ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

НАВЧАЛЬНИЙ ПОСІБНИК З ДИСЦИПЛІНИ

“ПОЛІТИКИ БЕЗПЕКИ”

КОЗАЧОК В.А., ГАЙДУР Г.І., ГАХОВ С.О.,
ХМЕЛЕВСЬКИЙ Р.М., ЧУМАК Н.С.

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

НАВЧАЛЬНИЙ ПОСІБНИК З ДИСЦИПЛІНИ

“ПОЛІТИКИ БЕЗПЕКИ”

КОЗАЧОК В.А., ГАЙДУР Г.І., ГАХОВ С.О.,
ХМЕЛЕВСЬКИЙ Р.М., ЧУМАК Н.С.

Затверджено вченою радою
Державного університету
телекомунікацій
як навчальний посібник для студентів
вищих навчальних закладів за
спеціальністю “Кібербезпека”
(Протокол № 3 від 16 вересня 2020 р.)

Київ – 2020

УДК 621.391.13
В 685
ББК 32.811

Рецензенти: проф., д.т.н
проф., д.т.н.

Навчальний посібник призначений для студентів вищих навчальних закладів з навчальної дисципліни “Політики безпеки” (ПБ) - циклу дисциплін професійної та практичної підготовки за галуззю знань “Інформаційні технології”, за спеціальністю “Кібербезпека”.

Навчальна дисципліна “Політики безпеки” вивчається протягом одного семестру. Матеріал відповідає програмі дисципліни.

Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.

У посібнику розглянуто основи сучасної теорії синтезу та аналізу політик інформаційної безпеки. Наведено нормативно-правову основу створення політик інформаційної безпеки, вимоги міжнародних стандартів, документи, що забезпечують реалізацію політики безпеки.

Розглянуто приклади реалізації політик інформаційної безпеки, налаштування основних компонентів системи захисту.

Контрольні запитання допоможуть студентам з підготовки до перевірки рівня їх знань.

Навчальний посібник призначений для студентів, які навчаються за спеціальністю “Кібербезпека”, а також може бути корисний для аспірантів, викладачів навчальних закладів відповідних спеціальностей, фахівців у цій галузі знань.

ЗМІСТ

ПЕРЕДМОВА

Навчальний посібник призначений для вивчення дисципліни “Політики безпеки” (ПБ) з циклу дисциплін професійної та практичної підготовки для студентів вищих навчальних закладів усіх форм навчання за спеціальністю “Кібербезпека”.

Навчальний посібник відповідає програмі дисципліни ПБ.

Посібник призначено для студентів, які вперше знайомляться з процесами синтезу та аналізу політик інформаційної безпеки. Творчий колектив авторів намагалися максимально використовувати термінологію доступну і зрозумілу студентам.

Робота з навчальним посібником не виключає використання інших підручників та посібників, список яких подано наприкінці.

Предметом навчальної дисципліни є сучасні технології синтезу та аналізу політик інформаційної безпеки.

Метою вивчення навчальної дисципліни є опанування навичками обґрунтування застосування механізмів захисту та оцінки рівня захищеності інформаційної системи (технології).

Завданнями навчальної дисципліни є формування наступних умінь:

- уміти характеризувати основні поняття та визначення теорії захищених інформаційних систем;
- уміти моделювати основні процеси забезпечення безпеки обчислювальних систем;
- уміти обґрунтовувати основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;
- уміти обґрунтовувати застосування національних та міжнародних стандартів безпеки інформаційних технологій;
- уміти характеризувати особливості забезпечення безпеки сучасних інформаційних технологій;
- уміти здійснити формування базових положень політики безпеки: врахувати взаємозв’язок понять живучості, захищеності, надійності, визначити основні рівні захисту ресурсів автоматизованої системи, розробити правила забезпечення інформаційної безпеки.

НАВЧАЛЬНИЙ ПОСІБНИК

ПОЛІТИКИ БЕЗПЕКИ

Тема 1. Технологія попереднього аудиту безпеки інформаційно-комунікаційної системи як передумова побудови політики безпеки

Вступ. Мета та задачі курсу ПБ. Досягнення сучасної теорії та техніки синтезу та аналізу політик інформаційної безпеки.

Опис інформаційно-телекомунікаційної системи та середовища її функціонування. Апаратне та програмне забезпечення інформаційно-комунікаційної системи. Обчислювальна мережа. Технології оброблювання інформації. Склад та характеристика існуючої системи захисту. Моделі порушника та загроз. Аналіз ризику функціонування. Управління ризиком. Витрати на розробку систем захисту.

Тема 2. Основи аналізу і синтезу політик безпеки

Основи аналізу політик безпеки. Класифікація політик безпеки. Декомпозиція політик безпеки та формалізація їх змісту. Основні показники політик безпеки. Оптимізація змісту політики безпеки. Аналіз кращих зразків створення політик безпеки.

Основи синтезу політик безпеки. Загальна методика синтезу політик безпеки. Синтез політик безпеки гарантовано захищених інформаційних і комунікаційних систем.

Тема 3. Розробка та реалізація політик безпеки

Нормативно-правова основа створення політик безпеки. Вимоги міжнародних стандартів. Національна традиція розроблення політик безпеки.

Формування базових положень політики безпеки. Методи та засоби створення політик безпеки. Документи, що забезпечують реалізацію політики безпеки.

Реалізація політик безпеки. Завдання правил інформаційної безпеки. Побудова архітектури системи захисту інформації. Налаштування основних компонентів системи захисту. Удосконалення політики безпеки та правил безпеки.

Тема 4. Оцінка політики безпеки

Гарантії правильності забезпечення політики безпеки. Живучість, захищеність, надійність. Рівні захисту ресурсів.

Розділ 1

ТЕХНОЛОГІЯ ПОПЕРЕДНЬОГО АУДИТУ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ЯК ПЕРЕДУМОВА ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ

1.1. Основні положення системно-концептуального підходу до захисту інформації. Класифікація цілей захисту

З позицій системно-концептуального підходу конструктивними елементами уніфікованої концепції захисту інформації (ЗІ) мають бути:

- функція захисту – сукупність однорідних у функціональному відношенні заходів, регулярно здійснюваних з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійної ЗІ;
- засоби захисту – пристрої, програми і заходи, спеціально призначені для вирішення завдань ЗІ;
- завдання захисту – організовані можливості засобів, методів і заходів з метою реалізації функцій захисту;
- система ЗІ – організована сукупність усіх засобів, методів і заходів, спрямованих на забезпечення необхідного рівня захищеності інформації в усіх структурних елементах інформаційних систем (ІС), на всіх ділянках і технологічних маршрутах її обробки та на всіх етапах її життєвого циклу з урахуванням взаємодії з зовнішнім середовищем, яка повинна охоплювати весь технологічний комплекс інформаційної діяльності, бути різноманітною по використовуваних засобах, багаторівневої з ієрархічною послідовністю доступу, бути відкритою для зміни й доповнення мер забезпечення безпеки інформації, бути нестандартною та різноманітною, бути простою для технічного обслуговування й зручної для експлуатації користувачами, бути надійною та комплексною, тобто, мати цілісність.

При цьому власне ЗІ має бути:

- безперервним (вимога виходить із того, що зловмисники тільки й шукають можливість, як би обійти систему захисту інформації, що цікавить);
- плановим (забезпечується шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції з урахуванням загальної мети);
- цілеспрямованим (захищається те, що повинне захищатися в інтересах конкретної мети, а не все підряд);
- конкретним (захисту підлягають конкретні дані, втрата яких може заподіяти організації певний збиток);
- активним (захищати інформацію слід з достатнім ступенем наполегливості);
- надійним (методи й форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних секретів, незалежно від форми їхнього подання, мови вираження й виду фізичного носія, на якому вони закріплені);
- універсальним (незалежно від виду каналу витоку або способу НСД до інформації їх необхідно перекривати, де б вони не були виявлені);
- комплексним (для захисту інформації у всьому різноманітті структурних елементів повинні застосовуватися всі його можливі види й форми в повному обсязі).

Враховуючи таке головними складовими системно-концептуального підходу нині є:

1) дослідження і розробка єдиних методологічних понять усієї сукупності питань, зв'язаних із ЗІ;
2) розгляд у єдиному комплексі усіх видів ЗІ: забезпечення фізичної цілісності, попередження несанкціонованої модифікації, попередження несанкціонованого одержання;
3) системне врахування всіх факторів, що впливають на захищеність інформації;
4) комплексне використання всіх наявних засобів ЗІ.

Загальна класифікація цілей захисту інформації приведена на рис. 1.1.

Аналіз класифікації показує, що друга мета захисту, а саме попередження несанкціонованої модифікації інформації значною мірою є комбінацією першої і третьої цілей. Дійсно, несанкціонована модифікація може бути випадковою або злочинною. Випадкова модифікація, у свою чергу, може бути наслідком перекручування інформації. Злочинна ж модифікація є результатом злочинних дій.

Об'єктами захисту у цьому випадку є:

1) вихідні дані, тобто дані, що надійшли від користувачів або абонентів;

2) довільні дані, тобто дані, отримані в процесі обробки вихідних даних;

3) нормативно-довідкові, службові і допоміжні дані, включаючи і дані системи захисту;

4) постановка завдань, методів і моделі, алгоритмів і програми, які використовуються при обробці даних;

5) технічна, технологічна, політична, військова й економічна документація.

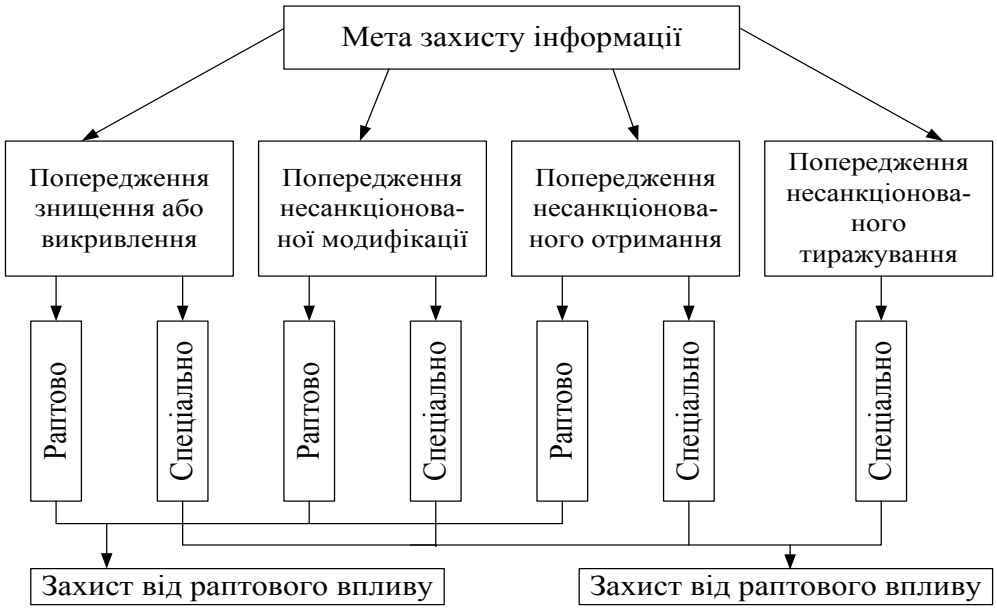


Рис. 1.1. Загальна класифікація цілей захисту інформації

З урахуванням такого ЗІ повинен здійснюватися в таких зонах:

- зоні ресурсів, тобто зоні функціонуючих технічних засобів;
- зоні помешкань, тобто сукупності помешкань, у яких розташовані технічні засоби і розміщуються люди, що мають відношення до них;
- зоні території, що охороняється, тобто тій частині території, на якій розташовані будинки з зоною помешкань і на якій може повністю регулюватися доступ людей, а також можуть регулюватися і контролюватися всі дії і заходи, здійснювані на ній;
- зоні, що не охороняється, але контрольованій території, тобто тій частині зовнішньої території, у процесах якої може здійснюватися регулярний контроль її стану і зроблених на ній дій;
- зовнішній зоні, тобто тій частині території, на якій можуть здійснюватися дії і відбуватися події, що роблять вплив на надійність інформації, але яка не може бути під постійним контролем.

