірки проводяться за необхідності, як правило, а не раніше, ніж через рік після попередньої перевірки)

планові, позапланові, з попередженням, раптові

Рис. 4.31. Види перевірок

В організації відповідно до проекту (плану) ТЗІ підрозділом ТЗІ також проводяться внутрішні контрольні перевірки стану інформаційної безпеки, результати яких фіксуються в *технічних паспортах на комплекс ТЗІ*.

Як підсумок, проведення робіт відповідно до сьомого етапу призводить до укладання таких документів (табл. 4.6).

Таблиця 4.6

Перелік документів для укладання

№ з/п	Найменування документа	Примітка
1	<i>Акт перевірки стану й ефективності заходів щодо технічного захисту інформації</i>	За результатами комплексної перевірки Держспецзв'язку
2	<i>Довідка щодо перевірки стану й ефективності заходів з технічного захисту інформації</i>	За результатами цільової та контрольної перевірки Держспецзв'язку

Таким чином, за допомогою представленої методології проведення експертизи та укладення відповідних документів можливе отримання більш якісних результатів під проведення будь-яких досліджень та дізнань.

5. ПРАВОВІ ОСНОВИ ІБ

5.1. Основні юридичні поняття ІЕБ ✓

5.2. Приклади економічних порушень ✓

5.3. Нормативні положення, що регламентують ІЕБ ✓

5. ПРАВОВІ ОСНОВИ ІБ

5.1. Основні юридичні поняття ІЕБ

Під **безпекою ІС** розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого одержання) інформації, модифікації або фізичного руйнування її компонентів. Інакше кажучи, це здатність протидіяти різним негативним впливам, **на ІС**.

Під **загрозою безпеки інформації** розуміються події або дії, які можуть привести до перекручування, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Якщо виходити із класичного розгляду кібернетичної моделі будь-якої керованої системи, що здійснюють впливи на неї, можуть носити випадковий характер. Тому серед загроз безпеки інформації варто виділяти як один із видів загрози випадкові, або *ненавмисні*. Їхнім джерелом можуть бути вихід із ладу апаратних засобів, неправильні дії працівників ІС або її користувачів, ненавмисні помилки в програмному забезпеченні й т. д. Такі загрози теж варто мати на увазі, тому що збиток від них може бути значним. Однак у даному розділі найбільша увага приділяється загрозам *навмисним*, які на відміну від випадкових мають на меті завдання збитків керованій системі або користувачам. Це робиться часто заради одержання особистого зиску.

Людину, що намагається порушити роботу інформаційної системи й одержати несанкціонований доступ до інформації, зазвичай називають зломщиком, а іноді "комп'ютерним піратом" (хакером). У своїх протиправних діях, спрямованих на оволодіння чужими секретами, зломщики прагнуть знайти такі джерела конфіденційної інформації, які б давали їм найбільш достовірну інформацію в максимальних обсягах з мінімальними втратами на її одержання. За допомогою різного роду хитрощів і безлічі прийомів і засобів підбираються шляхи й підходи до таких джерел. У цьому випадку під джерелом інформації розуміється матеріальний об'єкт, що володіє певними відомостями, які становлять конкретний інтерес для зловмисників або конкурентів.

Захист від навмисних загроз – це свого роду змагання оборони й нападу: хто більше знає, передбачає дійові заходи, той і виграє.

Численні публікації останніх років показують, що зловживання інформацією, яка циркулює в ІС або передається каналами зв'язку, удосконалювалися не менш інтенсивно, ніж міри захисту від них. У цей час для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємозалежних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних мір протидії й т. д.). Комплексний характер захисту виникає з комплексних дій зловмисників, що прагнуть будь-якими способами добути важливу для них інформацію. Сьогодні можна стверджувати, що народжується нова сучасна технологія – *технологія захисту інформації* в комп'ютерних інформаційних системах і в мережах передачі даних. Реалізація цієї технології вимагає збільшення витрат і зусиль. Однак все це дозволяє уникнути значно переважаючих втрат і збитку, які можуть виникнути при реальному здійсненні загроз ІС і ІТ.

5.1.1. Нормативно-правова база України у сфері ТЗІ

Відповідно до поданого вище визначення, нормативно-правова база є однією з базових складових частин системи технічного захисту інформації в Україні (дод. 3).

Нормативно-правову базу України можна умовно поділити на загальнодержавну й відомчу (рис. 5.1).

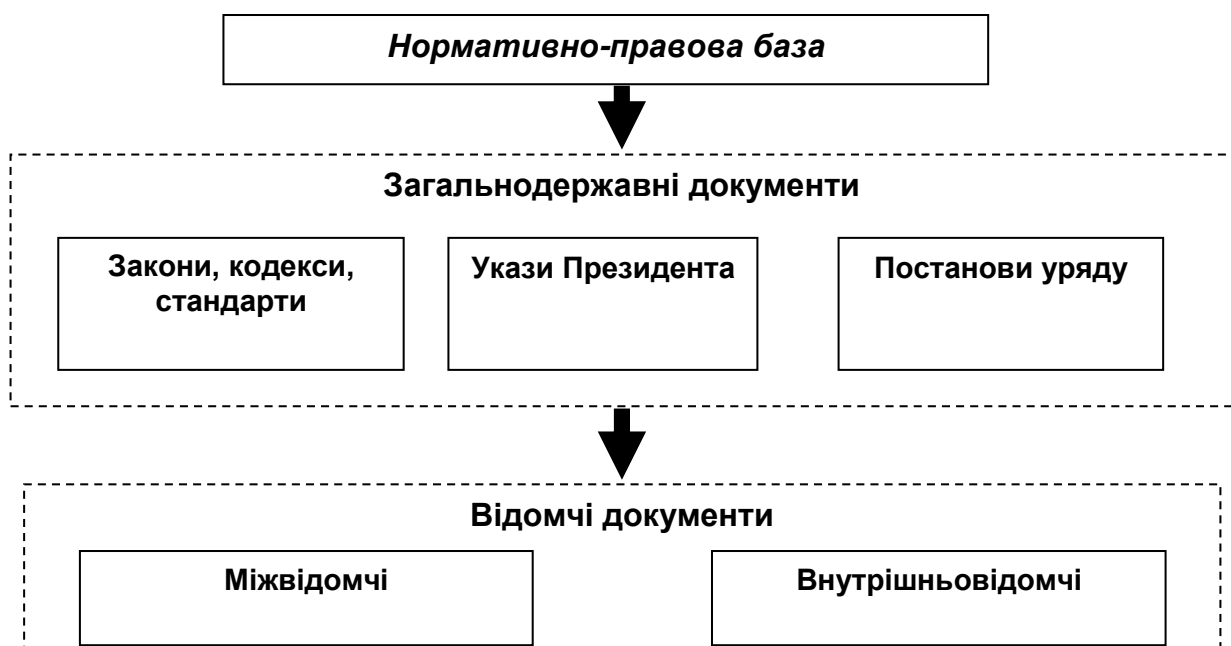


Рис. 5.1. Структура нормативно-правової бази України у сфері ТЗІ

Правову базу (основу) технічного захисту інформації в Україні складають:

Конституція України;

Закони України:

Про інформацію;

Про державну таємницю;

Про захист інформації в інформаційно-телекомунікаційних системах;

Про Національну систему конфіденційного зв'язку;

Про електронні документи й електронний документообіг;

Про електронно-цифровий підпис;

Положення "Про технічний захист інформації в Україні;

Концепція технічного захисту інформації в Україні;

Державні стандарти України із захисту інформації;

акти Президента України і Кабінету Міністрів України;

нормативно-правові акти Держспецзв'язку (і його попередника ДСТС ЗІ СБУ);

ратифіковані міжнародні договори України з питань технічного захисту інформації.

Окрім суто нормативно-правової, виділяють також методичну базу у сфері ТЗІ. На теперішній час нормативно-правову та методичну базу у сфері ТЗІ з урахуванням галузі застосування можна поділити на наступні види:

законодавчі та концептуальні документи України у сфері ТЗІ;

документи, що регламентують організацію ТЗІ в державних органах, організаціях, установах;

документи, що регламентують технічний захист інформації в телекомунікаційних системах;

документи, що регламентують захист інформації в комп'ютерних (інформаційно-телекомунікаційних) системах від несанкціонованого доступу;

документи, що регламентують криптографічний захист інформації;

документи, що регламентують захист інформації від витоку технічними каналами:

акустичних;

хімічних;
каналах побічних електромагнітних випромінювань і наведень (ПЕМВН);
документи із протидії технічним розвідкам;
документи, що регламентують господарську діяльність у сфері технічного захисту інформації;
спеціальні нормативні документи колишнього СРСР, що включають:
норми ефективності захисту;
вимоги, вказівки, інструкції та рекомендації із захисту;
методики контролю й проведення спеціальних досліджень.

Перелік відомої авторам на момент написання навчального посібника нормативно-правової й методичної бази у сфері ТЗІ України наведено в додатку 3. У джерелі [6] наведено витяги основних нормативно-правових документів із забезпечення інформаційних відносин, інформатизації, управління у сфері інформаційної діяльності та захисту інформації. Стан нормативно-правової й методичної бази у сфері ТЗІ можна відстежувати на цей час на сайті Держспецзв'язку (ДСТС ЗІ СБУ) www.dstshi.gov.ua.

5.2. Приклади економічних порушень

5.2.1. Типи шахрайства

Шахрайство, що включає в себе обман, може приймати різні форми. Ми часто підрозділяємо випадки шахрайства на шість типів. Перший з них – це *розтрата* або *розкрадання з боку найманого робітника*. У цьому випадку наймані робітники обманюють своїх наймачів, привласнюючи собі майно або кошти фірми. Розтрата й розкрадання з боку найманих робітників можуть відбуватися як безпосередньо ними самими, так і опосередковано, за допомогою й при участі інших осіб. У першому випадку ми маємо на увазі ті розкрадання, коли працівник краде з каси готівку, викрадає кошти безготівковим чином або просто тягне з роботи все, що йому сподобається. Це також належить до тих випадків, коли співробітник засновує підставну фірму і як її керівник одержує гроші за недоставлені товари або ненадані

послуги. При такому вигляді шахрайства кошти постраждалої фірми переходять до шахрая без свідомої участі третьої сторони.

Про опосередковане ж шахрайство ми говоримо тоді, коли працівники хабарничають і отримують подарунки від покупців, клієнтів і інших осіб, що не працюють у даній фірмі, за свої послуги із зниження продажних і завищення покупних цін, за непостачання товарів або поставки недоброякісних. При цьому платежі шахраям здійснюються організаціями, що мають справи з господарем даного працівника.

Другий тип шахрайства – це *шахрайство з боку керівників або менеджерів*. Таке шахрайство відрізняється від інших типів як становищем шахраїв, так і способами обману. У своєму найбільш загальному вигляді шахрайство з боку менеджерів є обманом, який вчиняється керівниками даної фірми вищої й середньої ланки шляхом маніпуляцій з фінансовою звітністю. В останні роки широку популярність одержали такі випадки шахрайства з боку менеджерів, як афера в "Pharmor and Crazy Eddie, Inc.", де, як передбачається, два керівники завищували деякі показники фінансової звітності, а також афери фірм "**ZZZZ** Best", "ESM Government", "Regina Vacuum Company" і "Miniscribe Corporation", де спотворювалися дані про прибутковість і дебіторські заборгованості даних фірм. У всіх цих випадках керівництво зазначених компаній прагнуло до того, щоб власники акцій вірили, що фінансове становище цих компаній набагато краще, ніж воно було насправді.

Тісно пов'язаний із шахрайством з боку менеджерів такий тип шахрайства, як *афери з інвестиціями*. У цьому випадку інвесторам пропонується зробити інвестиції, які, як виявляється згодом, у дійсності не справжні, що не становлять, як правило, ніякої цінності. До цієї категорії зазвичай входить так званий телемаркетинг, що становить пропозицію "мільних бульок" і інших можливостей вкладення вільного капіталу. "Батьком" афер з інвестиціями вважається Карло Понці, але, на жаль, у нього виявилось досить багато послідовників, і ця форма обману сьогодні надзвичайно поширена.

Четвертим типом шахрайства є *шахрайство з боку постачальників*. В останні роки через велику кількість афер з військовими й іншими урядовими замовленнями таке шахрайство часто висвітлювалося в пресі. Шахрайство з боку постачальників, широко розповсюджене в Сполучених Штатах, зустрічається у двох своїх основних різновидах: по-перше, у вигляді дій тільки цих постачальників і,

по-друге, у вигляді спільних дій як постачальників, так і представників замовника. Шахрайство з боку постачальників часто проявляється в завищенні кількості виробів, що постачаються, поставці бракованих товарів або непостачанню товарів взагалі, хоча платежі за них були отримані.

П'ятий тип шахрайства – це *шахрайство з боку замовника або клієнта*. Воно, звичайно, містить у собі неплатежі за поставлений товар, одержання плати за не пророблену роботу або обман різних фірм шляхом поставки їм зовсім непотрібних речей. Так, наприклад, одного суботнього ранку клієнтка прийшла в банк і переконала начальника відділу виписати їй чек на 525000 доларів – незважаючи на те, що в неї на рахунку їх було всього 13 000. Цей менеджер думав, що клієнтка відноситься до категорії дуже заможних, і не хотів пропустити можливість взяти участь у її угоді. На жаль, клієнтка відносилася до категорії злодіїв "з білим комірцем", що підставив банк більш ніж на півмільйона доларів. В іншому випадку шестеро чоловік, перебуваючи в дорогому номері готелю в центрі Чикаго, шляхом трьох дзвінків в "Чикаго Банк" умовили його службовців перевести приблизно 70 мільйонів доларів на їх рахунок в іншому банку.

Шостим типом шахрайства є обман, що не підпадає ні під жоден із попередніх типів і здатний здійснюватися з метою одержання не тільки фінансового прибутку. Такий тип обману просто позначається як *шахрайство змішаного типу*. Прикладами його можуть бути фальсифікація свідоцтв про народження гравців уже відомої нам дитячої футбольної команди, завдяки чому команда змогла успішно виступити в чемпіонаті, а також фальсифікація оцінок під час надходження в різні навчальні заклади.

5.2.2. Типові види шахрайства з боку найманих робітників

Крадіжка готівки з каси.

Крадіжка чеків.

Використання готівки не за призначенням.

Фальсифікація касових книг.

Фальсифікація сум на банківських рахунках.

Підробка чеків.

Використання надходжень у пенсійні фонди не за призначенням.

Дрібні крадіжки готівки з каси.
Оплата особистих рахунків чеками фірми.
Подання фальсифікованих рахунків-фактур.
Фальсифікація транспортних накладних.
Завищене фактурування.
Крадіжки інвентарю.
Змова із клієнтами або постачальниками.
"Кикбеки", тобто одержання "подяки" за певні послуги, іншими словами, різновид хабара.
Штучне здуття цін.
Використання підставних постачальників.
Завищення цін.
Переплата "зверху".
Видача дутих векселів, так званих кайтинг.
Використання майна фірми.
Використання співробітників, устаткування або матеріалів фірми в особистих цілях.
Надання замовлень за хабарі.
Маніпуляції із кредитними картками.
Шахрайство зі страховкою.
Не задекларовані доходи.
Фальсифікування податкових декларацій.
Шахрайство з рахунками від медичних установ.
Фальсифікація записів у бухгалтерських книгах:
для поліпшення звітності;
для покриття недостач.
Фальсифікація звітності про відрядження.
Завищення видатків.
Включення у звіт про відрядження особистих витрат.
Неповернення виданих авансом сум.
Несанкціонований продаж майна фірми:
інвентарю;
устаткування;
відходів виробництва.
Комп'ютерні злочини:
зміна втримування записів;
одержання готівки.

Шахрайство з виплатою заробітної плати.
Розготівковування незатребуваних чеків.
Фальсифікація годин переробки.
Оплата праці працівників-"пролісків".

5.2.3. Основні способи злочинних дій у системі обміну електронними документами

Загальноприйнятою є наступна модель автентифікації, у якій функціонують чотири учасники: А-передавач, В-приймач, С-супротивник і D-арбітр. А – посилає повідомлення, В – приймає, С – намагається зробити злочинні дії; D – приймає рішення в спірних випадках, тобто визначає, твердження чиєї сторони з найбільшою ймовірністю є помилковими. Природно, як С можуть виступати А та В. Метою автентифікації документів є захист від можливих видів злочинних дій, серед яких виділимо:

- 1) активне перехоплення – порушник (що підключився до мережі) перехоплює документи (файли) і змінює їх;
- 2) порушення конфіденційності;
- 3) маскарад – абонент С посилає документ від імені абонента А;
- 4) переробка – абонент В змінює документ і затверджує, що даний документ (змінений) одержав від абонента А;
- 5) підміна – абонент В формує документ (новий) і заявляє, що одержав його від абонента А;
- 6) повтор – абонент В повторює раніше переданий документ, що абонент А послав абонентові В.
- 7) втрата або знищення документа кожним із абонентів;
- 8) фальсифікація часу відправлення повідомлення;
- 9) руйнування електронних архівів.
- 10) ренегатство – абонент А повідомляє, що не посилав повідомлення абонентові В, хоча насправді посилав;
- 11) відмова від факту одержання – абонент В відмовляється від факту одержання документа від абонента А;
- 12) компрометація секретного ключа;
- 13) включення в каталог неверификованого відкритого ключа;
- 14) НСД до терміналу.

Ці види злочинних дій завдають істотної шкоди функціонуванню банківських, комерційних структур, державним підприємствам і організаціям, приватним особам, що застосовують у своїй діяльності комп'ютерні інформаційні технології. Крім того, можливість злочинних дій підриває довіра до комп'ютерної технології. У зв'язку із цим завдання автентифікації є важливим.

Аксиома. При виборі технології автентифікації повідомлень у мережі необхідно передбачити надійний захист від усіх перерахованих вище видів злочинних дій.

5.2.4. Основні заходи щодо забезпечення захисту електронних документів

Безпека електронних документів повинна досягатися застосуванням взаємозалежного комплексу заходів, до числа яких належать:

- електронний підпис документів;
- шифрування повідомлень при передачі каналами зв'язку;
- керування ключовою системою;
- розмежування повноважень при роботі з електронними документами;
- захист на рівні протоколів зв'язку;
- захист архівів від руйнування;
- існування арбітра;
- організаційні заходи.

Основою комплексу заходів із захисту інформації є **електронний підпис**, за відсутності якого важко досягти прийнятного рівня безпеки в системі. Винятком можуть бути ситуації, де існує повна довіра між сторонами, що обмінюються інформацією. У цьому випадку міри захисту повинні бути спрямовані на запобігання можливого проникнення в систему сторонніх осіб.

Електронний підпис повинен виконувати завдання, які виконує підпис, поставлений на документі від руки. Причому ніяких засобів для реалізації контролю дійсності інформації, крім аналізу самої інформації, не існує. Вирішення цієї проблеми стало можливим після створення криптографічних алгоритмів, що дозволяють одній або більше сторонам, що знають секретні частини інформації (ключі), здійснювати операції

обробки інформації, які з великою ймовірністю не можуть бути відтворені тими, хто не знає цих секретних ключів.

Тут необхідно використовувати схеми, засновані на двоключовій криптографії. У таких випадках у передавального абонента мережі є свій секретний ключ підпису, а в приймаючого абонента – несекретний відкритий ключ підпису передавального абонента. Цей відкритий ключ можна трактувати як набір перевірочних співвідношень, що дозволяють говорити про істинність підпису передавального абонента, але не дозволяють відновити секретний ключ підпису. Передавальний абонент несе одноосібну відповідальність за свій секретний ключ. Ніхто, крім нього, не в змозі згенерувати коректний підпис. Секретний ключ передавального абонента можна розглядати як особисту печатку, і власник повинен усіляко обмежувати доступ до нього сторонніх осіб.

Принцип їхньої дії заснований на застосуванні однобічних функцій, що дозволяють розділити функції шифрування й дешифрування. При цьому, не знаючи ключа шифрування, що є секретним, можна лише прочитати зашифрований текст.

На практиці, як правило, у схемах підпису замість документа x розглядають його хеш-функцію $h(x)$, що володіє рядом спеціальних властивостей, найважливіші з яких – відсутність "колізій", тобто практична неможливість створення двох різних документів з однаковим значенням хеш-функції (ХФ).

Найбільш відомі наступні математичні схеми підпису: RSA – названа за першими буквами прізвищ авторів (R. L. Rivest, A. Shamir, L. Adleman), OSS (H. Ong, C. P. Schnorr, A. Shamir), Ель-Гамаля (T. ElGamal), Рабина (M. Rabin), Окамото – Сапаісі (T. Okamoto, A. Shiraishi), Many-moto – Imai (T. Matsumoto, H. Imai).

Труднощі завдань підробки підпису в цих схемах полягають в обчислювальній складності завдань факторизації або дискретного логарифмування. Серед схем, запропонованих вітчизняними вченими, можна відзначити оригінальну схему А. А. Грушо (1992 р.). Її односпрямована функція, на відміну від перерахованих вище, заснована не на складності теоретико-числових завдань, а на складності рішення систем нелінійних бульових рівнянь.

Сьогодні практичні додатки найбільшого поширення одержали дві схеми: метод RSA і метод Ель-Гамаля.