Важливим результатом системно-концептуального підходу до проблеми, яка розглядається може бути висновок про неможливість надійного ЗІ без дотримання при її побудові цілого ряду достатньо специфічних умов, які виступають в якості зворотного зв'язку від конструктивних елементів концепції захисту до концепцій побудови й організації функціонування інформації.

1.2. Визначення і аналіз поняття загрози безпеці інформації

Загрозами безпеці інформації, що обробляється в інформаційних системах (ІС) і циркулює у зв'язку з цим у відповідних приміщеннях вважають події, які шляхом потенційно можливого впливу на ІС прямо та/або опосередковано завдають збитку її власникам і користувачам. Спроба реалізації загрози називається атакою, а той, хто вчиняє таку спробу, – зловмисником. Потенційні зловмисники називаються джерелами загроз. Усі загрози безпеці інформації в ІС можуть бути класифіковані за проявом, метою реалізації, засобами, методами і наслідками, а також за принципами, характером та способами впливу на певний об'єкт (рис. 1.2). Відповідно до процесу прояву вони розділяються на природні й техногенні. Природні загрози можуть бути викликані стихійними природними явищами й об'єктивними фізичними процесами. Техногенні – є наслідком діяльності людини, технічних засобів і систем.

Рис. 1.2 Класифікація загроз безпеці інформації

У свою чергу за мотивами походження техногенні загрози безпеці інформації розділяються на випадкові й навмисні (табл. 1.1).

Таблиця 1.1

Типи загроз безпеці інформації в інформаційній системі

Тип загрози		**Причини або спонукальні мотиви**
Навмисні загрози	**Ненавмисні загрози**	
Розкрадання носіїв інформації		Прагнення використовувати конфіденційну інформацію у своїх цілях
Застосування програмних пасток		
	Несправність апаратури, що може ініціювати несанкціоноване зчитування інформації	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Використання програм "троянський кінь"		Завдання збитків шляхом несанкціонованого доступу в систему

Продовження табл. 1.1

Тип загрози		Причини або спонукальні мотиви
Навмисні загрози	Ненавмисні загрози	
Впровадження комп'ютерного вірусу		Руйнування інформаційної системи з метою завдання збитків
Помилки в програмах обробки інформації		Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп'ютерного вірусу		Руйнування інформаційної системи з метою завдання збитків
Застосування програмних пасток		
	Несправність апаратури, що може ініціювати несанкціоноване зчитування інформації	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Використання програм "троянський кінь"		Завдання збитків шляхом несанкціонованого доступу в систему
Помилки в програмах обробки інформації		Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп'ютерного вірусу		Руйнування інформаційної системи з метою завдання збитків
	Помилки в програмах обробки інформації	Застосування несертифікованого програмного продукту
	Впровадження комп'ютерного вірусу	Не дотримання обслуговуючим персоналом вимог безпеки, порушення ним технологічної послідовності роботи із системою
Помилкова комутація в мережі ЕОМ		З метою створення каналу для витоку конфіденційної інформації
	Помилкова комутація в мережі ЕОМ	Низька кваліфікація обслуговуючого персоналу
	Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування інформаційної системи або її створення
	Перехресні наведення за рахунок ЕМВ	
Примусове електромагнітне опромінення		Вивід з ладу ІС з метою завдання збитків
Використання акустичних випромінювань		Одержання конфіденційної інформації
Копіювання за допомогою візу- ального й слухового контролю		
Маскування під користувача, підбор пароля		Несанкціоноване втручання в роботу системи в злочинних цілях
	Помилка в роботі оператора	Низька кваліфікація оператора, застосування несертифікованого програмного продукту
	Помилки користувача	Використання недостатнього захисту
Помилки програміста: опис і перекручування програмного за- хисту, розкриття кодів та паролів		З метою добування особистої вигоди або завдання збитків
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація		
	Помилки персоналу: перекручування схем захисту, помилкова комутація	Недостатня кваліфікація, порушення технології

Випадкові загрози можуть бути викликані помилками проектування ІС і системи захисту інформації, помилками в програмному забезпеченні (ПЗ), збоями та відмовами апаратури і систем забезпечення, помилками персоналу. Навмисні загрози обумовлені цілеспрямованими діями людей (порушників). За місцем розміщення джерела загроз відносно ІС останні розділяються на дистанційні та контактні. До дистанційних відносяться загрози, джерело яких (людина, апаратура, програма тощо) перебуває поза межами контрольованої території. Контактні загрози здійснюються в межах контрольованої зони, як правило, при проникненні в приміщення, де розташовані засоби обробки й зберігання інформації. На рис. 1.3 наведено варіант структурованої бази потенційних загроз для інформації, яка базується на наведених вище обґрунтуваннях.

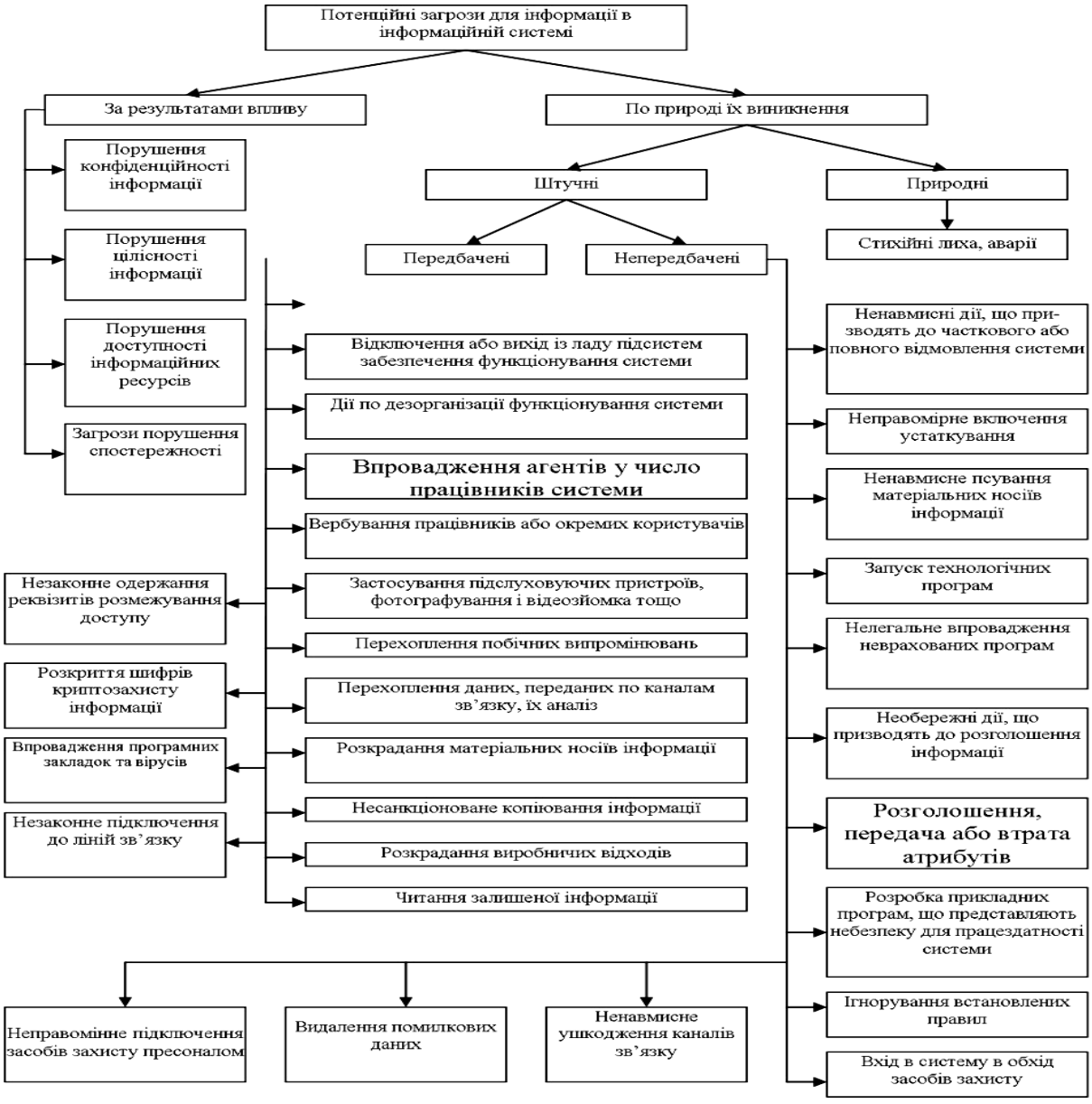


Рис. 1.3. Структурована база потенційних загроз для інформації в інформаційній системі

Перелік можливих загроз інформації, що обробляється в ІС та циркулює у відповідних приміщеннях поданий у табл. 1.2.

Таблиця 1.2

Перелік можливих загроз інформації, що обробляється в ІС та циркулює у відповідних приміщеннях

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
Загрози природного походження							
1	Катастрофа	Пожежа, повінь, землетрус, ураган, вибух	Середовище		+	+	
2	Умови	Вологість, запиленість, зміни температури	Середовище		+	+	
Випадкові загрози техногенного походження							
3	Вібрація	Вібрація	Апаратура		+	+	
4	Перешкоди	Небажаний вплив процесів один на одного	Апаратура		+	+	
5	ЕМВ	Зовнішні електромагнітні випромінювання (електромагнітна сумісність)	Апаратура		+	+	
6	Аварія	Аварія систем життєзабезпечення.	Середовище		+	+	
7	Відмова-Л	Відмови (повний вихід з ладу, систематичне неправильне виконання своїх функцій) людей	Люди			+	+
8	Відмова-А	Відмови основної апаратури, систем передачі даних, носіїв інформації	Апаратура		+	+	+
9	Відмова-П	Відмови програм	Програми		+	+	+
10	Відмова-З	Відмови систем живлення, систем забезпечення нормальних умов роботи апаратури й персоналу (електроживлення, охолодження й вентиляції, ліній зв’язку тощо).	Середовище, апаратура		+	+	
11	Збій-А	Збої основної апаратури систем передачі даних	Апаратура	+	+	+	+
12	Збій-З	Збої систем харчування, систем забезпечення нормальних умов роботи апаратури й персоналу	Середовище, апаратура		+	+	
13	Помилка-Л	Випадкові помилки користувачів, що обслуговує персоналу, помилкова конфігурація й адміністрування системи	Люди	+	+	+	+
14	Помилка-П	Помилки програм	Програми	+	+	+	+
15	Недбалість	Недбале зберігання й облік документів, носіїв інформації	Люди	+	+	+	+
16	Поломка-А	Поломка апаратури	Люди	+	+	+	