У стандарті США для цифрового підпису DSS – Digital Signature Standard використовуються спеціально створені алгоритми. В основу цих алгоритмів покладені схеми Ель-Гамала й Шнора.

У Росії прийняті стандарти: ДЕРЖСТАНДАРТ Р 34.10-94 "Процедури виробітку й перевірки електронного цифрового підпису на базі асиметричного криптографічного алгоритму" і ДЕРЖСТАНДАРТ Р 34.11-94 "Функція хешування". В основу ДЕРЖСТАНДАРТ Р 34.10-94 покладена односпрямована функція, заснована на дискретному зведенні в ступінь.

Конфіденційність і цілісність переданих каналами зв'язку даних забезпечуються застосуванням **засобів криптографічного захисту**, що використовують одноключові (той самий ключ, що є секретним, використовується й для шифрування й для дешифрування) алгоритми. Серед безлічі алгоритмів цього типу найбільшою довірою користуються криптографічні перетворення, що відповідають стандартам.

Найбільше поширення одержав уведений у дію в 1977 році національний стандарт США DES (Data Encryption Standard), практично повсюдно використовуваний у банківській сфері. Вітчизняний стандарт криптографічного перетворення інформації, – ДЕРЖСТАНДАРТ 28147-89, був уведений у дію з липня 1990 року. Обидва ці стандарти використовуються російськими комерційними банками для закриття повідомлень, переданих каналами зв'язку.

Цілісність фінансових повідомлень при передачі і їх захисту від різних маніпуляцій забезпечується перевіркою поля даних, що додається до повідомлення й змісті, що є функцією від повідомлення й секретного ключа. Спосіб формування цього поля також описується стандартами: обчислення коду перевірки дійсності даних (MAO в ISO 8730 і одержання імітовставки в ДЕРЖСТАНДАРТ 28147-89).

Використання криптографічних засобів вимагає створення **надійної ключової системи**, у якій операції генерації, зберігання, розсилання й знищення ключів задовольняли б вимоги безпеки. Для побудови ключової системи американськими банками в основному використовується стандарт на керування ключами фінансових повідомлень ANSI X9.17, що припускає існування в системі Центра розподілу ключів (ЦРК), що виконує всі операції з керування ключами.

У криптосистемі зі ЦРК існують три види ключів:

головний ключ;

ключі шифрування ключів;
сеансові ключі.

Міжнародний стандарт ISO 8532 (Banking-Key-Management) також описує ієрархічну ключову систему із центром розподілу ключів. Ці стандарти вимагають передачі старшого ключа неелектронним способом (фельдзв'язком), що виключає його компрометацію. Ієрархічні схеми є досить дорогими й вимагають повної довіри до ЦРК, що генерує й розсилає ключі.

Метод з відкритим ключем дозволяє значно спростити ключову систему. При тому відпадає необхідність використання захищених каналів зв'язку. Однак виникає необхідність надійної автентифікації абонента, що прислала відкритий ключ. Роль адміністратора в системі зводиться до перевірки приналежності відкритих ключів, переміщення їх у довідник і розсилання цього довідника всім абонентам системи. Ці функції виконуються Центром верифікації ключів (ЦВК).

Основна операція, здійснювана ЦВК – сертифікація ключів. Суть її полягає в наступному. Абонент, що бажає брати участь в обміні повідомленнями, посилає ЦВК свій відкритий ключ у роздрукованому вигляді, завіривши його мастичною печаткою своєї організації й підписами посадових осіб. Всі інші абоненти одержують цей ключ від ЦВК. Підставою для включення нового відкритого ключа в каталог є наявність електронного підпису ЦВК. Крім того, на ЦВК покладається завдання з повідомлення всіх учасників обміну електронними документами у випадку компрометації ключів.

Найслабкішою ланкою в системі електронних документів з погляду безпеки є секретний ключ. Тому найбільшу увагу варто приділяти збереженню його в таємниці. Із цього погляду надзвичайно важливо правильно вибрати тип носія для збереження секретного ключа. Критеріями оцінки при виборі носія є:

- наявність перезаписуваної пам'яті необхідного обсягу;
- складність копіювання інформації;
- зручність зберігання;
- захищеність від зовнішніх впливів.

Зазначені вимоги найбільшою мірою задовольняють електронні картки. (Один з варіантів – електронні картки Touch Memory американської фірми Dallas Semiconductor, розміщені в металевому корпусі, що мають унікальний код і до 2 Кб перезаписуваної пам'яті).

Застосовувані організаційні заходи повинні:

передбачати періодичну зміну секретних ключів,
визначати порядок зберігання носіїв і схему повідомлення про події, пов'язані з компрометацією ключів.

Заява про компрометацію секретного ключа спричиняє виключення з каталогів усіх абонентів відповідних відкритих ключів і припинення обробки документів, підписаних за допомогою даного ключа.

Крім загроз, пов'язаних із порушенням цілісності, конфіденційності й дійсності повідомлень у системах електронних документів, існують загрози, **пов'язані із впливом на повідомлення**. До їх числа належать знищення, затримка, дублювання, переупорядкування, переорієнтація окремих повідомлень, маскуванню під іншого абонента або інший вузол. Загрози цього типу нейтралізуються використанням у системі **захищених протоколів зв'язку**.

Захист на рівні протоколів досягається вживанням наступних заходів:

- керування з'єднанням;
- квотування;
- нумерація повідомлень;
- підтримка єдиного часу.

Керування з'єднанням необхідне при використанні ліній зв'язку, що комутуються, і містить у собі і запит **ідентифікатора**, автентифікацію джерела повідомлення й розрив з'єднання при одержанні неправильного ідентифікатора.

Існує кілька схем керування з'єднанням. Як правило, дається кілька спроб для уведення ідентифікатора, і якщо всі вони виявляються не-вдалими, зв'язок розривається.

Більш надійним способом керування з'єднанням є автоматичний зворотний виклик. При спробі встановити з'єднання прийомною стороною запитується ідентифікатор, після чого зв'язок розривається. Потім залежно від результатів перевірки або виробляється повторне з'єднання за обраним зі списку номером, або зв'язок припиняється. Надійність такого способу залежить від якості каналів зв'язку й правильності заповнення списку доступних номерів.

Квотування – це процедура видачі підтвердження (квитанції) про одержання повідомлення вузлом або адресатом, що дозволяє відслідковувати стан переданого документа. Додатковою гарантією може

бути включення до складу квитанції електронного підпису. Для запобігання можливості відмови однієї зі сторін від факту одержання повідомлення протокол може передбачати повернення копій отриманих документів (за аналогією з паперовим документообігом) з електронним підписом одержувача.

Значне число навмисних атак і випадкових помилок можна виявити, якщо ввести **нумерацію повідомлень**. Одержання документа із уже використаним номером або номером, що значно перевищує поточний, є подією, що вказує на порушення правильності роботи системи й потребує негайної реакції з боку відповідального за безпеку.

Установлення й підтримка в системі електронних платежів **єдиного часу** для всіх абонентів значно знижує ймовірність загроз, пов'язаних з відмовою від авторства повідомлення, а також зменшує кількість помилок. При цьому переданий документ повинен містити незмінні дату й час підписання, що заносяться в нього автоматично.

Захист від НСД до терміналів, на яких ведеться підготовка й обробка повідомлень, повинна забезпечуватися застосуванням програмних і програмно-апаратних засобів і організаційною підтримкою. Засоби захисту повинні забезпечувати ідентифікацію й надійне впізнавання користувачів, розмежування повноважень за доступом до ресурсів, реєстрацію роботи й облік спроб НСД.

Організаційні заходи в системах електронних документів, як правило, спрямовані на чіткий розподіл відповідальності при роботі з документами й створення декількох меж контролю.

Перелік посадових осіб і їх обов'язків може виглядати таким чином:

бухгалтер підприємства – уведення документа, підпис, шифрування документа на ключі директора, складання балансу;

директор підприємства – верифікація документа, підпис, шифрування на ключі банку;

оператор клієнта–відправлення й прийом зашифрованих повідомлень;

оператор банку – відправлення й прийом зашифрованих документів;

операціоніст – розшифрування й перевірка одержуваних документів, підготовка виписок, підпис, шифрування на ключі клієнта;

менеджер – верифікація документів і відбиття їх в операційному дні банку, підпис;

адміністратор – керування ключами, зв'язок із ЦБК, обробка облікових і реєстраційних журналів, підтримка системи захисту.

Обов'язковою умовою існування системи електронних платежів є підтримка архівів електронних документів. Строк зберігання архівного документа може становити кілька років. Тому необхідно вживати заходів для захисту архівів від руйнування. Досить ефективним способом захисту є завадостійке кодування.

Таким чином, можна кожному виду загроз поставити у відповідність певні заходи захисту (табл. 5.1).

Таблиця 5.1

Відповідність загрозам заходів захисту

Нейтралізовані загрози	Заходи захисту
Підробка документа. Відмова від авторства. Несанкціонована модифікація.	Застосування електронного цифрового підпису. Ведення електронних архівів
Порушення конфіденційності	Криптографічне закриття
Помилки при заповненні документів	Контроль правильності уведення документів Проходження документів за суворим певним маршрутом
Уведення помилкових даних	Контроль маршруту проходження документа. Персоніфікація документів
Помилки в роботі системи	Реєстрація й облік документів на етапах підготовки
Дублювання документів	Нумерація документів. Контроль часу відправлення документа. Забезпечення єдиничності виконання документа
Спроби одержання секретного ключа	Керування ключовою системою
Несанкціонована модифікація ПЗ	Верифікація ПЗ
Руйнування даних	Резервне копіювання
Несанкціонований доступ до конфіденційної інформації	Фізичний захист приміщень. Розмежування прав учасників електронного документообігу. Застосування засобів захисту інформації від НСД
Крадіжки й втрати документів	Контроль за виведенням документів на друк

Додатково необхідно враховувати практичні рекомендації з наступних позицій.

Персоніфікація документів

Недостатньо просто застосувати підпис. Необхідно домагатися того, щоб під документом стояло мінімум дві ЕЦП, що належать конкретним людям з конкретною відповідальністю.

Контроль за виведенням документів на друк

Не слід забувати, що електронний документообіг не скасовує звичні паперові документи. Частіше відбувається навпаки – кількість паперів зростає. І часто виникає парадоксальна ситуація: поки документ існує в електронному вигляді, його захищають всіма можливими способами. Потім його виводять на принтері незліченну кількість разів і зрештою розкидають по сміттєвих кошиках через непотрібність.

Забезпечення конфіденційності документів

Працівники режимно-секретних служб знають, що із введенням комп'ютерної техніки на робочі місця контролювати процес підготовки документів обмеженого поширення став набагато складнішим. Звичайні засоби захисту від несанкціонованого доступу, безумовно, полегшують життя, але не дають можливості автоматизувати процес обліку документів і контроль за їх підготовкою. Що ж необхідно зробити для забезпечення безпечного процесу виведення документів на друк? У документах Держтехкомісії Росії на це питання є вичерпна відповідь:

“...повинен бути передбачений адміністратор (служба) захисту інформації, відповідальний за ведення, нормальне функціонування й контроль роботи ЗЗІ від НСД. Адміністратор повинен мати свій термінал і необхідні засоби оперативного контролю й впливу на безпеку АС”;

“...повинна здійснюватися реєстрація видачі друкованих (графічних) документів на “тверду” копію. Видача повинна супроводжуватися автоматичним маркуванням кожного аркуша (сторінки) документа порядковим номером і обліковими реквізитами АС із зазначенням на останньому аркуші документа загальної кількості аркушів (сторінок). У параметрах реєстрації вказуються:

дата й час видачі (звертання до підсистеми виводу);

специфікація пристрою видачі (логічне ім'я (номер) зовнішнього пристрою);

короткий зміст (найменування, вид, шифр, код) і рівень конфіденційності документа;

ідентифікатор суб'єкта доступу, що запросив документ;

обсяг фактично виданого документа (кількість сторінок, аркушів, копій) і результат видачі: успішний (весь обсяг), неуспішний.

5.2.5. Напади

Розглянута вище модель автентифікації є досить абстрактною. Оскільки життя завжди різноманітне у своїх проявах, існують деякі досить "хитрі" види нападів, які важко передбачити теоретично. Зупинимось на трьох прикладах.

1) **"Лобові" напади.** Так можна назвати найбільш примітивні напади, від яких усі в основному й захищаються. Вважається, що зловмисник знає алгоритм постановки підпису й обчислення ХФ і має у своєму розпорядженні потужні обчислювальні ресурси.

Загальноприйнято, що стійкість системи підпису RSA заснована на трудомісткості завдання факторизації (розкладання більших цілих чисел на множники), а стійкість системи підпису Ель-Гамала заснований на трудомісткості завдання дискретного логарифмування. Ці два математичні завдання відомі досить давно, і дотепер для них не знайдено ефективних алгоритмів. Однак це зовсім не означає, що таких алгоритмів не існує. В останні роки (саме у зв'язку із криптографічною проблематикою) ці завдання активно вивчаються математиками всього світу. Якщо для них будуть знайдені ефективні алгоритми, це буде означати крах відповідних криптосистем. Ще сім-вісім років тому рішення зазначених завдань уважалося нереальним для чисел порядку 10^{100} . З тих пір розвиток теорії обчислювальних алгоритмів і самої обчислювальної техніки просунулися настільки, що навіть модулі порядку 10^{200} багатьма криптографами визнаються недостатньо більшими.

Варто мати на увазі, що описуваний напад навіть для порядків модуля близько 10^{100} вимагає колосальних обчислювальних витрат. Описана в літературі проведена факторизація чисел порядку 10^{10} здійснена в результаті місячної роботи мережі комп'ютерів VAX.

2) **Напади, у яких бере участь секретарка.** Припустимо, що документи вам на підпис готує секретарка, що (свідомо чи ні) працює в інтересах ваших супротивників. Ваші супротивники сформували документ, про який ви не підозрюєте, і який не має бажання підписувати (наприклад, який-небудь дарчий папір від вашого імені).

Тепер їм необхідно, щоб під даним документом стояв ваш підпис. Як це зробити? Можна запропонувати спосіб підбору документа з потрібною ХФ. Припустимо, ви дали вказівку секретарці сформуванати який-небудь черговий потрібний документ. Вона відносить його вашим конкурентам і ті намагаються видозмінити його так, щоб документ, з одного боку, зберіг потрібний зміст, а з іншого боку, щоб значення ХФ для нього збіглося б із значенням ХФ для документа, сформованого вашими конкурентами (дарчої). Далі ви підписуєте видозмінений документ, а зловмисники використовують ваш підпис під ним. Ваш підпис можна "відрізати" і "приклеїти" до іншого документа, і якщо в нового документа значення ХФ збіжиться зі значенням ХФ старого документа, то при перевірці підпису новий документ (дарчу) визнають справжньою.

Ця видозміна може бути зроблена так, що ви ні про що не здогадаєтеся, оскільки, наприклад, додавання зайвого пробілу ніяк не відіб'ється на змісті документа, але може значним чином змінити його ХФ. Робота зловмисників для здійснення такого нападу може тривати довгий час, багато місяців. При цьому вони будуть намагатися видозмінити черговий документ на підпис. Якщо цей проміжок часу помножити на швидкодію комп'ютерів, які є в розпорядженні зловмисників, то вийде досить значна цифра. Крім того, для рішення завдань такого типу існує своєрідний чисто алгоритмічний прийом, що в англійській літературі називають "методом зустрічі посередині". Суть цього прийому полягає в тому, що під одне значення ХФ можна "підганяти" одночасно обидва документи, той, котрий ви підпишете, і той, до якого ваш підпис потім "приклеять".

Описаний напад із криптографічної точки зору є нападом на ХФ; властивий алгоритм із відкритим ключем, що реалізує схему підпису, може бути як завгодно стійким. Факт існування пари документів з однаковим значенням ХФ в англійській літературі прийнято називати "колізією". Щоб протистояти описаним нападам, які можна назвати нападами, заснованими на підборі документів, що підписуються, ХФ обраної схеми підпису повинна задовольняти твердим криптографічним вимогам. З погляду можливих наслідків описаний напад є "необразливим" із усіх можливих, оскільки в розпорядженні зловмисника виявляється лише один-єдиний підроблений документ. Для підробки інших підписаних вами документів йому знову буде потрібна значна обчислювальна робота.

Далі, знайомство із секретаркою може виявитися на руку вашим конкурентам, якщо для підробки вашого підпису їм будуть потрібні які-небудь додаткові дані. Кожен документ, що ви підписуєте, може бути підготовлений зловмисниками спеціальним чином, наприклад, так, щоб одержати потрібні математичні рівняння щодо невідомих біт секретного ключа вашого підпису.

3) *Напади на того, хто перевіряє.*

Попередній приклад показує, що для одержання фальшивого документа зловмисникові не обов'язково розкривати секретний ключ підпису. Виявляється, для досягнення своїх цілей зловмисник може взагалі не вступати в контакт із особою, підпис якого він хоче підробити, і не проводити ніяких дій із розкриття. Існують напади на перевіряючу сторону.

Припустимо, що в нашій мережі немає центра й кожен абонент зберігає на своєму комп'ютері каталог відкритих ключів всіх тих, від кого він може одержувати повідомлення. Ця ситуація є цілком реальною й тоді, коли в мережі є центр, кожне підписане повідомлення супроводжується сертифікатом, тобто ще одним повідомленням, підписаним центром, у якому містяться ім'я й відкритий ключ відправника. В останньому випадку з міркувань тимчасових витрат є більш зручним не перевіряти щоразу підпис центра на сертифікаті, а робити це лише перший раз, з появою нового абонента. Коли надійде наступне повідомлення від цього абонента, можна зрівняти сертифікат з тим, що зберігається в каталозі, і для якого підпис центра вже перевірений.

Зловмисник, якщо, звичайно, він має доступ (хоча б короточасний) до перевіряючого ПК, може просто змінити відповідні записи в каталозі, написавши замість свого прізвища ваше. Якщо тепер він надішле повідомлення, підписане ним, то програма перевірки на комп'ютері зі зміненим каталогом покаже, що дане повідомлення підписане вами. Зрозуміло, що певну вигоду від такої операції зловмисник може одержати, і ця вигода може виявитися більшою, ніж витрати на секретарку, що включила для нього комп'ютер шефа. Слід зазначити, що необхідність підтримки каталогу відкритих ключів (уведення нових абонентів або нових ключів у старих абонентів, видалення ключів абонентів, що вийшли з мережі, перевірка термінів дії ключів і

сертифікатів, нарешті, цей каталог може просто переповнитися) створює передумови для описаного нападу.

Особливо слід зазначити, що описаний напад на каталог відкритих ключів можливий іноді й у тих випадках, коли інформація в ньому зашифрована. (Це може здатися неймовірним навіть для фахівців!) Наприклад, у каталозі в зашифрованому вигляді зберігаються відкриті ключі абонентів. Причому шифрування влаштоване так, що для закриття кожного запису використовується той самий шифр, нехай навіть дуже стійкий, наприклад, ДЕРЖСТАНДАРТ 28147 у режимі простої заміни (на тому самому ключі). Такий спосіб шифрування цілком природний, він зручний при уведенні нових і редагуванні старих записів. Однак зловмисникові для здійснення описаного нападу зовсім не обов'язково розкривати шифр! Він може просто змінити між собою шифровані записи відкритих ключів, свого й вашого, залишивши при цьому незмінними всі інші дані.

Розглянуті напади можна розкласифікувати за ступенем шкоди, яка наноситься зловмисником. Найважчі для мережі з виділеним центром наслідки має напад, при якому порушник може підробляти підпис центра. Це означає, що порушник зможе виступати як будь-яким абонентом мережі, виготовляючи відповідні сертифікати. Далі, якщо порушник зміг розкрити (або викрасти) секретні ключі якого-небудь абонента, то, мабуть, він може підписати будь-яке повідомлення від імені даного абонента. Нарешті, можливі напади, при яких зловмисник може підписати тільки одне складене ним повідомлення від імені даного абонента.

Для здійснення своїх планів зловмисник може застосовувати ті або інші "оперативні" методи.

По-перше, зловмисник може мати у своєму розпорядженні зразки документів, підписаних його потенційною "жертвою".

По-друге, зловмисник може готувати "на підпис" документи для "жертви" і використовувати поставлені під ними справжні підписи у своїх цілях.

По-третє, він може одержати доступ до комп'ютера абонента, підпис якого він хоче підробити. Тут треба розрізняти дві ситуації: або зловмисник може змінити програму підпису (наприклад, "посадити" криптовірус), або він може скористатися якою-небудь інформацією, що має відношення до цієї програми.

По-четверте, зловмисник може одержати доступ до комп'ютера абонента, що перевіряє, для того, щоб змінити програму перевірки підпису у своїх цілях.

В-п'ятих, зловмисником може виявитися розроблювач програмного комплексу (іншими словами, у систему закладені потенційні слабкості). Не слід думати, що це екзотична можливість. Принаймні у практиці створення систем захисту інформації таке іноді трапляється.

Більшість описаних нападів мають сенс тільки в тому випадку, коли зловмисникові відомі алгоритми обчислення й перевірки підпису, а також алгоритм обчислення ХФ. Як правило, у комерційних програмних продуктах ці алгоритми не афішуються, говориться лише про метод цифрового підпису (наприклад, RSA, Ель-Гамаль і пр.). Більш того, як правило, такі програми захищені від копіювання, і безпосереднє дизасемблювання неможливе.

З огляду на викладене вище, можна зробити наступні висновки. Якщо користувач поводить себе грамотно з погляду дотримання норм таємності (зберігання секретних ключів підпису, робота з "чистим" програмним продуктом, що здійснює функції підпису) і тим самим виключає можливість викрадення ключів або несанкціонованої зміни даних і програм, то стійкість системи підпису визначається винятково її криптографічними якостями. Якщо ці якості недостатньо високі, завдання підпису може бути вирішене, однак зловмисник при цьому повинен мати у своєму розпорядженні значні обчислювальні ресурси й мати високу кваліфікацію як криптограф.

5.3. Нормативні положення, що регламентують ІЕБ

5.3.1. Окремі положення Кодексу про адміністративні правопорушення

Стаття 164-9. Незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних. Розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, упаковки яких не марковані контрольними марками або марковані контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного

реєстру одержувачів контрольних марок, тягне за собою накладення штрафу від десяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, БД.

Та сама дія, вчинена особою, яка протягом року була піддано адміністративному стягненню за одне з правопорушень, зазначених у частині першій цієї статті, тягне за собою накладення штрафу від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, БД.

Стаття 195-5. Незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації.

Незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації – тягне за собою накладення штрафу на громадян від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та на посадових осіб – від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з конфіскацією спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації.

Стаття 212-6. Здійснення незаконного доступу до інформації в автоматизованих системах. Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, тягне за собою накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу або без такого.

Та сама дія, вчинена особою, яка протягом року було піддана адміністративному стягненню за порушення, передбачене в частині першій цієї статті, тягне за собою накладення штрафу від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

5.3.2. Окремі положення Кримінального кодексу

Стаття 176. Порухення авторського права і суміжних прав.

1. Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, **комп'ютерних програм і баз даних**, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у великому розмірі, караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк із конфіскацією всіх примірників творів, матеріальних носіїв комп'ютерних програм, БД, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

2. Ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди в особливо великому розмірі, караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років, з конфіскацією всіх примірників творів, матеріальних носіїв комп'ютерних програм, БД, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

3. Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища щодо підлеглої особи, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до двох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. У статтях 176 та 177 цього Кодексу матеріальна шкода вважається завданою у великому розмірі, якщо її розмір у двісті та більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі, якщо її розмір у тисячу й більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 359. Незаконне використання спеціальних технічних засобів негласного отримання інформації.

1. Незаконне використання спеціальних технічних засобів негласного отримання інформації – карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк.

2. Ті самі дії, якщо вони вчинені повторно, за попередньою змовою групою осіб або організованою групою, або заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, – караються позбавленням волі на строк від трьох до семи років.

Стаття 360. Умисне пошкодження ліній зв'язку. Умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, дротового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку, – карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до одного року, або обмеженням волі на строк до двох років.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років, або без такого та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено несанкціоноване втручання і які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та

з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено несанкціоноване втручання і які є власністю винної особи.

Примітка. Значною шкодою у статтях 361 – 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, караються штрафом від п'ятисот

до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут чи розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

1. Несанкціоновані зміна, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміни, знищення або блокування інформації, що є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду караються позбавленням волі на строк від трьох

до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років із позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, що є власністю винної особи.

Юридична практика, як завжди, відстає від досягнень техніки. На думку авторів, загальне подання про можливі правові наслідки використання вірусів, а також про правові наслідки публікації програм-

вірусів дає користувачам-програмістам фундаментальна робота *"Комп'ютерні віруси й право"*. Ця робота, відома дотепер лише вузькому колу фахівців, була написана кандидатом юридичних наук з Гамбургу Стефаном Акерманом, що цікавиться всіма правовими питаннями, яка належить до апаратного, ПЗ й телекомунікації. Первісна версія наведеного нижче тексту була вперше опублікована в гамбурзькій поштовій скриньці CLINCH (а потім і в деяких інших некомерційних поштових скриньках); тут вона вперше представляється широкій читацькій аудиторії в стислому й переробленому вигляді.

Завдяки зростаючій руйнівній силі комп'ютерних вірусів (КВ) вони стали улюбленою темою загальної й спеціальної преси, радіо й телебачення. У повідомленнях йдеться в основному про чисто технічні питання, наприклад, що таке вірус, як він програмується й застосовується й, зрозуміло, як можна захиститися від КВ.

Але при цьому майже зовсім ігноруються або розглядаються не компетентно не менш актуальні правові аспекти програмування й застосування КВ.

Матеріал призначений не тільки для юристів. У досить доступній і зв'язаній формі тут пояснено, які правові наслідки можуть мати розробка, публікація й поширення програм-вірусів. Зрозуміло, що обговорюються правові можливості відшкодування винуватцем потерпілому збитку, заподіяного дією програм-вірусів. При цьому не зупиняються на надзвичайно складному питанні доказу провини.

КВ, як і вся комп'ютерна технологія, досить нова проблема. А правова наука реагує на технічні нововведення з більшим запізненням. Наприклад, тема КВ практично не порушена в сучасній літературі і юридичній практиці. Тому висловлені тут ідеї не опираються на сформовані подання в літературних джерелах, і до них варто ставитися з розумною обережністю, а не розглядати як непорушний закон природи. Проте автор схильний думати, що доти, доки юридична практика не буде забезпечувати надійну правову захищеність і чітке формулювання правових норм, ці ідеї можуть бути необхідним орієнтиром.

Загальний огляд

З технічної точки зору різні види КВ відрізняються за принципом їхнього впливу. Але в правовому аспекті ці розходження несуттєві, оскільки всі види КВ змінюють, обробляють або руйнують дані. А це означає, що в правовому відношенні КВ рівнозначні. Насправді, якщо

такі КВ впроваджуються в чужу систему й заподіюють їй збиток, виникає природне запитання: хто повинен нести за це відповідальність. Така відповідальність може мати насамперед правову основу. Крім того, розглядається й цивільний позов про відшкодування збитку.

Тобто, застосування КВ може мати два зовсім різних наслідки відповідно до кримінально-правових і цивільно-правових норм. Обидва види відповідальності окремо розглянуті в наступних розділах. Описано основні норми і їх правові наслідки. Показано, що застосування цих норм при здійсненні злочину однією особою, без співучасників, проблем не викликає. Труднощі в правовому відношенні виникають тоді, коли потрібно розрізнити посереднє виконання або співвиконання, а також у випадках співучасті в чужому діянні, тобто у випадках підбурювання або пособництва. Для багатьох це області неусвідомленої правової відповідальності, оскільки не всі усвідомлюють те, що відповідальність може нести не тільки прямий виконавець. Тому в доступній формі пояснюється, за яких обставин розглядається виконання або співучасть.

І, нарешті, розглянутий ряд конкретних випадків, для яких застосовуються ці (а якщо необхідно, і інші) основні закони, щоб конкретно показати, для яких дій із КВ варто очікувати правових наслідків і яких дій безпечні.

5.3.3. Кримінально-правові наслідки

Спочатку розглянемо норми карного права, що стосуються в першу чергу використання КВ. Потім торкнемося питань виконавства й співучасті.

1. Існуючі норми карного права. КВ найчастіше руйнують програми, що зберігаються в пам'яті, або масиви даних або змінюють ці дані без їх руйнування.

2. Виконання й співучасть. Порівняно зі злочином, зробленим однією особою за чинними нормами, набагато складніше; класифікуються випадки посереднього виконання, співвиконання, підбурювання й пособництва. Йдеться про те, що злочинець не обов'язково сам впроваджує вірус, а сприяє іншому в здійсненні такого діяння. І тут настає карне покарання, оскільки співучасть у різних формах повинна класифікуватися з урахуванням ступеня участі, передбаченого спеціальною частиною КК.

Тут лише дається спроба коротко описати ситуації, коли настає караність за співучасть, посереднє виконання, підбурювання й пособництво.

3. Співвиконання. При впровадженні вірусу групою осіб однаковому покаранню піддається кожен із членів групи. Співвиконання має місце тоді, коли учасники ухвалили рішення щодо здійсненні діяння спільно, рівноправно, з поділом функцій, і відповідно до цього рішення зробили спільну дію, спрямовану на здійснення злочину. Співвиконання має місце також у тому випадку, якщо розподіл функцій характеризується тим, що один учасник програмує вірус, а інший його впроваджує. Отже, злочинцем є не тільки той, хто безпосередньо впровадив вірус у чужу систему.

4. Посереднє виконання. Злочинним вважається й діяння, коли злочинець діяв не сам, а спонукав діяти у своїх інтересах іншу особу, а сам як посередній виконавець залишився в тіні. Посереднє виконання має місце, якщо (посередній) виконавець використовується приблизно як інструмент (хоча інструмент проти самого себе). Використання як інструмент має місце найчастіше тоді, коли посередній виконавець знає набагато більше, ніж використовуваний ним "інструмент". Наприклад, злочинець знає, що дискета, яка лежить поруч із ПК, містить вірус. Власник комп'ютера цього не знає. Якщо посередній виконавець запропонує власникові завантажити дискету із цікавою ігровою програмою, і власник, нічого не підозрюючи, зробить це, то він як би сам впровадить шкідливий вірус. Проте діяння приписується посередньому виконавцеві, тому що в цьому випадку власник комп'ютера через перевагу злочинця в знаннях був використаний лише як інструмент проти самого себе.

5. Підбурювання. Покарання за підбурювання настає тоді, коли деяка модель поведження передбачається злочинцем, що мотивує небезпеку, щоб передбачувані виконавці прийняли відповідне рішення, а потім і реалізували його. Якщо злочинець дійсно приймає відповідне злочинне рішення й реалізує його в протиправному діянні, то підбурювач повинен зазнавати кари.

Караність за підбурювання до зміни даних і інші злочини, пов'язані із КВ, приховує у собі деякій мірі "підривно силу" у зв'язку з усе більшим поширенням програм-вірусів і радою про те, як використовувати КВ.

6. Пособництво. За своїм характером пособництво дуже близьке до підбурювання. Для складу злочину необхідне сприяння, запропоноване злочинцеві, прийняте ним і використане потім при здійсненні основного злочину. Злочинець не обов'язково повинен знати про те, що йому надана допомога. Запропоноване й прийняте сприяння, але не реалізоване потім в основному злочині, не розглядається як пособництво.

У деяких випадках пособництво важко відрізнити від співвиконання, причому особливості цих різновидів злочини є предметом запеклих суперечок. У досить спрощеному вигляді співвиконання має місце, якщо діюча особа здійснює діяння зі своєї волі, а пособництво – якщо із чужої волі. Відповідно до іншого трактування, яке поділяє автор посібника, варто виходити з того, хто здійснював панування над діянням.

5.3.4. Цивільно-правові наслідки

Спочатку розглянемо найбільш важливі норми громадянської відповідальності, а потім торкнемося питання про відповідальність учасників за відповідне діяння.

1. Норми відповідальності. У першу чергу розглядається відповідальність за відшкодування збитку.

2. Відповідно до закону збиток повинен бути відшкодований, якщо через недбайливість або навмисно було порушене право власності або інше право потерпілого.

Порушення права власності, безсумнівно, має місце, якщо КВ призвів до ушкодження апаратних засобів. Але на питання, чи можна кваліфікувати перекручування даних або програм як порушення права власності або якого-небудь іншого права, відповісти досить важко. Порушення права власності виключається, тому що дані й програми не є майном. Отже, закон застосуємо тільки щодо порушення "інших прав". Сумнівно, що "володіння" або "право власності" на програми й дані захищаються в які "інші права". Тут питання можна залишити відкритим, тому що воно розв'язується тільки в окремих конкретних ситуаціях.

3. Відповідно до закону повинен бути відшкодований збиток, заподіяний у результаті порушення того закону, що повинен (щонайменше) захищати потерпілого. Такими охоронними законами є

вже написані вище норми кримінального права. Це значить, що порушення цих норм спричиняє відшкодування збитку на користь потерпілого.

4. І, нарешті, діє параграф, що особа, яка порушила загальноприйняті моральні норми й тим самим навмисно заподіяла збиток іншій особі, повинна відшкодувати збиток. Це положення може, як правило, застосовуватися для тих випадків, коли навмисне впровадження вірусу завдало шкоди, яка має бути відшкодована.

5. Договірні претензії. Поряд із уже розглянутими делікатними претензіями, як виняток, розглядаються й договірні претензії. Але й у цих випадках найчастіше має місце делікатна відповідальність, строки дії якої за певних обставин більш сприятливі для потерпілого (а саме, якщо відповідальність за поставку продукції з порушенням договірних умов). Ці делікатні претензії втрачають силу за давниною через три роки після встановлення збитку і його винуватця (саме пізніше через 30 років).

6. Відповідальність при декількох виконавцях. Згідно з законом під час здійсненні злочинного діяння декількома виконавцями всі учасники відповідають за заподіяний збиток, як солідарні боржники. Форма участі не розрізняється. Це означає, що кожен, хто вніс який-небудь причинний внесок у виникнення збитку й хто несе відповідальність, може бути визнаний єдиним відповідачем із відшкодування всього збитку, навіть якщо він діяв не поодиноці або виступав як пособник або співучасник. Потерпілий може вибрати, зажадати або відшкодування збитку від всіх учасників з урахуванням частки збитку, заподіяного дією конкретної особи, або зажадати повної компенсації лише з одного учасника (найбільш платоспроможного або того, кого він хотів би покарати особисто). Правда, усередині є вимоги компенсації, згідно з яким кожному висуваються претензії лише відповідно до його часток заподіяного збитку. А якщо позов на повне відшкодування збитку висувається лише одному зі співучасників, виникає небезпека, що вимогу відшкодування збитку іншим особам, які заподіяли збиток, не вдається задовольнити.

Це досить ризиковано, оскільки суми збитку для КВ, що надзвичайно швидко поширюються й паралізують на тривалий строк велику кількість ЕОМ, можуть досягати сотень і навіть мільйонів. Мільярдні збитки не такі вже й немислимі! Це стане зрозумілим із наведеного нижче підрахунку, який підлягає відшкодуванню збитку.

7. Міра відповідальності. Існує принцип: повинен бути відновлений стан, що існував до заподіяння збитку, або бути зроблене капіталовкладення, необхідне для відновлення цього стану. Мають бути компенсовані всі адекватно-каузальні наслідки збитку, а також недоотриманий прибуток.

При виході з ладу ураженої вірусом центральної ЕОМ великого підприємства, наприклад великого банку, сума збитку може досягнути таких розмірів, що компенсувати його приватній особі не вдасться до кінця життя.

Окремі випадки

Віруси на дискетах з безкоштовним ПЗ. Одним із найбільш розповсюджених джерел програм-вірусів є безкоштовне ПЗ, що все частіше виявляється зараженим КВ. Відповідальність злочинця, який "заразив" таку програму безкоштовного ПЗ, можна без зусиль кваліфікувати відповідно до вже розглянутих норм. Він несе карну відповідальність, а також громадянську відповідальність за відшкодування збитку. Такий збиток може бути досить значним, якщо виходити із дуже швидкого розповсюдження безкоштовного ПЗ й великої кількості користувачів, які можуть постраждати.

Але питання про правові наслідки для постачальників безкоштовного ПЗ, що поставляють окремі із пропонованих ними програм зараженими КВ, проблематичний. Безкоштовне ПЗ поширюється численними відправниками, що регулярно публікують свої оголошення в журналах із обчислювальної техніки, а також через поштові скриньки, які дозволяють безпосередньо звертатися до областей загального користування лініями зв'язку. Варто розрізняти ці два види поширення безкоштовного ПЗ:

1. Відповідальність відправників дискет з безкоштовним ПЗ. Оскільки виходять із того, що відправник дискет з безкоштовним ПЗ ненавмисно поширює заражені КВ програми, його караність у цьому виключається. Невідомо, чи спроможний він нести цивільну відповідальність за збиток, заподіяний розповсюдженими ним "зараженими" програмами. Розглядається як відповідальність за договором, так і відповідальність, що впливає із правопорушення.

2. Відповідальність відповідно до договору. Для вирішення питання про договірну відповідальність відправника спочатку потрібно з'ясувати, чи існує взагалі договір, і якщо так, то який тип цього договору. Договір

був би відхилений через відсутність передбачених правом зобов'язань, якщо йдеться про так звані "дружні зв'язки". Дружні відносини мають місце при угодах на винятково позаправовій основі – так, наприклад, як дружба, порядність або честь. Тому потрібне підтвердження про наявність договору, тому що, очевидно, не можна виходити тільки із суто дружніх відносин, якщо пропонується пересилання дискет по оголошенню за більш-менш високу плату, що повинна служити не тільки для відшкодування витрат, але й для одержання прибутку. Тут має місце чиста угода.

Сумнівно, чи є це контрактом. Імовірно, може йтися про договір купівлі-продажу. Але це не вимагається до ПЗ, тому що в цьому випадку йдеться про некомерційні програми, не призначені для продажу. Це швидше відшкодування витрат на послугу (копіювання й пересилання), а також на поштові послуги, упакування, самі дискети й т. п. Отже, договір варто розглядати або як трудову угоду, або як змішаний договір з перевагою компонентів трудової угоди.

Можна розглядати відповідальність за позитивне порушення умов цієї трудової угоди, якщо відправник винний у порушенні передбачених договором додаткових зобов'язань.

Але викликає сумнів, чи можна пересилання зараженого КВ безкоштовного ПЗ кваліфікувати як порушення додаткових договірних зобов'язань.

Звичайно, до числа додаткових зобов'язань кожного договору включається пункт про запобігання збитку для свого партнера. Виходячи із цього, копіювання й пересилання заражених КВ програм повинні кваліфікуватися як порушення додаткових умов договору.

Проблематичною є винність у порушенні додаткових договірних зобов'язань. Це залежить від того, чи знав відправник або чи належний він знати про те, що відіслана програма заражена. В остаточному підсумку це питання знов-таки залежить від того, чи зобов'язаний розповсюджувач безкоштовного ПЗ перевіряти їх на зараженість КВ, і якщо так, то як далеко заходить обов'язок дослідження.

На думку автора, відправник зобов'язаний шукати КВ, що може бути легко виявлений, але він навряд чи заслуговує докору, якщо не зумів установити КВ, шкідлива дія яких виявляється тільки в ході тривалого використання програм або в результаті їх систематичного перегляду. Це означає, що відправник відповідає за позитивне

порушення договору, якщо користувачеві безкоштовної програми завданий збиток при її безпосередньому застосуванні. Прикладом може бути програма формування жорсткого диска (така програма часто є не KB, а так званим "троянським конем"). Можна виключити договірну відповідальність за заражені вірусом програми, які приводять до відчутного збитку в результаті тривалого використання, і тоді, коли це шкідливий вплив програми було неможливо виявити простими засобами (що швидше типово для KB).

3. Відповідальність за злочин. Якщо виходити з того, що навмисне діяння відправника не було регулярним, як підстава для висунення претензій за злочинне діяння може розглядатися тільки при заподіянні збитку. Часто правомірніше стає тільки постановка питання про порушення "інших прав". Особисто автор розглядав би "володіння" або "власність" на програми й дані як інше право, аналогічне праву власності. Питання в тому, як до цього поставиться судова практика.

Оскільки тут йдеться про порушення інших прав, умовами пред'явлення позову є заподіяння збитку через необережність відправника. Сюди відноситься все викладене вище щодо договірної відповідальності.

4. Відповідальність власників поштових скриньок – власник поштової скриньки також не є свідомим розповсюджувачем заражених KB програм лініями зв'язку. Отже, для нього виключається як карна, так і громадянська відповідальність за злочин (з урахуванням згаданого обмеження). Як і відправник безкоштовного ПЗ, власник може нести договірну відповідальність за відшкодування збитку.

Первинною умовою повинна бути наявність договору між власником і користувачем поштової скриньки. Наявність договору для комерційних поштових ящиків (наприклад, GEONET) обов'язкова. Але й некомерційні ящики часто засновані на договірних відносинах між власником і користувачем (наприклад, CLIN CH).

Зовсім інша справа з так званими "FreakBox", користувачем яких може стати будь-яка особа, часто без будь-яких формальностей. У цьому випадку оператор системи із чистої люб'язності надає свою поштову скриньку в розпорядження зацікавлених користувачів, не беручи на себе ніяких правових зобов'язань. Ця обставина відома й користувачеві. Тут відсутній договір між власником і користувачем поштової скриньки й, отже, відсутня і договірна відповідальність власників "FreakBox".

Власники інших видів поштових скриньок, заснованих на договірних відносинах між референтом і користувачем, відповідають за позитивне порушення договору. Тут справедливе все викладене вище щодо розповсюджувачів безкоштовного ПЗ. Відповідальність власника поштової скриньки в значній мірі залежить від того, чи спроможний він був розпізнати заражені КВ програми. Як і у випадку з відправником програм, на це питання можна було б відповісти ствердно, якщо шкідливий вплив КВ легко виявити, наприклад, шляхом виклику простої програми.