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
17	Поломка-Н	Ушкодження носіїв інформації	Люди, апаратура		+	+	
18	Вірус	Поразка програмного забезпечення комп'ютерними вірусами.	Люди, програми	+	+	+	+
19	Підключення	Підключення до каналів зв'язку через штатні або спеціально розроблені апаратні засоби (у тому числі підключення через установлені модемні, факс- модемні плати)	Люди, апаратура, програми	+		+	
Навмисні загрози техногенного походження дистанційної дії							
20	ПЕМВ	Одержання інформації з каналу побічного електромагнітного випромінювання основних технічних засобів (пристроїв наочного відображення, системних блоків, периферійної апаратури, апаратури зв'язку, ліній зв'язку, кабелів)	Апаратура	+			
21	Е-наведення	Одержання інформації з каналу побічних наведень у системах каналізації, у мережах теплопостачання, у системах вентиляції, у шинах заземлення, у ланцюгах телефонізації	Апаратура	+			
22	Віброакустика	Одержання інформації з віброакустичного каналу з використанням лазерних пристроїв зняття інформації	Апаратура	+			
23	Спецвпливи	Одержання інформації з каналів спеціального впливу (електромагнітне й високочастотне опромінення об'єкта захисту)	Апаратура	+			
24	Е-імпульс	Використання електромагнітних імпульсів з метою знищення інформації, засобів її обробки й зберігання	Апаратура		+	+	
25	Підслуховування-Т	Прослуховування телефонних мереж	Апаратура, люди	+			
26	Оптика	Використання оптичних засобів, дистанційне фотографування	Апаратура	+			
27	НСД-ЛВЗ	Несанкціонований дистанційний доступ до ЛВЗ	Люди, апаратура, програми	+	+	+	+

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
28	Переадресація	14ере адресація (зміна маршруту) передачі даних.	Люди, програми	+		+	+
29	Нав'язування	Нав'язування порочної інформації під ім'ям авторизованого користувача	Люди, програми		+		+
Навмисні загрози техногенного походження контактної дії							
30	Прослуховування	Прослуховування мережі за допомогою програмних або програмно-апаратних аналізаторів.	Апаратура, програми	+			+
31	Читання-З	Читання "сміття" (залишкової інформації із запам'ятовувальних пристроїв)	Люди, апаратура, програми	+			
32	Читання-Е	Оглядання даних, які виводяться на екран.	Люди, апаратура	+			
33	Читання-Д	Оглядання даних, які роздруковуються, читання залишених без огляду видрукуваних на принтері документів	Люди, апаратура	+			
34	Ушкодження	Фізичне знищення системи (у результаті вибуху, підпалу й т.п.), ушкодження всіх або окремих найбільш важливих компонентів АС (прибудував, носіїв важливої системної інформації, осіб із числа персоналу й т.п.), систем електроживлення тощо	Люди		+	+	
35	Відключення-О	Відключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження й вентиляції, ліній зв'язку тощо)	Люди, апаратура, програми		+	+	
36	Закладка	Використання й дистанційні пристрої, що підслуховують.	Люди, апаратура	+			
37	Випитування	Провокація до розмов осіб, що мають відношення до АС.	Люди	+			+
38	Копіювання	Копіювання вихідних документів, магнітних і інших носіїв інформації (у тому числі при проведенні ремонтних і регламентних робіт із ГМД)	Апаратура, програми, люди	+			
39	Розкрадання	Розкрадання магнітних носіїв і документів (оригінали й копії інформаційних матеріалів, ГМД, стрімерних стрічок), виробничих відходів	Люди	+			

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
		(відбитків, записів, носіїв інформації т.п.), одержання неврахованих копій					
40	Імітація	Незаконне одержання паролів і інших реквізитів розмежування доступу (агентурним шляхом, у результаті недбалості користувачів, підбором, імітацією інтерфейсу системи тощо) з наступним маскуванням під зареєстрованого користувача (“маскарад”)	Люди, програми	+	+		+
41	НСД-РС	Несанкціоноване використання робочі станції й терміналів ЛВЗ	Люди програма	+	+	+	+
42	НСД-П	Несанкціоноване використання технічних засобів (модем, апаратний блок кодування, периферійні пристрої)	Люди програми	+		+	+
43	Злом	Обхід механізмів захисту з метою забезпечити надалі псевдосанкціонований доступ порушника	Люди програми	+	+		
44	Перехоплення	Перехоплення паролів програмою-імітатором, перехоплення повідомлень.	Люди, програми	+	+	+	+
45	Закладка-П	Включення в програми програмних закладок типу "троянський кінь", "бомба" тощо.	Люди, програми	+	+	+	+
46	Підміна	Несанкціоновані зміни, підміна елементів програм, елементів БД, апаратури, магнітних носіїв	Люди, програми	+	+	+	+
47	Дезорганізація	Дії щодо дезорганізації функціонування системи (зміна режимів роботи пристроїв і програм, страйк, саботаж персоналу, постановка потужних активних перешкод на частотах роботи пристроїв системи й т.п.)	Люди, програми		+	+	
48	Вербування	Вербування персоналу або окремих користувачів, які мають певні повноваження	Люди	+	+		
49	Вади	Використання вад немов програмування, операційних систем (у тому числі параметрів системи захисту, установлених "за замовчуванням").	Люди, програми	+	+	+	+

Причинами виникнення таких загроз може бути, як це відзначено вище, намагання зловмисника порушити фізичну цілісність інформації (ПФЦІ), несанкціоновано її модифікувати (внаслідок викривлень з якої-небудь причини та злочинних дій людей по якомусь каналу) або несанкціоновано її одержати через канали несанкціонованого одержання інформації (КНОІ). Механізм формування причин порушення ЗІ подано на рис. 1.4. Ті чинники, наслідком яких можуть бути зазначені впливи на інформацію, назвемо дестабілізуючими.

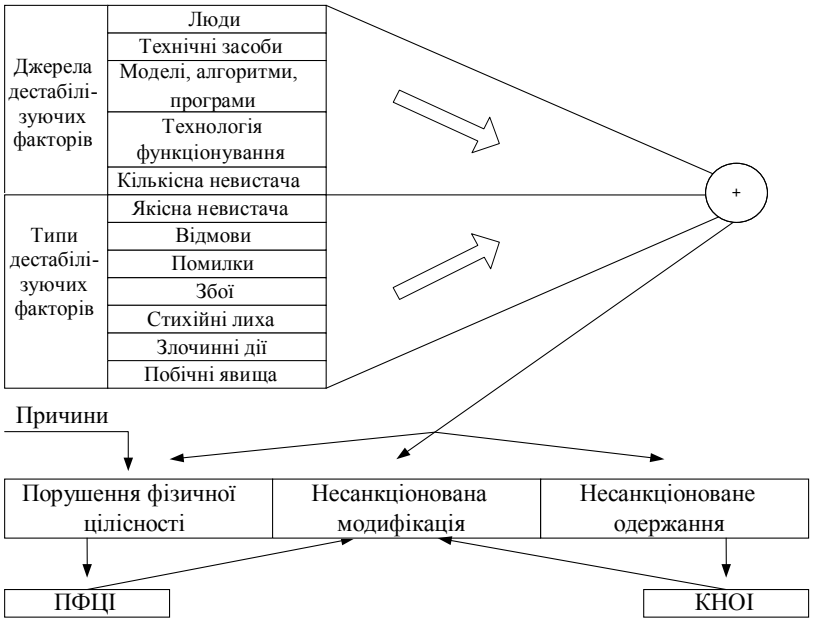


Рис. 1.4. Механізм формування причин порушення захисту інформації

Відповідно до технології і функціонування інформації, систему дестабілізуючих чинників складають такі:

- кількісна недостатність – фізична недостача одного або декількох технічних компонентів для забезпечення необхідної захищеності інформації з розглянутих показників;
- якісна недостатність – недосконаліть конструкції або організації одного або декількох компонентів, у силу чого не забезпечується необхідний ЗІ;
- відмова – порушення працездатності елемента, що призводить до неможливості виконання ним своїх функцій;
- збій – тимчасове порушення працездатності якогось елемента, наслідком чого може бути неправильне виконання ним у цей момент своїх функцій;
- стихійне лихо – спонтанне виникаюче неконтрольоване явище;
- злочинна дія – дію людей, спеціально спрямовані на порушення захищеності інформації;
- помилка – неправильне (одноразове або систематичне) виконання однієї або декількох функцій, що відбуваються внаслідок специфічного (постійного або тимчасового) його стану;
- побічне явище – явище, що супроводжує виконання елементом своїх основних функцій, але наслідком якого може бути порушення захищеності інформації.

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

- суспільство (окремі особи або групи осіб, дії яких можуть бути причиною порушення ЗІ);
- технічні пристрої і засоби;
- моделі, алгоритми і програми;
- технологія функціонування (сукупність засобів, прийомів, правил, заходів і угод, які використовуються у процесі опрацювання і передачі інформації);
- зовнішнє середовище (сукупність елементів, що можуть впливати на ЗІ).

Різні підходи у виявленні загроз безпеці інформації в інформаційних системах наведено в табл. 1.3 з погляду еталонної моделі взаємозв'язку відкритих систем.

Порушник розглядається як особа, яка може одержати доступ до роботи з включеними до складу інформаційної системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами інформаційної системи.

Таблиця 1.3

Підходи до виявлення загроз безпеці інформації
в інформаційних системах з погляду еталонної моделі взаємозв'язку відкритих систем

Загрози безпеці інформації	**Рівні еталонної моделі взаємозв'язку відкритих систем**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Землетруси	■	■	■	■	■	■	■
Пожежі	■	■	■	■	■	■	■
Урагани	■	■	■	■	■	■	■
Електромагнітні бурі	■	■	■	■	■	■	■
Радіо приглушені лінії зв'язку	■	■					
Віруси					■	■	■
Спеціальні програмно-технічні впливи			■	■	■	■	■
Вбудовані дефекти			■				
Руйнування	■	■	■	■	■	■	■
Підробка			■				■
Розсекречування						■	■
Дешифрування		■				■	■
Декодування						■	■
Перехоплення інформації		■	■	■	■	■	■
Крадіжка інформації і її носіїв						■	■
Втрата			■	■			■
Неправомірні дії					■	■	■
Помилка в роботі							■
Затримка інформації	■	■	■	■	■		
Інформаційне пригнічення						■	■
Порушення доступу законних користувачів						■	■

Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з інформаційною системою – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- третій рівень визначається можливістю управління функціонуванням інформаційної системи, тобто впливом на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;

- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів інформаційної системи, аж до включення до складу інформаційної системи власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про інформаційну систему і комплекс засобів захисту. У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, що повинна бути адекватна реальному порушнику для даної інформаційної системи. При розробці моделі порушника визначається:

- припущення про категорії осіб, до яких може належати порушник;

- припущення про кваліфікацію порушника і його технічної оснащеності (про використані для здійснення порушення методи і засоби);

- припущення про мотиви дій порушника (переслідуваних порушником цілях);

- обмеження та припущення про характер можливих дій порушників.

Стосовно інформаційної системи порушники можуть бути внутрішніми (з числа персоналу системи):

- користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби;

- співробітники підрозділу розробки і супроводу програмного забезпечення (прикладні та системні програмісти);

- технічний персонал, що обслуговує приміщення (прибиральниці, електрики, сантехніки та інші працівники, що мають доступ у приміщення, де розташована ІС);

- керівники різних рівнів посадової ієрархії,

або зовнішніми (сторонніми особами):

- відвідувачі (запрошені з будь-якого приводу);

представники організацій, що взаємодіють з питань забезпечення життєдіяльності установи (енергопостачання, водопостачання, теплопостачання тощо);

- представники конкуруючих організацій або особи, що діють за їхнім завданням;

- особи, що випадково або навмисно порушили перепускний режим (без мети порушення безпеки інформаційної системи);

- будь-які особи за межами контрольованої території.