Правда, проблема тут полягає в тому, часто власник поштової скриньки не завжди має можливість одержати доступ до програми, який він сам не розташовує. Тому він може просто не в змозі провести коротку перевірку програм. Відповідальність власника в таких випадках є сумнівною. Автор хотів би зробити "наголос" на вирішення цього питання й тому лише зазначив тему.

Віруси в комерційних програмах

Існує дві основні проблеми, пов'язані із КВ у комерційних програмах. По-перше, розроблювач може сам занести КВ до програми. Це може бути зроблено й через недогляд, хоча й розглядалося питання про можливість використання КВ як засобу захисту від копіювання. Але тут маються на увазі тільки певні види програм, що самі стираються. Хоча і виникають деякі складності правового характеру, вони ніяк не пов'язані з вірусами, і тому тут не розглядаються. КВ як засіб захисту від копіювання дотепер не зустрічалися й, на думку автора, безглузді.

З іншого боку, цілком можливе впровадження КВ у пакет програм третьої сторони, наприклад конкурентом, що хоче нашкодити виготовлювачеві й тим самим розширити збут власної продукції.

Нижче розглядається так зване стандартне ПЗ. Індивідуальне ПЗ, тобто програми, спеціально написані або дороблені для конкретного клієнта, не мають істотного значення для користувачів побутових або персональних комп'ютерів і тому тут не розглядаються.

Третя особа, що впровадила КВ у пакет програм, повністю підпадає під діючі норми як цивільного, так і кримінального права.

Інтерес становить відповідальність виготовлювача й, оскільки користувач не має прямого контакту з виготовлювачем, відповідальність продавця.

Для більшості ймовірних випадків через відсутність навмисності кримінальна відповідальність виключається. Можуть бути розглянуті тільки цивільні позови на відшкодування збитку.

Тут справедливо все викладене щодо відповідальності розповсюджувачів безкоштовного програмного забезпечення. Нижче розглянуті лише особливості, що стосуються комерційних програм.

1. Відповідальність виготовлювача. Якщо ПЗ здобувається в посередника, а не у виготовлювача, то договірні відносини існують тільки із продавцем. Отже, стосовно виготовлювача можуть розглядатися не договірні, а делікатні претензії. Інша справа, якщо виготовлювач добровільно бере на себе гарантійні зобов'язання. Але таке для програмного продукту дотепер не практикувалося. А якщо й зустрічається, то, як правило, з такими обмеженнями, які не дозволяють робити які-небудь певні висновки щодо розглянутих тут претензій.

Отже, залишаються відомі делікатні претензії, описані при розгляді безкоштовного ПЗ, з тією лише різницею, що значно раніше потрібно буде підтвердити необхідну необережність. До того ж виготовлювачі комерційного ПЗ мають у номенклатурі дуже небагато програм, які вони знають або у будь-якому випадку повинні знати як свої п'ять пальців. Тому важко припустити, що КВ може потрапити в програму просто через недбайливість виготовлювача.

Якщо виходити з того, що "власність" або "володіння" програмами й даними становлять інше право, опираючись на цю норму для того, щоб домогтися відшкодування збитку від виготовлювача програм.

Якщо ПЗ придбано безпосередньо у виготовлювача, додатково можуть розглядатися й договірні претензії.

2. Відповідальність продавця. Продавець несе як делікатну, так і договірну (позитивне порушення договору) відповідальність. При цьому важливий ступінь його провини, що залежить, зрозуміло, від конкретних обставин. Звичайно, посередник, по-перше, знає програми, що збуваються ним, не настільки добре, як виготовлювач, тому він менше заслуговує на докори в недбалості, ніж виготовлювач. З іншого боку, продавці мають ширші можливості для вивчення й перевірки програм, що поставляються ними, ніж розповсюджувачі безкоштовного ПЗ. Тому продавці повинні були б більш ретельно дотримуватися інтересів торговельного партнера, ніж відправники безкоштовних програм.

Сказане виглядає досить розпливчасто, однак точніше висловитися можна тільки в конкретних випадках.

Тобто, можна зазначити, що продавець також відповідає за збиток, заподіяний зараженими КВ комерційними програмами, якщо в конкретному випадку його вдається обвинуватити в недотриманні інтересів покупця.

КВ, що маніпулюють даними

Як уже було сказано, КВ найчастіше здійснюють руйнуючу дію. Однак існують і маніпулюючі КВ, які вимагають спеціальної правової оцінки. Тут розглядається тільки відповідальність за різні види маніпулюючих вірусів, на основі КК. Цивільно-правові аспекти не вимагають деталізації, тому що процес впровадження маніпулюючого вірусу, є кримінально карним діянням.

1. Віруси, що реалізують корисливі інтереси. Можна уявити собі впровадження КВ, що реалізують корисливі цілі в інтересах злочинця або третьої особи. Наприклад, можливий випадок, коли за допомогою КВ виробляється регулярне перерахування на рахунок злочинця. Майновий збиток карається позбавленням волі строком до п'яти років або грошовим штрафом. В особливо важких випадках можливе позбавлення волі до десяти років. Карна також і спроба здійснення такого злочинного діяння.

2. Віруси, що відкривають доступ до КС. Можливий різновид КВ, що відкриває користувачеві доступ до закритого для нього КС або до певних областей пам'яті. Такий вірус дає можливість користувачеві виконувати свої програми або використовувати систему яким-небудь іншим способом без відповідного дозволу. Він може також одержати можливість читати або заміняти дані, не маючи до них права доступу.

Законодавець, всупереч первісним планам, не включив у закон так звану крадіжку машинного часу, і тому користувач не несе відповідальності за використання ЕОМ у випадках, для нього не передбачених. Чи буде таке трактування застосовуватися в судовій практиці, покаже час. Але не дуже давно один із судів (суд другої інстанції м. Кельна, "Новий юридичний щотижневик" 87, с. 667) висловив сумнів у конституційності № 263а КК через нібито розпливчате формулювання з більшим числом застережень, так що можна чекати досить обмеженого застосування № 263а КК у судовій практиці й

покарання за крадіжку машинного часу не як за шахрайство з використанням ЕОМ. Тут лише можна почекати розвитку подій.

У результаті проникнення в КС або в певну область системи, закриту для користувача, він, мабуть, змушений буде прочитати дані, що зберігаються в цій системі. Звідси випливає, що користувач, який застосовує КВ (а не особу, що його впровадила!), відповідає за шпигунство відповідна. Його можуть піддати позбавленню волі строком до трьох років або грошових штрафів.

3. Віруси, що генерують файли реєстрації інфікованих програм. Обговорюються КВ, здатні генерувати файл реєстрації для певних програм, з якого можна одержати наступну інформацію: хто, коли, як і яку використовував програму, які роботи були виконані в результаті цього використання і яких паролів застосовувалися для доступу до програм.

Впровадження такого вірусу, зрозуміло, карає КК. Проблематичним є застосування № 202а КК (шпигунство за даними). Справді, № 202а КК визначає покарання за одержання або передачу іншій особі спеціально захищених даних, не призначених для користувача.

В № 202а КК йдеться про шпигунство за даними, що вже зберігаються в системі. Але в розглянутому тут випадку ці дані були сформовані в результаті втручання КВ у програму. Отже, йдеться не про існуючі дані.

Однак, таке судження не охоплює всі можливі випадки. Справді, при занесенні у файл реєстрації пароля йдеться про інформацію, що хоча й заноситься у файл реєстрації знову, але вже була записана в іншому місці системи, а тому її прочитання можна кваліфікувати як шпигунство. Із цього погляду генерація файлу реєстрації становить лише спеціальний метод шпигунства за даними, за яким покладається покарання.

4. КВ, що виготовляють фальшиві документи. Фальсифікація отриманих при зборі доказів даних, що знову уведений у КК у рамках другого закону про відповідальність за господарські злочини, той, хто з метою обману при оформленні правовідносин запишуть отримані при зборі доказів дані або змінить їх таким чином, що це привело б до перекручування або фальсифікації документів, карається позбавленням волі строком до п'яти років, а в особливо таких випадках строком до 15 років. Покаранню підпадають і ті, що використовують записані в такий спосіб або змінені дані. Це має місце при впровадженні маніпулюючих

КВ, зокрема, уже розглянутих КВ, що реалізують корисливі інтереси. Через передбачені законом досить більших меж покарання (позбавлення волі строком до 15 років – найбільший строк, передбачений КК!).

Підробленим документом були б дані, при сприйнятті яких підмінюється укладач документа, тобто походження даних виявляється іншим, ніж це треба. Документ фальсифікований, якщо справжні дані спочатку були змінені таким чином, що вміст уже не можна віднести до заявника.

Карне також уживання даних, змінених описаним вище шляхом. Уживанням вважається, наприклад, факт передачі даних особі, що вводиться в оману, на носії або вивід їх на екран.

Віруси протесту

У дискусіях про КВ з'явився новий термін "віруси протесту". Тут мається на увазі КВ, використовувані проти ПК, які певні суспільні групи вважають особливо небезпечними, нелюдськими або ті, що становлять яку-небудь загрозу. Зокрема, у пресі промайнули повідомлення про те, що група хакерів і прихильників бойкоту перепису населення планували застосувати віруси проти перепису населення 1987 року.

У зв'язку з цим варто коротко пояснити, якою мірою ці так звані "віруси протесту" можна розглядати як легальний засіб дозволу суспільної суперечності. Питання про те, наскільки легальним є використання "вірусів протесту" тут не розглядається, оскільки це питання не суто правовий, а швидше політичний або морально-етичний.

На питання про правову допустимість "вірусів протесту" відповісти дуже просто: ці КВ нічим не відрізняються від інших. Отже, їх застосування карає відповідно до типового, докладно тут розглянутими карними нормами.

Покарання не призначається лише в тому випадку, якщо застосування КВ виправдане. Навряд чи можна стверджувати, у будь-якому випадку з позиції судової практики, що перепис населення, навіть незаконний, загрожує сутності вільнодемократичного правопорядку. Але навіть якщо це припустити, варто було б спочатку застосувати всі доступні правові засоби, і лише потім скористатися формами протесту.

Із зазначеного випливає, що так звані "віруси протесту" настільки ж незаконні, як і "звичайні" КВ.

Розробка, публікація й поширення

1. Розробка вірусних програм. Розробка вірусних програм сама по собі не є карною з погляду як карного, так і цивільного права. Інша справа, якщо розроблені програми у вигляді вихідного тексту або у вигляді скомпільованої програми за згодою або без згоди автора публікуються або поширюються яким - небудь іншим способом.

2. Публікація або поширення вихідного тексту програми. За публікацію або поширення вихідного тексту програм вірусів для укладача програм або третьої особи, що опублікувала програму, передбачена як карна, так і громадянська відповідальність.

Відповідно до карного права публікація або поширення вихідного тексту програми-вірусу спричиняє покарання за підбурювання або пособництво у зміні даних. Крім того, при використанні спеціальних форм КВ може бути призначене покарання за підбурювання або пособництво відповідно до норм.

Є доцільним розрізняти передачу вихідного тексту окремим особистим знайомим програміста й публікацію програми в пресі або через пош-тові скриньки, доступні великій кількості анонімних користувачів.

3. Поширення вихідного тексту. Поширення вихідного тексту можна розглядати як підбурювання до зміни даних (або до інших злочинів), якщо програміст обговорює з одержувачем вихідного тексту відповідні лінії поведження, у тому числі й у прихованій формі, а одержувач розпоряджається згенерованим ним вірусом, що виконується злочинним чином. За відсутності змови, у тому числі прихованої, підбурювання як таке не може бути інкриміновано.

Проблематичним є доказ провини за пособництво в зміні даних (або в інших злочинах). Якщо одержувач вихідного тексту генерує з нього працездатну програму-вірус і використовує її злочинним чином, то програміст є пособником неправочинної дії, скоєної головним виконавцем злочину. Питання полягає лише в ступені його винності, тобто в навмисності діяння (пособництво через необережність не карна!) Визначальною тут є усвідомленість дій програміста в той момент, тобто розуміння ним усіх істотних ознак правопорушення або діяння (у кожному разі умовно). Програміст повинен, принаймні, усвідомлювати, що своїми діями він сприяв здійсненню іншим злочинного діяння. При цьому не потрібно знати про подробиці самого діяння, тобто хто його зробив і проти кого воно було спрямовано. Навіть заперечення програмістів факту

протиправного використання його вихідного тексту недостатньо, щоб зняти обвинувачення в навмисності. Тому вихідний текст можна передавати тільки особам, яких не можна запідозрити в зловмисному його використанні (або генерованого з нього вірусу).

4. Публікація вихідного тексту. Публікація вихідного тексту програми-вірусу не кваліфікується як пособництво або підбурювання.

Підбурюванням не вважається навіть заклик до протиправного діяння, оскільки підбурювання припускає навмисну дію, що тут відсутня. Навмисність має місце, якщо підбурювачі, навіть якщо їх дії не спрямовані проти конкретної особи, повинні принаймні звернутися до певного їм індивідуального кола осіб. Такий склад відсутній при публікації у вище-описаних середовищах. Із цих же причин, відпадає обвинувачення в карному пособництві.

Проте в публікації вихідного тексту може полягати склад злочину. Тут можна розглянути суспільний заклик до злочинних дій.

Ознакою події "заклик" вважається вплив на іншу особу з метою прийняття ним рішення про здійснення карних дій. Це може відбуватися у формі відмовлення ("обов'язково уникайте"...). Щоб уникнути покарання, важливо не намагатися спровокувати до здійснення протиправного діяння й не натякати на можливість такого рішення.

Із зазначеного випливає, що сама по собі публікація вихідного тексту програми-вірусу ще не несе в собі складу злочину. Залежно від обставин конкретного випадку з контексту публікації (наприклад, заклику бойкоту перепису населення може скластися зовнішнє враження, що йдеться про заклик до протиправного діяння – тут застосування вірусу проти перепису населення).

Тому при публікації вихідного тексту варто звертати увагу на те, щоб з контексту не склалося помилкове (!?) враження, що автор закликає до певної дії. Серйозне додаткове застереження про шкоду вірусу й суто "наукове" мотивування публікації, очевидно, недостатні, щоб виключити підозру в злочині.

Приклади

У журналі або в поштовій скриньці опублікований KB, як коментар подано: "Випробуйте цей вірус на одному з "гарних друзів". Але коментар типу: "Обережно, вірус небезпечний! Дивіться, щоб він не потрапив у ПК, призначений для перепису населення...!" – уже є проблематичним.

Це може бути необразлива, некарана витівка, але може бути й відкритий заклик, що тягне покарання. Все залежить від змісту сумнівного коментарю й від того, наскільки він був зрозумілий адресатом. Не можна однозначно відповісти на запитання, чи є склад злочину в цьому абстрактному прикладі. Але автори коментарю в кожному разі здивуються, якщо їм доведеться докладно розмовляти із прокурором щодо начебто необразливих слів...

Передача й публікація здійснюється програм-вірусів набагато небезпечніше передачі вихідного тексту. Проте можлива провина оцінюється так само, як сказано вище.

Але щодо цивільно-правової відповідальності варто особливо враховувати, що – у ще більшому ступені, ніж при передачі вихідного коду – безумовно, необхідна чітка рекомендація на безпеку програми, а також способу обігу з нею. Інакше при завданні користувачеві збитку за рахунок дії вірусу особа, що передала або опублікувало програму, відповідає за позитивне порушення договору й зобов'язана відшкодувати заподіяний збиток, якщо між партнерами існують договірні зобов'язання (наприклад, між власником і користувачем комерційної поштової скриньки).

Така думка Штефана Акермана про правове положення. Але навіть за допомогою таких докладних суджень неможливо відповісти на всі питання. На завершення зазначимо можливі проблеми, сформулювавши три прості питання:

а) чи порушує авторське право власник ЕОМ, що виявив у себе чужий КВ;

б) чи може автор КВ вимагати видачі або знищення інфікованого ПЗ, що містить програму-вірус;

в) чи може виготовлювач ПЗ, який піддався зараженню КВ, обвинуватити власника ЕОМ у навмисній зміні ПЗ?

На сьогоднішній день не найшлося нікого, хто б зміг або захотів виразно відповісти на ці питання, тому що до кожного питання довелося б становити висновок обсягом у цілу сторінку. У випадку правового конфлікту, безсумнівно, спочатку почнеться суперечка експертів з технічних питань, у якій судді, прокурор та інші учасники процесу будуть почуватися досить незручно.

Таким чином, представлений матеріал буде корисним для використання його як на практиці, наприклад, у службі ІБ підприємства

або у юридичному відділі, так й при теоретичних дослідження подібних областей.

Контрольні питання

МОДУЛЬ 2. Особливості застосування ІБ у бізнесі

ТЕМА 4. Організація інформаційної безпеки комп'ютерних мереж

1. Дайте визначення протоколу автентифікації при вилученому доступі.
2. Дайте визначення цілісності й конфіденційності.
3. Дайте визначення вразливості.
4. Класифікуйте основні типи брандмауерів та файерволів.
5. У чому полягають принципи захисту віртуальних локальних мереж.
6. Области використання програмних засобів запобігання несанкціонованого доступу.
7. Назвіть основні принципи побудови технології захисту мережі – IPSec.

ТЕМА 5. Правові основи ІБ

1. Дайте визначення видів інформації, що належать для захисту.
2. Дайте визначення державної таємниці.
3. У чому полягають принципи відмінності ліцензійної й сертифікаційної діяльності в області ІБ.
4. Области використання патентного й авторського права.
5. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.
6. Юридичний аспект функціонування ГУКБ на підприємстві.

Створення комісії з організації технічного захисту інформації

Варіант наказу керівника організації

Дата

Наказ №

м. Харків

Про створення комісії з організації технічного захисту інформації
на об'єктах інформаційної діяльності

З метою забезпечення інформаційної безпеки на об'єктах
інформаційної діяльності

НАКАЗУЮ:

Створити комісію з організації технічного захисту інформації на
об'єктах інформаційної діяльності (назва організації) у складі:

Голова комісії: заступник генерального директора з ...

Члени комісії:

начальник служби безпеки;

начальник відділу ТЗІ;

начальник відділу інформаційно-комп'ютерного забезпечення;

начальник відділу матеріально-технічного забезпечення;

начальник відділу забезпечення зв'язку;

начальник відділу кадрів

Обов'язки щодо організації робіт з технічного захисту інформації,
що потребує захисту (ІПЗ), покласти на структурний підрозділ ТЗІ.

Начальнику відділу ТЗІ в строк до _____ розробити план-графік
проведення заходів щодо створення системи захисту інформації і подати
для затвердження.

Затвердити Положення про комісію з організації ТЗІ організації
(додається).

Генеральний директор

Типове положення про комісію з організації ТЗІ

Основні завдання комісії з організації ТЗІ:

захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаєминах з іншими організаціями і службами;

дослідження інформаційної діяльності організації з метою виявлення можливих каналів витоку інформації та інших загроз безпеці інформації, формування моделі загроз; розробка політики безпеки інформації; визначення заходів, направлених на її реалізацію;

організація і координація робіт, пов'язаних із захистом інформації в приміщеннях, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

розробка проектів нормативних і розпорядчих документів, які діють у межах організації, відповідно до яких повинен забезпечуватися захист інформації в організації;

організація робіт із створення і використання комплексу СЗІ на всіх етапах інформаційної діяльності;

участь в організації професійної підготовки і підвищення кваліфікації співробітників організації з питань захисту інформації;

формування у співробітників розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

організація забезпечення виконання співробітниками організації вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації та проведення контрольних перевірок їх виконання.

Функції комісії з організації ТЗІ під час створення комплексної системи захисту інформації:

визначення переліку відомостей, які потребують захисту в процесі обробки, інших об'єктів захисту у підрозділах організації, класифікація інформації відповідно до вимог її конфіденційності або важливості;

розробка й коригування моделі загроз і моделі захисту інформації, політики безпеки інформації;

визначення і формування вимог до СЗІ;

організація й координація проектування та розробки СЗІ, безпосередня участь у проектних роботах зі створення СЗІ;

підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами і попередження спроб несанкціонованого доступу до інформації під час створення СЗІ;

організація робіт і участь у випробуваннях СЗІ, проведенні її експертизи;

вибір організацій-виконавців робіт із створення СЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт із захисту інформації, спільно з відділом ТЗІ узгодження основних технічних і розпорядчих документів, які супроводжують процес створення СЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);

участь у розробці нормативних документів, що діють в межах підрозділів організації, які встановлюють дисциплінарну відповідальність за порушення вимог безпеки інформації і встановлених правил експлуатації СЗІ.

Функції комісії з ТЗІ під час експлуатації комплексної системи захисту інформації:

організація процесу управління СЗІ;

розслідування випадків порушення політики безпеки, небезпечних і непередбачених подій, здійснення аналізу причин, що призвели до них;

вживання необхідних заходів у разі виявлення спроб порушення правил експлуатації засобів захисту інформації або інших дестабілізуючих чинників;

забезпечення контролю цілісності засобів захисту інформації і оперативне реагування на їх вихід з ладу або порушення режимів функціонування;

підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації, впровадження нових технологій захисту і модернізації СЗІ;

організація і проведення заходів щодо модернізації, тестування, оперативного відновлення функціонування комплексу СЗІ після збоїв, відмов, аварій комплексу СЗІ;

проведення аналітичної оцінки поточного стану безпеки інформації в підрозділі (прогнозування виникнення нових загроз та їх врахування у моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації та реалізованої політики безпеки поточної моделі загроз тощо);

регулярне подання звітів керівництву організації про виконання співробітниками вимог із захисту інформації;

аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо їх придбання для організації;

контроль за виконанням співробітниками вимог, норм, правил, інструкцій із захисту інформації відповідно до певної політики безпеки інформації, зокрема, контроль за забезпеченням режиму конфіденційності;

контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що потребують захисту;

розробка та реалізація спільно з відділом ТЗІ організації комплексних заходів із безпеки інформації під час проведення заходів щодо науково-технічної, економічної, інформаційної співпраці з іноземними фірмами, а також під час проведення нарад, переговорів тощо, здійснення їх технічного та інформаційного забезпечення.

Функції щодо навчання співробітників організації питанням забезпечення захисту інформації:

розробка планів навчання і підвищення кваліфікації фахівців СЗІ і співробітників;

розробка спеціальних програм навчання, які б враховували особливості технології обробки інформації у підрозділах організації, необхідний рівень його захищеності та ін.;

участь в організації та проведенні навчання співробітників організації правилам роботи з КСЗІ, захищеними технологіями та захищеними ресурсами;

взаємодія з державними органами, навчальними закладами, іншими організаціями з питань навчання і підвищення кваліфікації;

участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та ін.

Повноваження і відповідальність

Повноваження і відповідальність членів комісії з організації ТЗІ

Комісія з організації ТЗІ має право:

здійснювати контроль за діяльністю будь-якого структурного підрозділу організації щодо виконання ним вимог нормативно-правових актів та інших внутрішніх документів із захисту інформації;

подавати керівництву організації пропозиції щодо припинення процесу обробки інформації, заборони обробки, зміни режимів обробки тощо, у разі виявлення порушень політики безпеки або у разі виникнення реальної загрози порушення безпеки;

складати й подавати керівництву організації акти щодо виявлених порушень політики безпеки, пропонувати рекомендації щодо їх усунення;

проводити службові розслідування у випадках виявлення порушень;

діставати доступ до робіт і документів структурних підрозділів організації, необхідних для оцінки вжитих заходів із захисту інформації та підготовки пропозицій відносно їх подальшого удосконалення;

готувати пропозиції щодо залучення на договірній основі до виконання робіт із захисту інформації інших організацій, які мають ліцензії на відповідний вид діяльності;

готувати пропозиції щодо забезпечення організації необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, дозволеною для використання в Україні з метою забезпечення захисту інформації;

звертатися до керівництва організації з пропозиціями щодо подання заяв у відповідні органи і організації на проведення експертизи КСЗІ або сертифікації окремих засобів захисту інформації.

Комісія з організації ТЗІ зобов'язана:

організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів щодо захисту інформації в організації;

своєчасно і в повному обсязі надавати співробітникам організації інформацію про зміни у сфері захисту інформації, які їх стосуються;

перевіряти відповідність прийнятим правилам та інструкціям щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

здійснювати контрольні перевірки стану захищеності інформації в організації;

забезпечувати конфіденційність робіт із монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в організації;

періодично, не рідше одного разу на місяць (інший термін), подавати керівництву організації звіт про стан захищеності інформації в організації і дотримання співробітниками встановленого порядку і правил захисту інформації;

негайно повідомляти керівництво середньої ланки управління про виявлені атаки і викритих порушників;

виконувати інші обов'язки, встановлені для керівників і членів комісії з організації ТЗІ відповідно до специфіки і особливостей діяльності організації.

Відповідальність членів комісії з організації ТЗІ

Керівництво і співробітники комісії з організації ТЗІ за невиконання або неналежне виконання службових обов'язків, допущені ними порушення встановленого порядку захисту інформації в організації несуть дисциплінарну і іншу відповідальність відповідно до законодавства України.

Персональна відповідальність керівника і членів комісії визначається посадовими (функціональними) інструкціями.

Відповідальність за діяльність комісії з організації ТЗІ покладається на її керівника.

Керівник комісії з організації ТЗІ відповідає за:

організацію робіт із захисту інформації в організації, ефективність захисту інформації відповідно до чинних нормативно-правових актів і внутрішніх документів;

своєчасну розробку і виконання Плану захисту інформації в організації;

якісне виконання членами комісії завдань, функцій і обов'язків, вказаних у "Положенні про комісію з організації ТЗІ", посадових

інструкціях, а також планових заходів щодо захисту інформації, затверджених керівником організації;

координацію планів діяльності щодо питань захисту інформації;

створення системи навчання співробітників з питань захисту інформації;

виконання особисто і членами комісії розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони роботи і протипожежної охорони.

Члени комісії з організації ТЗІ відповідають за:

дотримання вимог нормативних документів, які визначають порядок організації робіт із захисту інформації, інформаційних ресурсів і технологій;

повноту і якість розробки, впровадження організаційно-технічних заходів щодо захисту інформації в організації, точність і достовірність отриманих результатів і висновків з питань, які відносяться до компетенції комісії;

дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів за оцінкою стану захищеності інформації в організації, включених в план роботи комісії;

якість і правомірність документального оформлення результатів робіт окремих етапів створення СЗІ, документального оформлення результатів перевірок;

вирішення інших питань, які покладені на керівника і членів комісії відповідно до специфіки і особливостей діяльності організації.

Зразок акта категоріювання об'єкта

Гриф обмеження доступу

Прим. єдиний

ЗАТВЕРДЖУЮ

Керівник організації

"__" _____ 20__ р.

АКТ

категоріювання _____
(найменування об'єкта)

1. Період проведення робіт _____
2. Вищий гриф секретності інформації, що циркулює на об'єкті _____
3. Обсяг інформації, що циркулює на об'єкті, з вищим грифом секретності (звичайний, значний) _____
4. Вид категоріювання (первинне, планове повторне, позачергове повторне) _____
5. Відомості про можливість застосування стаціонарних засобів розвідки поблизу об'єктів:

Найменування і номер представництва _____

Відстань до об'єкта – _____ м.

6. Підстава для категоріювання _____
7. Раніше встановлена категорія _____
8. Встановлена категорія _____

Голова комісії

Члени комісії

(підписи)

"__" _____ 200__ р.

Зразок акта встановлення меж контрольованої зони

Гриф обмеження доступу
Прим. єдиний

ЗАТВЕРДЖУЮ
Голова комісії
з питань ТЗІ

"_____" _____ 200_ р.

А К Т

**встановлення контрольованої зони,
в межах якої здійснюється технічний захист інформації**

"_____" _____ 200_ р.

Комісія у складі:

Голова – _____.

Члени комісії: _____

За участю: (організація, що має ліцензію на проведення робіт із ТЗІ)

розглянула проведені роботи із встановлення меж контрольованої зони навколо (організація) _____.

Під час розгляду проведених робіт із встановлення меж контрольованої зони комісія керувалася рекомендаціями _____ (розділ __) і "Тимчасовим положенням з категоріювання об'єктів (ТПКО-95).

Відповідно до рекомендацій "Керівних документів з ТЗІ" і з урахуванням дислокації будівлі(ель), в якій(их) розташовані об'єкти захисту, ситуаційної обстановки в районі їх дислокації, місць розташування "виділених" приміщень у будівлі(ях), на підставі "Протоколу..." (див. Додаток 3) та Акта встановлення меж контрольованої зони навколо "виділених" приміщень від "_____" _____ 200_ р.

Комісія констатує:

з метою визначення рівня захисту інформації з обмеженим доступом, відповідного захисту об'єктів ___-ї категорії, межі контрольованої зони навколо "виділених" приміщень (організації) встановити по периметру зовнішньої огорожі (організації).

Голова комісії _____

Члени комісії: _____

За участю: _____

Зразок оформлення акта обстеження виділеного об'єкта

Гриф обмеження доступу

Прим. єдиний

ЗАТВЕРДЖУЮ

Голова комісії

з питань ТЗІ

" ____ " _____ 200_ р.

А К Т

Обстеження _____ як виділеного об'єкта _____
(назва ОІД) (назва організації)

" ____ " _____ 20__ р.

Комісія у складі:

Голова –

Члени комісії:

За участю:

відповідно до наказу по організації від " ____ " _____ 20__ р.

№ _____ провела первинне обстеження виділеного приміщення кабінету

№ _____ в _____ організації і встановила:

1. Засоби забезпечення інформаційної діяльності, що мають вихід за межі контрольованої території:

№ з/п	Найменування, тип, заводський номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

2. Перелік основних технічних засобів (ОТЗ), які оброблюють ІзОД:

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

2.2. Компоненти автоматизованих (комп'ютерних) систем (АС, КС) і технології обробки інформації:

3. Перелік основних технічних засобів, які обробляють ІПЗ:

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

3.1. Компоненти автоматизованих (комп'ютерних) систем (АС, КС) і технології обробки інформації

4. Перелік допоміжних технічних засобів і систем (ДТЗС)

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

5. Схеми засобів і систем життєзабезпечення виділеного об'єкта:

електроживлення;

заземлення;

автоматизації;

пожежної та охоронної сигналізації;

інженерних комунікацій і металоконструкцій;

наведені в Додатках №__ до Акта обстеження...

6. Відповідно до Протоколів вимірювань (Додаток №__ до Акта обстеження...) наступні технічні засоби створюють потенційну можливість витоків ІзОД і вимагають переобладнання (перемонтажу) і встановлення засобів ТЗІ:

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

7. Виявлено наявність на виділеному об'єкті наступних транзитних, незадіяних (повітря, настінне, зовнішнє, закладене в каналізацію) кабелів, ланцюгів і дротів:

схеми в Додатках №__ до Акта обстеження...

8. Перелік технічних засобів і систем, застосування яких не обґрунтоване службовою необхідністю і які підлягають демонтажу:

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	У якому виконанні (захищеному, незахищеному)	Примітка

9. Перелік встановлених засобів ТЗІ

№ з/п	Найменування, тип, заводський (інвентарний) номер	Кількість	Технічний стан	Примітка

Голова комісії _____

Члени комісії: _____

За участю: _____

Зразки інструкцій

ІНСТРУКЦІЯ

з прийому на роботу нових співробітників, їх допуску до роботи в комп'ютерній системі і наділення їх необхідними повноваженнями доступу до ресурсів системи

Під час прийому на роботу нового співробітника адміністратор безпеки зобов'язаний ознайомити користувача з необхідними нормативними документами та інструкціями, а також з політикою безпеки компанії. Після ознайомлення користувача з вищезазначеними документами проводиться його інструктаж і перевірка знань за допомогою заліку. У разі неспаді заліку співробітником допускається одна повторна спроба перездати заліку. Якщо протягом місяця з дня прийому на роботу залік не буде зданий, то співробітник не може бути допущений до комп'ютерних систем організації. Після успішної здачі заліку адміністратор безпеки присвоює користувачеві відповідний ідентифікатор для доступу в систему. Співробітник самостійно придумує пароль доступу в систему (відповідно до правил парольного захисту) і вводить його в систему. Пароль співробітника повинен бути відомий тільки особисто йому і не повідомляється нікому. Вище керівництво організації (генеральний директор або технічний директор) своїм наказом або розпорядженням призначають співробітнику рівень доступу до інформації.

Відповідно до розпорядження керівництва співробітнику може бути надано доступ на читання лише частини інформації рівнем вище, ніж «конфіденційно».

Технічний директор є безпосереднім керівником начальника служби безпеки організації, який у свою чергу є безпосереднім начальником адміністратора безпеки. У разі відсутності начальника служби безпеки, адміністратор безпеки підпорядковується безпосередньо генеральному або технічному директорові. Адміністратор інформаційних технологій підпорядковується керівнику інформаційних технологій, який підпорядковується технічному директорові. У разі відсутності керівника

інформаційних технологій адміністратор інформаційних технологій підпорядковується технічному директору.

ІНСТРУКЦІЯ

із звільнення (усунення від роботи) співробітників і позбавлення їх прав доступу до системи

1. У разі звільнення співробітника, в останній день його роботи (до отримання ним вихідної допомоги) виконуються наступні дії (окрім випадку звільнення адміністратора безпеки або адміністратора інформаційних технологій; у цьому випадку необхідно керуватися частиною II даної інструкції):

1) ідентифікатор і пароль співробітника видаляються із системи адміністратором безпеки;

2) електронні ключі доступу здаються співробітником адміністраторові безпеки, а у разі відсутності адміністратора безпеки начальникові служби безпеки організації. Можливість доступу з використанням старих ключів блокується;

3) адміністратор безпеки разом з адміністратором інформаційних технологій під контролем начальника служби безпеки аналізують робоче місце звільненого (відстороненого) співробітника на наявність закладних пристроїв, вірусів і т. д., після чого інформація, що є власністю організації, переписується на зовнішній носій, решта даних на жорсткому диску комп'ютера співробітника знищується, а операційна система на робочому місці потребує переустановлення;

4) адміністратор безпеки аналізує всі дані, до яких мав доступ співробітник на предмет їх зараженості вірусами і наявності прикріплених закладних пристроїв;

5) адміністратор безпеки разом із безпосереднім керівником співробітника аналізує цілісність і доступність даних, до яких співробітник мав доступ;

6) у разі виявлення неправочинних дій співробітника (видалення інформації, внесення в систему закладних пристроїв і вірусів) про це письмово повідомляється начальник служби безпеки або технічний директор, після чого, згідно з контрактом, співробітник звільняється без виплати вихідної допомоги. А також розв'язується питання про повідомлення правоохоронних органів про дії співробітника з метою притягнення його до відповідальності.

2. У разі звільнення адміністратора (безпеки або інформаційних технологій) в останній день його роботи (до отримання ним вихідної допомоги) проводяться наступні дії:

1) призначається новий адміністратор. Йому привласнюється ім'я, пароль і змінюється головний пароль суперкористувача;

2) ідентифікатор і пароль адміністратора, що звільняється, видаляються з системи;

3) електронні ключі доступу здаються новому адміністратору безпеки. Можливість доступу за старими ключами блокується;

4) новий адміністратор безпеки аналізує робоче місце на наявність закладних пристроїв, вірусів і т.д., після чого інформація, що є власністю організації, переписується на зовнішній носій, решта даних на жорсткому диску ПК співробітника знищується, ОС на робочому місці потребує переустановлення;

5) новий адміністратор безпеки аналізує всі дані, до яких мав доступ старий адміністратор на предмет їх зараженості вірусами і наявність прикріплених закладних пристроїв;

6) новий адміністратор безпеки разом із начальником служби безпеки аналізує цілісність і доступність даних, до яких мав доступ старий адміністратор;

7) у разі виявлення неправомірних дій старого адміністратора (видалення інформації, внесення в систему закладних пристроїв і вірусів) про це письмово повідомляється начальник служби безпеки або технічний директор, після чого, згідно з контрактом, співробітник звільняється без виплати вихідної допомоги. А також розв'язується питання про повідомлення правоохоронних органів про дії співробітника з метою притягнення його до відповідальності.

ІНСТРУКЦІЯ

про порядок проведення заходів різними категоріями персоналу з ліквідації наслідків кризових (аварійних або нештатних) ситуацій у разі їх виникнення

Можливі наступні кризові ситуації:

1. Знищення даних внаслідок стихійного лиха, пожежі або повені.

2. Знищення, крадіжка, розкриття або модифікація даних внаслідок фізичного злому і проникнення у приміщення.

3. Знищення, модифікація, розкриття даних або порушення працездатності системи внаслідок успішно проведеної атаки.

4. Інші ситуації.

Дії персоналу з ліквідації наслідків кризових (аварійних або нештатних) ситуацій у разі їх виникнення:

Знищення даних внаслідок стихійного лиха, пожежі або повені.

У разі виникнення такої ситуації співробітник, який виявив факт виникнення кризової ситуації, зобов'язаний:

негайно сповістити інших співробітників і вжити всіх можливих заходів для самостійного захисту приміщення, крім випадків, коли існує загроза життю або здоров'ю співробітника;

негайно сповістити відповідні служби допомоги (пожежну, міліцію і т. д.);

негайно доповісти про те, що відбулося, президентові компанії, генеральному і технічному директору, начальнику служби безпеки або адміністратору безпеки.

Після оперативної ліквідації причин, що викликали кризу, призначається комісія з усунення наслідків кризи. Головою комісії призначається генеральний директор.

Комісія визначає збиток (яка інформація і устаткування знищені), встановлює причини події та виявляє винних.

Знищення, крадіжка, розкриття або модифікація даних внаслідок фізичного злому і проникнення в приміщення.

У разі виникнення такої ситуації будь-якому співробітнику, який виявив факт злому приміщення або пропажі важливого устаткування, необхідно:

1) негайно доповісти президенту компанії, генеральному і технічному директору, начальнику служби безпеки;

2) зберігати приміщення в первинному вигляді, перешкодити проходу решти співробітників і можливого знищенню доказів у приміщенні.

Президент компанії або генеральний директор, ознайомившись з обставинами на місці події, ухвалює рішення про необхідність виклику правоохоронних органів.

Після оперативної ліквідації причин, що викликали кризу, призначається комісія на чолі з генеральним директором з усунення наслідків кризи.

Комісія визначає збиток (яка інформація і устаткування знищені або вкрадені), встановлює причини події та виявляє винних.

Знищення, модифікація, розкриття даних або порушення працездатності системи внаслідок успішно проведеної атаки.

У разі виникнення такої ситуації будь-якому співробітнику, що виявив факт її виникнення, необхідно негайно сповістити адміністратора безпеки. Адміністратор безпеки зобов'язаний негайно доповісти начальникові служби безпеки, генеральному і технічному директору про інцидент.

Негайно після виявлення факту інциденту або у випадку підозри про інцидент створюється комісія, куди входять адміністратор безпеки, експерт у сфері інформаційної безпеки, начальник служби безпеки і технічний директор. Комісія визначає збиток (яка інформація зазнала атаки), встановлює причини події та виявляє винних.

Можливі варіанти дій при різних атаках

Зовнішнє проникнення

У разі підозри віддаленої атаки і проникнення зловмисника в корпоративну мережу ззовні негайно відключаються всі зовнішні зв'язки, мережа компанії ізолюється від зовнішньої мережі і починається розслідування, яке встановлює:

- обставини й умови проникнення зловмисника в мережу;
- перелік даних, до яких був отриманий доступ;
- наслідки для компанії.

Після виявлення причин, внаслідок яких стала можливою атака, ці причини усуваються, і система вводиться в експлуатацію.

За наслідками роботи комісії здійснюється спроба пошуку зловмисника і розробляються адекватні заходи щодо зниження збитку і недопущення такого типу атак у майбутньому.

Внутрішнє проникнення

У разі підозри атаки і проникнення зловмисника в корпоративну мережу зсередини (можливо, атака здійснена власним персоналом) негласно створюється комісія, яка здійснює внутрішнє розслідування причин цієї атаки і визначає завданий збиток. У результаті роботи комісії

визначаються винні і виробляються адекватні заходи щодо зниження збитку і недопущення таких атак у майбутньому.

Примітка: характерними зовнішніми рисами зовнішнього або внутрішнього проникнення є ознаки втрати компанією конфіденційної інформації (виявлення її у конкурентів, виявлення специфічної інформації, яку конкурент не міг би одержати без проникнення в мережу і т. д.).

Дії адміністратора безпеки при виявленні спроб сканування, проникнення або атак на відмову в обслуговуванні.

Адміністратор безпеки зобов'язаний здійснювати щоденний аналіз лог-файлів (файлів журналів аудиту) серверів віддаленого доступу і систем виявлення атак з метою виявлення підозрілої активності, спроб сканування і несанкціонованого проникнення в мережу. У разі виявлення подібної активності адміністратор зобов'язаний:

1) запротоколювати даний випадок і повідомити про нього у своєму щотижневому звіті;

2) у разі підозри про цілеспрямовану постійно здійснювану атаку зловмисника (не автоматизованих засобів або «черваків», а саме людини) необхідно негайно повідомити начальникові служби безпеки і технічному директору;

3) переконатися, що атака успішно відбита і не спричинила негативних наслідків;

4) вжити адекватних заходів, що включають:

виявлення джерела атаки (діапазони IP-адрес, з яких здійснена атака);

аналіз приналежності IP-адрес, з яких було здійснено атаку;

виявлення відповідальних осіб за даний діапазон адрес і приналежності цього діапазону адрес до певної організації;

відправка повідомлень про атаки за офіційними адресами;

у разі відсутності відповіді (офіційні адреси застаріли) необхідно провести самостійне дослідження діапазону адрес, з яких здійснено атаку, виявити їх приналежність якій-небудь організації, здійснити пошук за наявною відкритою інформацією актуальних адрес системних адміністраторів і відправити їм повідомлення про проведену атаку.

Інші ситуації

У разі виникнення інших нештатних ситуацій співробітник, що виявив ситуацію, зобов'язаний негайно доповісти про це начальникові служби безпеки. Після цього усі подальші заходи проводяться тільки із санкції начальника служби безпеки або уповноваженої ним особи.

Процедури контролю в разі виникнення інцидентів

Процедури повинні бути розроблені з метою охоплення усіх можливих типів інцидентів порушення безпеки і включають випадки:

- збоїв в інформаційних системах;
- відмов в обслуговуванні;
- помилки внаслідок незавершених або неправильних даних;
- невиконання вимог конфіденційності.