Можливо виділити три основні мотиви порушень: безвідповідальність, самоствердження, корисливий інтерес. Усіх порушників можливо класифікувати в такий спосіб. За рівнем знань про інформаційну систему:

- знає функціональні особливості інформаційної системи, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

- має високий рівень знань та досвід роботи з технічними засобами системи і їхнього обслуговування;

- має високий рівень знань у галузі програмування, проектування та експлуатації інформаційних систем;

- знає структуру, функції та механізм дії засобів захисту, їхні сильні і слабкі сторони.

За рівнем можливостей (використаним методом і засобом):

- застосовуючи часто агентурні методи оволодіння відомостями;

- застосовуючи пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- використовуючи тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, що можуть бути потай пронесені через охорону;

- застосовуючи методи та засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, упровадження програмних закладок та використання спеціальних інструментальних і технологічних програм).

За часом дії:

- у процесі функціонування ІС (під час роботи компонентів системи);

- у період неактивних компонентів системи (у неробочий час, під час планових перерв у її роботі, перерв з метою обслуговування і ремонту тощо);

- як у процесі функціонування ІС, так і в період активності компонентів системи.

За місцем дії:

- без доступу на контрольовану територію організації;

- із контрольованої території без доступу у приміщення;

- усередині приміщень, але без доступу до технічних засобів ІС;

із робочих місць кінцевих користувачів інформаційної системи;

- із доступом у зону даних (баз даних, архівів тощо);

- із доступом у зону керування засобами забезпечення безпеки системи.

Структурна схема потенційних дій порушника для інформацій в інформаційній системі наведена на рис. 1.5.

Визначення конкретних значень характеристик можливих порушників у значній мірі суб’єктивне. Модель порушника, побудована з урахуванням особливостей конкретної предметної галузі та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду. Кожен вид порушника повинен бути охарактеризований значеннями характеристик, наведених вище. Методи перевірки отриманих моделей, їхньої відповідності до реальної системи і порядок визначення потенційно вразливих місць у системі, є обов’язковим при створенні моделі. Так, помилки персоналу можуть становити 55%, нечесні співробітники – 10%, скривджені особи – 9%, зовнішній напад – 1..3%, віруси – 4%, проблеми фізичного захисту (стихійні лиха, порушення електроживлення зниження або підвищення напруги, коливання потужності і опалення тощо) – 20%.

Формалізована модель оцінювання загроз безпеці інформації за метою реалізації. З позицій впливу на інформацію та систему її обробки найбільший інтерес представляють загрози за метою реалізації.

На їх підґрунті формується, як правило, формалізована модель оцінювання ступеня порушення системи захисту інформації у досліджуваній системі. Згідно з нормативними документами ТЗІ України (НД ТЗІ 1.1-002-99 та НД ТЗІ 2.5-004-99) такі загрози полягають у порушенні:

- конфіденційності інформації (властивість інформації бути відомою в плані читання або копіювання тільки допущеним або інакше авторизованим суб'єктам ІС – користувачам, програмам, процесам);

- цілісності інформації (властивість інформації бути незмінною в семантичному змісті, що досягається сукупністю заходів щодо її захисту від збоїв, видалення і несанкціонованого доступу до неї); - доступності до інформації (властивість інформації бути захищеною від

несанкціонованого блокування, часткової або повної втрати працездатності системи).

При цьому до загроз порушення конфіденційності інформації в ІС відносимо спроби:

- несанкціонованого перехоплення електронних і акустичних випромінювань;
- примусового електромагнітного опромінення (підсвічування) ліній зв'язку;
- несанкціонованого застосування закладених пристроїв і програмних закладок;
- відновлення тексту принтера та дистанційного фотографування;
- розкрадання носіїв інформації й документальних відходів;
- читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що відносяться до різних класів захищеності;
- копіювання носіїв інформації з подоланням засобів захисту;
- маскування під зареєстрованого користувача або під під запити системи;
- використання недоліків мов програмування й операційних систем;
- незаконне підключення до апаратури і ліній зв'язку;
- виведення з ладу механізмів захисту;
- впровадження і використання комп'ютерних вірусів тощо.

Вони ймовірно можуть бути реалізовані порушником за умови подолання ним засобів:

- організаційного обмеження доступу (p_{ood});

охоронної сигналізації (p_{oc});

- захисту від вірусних атак ($p_{атак}$);
- канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ ($p_{кзткм}$);
- управління доступу, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{уфд}$);
- адміністрування доступу до відповідних суб'єктів і об'єктів з використанням механізмів загального і спеціального ПЗ ($p_{ад}$).

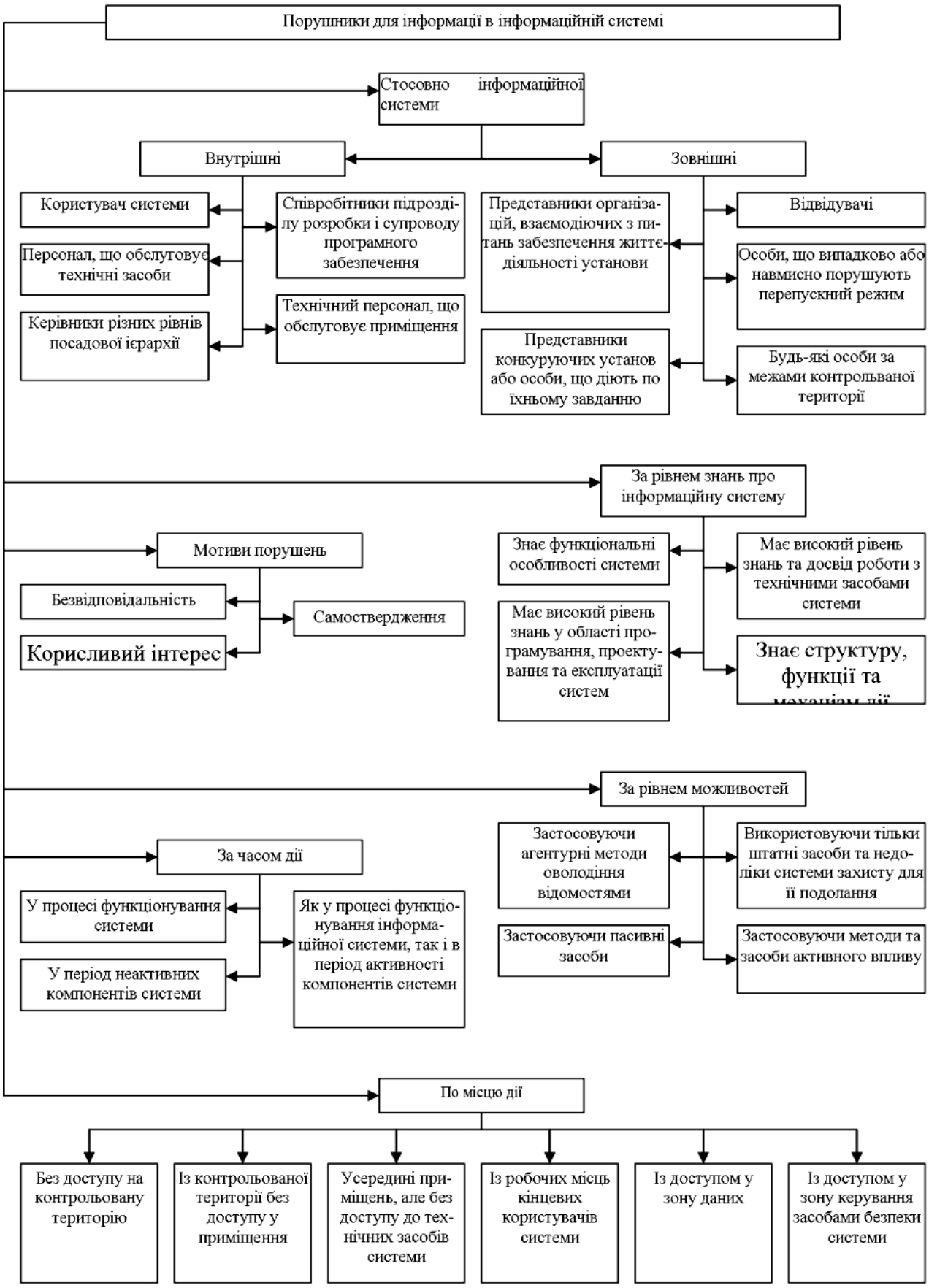


Рис. 1.5. Структурна схема потенційних дій порушника

Виходячи з такого, ймовірність подолання неавторизованим користувачем зазначених засобів захисту може бути визначена з виразу:

$$p_{пзз} = p_{уфд} \cdot p_{ад} \cdot \left[1 - (1 - p_{ооД}) \cdot (1 - p_{ос}) \cdot (1 - p_{атак}) \cdot (1 - p_{кзктм})\right]. \quad (1.1)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за умови, якщо порушник після її отримання:

- знає мову, якою інформація представляється (ймовірність події – $p_{мова}$);
- знає і може застосовувати програмні засоби або апаратуру криптографічного перетворення (ймовірність події – $p_{пз/ктп}$);
- має необхідні ключі або ключові набори для такого перетворення (ймовірність події – $p_{ключі}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем засобів криптографічного захисту з урахуванням положень [97, 98, 100] може бути визначена з виразу:

$$p_{кзі} = p_{мова} \cdot p_{пз/ктп} \cdot p_{ключі}. \quad (1.2)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих вище засобів може бути визначена як:

$$P_{ПКІ} = p_{кзі} \cdot \left[1 - (1 - p_{пзз})\right]. \quad (1.3)$$

До загроз порушення цілісності інформації відносимо:

- несанкціоновану модифікацію та/або видалення програм і даних;
- вставку, зміну або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі;
- втрату даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо.

Вони можуть бути реалізовані порушником за умови подолання засобів:

- організаційного обмеження доступу, охоронної сигналізації та управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо та адміністрування доступу, як й при аналізі загроз конфіденційності інформації (ймовірність такої події – $p_{пзз}$ визначена раніше);
- захисту цілісності від загроз у телекомунікаційних мережах ($p_{цткм}$);
- захисту від спеціальних впливів на інформацію по ТКМ ($p_{сп.вп}$);
- контролю та поновлення цілісності інформації ($p_{конт.ц}$).

З урахуванням можливостей попереднього підходу, ймовірність порушення цілісності $P_{ПЦІ}$ може бути знайдена з виразу:

$$P_{ПЦІ} = p_{конт.ц} \cdot \left[1 - (1 - p_{пзз}) \cdot (1 - p_{сп.вп}) \cdot (1 - p_{цткм})\right]. \quad (1.4)$$

До загроз порушення доступності інформації відносимо:

- повторення або вповільнення елементів протоколу;
- придушення обміну в телекомунікаційних мережах;
- використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні;

- перевитрата обчислювальних або телекомунікаційних ресурсів тощо.

Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до ІР ЛОМ (ідентифікації, аутентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації. Виходячи з такого стійкість системи управління доступом – (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та аутентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{пзз}. \tag{1.5}$$

Ця задача може вирішуватися застосуванням у ІС засобів фільтрації типу міжмережевих екранів (firewall, брандмауерів), сервісів-посередників (proxyservices) тощо. При середній тривалості обслуговування в ІТС одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, дорівнює:

$$p_{вик.рес} = 1 - p_0 = 1 - \exp\left\{-t_{вик.рес} \cdot \lambda_{зап}\right\}, \tag{1.6}$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів);

$t_{вик.рес}$ – середнє значення часу використання ресурсу.