На додаток до звичайного плану відновлення (розробленого для якомога більш оперативного відновлення систем або служб) процедури повинні також передбачати:

- аналіз та ідентифікацію причин інциденту;
- планування і впровадження заходів для запобігання повторенню (за потреби);
- аналіз і збереження доказів, наслідків інциденту, доказів і свідчень;
- взаємодію між потерпілими або тими, хто був залучений у процес відновлення;
- повідомлення про проведені заходи відповідному керівництву.

Наслідки інциденту, докази і свідчення повинні бути задокументовані. Стосовно них необхідно застосувати відповідні заходи безпеки. Цілі документування такі:

- аналіз внутрішніх проблем;
- використання доказів щодо потенційних порушників контрактів, порушників корпоративних вимог або законів України;
- переговори про компенсації з постачальниками апаратного та програмного забезпечення.

Заходи щодо відновлення в системі безпеки, виправлення системних помилок і несправностей повинні бути уважно й формально запротокольовані. Процедура повинна гарантувати наступне:

- тільки ідентифікований і авторизований персонал може отримувати доступ до відновлених систем і даних;
- усі аварійні дії детально задокументовані;

про всі заходи у встановленому порядку зроблено доповідь керівництву;

цілісність системи та її керованість підтверджена з мінімальними затримками.

ЗАТВЕРДЖУЮ

(назва установи, організації)

(керівник установи, організації, інша посадова

ПОСАДОВА ІНСТРУКЦІЯ АНАЛІТИКА КОМП'ЮТЕРНИХ СИСТЕМ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

особа, уповноважена затверджувати

посадову інструкцію)

(підпис)

(прізвище, ініціали)

" ____ " _____ р.

I. Загальні положення

1. Аналітик комп'ютерних систем із забезпечення інформаційної безпеки належить до професійної групи "Професіонали".
2. Призначення на посаду аналітика комп'ютерних систем із забезпечення інформаційної безпеки та звільнення з неї здійснюється керівником підприємства за поданням начальника обчислювального (інформаційно-обчислювального) центру (начальника служби захисту інформації) з дотриманням вимог Кодексу законів про працю України та інших законодавчих актів про працю.
3. Аналітик комп'ютерних систем із забезпечення інформаційної безпеки безпосередньо підпорядковується начальникові обчислювального (інформаційно-обчислювального) центру (начальникові служби захисту інформації).

II. Завдання та обов'язки (функції)

Аналітик комп'ютерних систем із забезпечення інформаційної безпеки

під час створення комплексної системи захисту інформації:

1. Організує визначення переліків відомостей, які потребують захисту в процесі обробки в інформаційно-телекомунікаційній системі (ІТС),

класифікує інформацію за вимогами до її конфіденційності або важливості для організації.

2. Визначає носії інформації та об'єкти, що потребують захисту в ІТС.

3. Організує комплексне дослідження внутрішньої структури, зовнішніх зв'язків, умов функціонування і зовнішнього середовища ІТС щодо виявлених об'єктів, які потребують захисту.

4. Розробляє та коригує окремі моделі загроз інформаційним ресурсам, що потребують захисту, техногенних і стихійних джерел загроз та моделі порушників інформаційної безпеки.

5. Оцінює вразливості інформаційних ресурсів, що потребують захисту.

6. Обирає методику оцінки та оцінює ризики для інформаційних ресурсів, що потребують захисту.

7. Визначає і формує вимоги до комплексної системи захисту інформації (КСЗІ), що знижує за обраним критерієм ризики для інформаційних ресурсів, які потребують захисту.

8. Розробляє "Технічне завдання на створення КСЗІ", відповідно до якого проводиться експертиза ІТС на відповідність вимогам захищеності інформації, і "План захисту інформації", відповідно до якого функціонує КСЗІ.

9. Розробляє політику інформаційної безпеки організації, що описує цілі, завдання, загальні вимоги, правила, обмеження, рекомендації у сфері інформаційної безпеки.

10. Організує і координує роботи з проектування та розробки КСЗІ, безпосередньо бере участь у проектних роботах зі створення КСЗІ.

11. Готує технічні пропозиції, рекомендації щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ.

12. Здійснює вибір організацій-виконавців робіт зі створення КСЗІ, контролює дотримання встановленого порядку проведення робіт із захисту інформації, погоджує основні технічні й розпорядчі документи, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.)

13. Організує і бере участь у випробуваннях КСЗІ, проведенні її експертизи.

14. Бере участь у розробці нормативних документів, чинних у межах організації та ІТС, які встановлюють дисциплінарну відповідальність за

порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ.

15. Бере участь у розробці нормативних документів, чинних у межах організації та ІТС, які встановлюють правила доступу користувачів до ресурсів ІТС, визначають порядок, норми, правила із захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

Під час експлуатації комплексної системи захисту інформації:

1. Організує процес керування КСЗІ.
2. Організує розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, аналізує причини, що призвели до них, супроводжує банк даних таких подій.
3. Вживає заходів у разі виявлення спроб несанкціонованого доступу (НСД) до ресурсів ІТС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів.
4. Забезпечує контроль цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування.
5. Організує керування доступом до ресурсів ІТС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.).
6. Супроводжує і актуалізує бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів тощо).
7. Спостерігає (реєстрація і аудит подій в ІТС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів.
8. Готує пропозиції щодо удосконалення порядку забезпечення захисту інформації в ІТС, впровадження нових технологій захисту і модернізації КСЗІ.
9. Організовує та проводить заходи з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС або КСЗІ.
10. Бере участь у роботах з модернізації ІТС – узгоджує пропозиції щодо введення до складу ІТС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо.
11. Забезпечує супроводження і актуалізацію еталонних, архівних і

резервних копій програмних компонентів КСЗІ, забезпечує їх зберігання і тестування.

12. Проводить аналітичну оцінку поточного стану безпеки інформації в ІТС (прогнозування виникнення нових загроз та їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації та реалізованої політики безпеки поточній моделі загроз та ін.).

13. Інформує власників інформації про технічні можливості захисту інформації в ІТС і типові правила, встановлені для персоналу і користувачів ІТС.

14. негайно втручається в процес роботи ІТС у разі виявлення атаки на КСЗІ, проводить у таких випадках роботу з викриття порушника.

15. Регулярно подає звіти керівництву організації-власника (розпорядника) ІТС про виконання користувачами ІТС вимог щодо захисту інформації.

16. Аналізує відомості щодо технічних засобів захисту інформації нового покоління, обґрунтовує пропозиції щодо придбання засобів для організації.

17. Контролює виконання персоналом і користувачами ІТС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контролює забезпечення режиму секретності у разі обробки в ІТС інформації, що становить державну таємницю.

18. Контролює забезпечення охорони і порядок зберігання документів (носіїв інформації), які містять відомості, що потребують захисту.

19. Розробляє і реалізує спільно з режимно-секретним органом (РСО) (підрозділом ТЗІ, службою безпеки) організації комплексних заходів із безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів та ін., здійснення їх технічного та інформаційного забезпечення.

Під час організації навчання персоналу з питань забезпечення захисту інформації:

1. Розробляє плани навчання і підвищення кваліфікації спеціалістів служби захисту інформації та персоналу ІТС.

2. Розробляє спеціальні програми навчання, які враховують особливості

технології обробки інформації в організації (ІТС), необхідний рівень її захищеності та ін.

3. Бере участь в організації та проведенні навчання користувачів і персоналу ІТС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами.

4. Взаємодіє з державними органами, навчальними закладами, іншими організаціями з питань навчання та підвищення кваліфікації.

5. Бере участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та ін.

III. Права

Аналітик комп'ютерних систем із забезпечення інформаційної безпеки має право:

1. Здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (ІТС) щодо виконання ним вимог нормативно-правових актів і нормативних документів із захисту інформації.

2. Подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки.

3. Складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їх усунення.

4. Проводити службові розслідування у випадках виявлення порушень.

5. Отримувати доступ до робіт та документів структурних підрозділів організації (ІТС), необхідних для оцінки вжитих заходів із захисту інформації та підготовки пропозицій щодо їх подальшого удосконалення.

6. Готувати пропозиції щодо залучення на договірній основі до виконання робіт із захисту інформації інших організацій, які мають ліцензії на відповідний вид діяльності.

7. Готувати пропозиції щодо забезпечення ІТС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації.

8. Виходити до керівництва організації з пропозиціями щодо подання

заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації.

9. Узгоджувати умови включення до складу ІТС нових компонентів і подавати керівництву пропозиції щодо заборони такого включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів ІТС.

10. Готувати висновки з питань, що належать до компетенції служби захисту інформації, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників служби захисту інформації.

11. Виступати з пропозиціями до керівництва організації щодо узгодження планів і регламенту відвідування ІТС сторонніми особами.

12. Ознайомлюватися з проектами рішень керівництва організації, що стосуються його діяльності.

13. Ознайомлюватися з документами, що визначають його права та обов'язки за посадою, критерії оцінки якості виконання ним посадових обов'язків.

14. Вносити на розгляд керівництва підприємства пропозиції щодо вдосконалення роботи, пов'язаної з обов'язками, передбаченими цією інструкцією.

15. У межах своєї компетенції повідомляти безпосередньому керівникові про всі недоліки, виявлені в процесі його діяльності, та вносити пропозиції щодо їх усунення.

16. Залучати фахівців усіх структурних підрозділів до вирішення покладених на нього завдань.

17. Вимагати та отримувати особисто або за дорученням безпосереднього керівника від керівників структурних підрозділів і фахівців інформацію та документи, необхідні для виконання його посадових обов'язків.

18. Вимагати від керівництва підприємства сприяння у виконанні ним посадових обов'язків.

19. Реалізовувати інші права, надані службі захисту інформації відповідно до специфіки та особливостей діяльності організації (ІТС).

IV. Відповідальність

Аналітик комп'ютерних систем із забезпечення інформаційної безпеки несе відповідальність за:

1. Організацію робіт із захисту інформації в ІТС, ефективність захисту інформації відповідно до чинних нормативно-правових актів.
2. Своєчасне розроблення і виконання “Плану захисту інформації в ІТС”.
3. Повноту та якість розроблення і впровадження організаційно-технічних заходів із захисту інформації в ІТС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції служби захисту інформації.
4. Створення системи навчання співробітників, користувачів, персоналу ІТС з питань захисту інформації.
5. Координацію планів діяльності підрозділів та служб ІТС (організації) з питань захисту інформації.
6. Дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в ІТС, які включені до плану робіт служби захисту інформації.
7. Якість та правочинність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок
8. Неналежне виконання або невиконання своїх посадових обов'язків, а також за невикористання або неповне використання своїх функціональних прав, передбачених цією посадовою інструкцією, – в межах, визначених чинним законодавством України про працю.
9. Правопорушення, вчинені в процесі здійснення своєї діяльності, – в межах, визначених чинним адміністративним, кримінальним і цивільним законодавством України.
10. Заподіяння матеріальної шкоди – в межах, визначених чинним цивільним законодавством та законодавством про працю України.

V. Аналітик комп'ютерних систем із забезпечення інформаційної безпеки повинен знати:

1. Чинне законодавство України, нормативно-правові акти і нормативні документи із захисту інформації.
2. Сучасні технології зберігання та накопичення інформаційних ресурсів.
3. Структуру та принципи функціонування сучасних ІТС.
4. Принципи та особливості функціонування сучасних технологій

передачі інформації.

5. Архітектуру та сервіси безпеки основних операційних систем і програмно-апаратного забезпечення, що використовуються в ІТС.
6. Основні положення та терміни щодо інформаційної безпеки.
7. Сучасні (типові) методи і засоби здійснення несанкціонованого доступу до ІТС.
8. Сучасні методи та можливості засобів технічної розвідки.
9. Уразливі для несанкціонованого доступу елементи типових ІТС.
10. Методики оцінки ризиків для інформаційних ресурсів.
11. Сучасні методи та засоби захисту від несанкціонованого доступу до ІТС.
12. Сучасні методи та засоби захисту інформації від витоку технічними каналами.
13. Основні принципи використання засобів криптографічного захисту та принципи роботи сучасних криптопротоколів (технологій).
14. Тенденції розвитку методів і засобів здійснення несанкціонованого доступу до ІТС і захисту від нього.
15. Типові політики інформаційної безпеки організації.
16. Нормативно-технічну документацію щодо експертизи та атестації в галузі технічного захисту інформації.
17. Загальні правила проведення розслідування випадків порушення політики інформаційної безпеки.

VI. Кваліфікаційні вимоги

Повна вища освіта (магістр, спеціаліст) за напрямком підготовки "Інформаційна безпека".

VII. Взаємовідносини (зв'язки) за посадою

1. За відсутності аналітика комп'ютерних систем із забезпечення інформаційної безпеки його обов'язки виконує особа, призначена у встановленому порядку, яка набуває відповідних прав і несе відповідальність за належне виконання покладених на неї обов'язків.
2. Для виконання обов'язків та реалізації прав аналітика комп'ютерних систем із забезпечення інформаційної безпеки взаємодіє:
 - 2.1. З режимно-секретним відділом організації з питань охорони державної

таємниці.

2.2. З підрозділом ТЗІ, службою безпеки організації з питань узгодження робіт із захисту інформації.

2.3. З адміністрацією організації та ІТС з питань створення необхідних умов здійснення своїх функціональних обов'язків.

2.4. З зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт з відповідних питань.

2.5. З підрозділами служб безпеки іноземних фірм (що є для організації партнерами, користувачами, постачальниками, виконавцями робіт), їх представництвами (на договірних або інших засадах) з відповідних питань.

3. Аналітик комп'ютерних систем із забезпечення інформаційної безпеки координує свою діяльність з аудиторською службою під час проведення аудиторських перевірок.

4. Взаємодія з іншими підрозділами організації з питань, що безпосередньо не пов'язані із захистом інформації, здійснюється відповідно до наказів та (або) розпоряджень керівника організації.

Керівник

структурного підрозділу

(підпис) (прізвище, ініціали)

" ____ " _____ р.

ПОГОДЖЕНО:

Начальник юридичного відділу

(підпис) (прізвище, ініціали)

" ____ " _____ р.

З інструкцією ознайомлений

(підпис) (прізвище, ініціали)

" ____ " _____ р.

Перелік нормативно-методичних документів у галузі захисту інформації (станом на квітень 2007 р.)

№ з/п	Шифр документа	Найменування документа
1	2	3
Технічний захист інформації на програмно-керованих АТС загального призначення		
1	НД ТЗІ 1.1-001-99	Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення
2	НД ТЗІ 2.5-001-99	ТЗІ на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту
3	НД ТЗІ 2.5-002-99	Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту
4	НД ТЗІ 2.7-001-99	Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт
5	НД ТЗІ 3.7-002-99	ТЗІ на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)
6	НД ТЗІ 2.5-003-99	ТЗІ на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту
7	НД ТЗІ 4.7-001-2001	Технічний захист мовної інформації (ТЗМІ) в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань
8	НД ТЗІ 2.3.-002-2001	ТЗМІ в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування МІ. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань
9	НД ТЗІ 2.3-003-2001	Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань
Технічний захист інформації в комп'ютерних (автоматизованих) системах (АС, КС) від несанкціонованого доступу (НСД)		
10	НД ТЗІ 1.1-002-99	Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу
11	НД ТЗІ 1.1-003-99	Термінологія в галузі захисту інформації в КС від НСД

Продовження табл. 3.1

1	2	3
12	НД ТЗІ 1.4-001-2000	Типове положення про службу захисту інформації в АС
13	НД ТЗІ 2.5-004-99	Критерії оцінки захищеності інформації в КС від НСД
14	НД ТЗІ 2.5-005-99	Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД
15	НД ТЗІ 3.6-001-2000	Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів ТЗІ від НСД
16	НД ТЗІ 2.1-001-2001	Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення
17	НД ТЗІ 3.7-001-99	Методичні рекомендації щодо розробки технічного завдання на створення КСЗІ в АС (зі зміною № 1, затвердженою наказом ДСТСЗІ СБУ від 18.06.02 № 37)
18	НД ТЗІ 2.5-008-2002	Вимоги із захисту конфіденційної інформації від НСД під час оброблення в АС класу 2
19	НД ТЗІ 2.5-010-2003	Вимоги до захисту інформації WEB-сторінки від НСД
20	НД ТЗІ 3.7- 003-05	Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
21	31.05.05 № 2594-15	Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"
Захист інформації від витоку каналами ПЕМВН		
22	ТР ЕОТ-95	Тимчасові рекомендації з ТЗІ у засобах обчислювальної техніки, АС і мережах від витоку каналами ПЕМВН
23	НД ТЗІ 1.5-001-2000	Радіовиявлювачі. Класифікація. Загальні технічні вимоги
24	НД ТЗІ 2.3-001-2001	Радіовиявлювачі вимірювальні. Методи та засоби випробувань
25	НД ТЗІ 2.3-004-2001	Радіовиявлювачі індикаторні. Методи та засоби випробувань
26	НД ТЗІ 2.3-005-2001	Радіовиявлювачі панорамні. Методи та засоби випробувань
27	НД ТЗІ 2.3-006-2001	Радіовиявлювачі аналізуювальні. Методи та засоби випробувань
28	НД ТЗІ 2.5-006-99	Класифікатор засобів копіювально-розмножувальної техніки

Продовження табл. 3.1

1	2	3
29	НД ТЗІ 2.7-002-99	Методичні рекомендації з використання засобів копіювально-розмножувальної техніки
30	P-001-2000	Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації
31	ПЕМВН-95	Тимчасові рекомендації з ТЗІ від витоку каналами ПЕМВН
32	НД ТЗІ (проект)	Захист мовної інформації від витоку акустоелектричними каналами
33	НД ТЗІ (проект)	Захист мовної інформації від витоку лазерними акустичними каналами
Спеціальні документи ДСТСЗІ		
34	НД ТЗІ 2.5-007-2001	Вимоги до комплексу засобів ТЗІ, що становить державну таємницю, від НСД при її обробці в АС класу «1»
35	НД ТЗІ 3.6-002-2001	ТЗІ щодо озброєнь і військової техніки (ВТ). Інструкції з протидії технічним розвідкам під час створення зразків озброєнь та військової техніки. Методичні рекомендації
36	НД ТЗІ 2.5-009-2002	ТЗІ щодо озброєнь та ВТ. Класифікація зразків озброєння та ВТ. Загальні вимоги з протидії технічним розвідкам під час створення та експлуатації зразків озброєння та ВТ
37	НД ТЗІ 2.7-005-2001	Методичні рекомендації щодо організації проведення робіт з протидії та порядок оцінки розвідзахищеності озброєння та ВТ від радіолокаційних засобів повітряної та космічної розвідки
38	НД ТЗІ 2.7-006-04	ТЗІ щодо озброєнь та ВТ. Оцінка витрат на заходи з протидії технічним розвідкам. Методичні рекомендації
39	ТР-2015 2001 р.	Моделі технічних розвідок (ТР-2015)
40	Зм ТР	Зміни до моделі технічних розвідок (ТР-2015). Довідкові відомості щодо тактико-технічних характеристик систем і засобів технічних розвідок та їх носіїв
41	Бюлетень 1	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1 – 2001
42	Бюлетень 2	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2 – 2001
43	Бюлетень 3	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1(3) – 2002
44	Бюлетень 4	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2(4) – 2002

Продовження табл. 3.1

1	2	3
45	Бюлетень 5	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1(5) – 2003
46	Бюлетень 6	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2(6) – 2003
47	Бюлетень 7	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1(7) – 2004
48	Бюлетень 8	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2(8) – 2004
49	Бюлетень 9	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1(9) – 2005
50	Бюлетень 10	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2(10) – 2005
51	Бюлетень 11	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 1(11) – 2006
52	Бюлетень 12	Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 2(12) – 2006
53	НД ТЗІ 1.6-003-04	Створення комплексів ТЗІ на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації
54	НД ТЗІ 1.1-004-2003	Протидія технічним розвідкам. Терміни та визначення
55	НД ТЗІ 2.7-003-2000	Методичні рекомендації щодо виявлення хімічних КВІ з обмеження доступом при створенні і впровадженні нових технологій та матеріалів
56	НД ТЗІ 2.7-004-2000	Інформаційно-аналітична модель мінімальних рівнів доступності інформації у хімічних каналах
57	НД ТЗІ 4.7-002-01	Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні рекомендації
58	ВПКО-95	Тимчасове положення про категорювання об'єктів. ВПКО-95 (ТПКО-95 зі спец. додатком)
Законодавчі та концептуальні документи України		
59	02.10.92 № 2657	Закон України «Про інформацію»
60	1994 р. № 16	Закон України «Про державну таємницю» (в редакції Закону № 1079-14 від 21.09.99) [1]

1	2	3
61	Пост. КМУ № 1126 8.10.97	Концепція технічного захисту інформації в Україні

Продовження табл. 3.1

1	2	3
62	27.09.99 № 1229	Положення про технічний захист інформації в Україні УП №1№29/99 від 27.09.99
63	Пост. КМУ № 281 від 13.03.02	Про деякі питання захисту інформації, охорона якої забезпечується державою (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
64	Пост. КМУ № 288 від 13.03.02	Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
65	№ 1775 від 01.06.00	Закон України «Про ліцензування певних видів господарської діяльності»
66	Пост. КМУ № 1698 від 14.11.00	Про затвердження переліку органів ліцензування (із змінами включно пост. КМУ № 80 від 31.01.2007)
67	Пост. КМУ № 756 від 04.07.01	Перелік документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності (із змінами включно пост. КМУ № 80 від 31.01.2007)
68	Пост. КМУ № 1755 29.11.00	Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу
69	17.05.01 № 2408	Закон України «Про стандартизацію»
70	10.01.02 № 2919	Закон України «Про Національну систему конфіденційного зв'язку»
71	17.05.01 № 2407	Закон України «Про акредитацію органів з оцінки відповідності»
72	22.05.03 № 852	Закон України «Про електронний цифровий підпис»
73	22.05.03 № 851	Закон України «Про електронні документи та електронний документообіг»
74	19.06.03 № 964	Закон України «Про основи національної безпеки України»

1	2	3
75	13.12.91 № 1977	Закон України «Про наукову і науково-технічну діяльність»
76	10.02.95 № 51/95	Закон України «Про наукову і науково-технічну експертизу»
77	18.11.03 № 1280	Закон України «Про телекомунікації»

Продовження табл. 3.1

1	2	3
78	Пост. КМУ № 1772 від 16.11.02	Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних і телекомунікаційних системах (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
79	Пост. КМУ № 373 від 29.03.06	Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (із змінами включно пост. КМУ № 80 від 31.01.2007)
80	Пост. КМУ № 1519 від 11.10.02	Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям
81	20.02.03 № 549	Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання
82	Пост. КМУ № 680 від 26.05.04	Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу
83	Пост. КМУ № 903 від 13.06.04	Порядок акредитації центру сертифікації ключів (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
84	Пост. КМУ № 1451 від 28.10.04	Положення про центральний засвідчувальний орган (із змінами, включно пост. КМУ № 147 від 15.02.2006)
85	Пост. КМУ № 1452 від 28.10.04	Порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
86	Пост. КМУ № 1453 від 28.10.04	Типовий порядок здійснення електронного документообігу в органах виконавчої влади (із змінами, включно пост. КМУ № 1700 від 08.12.2006)
87	Пост. КМУ № 1454 від 28.10.04	Порядок обов'язкової передачі документованої інформації

1	2	3
88	Р–СП	Рекомендації з ТЗІ в приміщеннях серверних, електронної пошти та інших спеціальних приміщень
Охорона державної таємниці		
89	СБУ № 440 від 12.08.05	Звід відомостей, що становлять державну таємницю (із змінами, включно н. СБУ № 680 від 12.10.2006)
90	Пост. КМУ № 1000 від 19.07.06	Деякі питання обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави

Продовження табл. 3.1

1	2	3
91	Пост. КМУ № 1893 від 27.11.98	Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. (Із змінами, включно пост. КМУ № 1700 від 08.12.2006)
92	Пост. КМУ № 1082 від ДСК 17.07.03	Порядок здійснення заходів з охорони державної таємниці під час проведення секретних науково-дослідних та дослідно-конструкторських робіт
93	Пост. КМУ № 1084 від ДСК 17.07.03	Положення про технічну комісію органу виконавчої влади, підприємства, установи і організації, які беруть участь у виконанні секретних робіт або є їх замовниками
94	Пост. КМУ № 414 від ДСК 15.06.94	Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці
95	03.03.97 № 26/8	Типове положення про секретний архівний підрозділ державного органу, підприємства, установи і організації
96	03.03.97 № 25/7	Інструкція про порядок відбору та передачі секретних документів на архівне зберігання
97	14.12.2004 № 696	Про затвердження Положення про експертні комісії з питань державної таємниці
Організація захисту інформації		

1	2	3
98	ДСТСЗІ № 151/72 від 12.12.01	Порядок контролю за додержанням ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів крипт. захисту інформації, торгівлі криптосистемами і засобами крипт. захисту інформації; розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів ТЗІ, надання послуг в галузі ТЗІ; розроблення, провадження, сертифікаційних випробувань, ввезення, вивезення голографічних захисних елементів
99	ТПКО-95	Тимчасове положення про категоріювання об'єктів від 10.07.95 № 35 (без спец. додатку)

Продовження табл. 3.1

1	2	3
Технічний захист інформації		
100	НД ТЗІ 1.6-002-03	Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ. Введено на заміну НД ТЗІ 1.6-001-96 з 05.05.2003
101	ДСТСЗІ № 61 від 22.12.99	Положення про контроль за функціонуванням системи ТЗІ
102	ДСТСЗІ № 62 від 29.12.99	Положення про державну експертизу в сфері ТЗІ
103	ДСТСЗІ від 22.12.00	Перелік засобів забезпечення ТЗІ. Засоби загального призначення (станом на 15.11.2004)
104	Пост. КМУ № 180ДСК від 16.02.98	Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС (із змінами згідно з пост. КМУ від 13.03.2002 р. № 281)
105	ДСТСЗІ № 89/67 від 29.12.00	Ліцензійні умови провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів ТЗІ, наданням послуг у галузі ТЗІ

1	2	3
106	ДСТСЗІ № 9 від 23.02.02	Положення про дозвільний порядок проведення робіт із ТЗІ для власних потреб
107	ДСТСЗІ № 35 від 07.06.02	Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи ТЗІ
108	ДСТСЗІ № 52 від 09.07.04	Порядок формування Реєстру експертів з питань ТЗІ. Порядок формування Реєстру організаторів державної експертизи у сфері ТЗІ
109	ДСТСЗІ № 56 від 14.07.04	Про затвердження Граничних тарифів на послуги конфіденційного зв'язку
110	ДСТСЗІ №329/32 від 09.07.01	Порядок проведення робіт із сертифікації засобів забезпечення ТЗІ загального призначення
111	ДСТСЗІ від 10.11.2005	Перелік нормативно-правових документів України з питань ТЗІ станом на 10.11.2005 р.
Криптографічний захист інформації		
112	СБУ № 202/213 від 24.09.99	Порядок проведення сертифікації засобів криптографічного захисту інформації
113	ДСТСЗІ № 31 від 30.04.04	Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації

Продовження табл. 3.1

1	2	3
114	22.05.98 № 505	Положення про порядок здійснення криптографічного ЗІ в Україні УП № 505/98 від 22.05.98.
115	ДСТСЗІ № 88/66 від 29.12.00	Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного ЗІ, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного ЗІ (із змінами згідно з наказом ДСТСЗІ СБУ № 121/80 від 15.11.04)
116	ДСТСЗІ № 708/156 від 28.11.97	Тимчасова інструкція про порядок постачання і використання ключів до засобів криптографічного ЗІ

1	2	3
117	ДСТСЗІ № 62/К від 25.12.00	Положення про державну експертизу у сфері криптографічного ЗІ
118	ДСТСЗІ № 3 від 13.01.05	Правила посиленої сертифікації
119	ДСТСЗІ № 45 від 22.10.99	Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави (із змінами, внесеними наказом ДСТСЗІ СБУ від. 24.12.04 за № 111)
Спеціальні документи в галузі криптографічного ЗІ		
120	ДСТСЗІ № 28/ДСК від 04.04.05	Положення про порядок розроблення, виробництва, уведення в експлуатацію та експлуатації засобів криптографічного захисту конфіденційної інформації, яка є державною власністю (замість наказу № 48/ДСК від 30.10.2000)
121	ДСТСЗІ № 014 від 28.02.00	Положення про порядок розроблення, виробництва, введення в експлуатацію та експлуатації засобів криптографічного ЗІ, що становить державну таємницю
122	ДСТСЗІ № 06 від 05.11.02	Зміни та доповнення до Положення про порядок розроблення, виробництва, введення в експлуатацію та експлуатації засобів криптографічного ЗІ, що становить державну таємницю

Продовження табл. 3.1

1	2	3
123	Зб. Безпека VI	Збірник доповідей на «закритій» секції VI Міжнародної науково-практичної конференції «Безпека інформації в інформаційних і телекомунікаційних системах»
Нормативні документи колишнього СРСР		
124	РД 50-680-88	Методические указания. Автоматизированные системы. Основные положения

1	2	3
125	РД 50-682-89	Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы (ГОСТ 34.201-89, ГОСТ 34.602-89, РД 50-682-89)
126	РД 50-34-698-90	Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов
Спеціальні нормативні документи колишнього СРСР		
127	*Нр АСУ, ЭВМ	Нормы эффективности защиты АСУ и ЭВМ от утечки информации за счет побочных излучений и наводок. ГТК СССР, 1977 г.
128	ПКО-ЭВТ	Положение по категорированию объектов ЭВТ на территории СССР (ПКО-ЭВТ). ГТК СССР, 1981 г.
129	СТР-2	Специальные требования и рекомендации по защите военно-промышленных объектов ЭВТ второй категории за счет побочных излучений и наводок (СТР-2). ГТК СССР, 1987 г.
130	СТР-3	Специальные требования и рекомендации по защите военно-промышленных объектов ЭВТ третьей категории за счет побочных излучений и наводок (СТР-3). ГТК СССР, 1987 г.
131	*Спец. иссл. АСУ, ЭВМ	Сборник методических материалов по проведению спец. исследований ТС АСУ и ЭВМ, предназначенных для работы с закрытой информацией. МРП СССР -77
132	*МКЗО	Методика контроля защищенности объектов ЭВТ. МРП СССР от 17.07.79 г.
133	Дпл МКЗО	Дополнение к «Методике контроля защищенности объектов ЭВТ» от 17.07.79 г. при применении средств активной защиты». МРП СССР 17.03.83

Продовження табл. 3.1

1	2	3
134	Бумер-2Г	Сборник методических рекомендаций по применению изделия «Бумеранг-2Г»
135	Нр фото, ОЭ	Нормативно-методические документы по противодействию средствам фотографической и оптико-электронной разведок. ГТК СССР № 86-2 12.06.90

1	2	3
136	ВНр ТПвЗ	Временные нормы противодействия тепловизионным средствам иностранной инфракрасной разведки
137	Мтд ЛАЗ	Методика контроля выполнения норм защиты лазерного излучения от оптико-электронных средств ИТР. ГТК СССР № 70-3 16.09.87
138	*Нр РЕЧ	Нормы эффективности защиты технических средств передачи речевой информации от утечки за счет побочных излучений и наводок. ГТК СССР № 13 от 26.09.77 г.
139	Нр ЛАЗ	Нормы защиты лазерного излучения от оптико-электронных средств ИТР. ГТК СССР № 61-2 от 23.10.85 г.
140	*СПУ-77	Специальные указания по обеспечению защиты технических средств от утечки речевой информации за счет побочных электромагнитных излучений и наводок. ГТК СССР-78
141	РВТС-83	Рекомендации по применению изделий общепромышленной продукции в качестве вспомогательных технических средств и систем на ВПО и в режимных организациях (РВТС-83) ГТК СССР-83
142	Дпл РВТС-83	Дополнение № 2 к РВТС-83
143	*Нр ТВЗ	Нормы эффективности защиты технических средств передачи телевизионной информации от утечки за счет побочных излучений и наводок. ГТК СССР от 26.09.77 № 13
144	АЗП-81	Руководящий материал. Акустическая защищенность помещений, выделенных для проведения совещаний и переговоров. Нормы эффективности. Методика контроля. АЗП-81
145	РД 107 (общ.тр.)	Методика измерения эффективности экранирования сооружений, обеспечивающих защиту вычислительных центров и АСУ от ИТР в диапазоне частот 150 кГц – 1000 МГц. Общие требования

Продовження табл. 3.1

1	2	3
---	---	---

1	2	3
146	*СБ Мтд РЕЧ	Сборник методик измерений и расчета параметров технических средств передачи информации с целью определения их соответствия установленным нормам на параметры в речевом диапазоне частот. МПСС СССР 17.03.78
147	Мтд ТВЗ	Методика контроля защищенности технических средств передачи телевизионной информации
148	*ВТСС-78	Сборник методик измерений и расчета параметров вспомогательных технических средств и систем с целью определения их соответствия установленным нормам на параметры в речевом диапазоне частот
149	107 (метод.)	Измерение эффективности экранирования сооружений, обеспечивающих защиту от ИТР в диапазоне частот 30 МГц – 40 ГГц
150	*СВТР-78	Специальные временные требования и рекомендации по размещению и монтажу оборудования АСУ и ЭВМ на проектируемых объектах (СВТР-78). МРП СССР-79
151	НТД акуст	Нормативно-технические документы по противодействию акустической разведке при защите речевой информации
152	29339-92	Защита информации от утечки за счет побочных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования
153	Гранит	Рекомендации по применению и монтажу средств защиты и защищенных устройств типа «Гранит». УРЭБ сухопутных войск, 1986 г.
154	Мтд ЭВТ	Методика технического контроля специальной защиты объектов электронно-вычислительной техники (ЭВТ). УРЭБ сухопутных войск, 1986 г.
155	НМТД РТР	Нормативно-методическая документация по противодействию средствам иностранной радиотехнической разведки. ГТК СССР от 12.06.90 № 86-2
156	*РТМ 25 31-83	Комплексное противодействие ИТР на объектах министерства приборостроения, средств автоматизации и систем управления, выпускающих оборонную продукцию

Продовження табл. 3.1

1	2	3
157	РТМ 25 32-83	Контроль состояния комплексного противодействия ИТР на объектах министерства приборостроения, средств автоматизации и систем управления, выпускающих оборонную продукцию
158	РТМ 25 33-84	Общие требования к методам измерений параметров каналов утечки. Минприбор, 1984 г.
159	М2Г 0037-83	Специсследования и проектирование защищенных от утечки информации АСУ промышленного назначения. Минприбор, 1983 г.
160	МВТР-87	Методики оценки возможностей ИТР. ГТК СССР
161	*Нр ТЛГР	Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет побочных излучений и наводок. ГТК СССР от 26.09.77 № 13
162	*ПК-ПД	Порядок контроля за эффективностью противодействия ИТР (ПК-ПД) ГТК СССР 16.09.87 № 703
163	Нр РЛР	Временные нормы противодействия радиолокационным средствам воздушной и космической разведки. ГТК СССР от 28.03.79 № 22-3
164	РекЛАЗ	Рекомендации по защите лазерного излучения от оптико-электронных средств ИТР. ГТК СССР 1990
165	ОСТ 4.169.001-83С	Система противодействия иностранным техническим разведкам. Средства управления автоматизированные и электронно-вычислительная техника. Организация работ по защите
166	*ОСТ 4.169.006-89	Технические средства, не предназначенные для передачи и обработки закрытой информации. Технические требования по защите от ПЭМИН. ОСТ 4.169.006-89
167	*ОСТ 4.169.011-89	Технические средства, предназначенные для передачи и обработки закрытой речевой непреработанной информации. Тех. требования по защите от ПЭМИН. ОСТ 4.169.011-89
168	ОСТ 4.169.003-89	Средства передачи данных. Технические требования по защите от ПЭМИН. ОСТ 4.169.003-89
169	ОСТ 45.169.000-90	Система противодействия иностранным техническим разведкам. Техническое задание на проектирование комплексных защитных мероприятий

Продовження табл. 3.1

1	2	3
170	ВСН 01-91	Инструкция по разработке защиты военно-промышленных объектов от ИТР. Основы и организация проектирования. ВСН 01-91. ГТК СССР, 1991 г.
171	ПСБ Ч2	Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР. Часть 2 «Особенности проектирования генеральных планов, зданий, сооружений с учетом защиты от иностранной радиолокационной разведки». Приложение к Инструкции ВСН 01-82, 1983 г.
172	ПСБ Ч4	Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР. Часть 4 «Пособие по проектированию экранированных и безэховых сооружений, зданий, помещений, камер, боксов с учетом защиты от ИТР». Прилож. к Инструкции ВСН 01-82, 1985 г.
173	*ПСБ Ч5	Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР. Часть 5 «Проектирование мероприятий защиты технических средств передачи, обработки и хранения речевой информации». Приложение к Инструкции ВСН 01-82, 1983 г.
174	ПСБ Ч6	Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР. Часть 6 «Пособие по проектир. тех. мероприятий зашиты зданий, сооружений, помещений со средствами вычисл. техники от утечки информации за счет излучений и наводок». Прилож. к Инструкции ВСН 01-82, 1985 г.
175	РД ПД ИТР	Руководящие документы по противодействию ИТР. ГТК СССР, 1984 г.
176	МтДИКраз	Методика контроля выполнения Временных норм противодействия средствам иностранной инфракрасной разведки. Часть 1
177	Активн ЗЩТ ПЭМИН	Средства активной защиты объектов ЭВТ от утечки информации по побочным излучениям и наводкам. Основные технические требования. Минрадиопром – 1987 г.

Продовження табл. 3.1

1	2	3
178	РМП.ПДЖ.029-88	Инструкция по проектированию экранированных помещений с учетом требований ПД ИТР РМП.ПДЖ.029-88. МЭП 1988
179	X-5806	Звукоизоляция помещений, выделенных для проведения секретных совещаний и переговоров. МЭП 1979 г.
180	РД 11 0595-88	Противодействие иностранным техническим разведкам. Выделенные помещения. Организация защиты. РД 11 0595-88. МЭП 1988 г.
181	МтдРЕЧорг	Методика контроля состояния защиты от утечки речевой специальной информации на режимных предприятиях отрасли. Этап организационных и организационно-технических мероприятий. МЭП 1978 г.
182	ВНр РТР40–300	Временные нормы противодействия иностранной радиотехнической разведке в диапазоне частот 40–300 ГГц. МЭП 1987 г.
183	Мтд РТР40–300	Методика контроля норм противодействия иностранной радиотехнической разведке в диапазоне частот 40–300 ГГц. МЭП 1990 г.
184	ВНр РТР10–30	Временные нормы противодействия иностранной радиотехнической разведке в диапазоне частот от 10 Гц до 30 МГц. МЭП 1987 г.
185	ПД ИТР испт	Рекомендации по противодействию иностранным радио- и радиотехнической разведкам при испытаниях вооружения и военной техники. ГТК СССР, 1986 г.
186	Спрв РТМ	Методические материалы по радиотехнической маскировке и радиотехническому контролю на предприятиях МЭП. 1985 г.
187	Акт РТМ ЭВТ	Методические указания по оценке эффективности систем активной радиотехнической маскировки объектов электронно-вычислительной техники. МЭП СССР, 1986 г.
188	РД 11 0703–89	ПД ИТР. Защита предприятий, выполняемых ими работ и выпускаемой продукции оборонного назначения от фотографических и визуально-оптических средств ИТР. РД 11 0703–89, МЭП, 1989 г.

Закінчення табл. 3.1

1	2	3
189	Мтд ПД ИТР	Методика контроля эффективности мероприятий ПД ИТР на предприятиях МЭП. 1985 г.
190	ВСН 33–87	Инструкция о порядке разработки задания на проектирование технических мероприятий защиты военно-промышленных объектов отрасли от ИТР. Ведомственные строительные нормы ВСН 33-87. МЭП 1987 г.
191	*РД В 25 48-88	Временные нормы эффективности защиты средств изготовления и размножения текстовых документов от утечки информации за счет побочных электромагнитных излучений и наводок РД В 25 48-88
192	РД В 25 49-88	Специальные указания по объектовой защите канцелярских пишущих машин и автоматов, средств копирования и оперативного размножения от утечки секретной текстовой информации за счет ПЭМИН и неравномерности потребления тока. СПУ СИРД РД В 25 49-88 МПСС, 1988 г.
193	ВрМТ СИРД	Временные методические рекомендации по оценке эффективности защиты средств изготовления и размножения документов от утечки секретной текстовой информации за счет ПЭМИН. МПСС, 1988 г.

*(На основі матеріалів фірми НікС, 02002, м. Київ, вул. Флоренції 1/11, розміщених на сайті <http://www.nics.com.ua>)

Гриф обмеження доступу
Прим. єдиний
від " ____ " _____ 20__ р.

ПРОТОКОЛ

встановлення меж контрольованої зони, в межах якої здійснюється технічний захист інформації

" ____ " _____ 20__ р.

1. Об'єкт дослідження:

виділені приміщення _____ як об'єкти захисту ІЗОД.

2. Мета проведення обстеження:

встановлення межі контрольованої зони навколо "виділених" приміщень з метою виключення безконтрольного (прихованого) розміщення технічних засобів розвідки інформації з обмеженим доступом.

3. Методика проведення обстеження:

обстеження проводиться на підставі вивчення дислокації та ситуаційної обстановки в районі розташування будівель, в яких знаходяться "виділені" приміщення, а також з урахуванням тактико-технічних характеристик, способів і методів дії технічної розвідки з отримання інформації, що охороняється.

4. Порядок проведення обстеження:

візуально-оптичний огляд території, прилеглої до будівель, в яких розташовані "виділені" приміщення;

вивчення внутрішнього розташування службових приміщень щодо "виділених" приміщень у плані будівель;

вивчення можливості неконтрольованого перебування сторонніх осіб поблизу "виділених" приміщень.