Враховуючи таке ймовірність порушення доступності ресурсу з дорівнюватиме:

$$P_{ПДІ} = 1 - \left(1 - p_{вик.рес}\right) \cdot \left(1 - p_{ссуд}\right). \tag{1.7}$$

Виходячи з наведених вище формульних залежностей комплексна величина ймовірності порушення системи захисту інформації у ІС та їх специфічному класі – ЛОМ за метою реалізації з урахуванням пропозицій може бути, як результат, знайдена з виразу:

$$P_{ПСЗІ} = 1 - \left(1 - P_{ПКІ}\right) \cdot \left(1 - P_{ПЦІ}\right) \cdot \left(1 - P_{ПДІ}\right). \tag{1.8}$$

Наряду з загрозами за метою реалізації у окремий клас загроз варто виділити події, які залежно від умов можуть вплинути на кожну з відомих складових безпеки інформації шляхом:

- несанкціонованого доступу до ресурсів обчислювальної мережі без використання штатних засобів обчислювальної техніки;

- несанкціонованого включення до складу комплексів засобів обробки й захисту інформації нових елементів або зміни режимів їхньої роботи;

- виконання програм або дій в обхід системи захисту;

- підбору, перехоплення, розголошення або використання нестійких параметрів аутентифікації і ключів шифрування (дешифрування);

- нав’язування раніше переданого або помилкового повідомлення, заперечення факту його передачі або прийому;

- некомпетентного використання, настроювання або адміністрування комплексів засобів обробки і захисту інформації;

- внесення деструктивних дій у технологію обробки даних тощо.

За принципами, характером та способами активного впливу на певний об'єкт, який може перебувати у стані зберігання, обробки або передачі інформації між вузлами ІС або усередині вузла, такі події можуть бути поділені на загрози, що:

1) використовують принцип доступу суб'єкта ІС (користувача, процесу) до певного об'єкта (файлу даних, каналу зв'язку) або до прихованих каналів, тобто шляхів передачі інформації;

2) забезпечують активний або пасивний впливи на складові безпеки інформації в ІС;

3) реалізують опосередкований та безпосередній впливи, а також вплив на систему дозволів в ІС.

До перерахованих вище загроз безпеки інформації у ІС варто додати ще й такі, як: загроза несанкціонованого обміну інформацією між користувачами; загроза відмови від інформації, тобто невизнання одержувачем (відправником) факту її одержання (відправлення) тощо. Якщо вести мову конкретно про загрози безпеці інформації в ІС за метою реалізації, то з метою забезпечення конфіденційності й цілісності інформації у системі за рахунок унеможливлення доступу до неї та модифікації неавторизованим користувачем її змісту, окрім заходів організаційного обмеження доступом, необхідно перш за все застосовувати засоби: адміністрування доступу, управління фізичним доступом, криптографічного перетворення, контролю цілісності та охоронної сигналізації. З метою недопущення переводу ресурсу в режим штучної відмови – порушення доступності об'єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, необхідно додатково передбачити механізми: запобігання постійного чи занадто тривалого використання такого ресурсу, забезпечення стійкості та відновлення процесів в умовах збоїв, резервування інформаційних об'єктів, аналізу потоків запитів від суб'єктів ЛОМ та телекомунікаційних мереж, контролю та поновленню цілісності інформаційних об'єктів (наприклад, в каналах ІС).

Аналіз функціонування інформаційних систем в умовах загроз системам обробки інформації з обмеженим доступом

При аналізі функціонування інформаційних систем потрібно розглядати всі можливі варіанти комбінацій загроз на основі використання їхнього об'єднання та перерізу. Так, наприклад, для інформаційної системи обробки інформації з обмеженим доступом задано конкретний скінченний вектор загроз

$$X_n = (x_1, ..., x_n), \tag{1.9}$$

де {x} – множина потенційних загроз різного характеру, N – натуральна множина чисел, $n \in N$.

Тоді аналіз функціонування такої інформаційної системи базується на розв'язанні таких операторних рівнянь:

$$y_k = L_k\left[\bigcup_{i=1}^{m} x_i \bigcap_{j=1}^{q} x_j\right], k \in N \tag{1.10}$$

де y_k – це відгук інформаційної системи при вхідній дії об'єднання $\bigcup_{i=1}^{m} x_i$ та перетину $\bigcap_{j=1}^{q} x_j$ потенційних загроз; $L_k\{.\}$ – відповідний оператор дії інформаційної системи на вказану комбінацію вхідних потенційних загроз.

Сучасні інформаційні системи обробки інформації з обмеженим доступом є адаптованими до різних комбінацій потенційних загроз, тому їх функціонування можна описати певною послідовністю відповідних операторів дії у залежності від конкретної комбінації вхідних потенційних загроз. У більшості випадків математичні моделі потенційних загроз є випадковими, а послідовність (1.9) – детермінованим, інтегральним диференційним оператором. Тому методологія аналізу функціонування інформаційної системи є статистичною.

При створенні інформаційних систем обробки інформації з обмеженим доступом аналіз оперативних рівнянь (1.10) є певним станом, результати якого дають можливість сформулювати рекомендації забезпечення захисту інформації з подальшою їхньою реалізацією у конкретній інформаційній системі, на основі деталізації технічних характеристик розробки структури системи використання відповідної елементної бази, засобів обчислювальної техніки і т. ін.

Витрати на систему захисту інформації з обмеженим доступом в інформаційній системі від несанкціонованого доступу необхідно зіставляти і приводити у відповідність з цінністю інформації, що захищається та інших інформаційних ресурсів, що підлягають захисту, а також із збитками, що можуть бути завдані несанкціонованим доступом. Варто відзначити, що для досягнення поставленої мети несанкціонованих дій зловмисники використовують не одну, а деяку сукупність загроз. Зупинимось на основних етапах оцінки дій загроз в інформаційних системах обробки інформації, які мають чітку логічну послідовність у часі при вирішенні складних науково-технічних проблем, до яких належить і проблема захисту інформації в інформаційних системах.

1. Етап розробки фізичних і математичних моделей потенційних загроз і досліджуваних інформаційних систем. Методологія проведення етапу теоретичних досліджень базується на:

- обґрунтуванні і постановці завдань;
- виборі методів вирішення завдань;
- аналізі результатів теоретичних досліджень.

2. Етап імітаційних досліджень зводиться, як правило, до комп'ютерного моделювання. Останнє за своєю суттю є основним етапом аналізу функціонування інформаційної системи обробки інформації, при цьому моделюється та оцінюється дія загроз для всіх можливих підсистем захисту інформації. Методологія і результати моделювання визначають цінність сучасник новітніх інформаційних технологій, розробкою яких на сьогодні займаються дослідники і фахівці всіх розвинених країн світу.

3. Етап створення інформаційних систем є найтривалішим за часом й комплексним за своїм змістом.

4. На етапі налагодження, випробувань і введення в експлуатацію інформаційних систем є можливість формування бази знань функціонування розробленої системи з метою визначення її життєвого циклу на основі:

- розрахунків характеристик надійності;

- розробки методології регламентних і ремонтних робіт;

- створення відповідних баз даних вимірювань поточних характеристик і параметрів механізмів, пристроїв системи;

- методик прогнозу стану системи та інших.

Необхідно відмітити, що до завдань захисту інформації відносяться класичні завдання виявлення корисних сигналів при дії перешкод, завдання визначення їхніх характеристик, завдання розпізнавання. Як правило, для вирішення таких завдань використовуються статистичні методи Теогіі' випадкових процесів і математичної статистики. Найбільш обґрунтований підхід до аналізу функціонування інформаційної системи зводиться до аналізу такої структурної схеми (рис. 1.6).

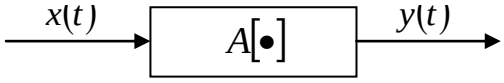


Рис. 1.6. Структурна схема еквівалентної системи

На рис. 1.6 x(t), t є T – вхідна дія; A[.] - оператор перетворення вхідної дії; y(t) – відгук оператора. На практиці, залежно від рівня деталізації, структурна схема аналізу досліджуваної системи (див. рис. 2.6) набуватиме вигляду (рис. 1.7).

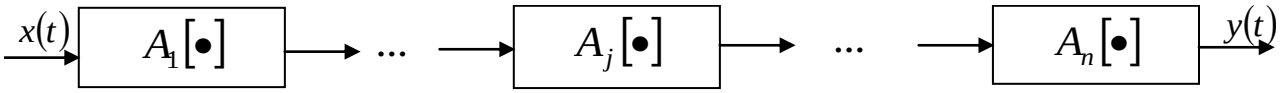


Рис 1.7 Структурна схема системи: практичний аспект

Таким чином, на практиці аналіз функціонування системи зводиться до аналізу перетворення вхідної дії x(t) складовим оператором

$$A[\cdot] = A_1[\cdot]\dots A_j[\cdot]\dots A_n[\cdot] = \prod_{j=1}^{n} A_j[\cdot] \tag{1.11}$$

У якості прикладу розглянемо лінійну систему з двох лінійних функцій, які описуються відповідними імпульсними перехідними функціями $\{\varphi_j(t), j = 1,2\}$ і мають постійні у часі параметри, тобто

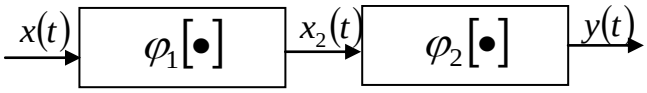


Рис 1.7 Структурна схема лінійної системи

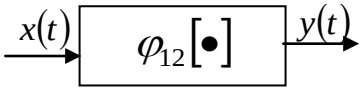


Рис 1.8. Структурна схема еквівалентної лінійної системи

Відповідні співвідношення опису відгуку лінійної системи мають такий вигляд

$$x_1(t) = \int_{-\infty}^{\infty} \varphi_1(t-\tau)x(\tau)d\tau,\ x_2(t) = \int_{-\infty}^{\infty} \varphi_2(t-\tau)x_1(\tau)dt = \int_{-\infty}^{\infty} \varphi_2(t-\tau)\int_{-\infty}^{\infty} \varphi(\tau-s)x(s)d\tau ds = \int_{-\infty}^{\infty} \varphi_{\Delta 2}(t-\tau)x(\tau)d\tau,$$

$$\varphi_{12}(t) = \int_{-\infty}^{\infty} \varphi_2(t-\tau)\varphi_1(\tau)d\tau$$

де , для n-модульної лінійної системи маємо

$$\varphi_{1\ldots n}(t) = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{t-\tau_1-\ldots-\tau_{n-3}|t-\tau_1-\ldots-\tau_n\ldots 2} \int \varphi_n(t-\tau_1-\ldots-\tau_{n-1})\varphi_{n-1}(\tau_{n-1})\ldots\varphi_1(\tau_1)d\tau_{n-1}\ldots d\tau_1$$

У більшості випадків оператор (1.11) складається з лінійних і нелінійних операторів відповідних модулів інформаційної системи.

Наведений приклад підтверджує факт використання класичних результатів теорії сигналів і систем для аналізу інформаційних систем обробки сигналів.

1.3. Особливості реалізації атак та заходи послаблення їх деструктивного впливу

Нині достеменно невідомо, скільки видів атак (сукупність узгоджених за метою, змістом і часом дій або заходів, так званих кіберакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації, а також порушення роботи його ІТС) та методів їх застосування з моменту виникнення цього поняття і до цього часу розробило людство. Комплексні статистичні дослідження з цього приводу до останнього часу не проводилися. Ф.Коен (F. Cohen), описуючи математичні основи вірусної технології, довів, що оскільки кількість злоякісних кодів, які є підмножиною множини кібератак, нескінченна, то й кількість самих атак, загальну структуру яких подано на рис. 1.10, є також нескінченна.