5. У результаті обстеження встановлено:

5.1. Територіальне розташування будівель, в якому розташовані "виділені" приміщення:

будівлі, в яких знаходяться "виділені" приміщення, розташовані в центральній частині міста за адресою: вул. _____ №__;

ситуаційна обстановка в місці розташування будівель наведена в Додатку А до Акта оцінки ситуаційної обстановки...

5.2. Відстань від об'єкта захисту до меж території, що охороняється:

межа території, що охороняється, проходить:
по зовнішній огорожі будівель організації.

5.3. Можливість безконтрольного проникнення сторонніх осіб у зону, що охороняється:

можливість безконтрольного проникнення сторонніх осіб виключається наявністю охорони і пропускного режиму.

5.4. Можливість перебування сторонніх осіб поблизу "виділеного" або суміжних приміщень під час проведення заходів, пов'язаних з обговоренням інформації з обмеженим доступом:

виключена можливість перебування сторонніх осіб у суміжних приміщеннях.

5.5. Словесний опис можливих меж контрольованої зони:

з метою встановлення рівня захисту інформації з обмеженим доступом, відповідного захисту об'єктів ___-ї категорії, межі контрольованої зони навколо "виділених" приміщень як об'єктів захисту інформації з обмеженим доступом, доцільно встановити за периметром зовнішньої огорожі організації.

Голова комісії _____

Члени комісії: _____

За участю: _____

Зразок паспорта на приміщення об'єкта захисту

Гриф обмеження доступу

Прим. єдиний

ЗАТВЕРДЖУЮ

Керівник організації

"__" _____ 20__р.

ПАСПОРТ
на приміщення № _____

Приміщення № ____ корпус ____ визначено як виділене приміщення
____ категорії наказом по організації № _____.

1. Характеристика робіт з ІзОД:

ступінь конфіденційності _____

характер робіт _____

тимчасовий або постійний

короткий зміст:

2. Загальна характеристика приміщення:

Розташоване на ____ поверсі адміністративної будівлі (організації) за адресою:

площа – ____ м²

висота стін – ____ м

характеристика стін – _____

характеристика даху – _____

характеристика вхідних дверей _____

розміри вхідних дверей _____ × _____ м

замки _____

кількість вікон _____

характеристика вікон _____

внутрішні ґрати, внутрішні стекла рифлені

або відповідність Акту первинного обстеження

Охоронна сигналізація:

тип, характеристика, які елементи приміщення підключені, куди виведена

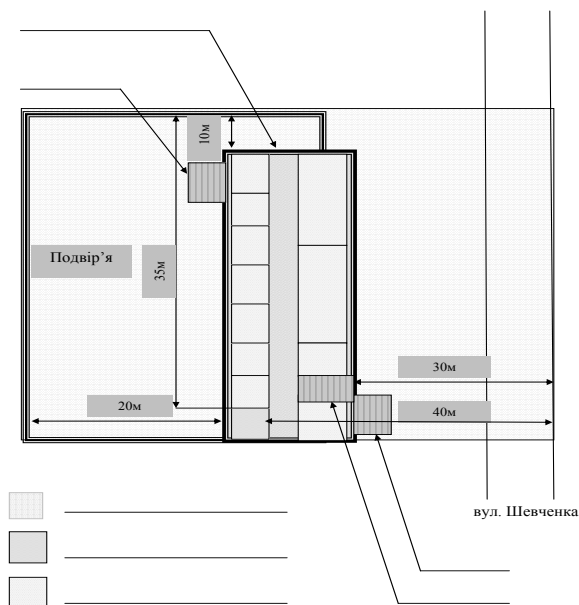
Пожежна сигналізація:

тип, характеристика, які елементи приміщення підключені, куди виведена

3. Відомості про керівні документи (акти прийому системи захисту, акти перевірок тощо, а також інструкції про порядок виконання робіт, проведення нарад та ін.):

№ з/п	Реєстраційний № документа	Найменування	Місцезнаходження (справа, лист)	Примітка

4. Схема розташування приміщення на плані контрольованої зони:
рисунок поверху, межа контрольованої зони (КЗ) на місцевості, відстань від приміщення до межі КЗ. Призначення суміжних із виділеними приміщеннями.



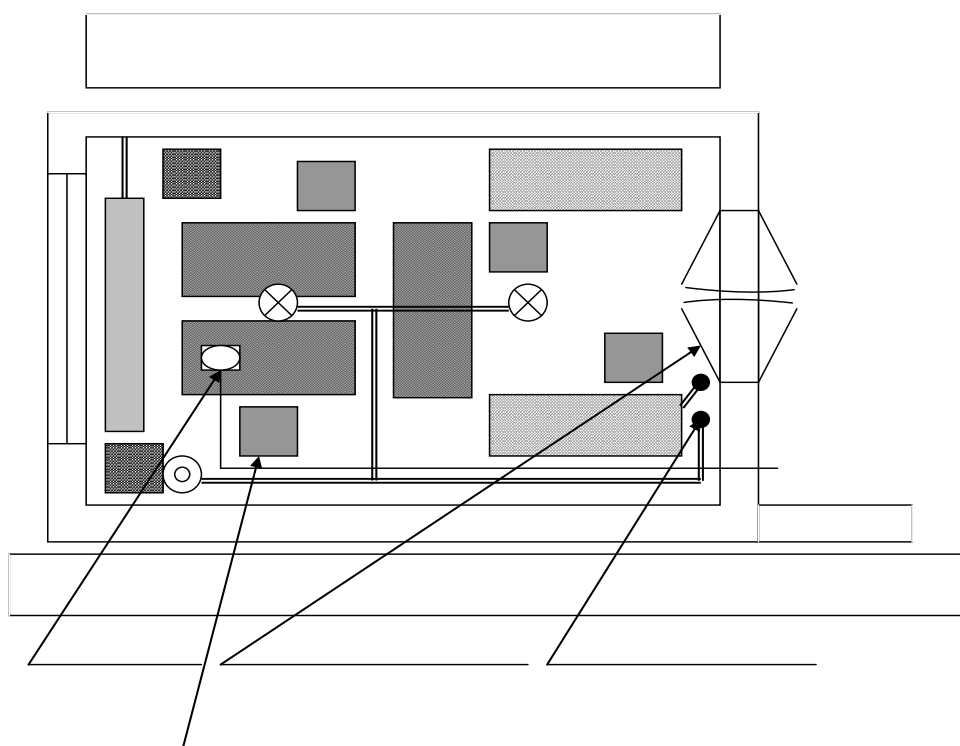
5. Перелік технічних засобів, встановлених у приміщенні:

№ з/п	Найменування, тип, заводський номер	Кількість	Спосіб захисту	Примітка

6. План розміщення технічних засобів і трас прокладання комунікацій:

схематичний рисунок плану приміщення, на якому зазначені місця установки технічних засобів, траси проходження кабелів (зв'язку, передачі даних, електроживлення і заземлень), інженерні комунікації (водопровід, опалювання, вентиляція).

Вказуються відстані від технічних засобів і кабелів до межі КЗ, відстані між окремими видами технічних засобів.



7. Організаційні заходи щодо захисту інформації:

Стисло описуються заходи, наприклад:

включення ПЕОМ № ____ під час проведення конфіденційних переговорів, нарад, бесід забороняється.

Телефонні апарати міської та внутрішньої АТС розташовувати не ближче 0,5 м від апарату зі скремблером і т. д.

8. Відповідальний за приміщення:

із заходами захисту інформації, реалізованими в приміщенні

№ _____, ознайомлений:

№ з/п	Дата ознайомлення	Прізвище, ім'я, по батькові	Особистий підпис

9. Відомості про атестаційні перевірки:

Дата перевірки	Перелік зауважень за результатами перевірки	ПІБ і посада особи, яка перевіряє	Дата і підпис	Документ про усунення порушень	Дата і підпис відповідального за експлуатацію об'єкта захисту
1	2	3	4	5	6

Примітки:

У графі 2 за відсутності зауважень вказується: "Порушення не виявлені"; за наявності порушень вказується їх характер і пропозиції щодо термінів ліквідації.

У графі 5 робиться посилання на акт, що засвідчує факт усунення виявленого порушення. Акт складається представником підрозділу ТЗІ і відповідальним за забезпечення режиму у виділеному приміщенні в довільній формі і затверджується керівництвом організації.

10. Відомості про зміни в паспорті:

№ з/п	Дата, № документа	Замінені (змінені) аркуші	Примітка

(Складено з використанням рекомендацій ЦТЗІ МВС України)

Паспорт складений:

ким, коли, підпис

* З 2007 р. ЦТЗІ має назву Управління технічного захисту та криптографічної обробки інформації ДДЗР МВС України.

Використана література

1. Закон України "Про державну таємницю" від 21.01.1994 р. // Закони України. – К., 1997. – Т.7.
2. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 р. // Закони України. – К., 1997. – Т.7.
3. Постанова Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" від 9 серпня 1993 р. № 611 // Збірник постанов Уряду України. – 1993. – №12.
4. Постанова Верховної Ради України "Про Концепцію [основи державної політики] національної безпеки України" від 16 січня 1997 р. № 3/97-ВР // Право України. – 1997. – № 3. – С. 84-89.
5. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, – М.: ГТК РФ, 1992. – 39 с.
6. Андрианов В. И. Охранные системы для дома и офиса / В. И. Андрианов, А. В. Соколов. – СПб.: БХВ-Петербург; Арлит, 2002. – 304 с.
7. Андрианов В. И. Устройства для защиты объектов и информации. ("Шпионские штучки") / В. И. Андрианов, А. В. Соколов. – М.: ООО "Фир-ма "Издательство АСТ"; ООО "Издательство "Полигон", 2000. – 256 с.
8. Анин Б. Ю. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.
9. Вакуленко Р. Я. Защита бизнеса и стратегия предприятия. Экономический и правовой аспект / Р. Я. Вакуленко, Е. В. Новоселов. – М.: Юркнига, 2005. – 160 с.
10. Варфоломеев А. А. Методы криптографии и их применение в банковских технологиях / А. А. Варфоломеев, М. Б. Пеленицын – М.: Изд. "Банковское дело", 1995. – 224 с.
11. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 29 с.

12. Гайкович В. Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 324 с.

13. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович, А. Ю. Першин. – М.: Единая Европа, 1994. – 363 с.

14. Гаффин Адам. Путеводитель по глобальной компьютерной сети. – М.: ТПП «Сфера», 1995. – 282 с.

15. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: МОПО РФ – МГИФИ, 1997. – 538 с.

16. Герасимов П. А. Основы экономической безопасности: Учебно-метод. комплекс (для студ. обучающихся по спец. 08050365 "Антикризисное управление", 08011665 "Математические методы в экономике"). – М.: Фин. акад. при Правительстве РФ, 2005. – 58 с.

17. Герасимов П. А. Экономическая безопасность хозяйствующего субъекта. Учебно-метод. комплекс (для студ., обучающихся в Институте экономической безопасности по специальности 08010565 "Финансы и кредит") – М.: Фин. акад. при Правительстве РФ, 2005. – 73 с.

18. Давыдовский А. И. Введение в защиту информации/ А. И. Давыдовский, В. А. Максимов // Интеркомпьютер. – 1990. – № 1. – С.17 – 20.

19. Дейтел Г. Введение в операционные системы: В 2-х т. Т. 2. Пер. с англ. – М.: Мир, 1987. – 398 с.

20. Дружинин Г. В. Качество информации/Г. В. Дружинин, И. В. Сергеева. – М.: Радио и связь, 1990. – 172 с.

21. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1997. – 336 с.

22. Защита информации в компьютерных системах / Под ред. Э. М. Шмакова. – СПб.: СПбГТУ, 1993. – 100 с.

23. Защита информации в персональных ЭВМ/ А. В. Слесивцев, В. А. Вегнер, А. Ю. Крутяков и др. – М.: Радио и связь, МП "Веста", 1992. – 192 с.

24. Защита прав создателей и пользователей программ для ЭВМ и баз данных. – М.: Ось, 1996. – 186 с.

25. Зимин Н. Е. Анализ и диагностика финансово-хозяйственной деятельности предприятия: Учебник для вузов / Н. Е. Зимин, В. Н. Солопова. – М.: КолосС, 2004. – 383 с.

26. Зиннуров У. Г. Методология обеспечения экономической безопасности предприятия на основе стратегического маркетингового планирования и управления / У. Г. Зиннуров, В. С. Исмаилова. – М.: Изд.

МАИ, 2004. – 375 с.

27. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

28. Кавун С. В. Методика построения политики безопасности организации: [Текст] / С. В. Кавун, Г. В. Шубина // "Бизнес Информ". – Х.: 2005. – № 1/2. – С. 96 – 102.

29. Леонтьев Б. Хакеры и Интернет. – М.: ЦФТИ, 1998. – 338 с.

30. Малый бизнес. Организация, экономика, управление / Под ред. проф. В. Я. Горфинкеля, проф. В. А. Швандара. Учеб. пособие. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2003. – 430 с.

31. Моисеенков И. Э. Американская классификация и принципы оценивания безопасности компьютерных систем//Компьютер-пресс. – 1992. – №2/3. – С. 47 – 54.

32. Моисеенков И. Э. Основы безопасности компьютерных систем//Компьютерпресс. – 1991. – №10. – С. 19 – 24; №11. – С. 7 – 21.

33. Олейников Е. А. Экономическая и национальная безопасность: учебник для вузов. – М.: Экзамен, 2005. – 766 с.

34. Паштова Л. Г. Формирование многоуровневой инвестиционной политики как фактор обеспечения экономической безопасности: дис. докт. экон. наук: 08.00.05/Л. Г. Паштова. – М., 2001. – 46 с.

35. Петраков А. В. Основы практической защиты информации. Учебн. пособие. – 2-е изд. – М.: Радио и связь, 2000. – 368 с.

36. Петренко И. О. Экономическая безопасность России: денежный фактор. – М.: Маркет ДС, 2003. – 240 с.

37. Пярин В. Российская интеллектуальная карта создана и работает// Бюллетень финансовой информации. – 1999. – № 12. – С. 45 – 49.

38. Расторгуев С. П. Искусство защиты и разведения программ. – М.: Радио и связь, 1991. – 224 с.

39. Родин Г. Некоторые соображения о защите программ//Компьютер-пресс. – 1991. – № 10. – С. 15 – 18.

40. Румянцева Е. Е. Новая экономическая энциклопедия. – 2-е изд. – М.: ИНФРА-М, 2006. – Т.VI. – 810 с.

41. Сажина М. А. Фирма: управление кризисом: Учеб. пособие / М. А. Сажина. – М.: Деловая литература, 2004. – 191 с.

42. Слепов В. А. Финансовая политика компании: учеб. пособие / В. А. Слепов, Е. И. Громова, И. Т. Кери; под ред. проф. Слепова С. А. –

М.: Экономист, 2005. – 283 с.

43. Соколов А. В. Защита от компьютерного терроризма. Справочное пособие / А. В. Соколов, О. М. Степанюк. – СПб.: БВХ-Петербург; Арлит, 2002. – 496 с.

44. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах/ А. В. Соколов, В. Ф. Шаньш. – М.: ДМК Пресс, 2002. – 656 с.

45. Специвцев А. В. Защита информации в персональных ЭВМ/ А. В. Специвцев, В. А. Вегнер, А. Ю. Крутяков. – М.: Радио и связь, 1992. – 192 с.

46. Стенг Дэвид. Секреты безопасности сетей / Дэвид Стенг, Сильвия Муи. – К.: "Диалектика", Информейшн Компьютер Энтерпрайз, 1996. – 544 с.

47. Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 13 с.

48. Технические средства защиты информации. Каталог ЗАО "Анна". – М.: Изд. "Анна", 1999. – 112 с.

49. Технические средства защиты информации. Каталог НПЦ фирмы "НЕЛК". – М.: Изд. "НЕЛК", 1999. – 92 с.

50. Торокин А. А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998. – 336 с.

51. Тэпман Л. Н. Риски в экономике / Под ред. проф. В. А. Швандара. – М.: ЮНИТИ, 2003. – 380 с.

52. Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1995. – 128 с.

53. Хорев А. А. Способы и средства защиты информации. – М.: МО РФ, 1998. – 316 с.

54. Хорев А. А. Технические средства и способы технического шпионажа. – М.: ЗАТ "Дальснаб", 1997. – 242 с.

55. Хоффман Л. Д. Современные методы защиты информации: Пер. с англ. – М.: Сов. радио, 1980. – 264 с.

56. Цыгичко В. Н. Информационное оружие как геополитический фактор и инструмент силовой политики/ В. Н. Цыгичко, Г. Л. Смоляк, Д. С. Черепекин. – М.: ИСА АН РФ, 1997. – 252 с.

57. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций. – М.: Дашков и К⁰, 2005. – 544 с.

58. Шарый Л. Д. Безопасность предпринимательской деятельности: учебник / Л. Д. Шарый, В. М. Родачин. – 2-е изд., доп. и перераб. – М.,

Нац. институт бизнеса. 2005. – 477 с.

59. Ярочкин В. И. Безопасность информационных систем. – М.: Ось-89, 1997. – 320 с.

60. Ярочкин В. И. Аудит безопасности фирмы: теория и практика: учеб. пособие для вузов / В. И. Ярочкин, Я. В. Бузанова. – М.: Акад. Проект; Королёв: Парадигма, 2005. – 351 с.

61. Яскевич В. И. Секьюрити: Организационные основы безопасности фирмы. – М.: Ось-89, 2005. – 368 с.

62. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом РФ 9 сентября 2000 года, № Пр-1895. // Российская газета/ http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm.

63. Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House, 66-74, V22. – P. 66-74. // Безопасность информационных технологий/ <http://www.security.ukrnet.net/modules/sections/index.php?artid=181&op=viewarticle>.

64. ISO/DIS 2382/8. Data processing. - Vocabulary - Part 8 : Control, integrity and security. – ISO, 1985. – 35 p. // Безопасность информационных технологий / <http://www.security.ukrnet.net/modules/sections/index.php?artid=181&op=viewarticle>.

65. ISO/DIS 7498/2. Information Processing Systems - Open Systems Interconnection Reference Model. Part 2: Security Architecture. – ISO, 1989. // Network security / <http://www.springerlink.com/index/w86vumr5fd7jc18q.pdf>.

66. NCSC-TG-001. A Guide to Understanding Audit in Trusted Systems // Federation of American Scientist / fas.org/irp/nsa/rainbow/tg001.htm.

67. NCSC-TG-003. A Guide to Understanding Discretionary Access Control in Trusted Systems // Federation of American Scientist / ftp.fas.org/irp/nsa/rainbow/tg003.htm.

68. NCSC-TG-005. Version-1 Trusted Network Interpretation of the trusted Computer System Evaluation Criteria // National Technical Information Service / <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA255422>.

69. NCSC-TG-006. A Guide to Understanding Configuration Management in Trusted Systems // Federation of American Scientist / www.fas.org/irp/nsa/rainbow/tg006.htm.

70. NCSC-TG-009. Version-1, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria// Federation of American Scientist / <ftp.fas.org/irp/nsa/rainbow/tg009.htm>.

NCSC-TG-021. Version-1 Draft Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria// Безопасность информационных технологий/ <http://www.security.ukrnet.net/modules/sections/index.php?artid=181&op=viewarticle>.

Зміст

Вступ.....	3
Модуль 2. Особливості застосування ІБ у бізнесі	6
4. ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ (КМ) ..	6
4.1. Стандарти ІЕБ	6
4.1.1. Основні положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку)...	12
4.1.2. Основні положення "Загальних критеріїв"	21
4.1.3. Базова технічна модель ІТ-безпеки у відповідності з NIST Special Publication 800-33	38
4.1.4. Оцінка безпеки ІС	46
4.1.5. Стандарт ISO	50
4.1.6. Механізми безпеки.....	53
4.1.7. Стандарти ЕСМА	55
4.1.8. Система стандартів Міністерства оборони США в області комп'ютерної безпеки.....	60
4.2. Ідентифікація та автентифікація КС	64
4.3. Методи та засоби ІЕБ в комп'ютерних системах	68
4.3.1. Криптографічні методи захисту інформації.....	75
4.3.2. Етапи розробки систем захисту	81
4.3.3. Критерії і особливості проектування оптимальної СЗІ.....	84
4.3.4. Технічне завдання на розробку СЗІ і план захисту інформації ..	87
4.3.5. Визначення якості реалізованої системи захисту	90
5. ПРАВОВІ ОСНОВИ ІБ	102
5.1. Основні юридичні поняття ІЕБ	102
5.1.1. Нормативно-правова база України у сфері ТЗІ	103
5.2. Приклади економічних порушень.....	106
5.2.1. Типи шахрайства	106
5.2.2. Найбільш типові види шахрайства з боку найманих робітників.....	108
5.2.3. Основні способи злочинних дій у системі обміну електронними документами	109
5.2.4. Основні заходи щодо забезпечення захисту електронних документів	110
5.2.5. Напади.....	119
5.3. Нормативні положення, що регламентують ІЕБ	123
5.3.1. Закони України із "Кодексу про адміністративні правопорушення"...	123
5.3.2. Закони України із "Кримінального кодексу"	125
5.3.3. Кримінально-правові наслідки.....	131
5.3.4. Цивільно-правові наслідки.....	133

Кавун С. В.
Носов В. В.
Манжай О. В.

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник

Частина 2