Сучасні кібератаки класифікують за такими ознаками:

1) за метою впливу на об’єкт атаки, що може бути спрямований, наприклад, на порушення цілісності (integrity) або конфіденційності (confidentiality) інформації, її захищеності від несанкціонованого доступу (authentication), а також забезпечення живучості (survivability) системи та надійності (availability) її функціонування. Закордонний і вітчизняний досвід показує, що вирішення цих завдань використовують методи криптографії в поєднанні з перевіреним і ліцензованим програмним забезпеченням (ПЗ), а також надійні інтелектуальні носії важливої інформації (матеріал ключа). При цьому саме живучості (здатності системи вчасно виконувати свої функції в умовах фізичного руйнування, часткової втрати ресурсів, відмов і збоїв елементів, несанкціонованого втручання в систему управління), яка визначає мобілізаційну готовність збройних сил, промисловості, економіки, народного господарства й суспільства в цілому як до ведення війни, так і до ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф, приділяють останнім часом найбільшу увагу;

2) за принципом впливу на об’єкт атаки:

- використання прихованих каналів (шляхів передачі інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки);

- використання прав суб’єкта системи (користувача, процесу) до об’єкта (файлів даних, каналів зв’язку тощо);

3) за характером впливу на об’єкт атаки:

- активний вплив (користувач виконує деякі дії, що виходять за рамки його обов’язків і порушують наявну політику безпеки, наприклад, розкриття пароля тощо);

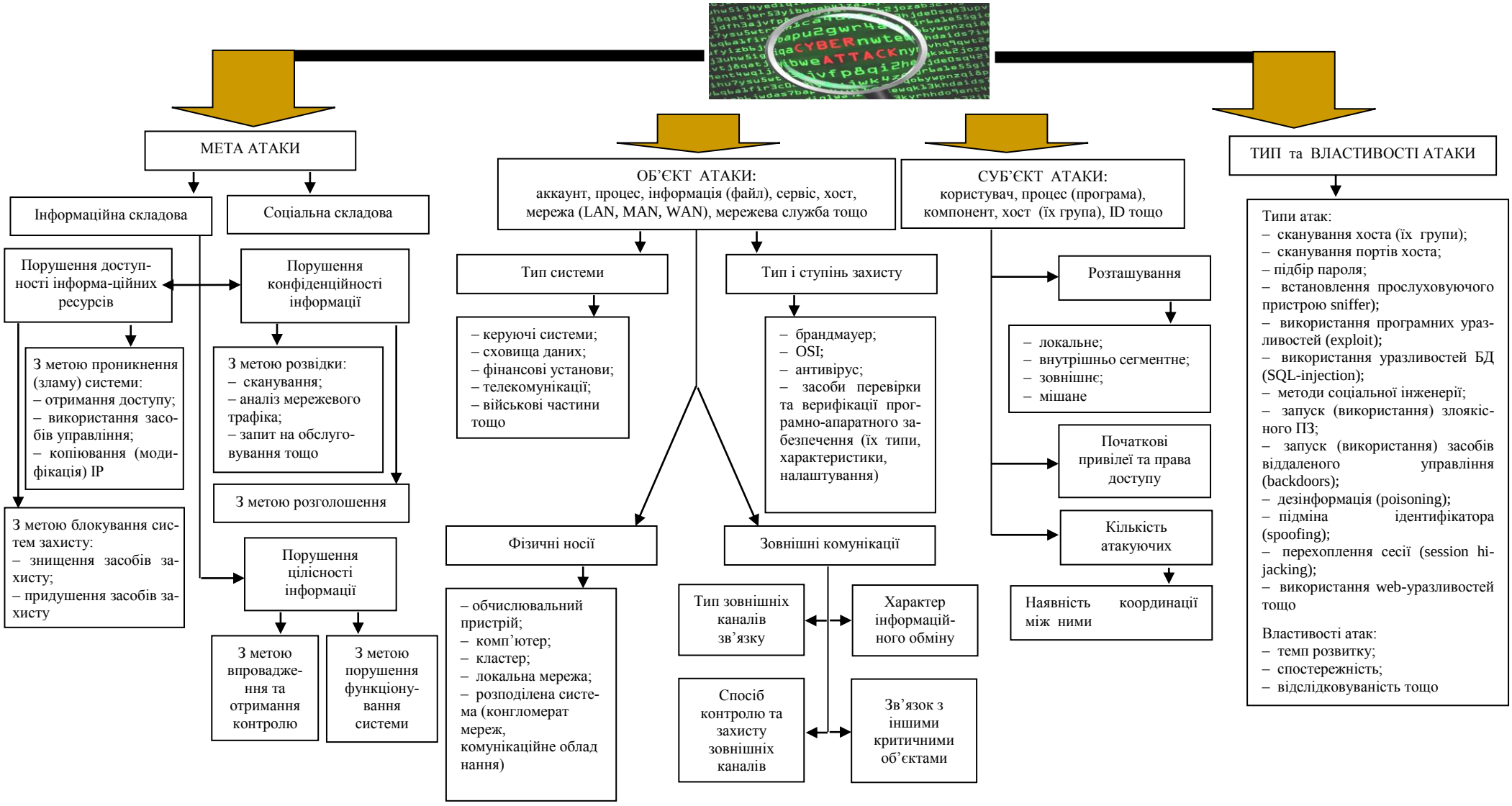


Рис. 1.10. Загальна структура кібератаки

- пасивний вплив (користувач прослуховує лінії зв'язку між двома вузлами мережі тощо);

4) за способом впливу на об'єкт атаки, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв;

5) за засобами впливу на об'єкт атаки, що передбачають використання або стандартного ПЗ, або спеціально розроблених програм;

6) за об'єктом атаки: напад може здійснюватися саме на систему в цілому; на дані і програми, що знаходяться на зовнішніх (дисководи, мережеві пристрої, термінали) або внутрішніх (оперативна пам'ять, процесор) пристроях системи, а також у каналах передачі даних; на процеси і підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях);

7) за станом об'єкта: безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися. Наприклад, у ході передавання інформації лініями зв'язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації шляхом перехоплення пакетів на ретрансляторі мережі, або ж прослуховування з використанням прихованих каналів;

8) за використовуваною системою захисту, за кількістю атакуючих, за джерелами атак, за розміщенням атакуючого об'єкта відносно до атакованого, за наявністю зв'язку з атакованим об'єктом, за рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив тощо. При цьому помилки системи захисту інформації (СЗІ) можуть бути зумовлені, наприклад, помилками адміністративного управління, помилками в алгоритмах програм, а також у зв'язках між ними, помилками кодування тощо.

Зважаючи на те, що нині переважну кількість кібератак на практиці не застосовують, більш життєздатною вважається класифікація, запропонована П.Нойманом, який пропонує сконцентрувати увагу на двадцяти шести основних типах таких дій (табл. 1.4), які можуть бути спрямованими проти ІТС спецпризначення. Найбільш розповсюдженими способами їх здійснення є mailbombing, sniffer пакетів та IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки типу Man-in-the-Middle та/або Side Channel Attack, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки, атаки з використанням мережевих черв'яків та так звані Ін'єкції.

Наприклад, mailbombing, як спосіб здійснення кібератаки, за розумінням П. Ноймана та інших фахівців полягає в бомбардуванні ПК протиборчої сторони електронною поштою. Сьогодні mailbombing практично не використовується. Сніфер пакетів – програма, яка використовує мережевий інтерфейс є у так званому нерозбірливому (promiscuous mode) режимі, перехоплює мережевий трафік, призначений для інших вузлів, та здійснює його подальший аналіз. Результати застосування дають можливість виявити паразитний, вірусний і закільцьований трафік; виявити в мережі шкідливе і несанкціоноване ПЗ (мережеві сканери, флудери, троянські програми тощо); перехопити будь-який, призначений для користувача, незашифрований, а деколи і зашифрований трафік з метою отримання паролів та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережевих агентів).

Таблиця 1.4

Основні типи кібератак відповідно до класифікації П.Ноймана

Тип атаки		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Омана операторів або користувачів
		Вилучення сміття	Вилучення інформації із сміттєвих корзин
Апаратні		Логічне відновлення	Вилучення інформації з викрадених носіїв
		Прослуховування	Перехоплення даних
		Втручання	
		Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
		Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні		Імітування	Використання хибних ідентифікаторів
		Узурпація ліній зв'язку або хостів	
		Атака з підміною параметрів	
		Заплутування мереж	Маскування фізичного місця розташування або маршруту
Злоякісні програмні коди		Троянські коні	Упровадження злоякісного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	
		Зламування паролів	
Зловживання	Активне	Інкрементальні атаки	Поступова ескалація привілей, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	Пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації

Для зниження загрози сніффінгу пакетів потрібно вживати таких заходів:

- застосовувати такі методи аутентифікації, як однократні паролі типу One-Time Passwords (OTP) та DTP. В інших випадках, наприклад, у разі перехоплення електронної пошти зазначені методи не ефективні;

- створити комутуючу інфраструктуру (у разі використання комутуючого Ethernet протоколу це дозволить хакерам отримати доступ лише до трафіка, що поступає на порт, до якого вони підключені);

- встановити антисніфери або ПЗ, що розпізнають сніфер пакетів, функціонуючий у визначеній мережі (антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік);

- створити систему криптозахисту. Це найбільш ефективний спосіб боротьби зі sniffer пакетів. Якщо канал зв'язку є криптографічно захищеним, то хакер перехоплює не повідомлення, а зашифрований текст.

IP-спуфінг (spoof –обман, містифікація, підроблення) – вид хакерської атаки (рис. 1.11) з якою використання чужої IP-адреси, тобто введення в оману системи безпеки або приховування реальної адреси атакуючого для того, щоб відправити/надіслати відповідний пакет на потрібну адресу чи атакованого (зловмисник, який перебуває всередині корпорації/установи або поза нею, видає себе за санкціонованого користувача).

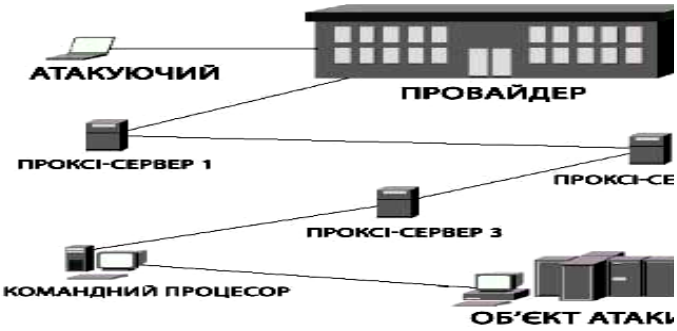


Рис. 1.11. Схема IP-спуфінгу

Часто використовується як складова частина комплексної атаки. Типовий приклад – DDoS атака, для здійснення якої хакер розміщує відповідну програму за чужою IP-адресою, щоб приховати власну.

Послабити загрозу IP-спуфінгу, а кібератаку зробити абсолютно неефективною можна завдяки:

- застосування фільтрації RFC 2827 (передбачає заборону будь-якого трафіка, вихідна адреса якого не є однією з IP-адрес певної установи);
- правильному настроюванню управління доступом (передбачає заборону будь-якого трафіка, що надходить із зовнішньої мережі з вихідною адресою, яка має перебувати всередині власної мережі);
- упровадженню додаткових заходів аутентифікації, а саме створенню системи криптографічного захисту.

Разом з тим слід зазначити, що на цей час розроблено велику кількість автоматизованих систем захисту, які взагалі роблять IP-спуфінг неефективним.

Відмова в обслуговуванні (Denial of Service – DoS) – атака на комп'ютерну систему з метою зробити комп'ютерні ресурси/мережу недоступними для користувачів внаслідок перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесор та зме-
ншення пропускної можливості каналу зв'язку (рис. 1.12).

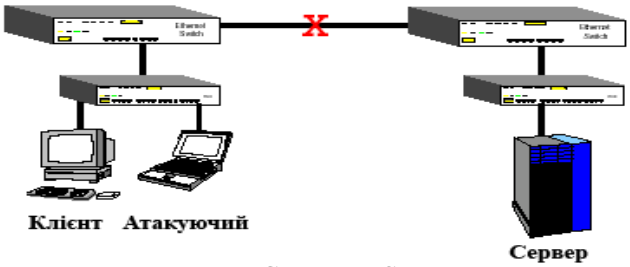


Рис. 1.12 Схема DoS атаки

Найвідомішими різновидами DoS атак є такі: Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity та багато інших. Серед них лише атаку TCP SYN flood, що полягає у надсиланні великої кількості запитів на ініціалізацію TCP-з'єднань з вузлом-мішенню, якому в результаті доводиться витрачати всі свої ресурси на те, щоб відстежувати ці частково відкриті з'єднання, – фахівці відзначають найбільш ефективною. Вона є найвідомішим способом переповнення інформаційного каналу SYN-пакетами, внаслідок якого сервер не відповідає на запити користувачів. Під час Flood ("затоплення") та ICMP flood (flood ping – "потік пінгів") атак на систему надсилається відповідно велика кількість ICMP

(найчастіше) або UDP-пакетів, які не несуть корисної інформації та так званих ехо-запитів ICMP (пінг системи). У результаті відбувається зменшення перепускної смуги каналу, незначне завантаження комп'ютерної системи аналізом "сміття", що надійшло, та генерацією на нього відповідей (довідково: ICMP-пакети не аналізуються системою за умовчанням, а відповіді на них не займають багато CPU-time). Атака Identification flood (запит ідентифікації системи) дуже схожа на ICMP flood. Відрізняється від неї тільки тим, що додатковою умовою її проведення є запит інформації про комп'ютерну систему (TCP порт 113). Зважаючи на те, що аналіз цих запитів і генерування на них відповідей потребують більше процесорного часу, ніж при пінгах, така атака вважається більш ефективною. Результатом атаки Ping Of Death є зависання ОС системи, включаючи мишу й клавіатуру. Це, як правило, є відповіддю системи на надходження сильно фрагментованого ICMP пакету великого обсягу (64Kb). На даний час майже не використовується. UDP flood (User Datagram Protocol) та TCP flood атаки полягають у відправленні на адресу системи-мішені безлічі пакетів UDP та TCP, що призводить до "зв'язування" мережевих ресурсів. На сьогодні вони вважаються найменш небезпечними. Це пояснюється їх легким виявленням зважаючи на застосування при обміні пакетами головного контролера й агентів нешифрованих протоколів TCP і UDP.

Загрозу DoS атак можна послабити у результаті:

- правильної конфігурації на маршрутизаторах і міжмережевих екранах функцій антиспуфінга (впровадження фільтрації RFC 2827) та функцій антиDoS;

- обмеження обсягу некритичного трафіка (non-critical traffic – визначає імовірність того, що мережа зв'язку відповідає заданому та узгодженому трафіку), що проходить мережею. Типовим прикладом такого є обмеження обсягів трафіка ICMP, що використовується тільки для діагностичних цілей.

Розподілена DDoS атака (Distributed Denial of Service) – це підтип DoS атаки, що здійснюється одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки та має за мету зробити мережу недоступною для звичайного використання (рис. 1.13). Для цього створюються так звані ботнети (інакше бот-мережі або зомбі-мережі) із групи заражених шкідливими програмами комп'ютерів, які одночасно надсилають запити до ресурсу, що атакується (рис. 1.14). У результаті сервер не справляється з навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливим. Вартість атаки з використанням ботнетів, що налічує 10–20 тисяч комп'ютерів, становить нині (у разі потреби "завалити", наприклад, портал новин) від 100–150 до 1000 доларів за добу. Збиток від такої атаки становить згідно з останніми даними приблизно 10 000 доларів за годину. Найбільш відомими різновидами DDoS атак є UDP flood, TCP flood, TCP SYN flood, Smurf та ICMP flood атаки. При цьому найнебезпечнішими є програми, що використовують одночасно кілька видів описаних атак, наприклад, TFN і TFN2K . Для створення програм у хакера має бути високий рівень підготовки. Однією з останніх програм для організації DDoS-атак є Stacheldracht, що дозволяє організовувати всілякі типи атак і лавини широкомовних ping-запитів із шифруванням обміну даними між контролерами й агентами. З погляду інформаційного захисту, DDoS-атаки є однією з найскладніших мережевих загроз, тому вживання ефективних заходів протидії є винятково складним завданням для організацій, діяльність яких залежить від Internet.

Основними методами протидії DDoS атакам є такі:

- профілактика причин, що спонукають тих або інших осіб організовувати DDoS атаки.

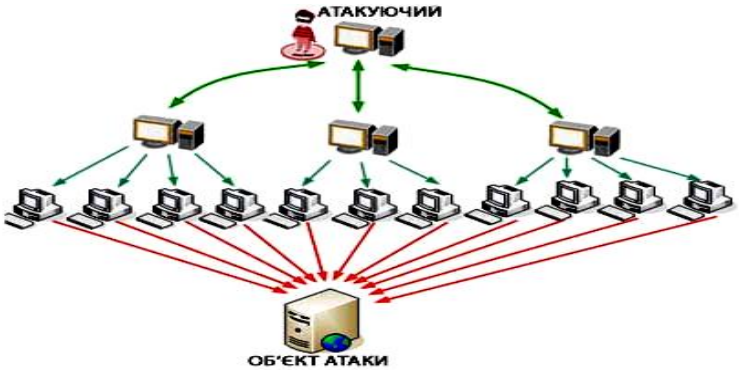


Рис. 1.13 Схема DDoS атаки

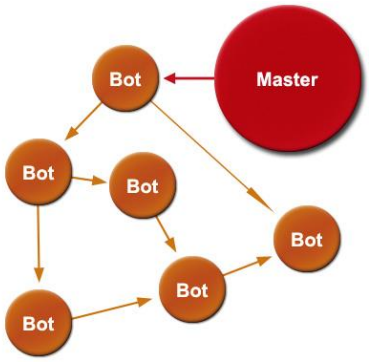


Рис. 1.14. Загальна схема організації бот-мережі

Дуже часто атаки є наслідками особистої образи або політичних, релігійних розбіжностей;

- розосередження або побудова розподілених і резервних систем, які не припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступними;

- фільтрація трафіка на маршрутизаторах (міжмережеві екрани та спеціалізовані antiflood засоби фільтрації – найбільш ефективний, але й найбільш дорогий метод. За можливості їх встановлюють якнайближче до джерела flood. Наприклад, програмний засіб ADoS, який є динамічним фільтром TCP-пакетів, здатний блокувати в реальному часі доступ до Web-сервера з IP-адрес, що генерують інтенсивний потік HTTP-запитів);

- розміщення (розташування) безпосередньої цілі атаки – доменного імені або IP-адреси - подалі від інших ресурсів, які часто піддаються впливу разом з безпосередньою ціллю;

- нарощування ресурсів системи (якщо flood спрямований на вичерпання ресурсів, то примітивнішим способом протидії цьому є нарощування власних ресурсів, щоб протиборча сторона не змогла їх вичерпати).

Сучасні засоби захисту від DDoS атак дають можливість з високим ступенем досить ефективності виявити атаку й зменшити або запобігти збитку ресурсам операторів і їхніх клієнтів. Нині, наприклад, компанія “NVisionGroup” пропонує комплексне рішення для захисту від DDoS атак на основі технології Cisco Clean Pipes, що забезпечує оперативну реакцію на DDoS атаки, легко масштабується, має високу надійність і швидкодію. Технологія Cisco Clean Pipes припускає використання модулів Cisco Anomaly Detector і Cisco Guard, а також різні системи статистичного аналізу мережевого трафіка, основані на даних, одержуваних з маршрутизаторів за протоколом Cisco Netflow. При цьому Anomaly Detector і системи статистичного аналізу трафіка виступають як системи виявлення DDoS атак, а Cisco Guard як засіб протидії вже виявленій атаці. У загальному випадку технологія Clean Pipes припускає наявність етапу тестування (навчання), що проводиться в період відсутності DDoS атак на ресурс, що захищається. На цьому етапі пристрої виявлення визначають і запам’ятовують, який трафік для ресурсу, що захищається, є нормальним. Ситуація, за якої поточний трафік на ресурс, що захищається, різко відрізняється від нормального, вважається DDoS-атакою. У разі DDoS-атаки система виявлення повідомляє оператору та активує підсистему захисту Cisco Guard. Найбільш великого значення боротьбі із DDoS атаками надано керівництвом Південної Кореї. Зокрема з метою запобігання масштабного виходу з ладу критично важливих IT ресурсів корейський національний центр з боротьби з кіберзагрозами (KrCERT)

створює так звані цифрові “бункери”, потужності яких планується надавати власникам корейських IT проектів, які потрапили під дію DDoS атаки. Але, зважаючи на те що хакери постійно використовують новітні технології та методи здійснення впливу на СІТС та їх складові, такі засоби захисту здатні лише частково захистити чи лише виявити атаку на об’єкт, що охороняється.

Для викрадення й подальшого передавання інформації третій стороні використовують програми-шпигуни або так звані кіберрозвідники. Їх поділяють на:

- сканери портів – збирають інформацію, що передається мережею, через відповідний принтерний, модемний або інший порт комп’ютера (найбільш відомою серед них є, наприклад, програма Neo Trace);

- клавіатурні та екранні шпигуни – збирають все, що вводиться у комп’ютер з клавіатури (програма Hook Dump) або ж, відповідно, копіюють зображення з монітора комп’ютера (програма Ghost spy);

- модемні та мережеві кіберрозвідники – автоматично записують телефонні розмови у режимі диктофона, програвання записів через телефонну лінію або через звукову карту з подальшим надсиланням записів електронною поштою (програми Modem spy, Flexispy, Mobile Spy й Mobistealth) або ж, відповідно, визначають версію ОС, встановленої на ПЕОМ, обсяг пам’яті та процесор, здійснюють моніторинг адрес електронної пошти, відстежують масиви інформації, передані всередині мережі, відвідувані сайти та інформацію з них, а також розділи, які викликають інтерес у користувачів.

На початку 2011 року компанія ESET опублікувала список найпоширеніших Internet-загроз, виявлених фахівцями її вірусної лабораторії за допомогою технології раннього виявлення ThreatSense.Net. Згідно нього лідером у російській двадцятці шкідливого ПЗ у першій декаді поточного року стало сімейство Win32/Spy.Ursnif.A з показником поширеності у 3,62 %, що на 0,07 % більше, ніж в останню декаду 2010 року. Згідно нього лідером у російській двадцятці шкідливого ПЗ у першій декаді поточного року стало сімейство Win32/Spy.Ursnif.A з показником поширеності у 3,62 %, що на 0,07 % більше, ніж в останню декаду 2010 року. Цей клас зловмисного ПЗ краде персональну інформацію й облікові записи із зараженого комп’ютера, після чого відправляє їх на вилучений сервер. Друге місце рейтингу належить загрозі INF/Autorun, частка проникнення якої знизилася на 0,87 % і склала 3,54 %. Цей тип шкідливих програм використовує для проникнення на комп’ютер користувача функцію автозапуску Windows Autorun і поширюється через змінні носії. На третє місце вийшли ПЗ, що провокують користувачів відправити SMS-повідомлення на певний номер для одержання нібито бажаного контента. Почесне місце у російській двадцятці займає шахрайська програма Win32/Packed.ZipMonster.A, що маскується під піратський контент у вигляді архіву. Окрім неї відзначається підвищена активність й інших програм, що увійшли в російський рейтинг найпоширеніших загроз: Win32/RegistryBooster (0,86 %), Win32/Hoax.ArchSMS.EP (0,77 %), Win32/HackKMS. A (0,76 %), Win32/Hoax. ArchSMS.ER (0,73 %). Рівень зростання присутності кожної з цих загроз склав близько 0,1 %. Десяте місце займає загроза PDF/Exploit.Pidief.PDS.Gen з показником в 1,00 %. У той же час, залишаються популярними шкідливі експлойти для платформи Java. Так, наприклад, шкідливе ПЗ Java/Exploit.CVE-2010-0094 C, що експлуатує уразливість CVE-2010-0094, дотепер є присутнім у рейтингу із часткою поширення в 0,6 %. Що стосується десяти найпоширеніших загроз у світі, то в рейтингу першої декади 2011 року перше місце знову ж таки належить черв’яку Win32/Conficker з відсотком проникнення в 5,38 %, що ненабагато випереджає попереднього лідера – сімейство шкідливих програм INF/Autorun (5,30 %). Третє місце світової десятки займає загроза Win32/PSW.OnLineGames, що використовується хакерами для крадіжки аккаунтів гравців

багато користувальницьких ігор, з показником поширеності у 2,17 %. У цілому ж світовий рейтинг найпоширеніших Internet-загроз нині включає: Win32/Conficker – 5,38 %; INF/Autorun – 5,30 %; Win32/PSW. OnLineGames – 2,17 %; Win32/Sality – 1,82 %; INF/Conficker – 1,39 %; Win32/Bflient.K – 1,19 %; Win32/Tifaut.C – 1,09 %; HTML/ScrIngect.B – 0,84 %; Win32/Spy.Ursnif.A – 0,83 %; Java/TrojanDownloader.Agent.NCA – 0,76 %.

Беручи до уваги те, що сучасні ІС є системами відкритого типу, майже всі з розглянутих методів і способів їх реалізації досягають очікуваного результату. Цьому не в останню чергу сприяє:

- складність організації захисту міжмережевої взаємодії;
- наявність помилок у загальному та спеціальному ПЗ, ОС та утилітах, що відкрито розповсюджуються мережею;
- неправильне чи помилкове адміністрування систем;
- відсутність адекватного захисту даних у більшості з сучасних мережевих протоколів;
- наявність помилок у конфігурації систем і засобів забезпечення безпеки, “економія” або взагалі повне ігнорування необхідності їх впровадження тощо.

Виходячи з цього, можна стверджувати, що позбутися деструктивного впливу кібератак нині практично неможливо. Тим не менш, запропоновано певні загальні шляхи для послаблення їх негативних наслідків. Вони ґрунтуються передусім на вивченні слабких місць прикладних програм за даними корпорацій Bugtrad (http://www.securityfocus.com) і CERT (http://www.cert.com); застосуванні крім системного адміністрування систем розпізнавання атак (IDS технологій) додаткового ПЗ, що дасть можливість відстежувати всі пакети, які проходять через визначений мережевий інтерфейс; проведенні аналізу спеціальних аналітичних додатків із застосуванням лог-файлів операційних систем та мережевих лог-файлів; застосуванні евристичних механізмів захисту, антивірусних програм та персонального Firewall тощо.

1.4. Система показників уразливості інформації і вимоги до первинних даних

Для системної оцінки уразливості інформації необхідна система показників, яка б відбивала усі вимоги захисту інформації, а також технологію та умови функціонування інформації у процесі:

- розробки ІС (обумовлюється уразливістю утворюваних компонентів систем і утворюваних баз даних);
- автоматизованого опрацювання інформації (характеризуєься складом підлягаючих захисту об’єктів і елементів; наявністю і кількістю ППЦІ і КНОІ; кількістю і категоріями осіб, що можуть бути потенційними порушниками статусу інформації; режимами автоматизованого опрацювання інформації);
- функціонування системи незалежно від опрацювання інформації (обумовлюється тим, що сучасні системи являють собою організаційну структуру з високою концентрацією інформації, що може бути об’єктом випадкових або злочинних впливів навіть у тих випадках, якщо автоматизоване опрацювання її не здійснюється).

За кількісну міру оцінки уразливості інформації доцільно прийняти можливість порушення її цілісності або можливість несанкціонованого одержання інформації при існуючих умовах її збору, передавання, обробки і збереження. Основними параметрами, що визначають можливість порушення цілісності інформації, є:

- кількість і типи тих структурних компонентів, в яких оцінюється уразливість інформації;
- кількість і типи ППЦІ, відносно яких оцінюється уразливість;

- види інформації, уразливість яких оцінюється.

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

- кількість і типи структурних компонентів, в яких оцінюється уразливість;
- кількість і типи КНОІ, відносно яких оцінюється уразливість;
- число і типи потенційних порушників, що намагаються порушити уразливість інформації.

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

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

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

- дуже малі – інтервали, що можна вважати точками;
- малі – інтервали, що не можна зводити до точки;
- середні – інтервали, що не можна вважати малими, але на котрих заздалегідь можна встановити стан кожного структурного елемента на кожному його малому інтервалі;
- великі – інтервали, для яких не може бути виконана умова середніх інтервалів, але на яких із достатньою точністю все ж можна спрогнозувати послідовність і зміст функціонування основних компонентів;
- дуже великі – інтервали, для яких не представляється можливим виконати умову великих інтервалів.

Відзначимо, що параметри інтервалів істотно залежать від параметрів інформації і конкретних умов її функціонування. Відповідно до викладеного, загальна класифікація й ідентифікація системи показників інформації зведена в табл. 1.5.

Таблиця 1.5

Ідентифікація показників уразливості інформації

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

1.5. Аналіз організації функціонування автоматизованої системи

Відповідно до НД ТЗІ 3.7-001-99 рекомендується відзначати такі моменти, які впливають на безпеку інформації під час її оброблення в АС:

- загальну структурну схему і склад ОС АС (перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо);

- технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);

- характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);

- характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);

- характеристики фізичного середовища (наявність категорованих приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т. ін.);

- загальну технічну характеристику АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.);

- особливості функціонування АС (надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо);

- особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.);

- потенційні загрози інформації (способи здійснення НСД, можливі технічні канали витоку інформації і умови їх формування, стихійні лиха і т. ін.), а також можливі наслідки їх реалізації;

- клас АС згідно з НД ТЗІ 2.5-005-99;

- опис функціонуючих в складі АС (для існуючої АС) засобів захисту, а також засобів захисту, реалізовані в компонентах, які планується використовувати для побудови АС.

З точки зору створення систем захисту сучасних АС в першу чергу важливим є аналіз їх обчислювальних середовищ (складу та організації апаратного та програмного забезпечення, технологій оброблення інформації).

Аналіз складу апаратного та програмного забезпечення

Визначення:

- складу та основних характеристик ПЕОМ, в тому числі типу апаратної платформи; системного, прикладного та спеціального програмного забезпечення; функціонального призначення; наявності підключення до мережі та якої;

- складу та основних характеристик серверів, в тому числі типу апаратної платформи; системного, прикладного та спеціального програмного забезпечення; функціонального призначення; до яких мереж підключені;

- складу та основних характеристик спеціалізованих засобів (наприклад, спеціалізованих ЕОМ), в тому числі типу; програмного забезпечення; функціонального призначення; наявності підключення до мєрєжі та якої;

- складу та основних характеристик засобів вводу та виводу даних (принтерів, сканерів та ін.), в тому числі їх продуктивності, місць підключення.

Аналіз обчислювальної мережі Визначення:

- складу та основних характеристик активного мережного обладнання, в тому числі типу обладнання; системного програмного забезпечення; функціонального призначення;

- структури мережі та її основних характеристик (тип каналів, наявність резервних каналів, дублюючих каналів та ін.);

- логічної організації мережі (визначення підмереж, основних правил маршрутизації та ін.);

- наявності та характеристик шляхів взаємодії з іншими системами.

Аналіз технологій оброблення формації

Визначення:

- режимів функціонування автоматизованої системи;

- типів цінної інформації, що обробляється в автоматизованій системі;

- основних технологій оброблення інформації для кожного режиму;

- місць накопичення інформації для кожної технології її оброблення (обсяги, ступінь цінності);

- основних інформаційних потоків для кожної технології оброблення інформації, та їх характеристик (ступінь цінності, обсяги даних, що передаються, протоколи, та ін).

Аналіз складу та характеристик існуючої системи захисту

Визначення:

- організації системи захисту та її завдань;

- складу та характеристик засобів захисту (НСД, криптографічних), їх розташування в автоматизованій системі;

- наявності та організації системи управління ключами;

- реалізованих організаційних заходів щодо управлшня системою захисту та їх документального оформлення.

Порядок проведення робіт з обстеження АС

Як звісно, основним призначенням об’єктів інформаційної діяльності (ОІД) є найбільш повне задоволення інформаційних потреб посадових осіб органів управління в цілях підвищення оперативності, обґрунтованості та якості рішень, що ними приймаються у різних сферах діяльності. Інформація з обмеженим доступом (ІзОД) в процесі інформаційної діяльності цих

об’єктів може зазнавати впливу загроз її безпеці, у результаті чого може відбутися її витік або порушення цілісності.

Зміст та послідовність робіт з протидії цим загрозам або їхньої нейтралізації повинні відповідати етапам функціонування систем захисту інформації і як показано у ДСТУ 3396.1 полягає в:

- проведенні обстеження ОІД;
- розробці та реалізації в них організаційних і технічних заходів захисту інформації;
- прийманні робіт з технічного захисту інформації;
- проведенні атестації засобів забезпечення інформаційної діяльності.

Метою обстеження ОІД є вивчення їх інформаційної діяльності, визначення об`єктів захисту, виявлення загроз, їхній аналіз та побудова окремих моделей загроз.

Для проведення обстеження ОІД призначається комісія до складу якої включаються відповідальні особи за забезпечення безпеки інформації та начальники служб матеріально-технічного забезпечення. Також до проведення обстеження можуть бути залучені представники організації–розробника комплексних систем захисту інформації (КСЗІ).

Послідовність проведення робіт з обстеження здійснюється у відповідності з ДСТУ 3396.1 та у загальному випадку включає:

- аналіз умов функціонування ОІД, його розташування на місцевості (складання ситуаційного плану, план-схеми ОІД та їх опис);
- характеристика приміщень (генеральні плани поверхів будівлі, на яких розташовано ОІД);
- визначення складу, схеми розташування основних технічних засобів (ОТЗ) на ОІД та їх опис;
- визначення складу, схеми розташування додаткових технічних засобів та систем (ДТЗС) на ОІД та їх опис;
- виявлення незадіяних та транзитних електропровідних кабелів, дротів, ланцюгів та інженерних комунікацій, що проходять через виділені приміщення;
- визначення наявності на ОІД систем захисту інформації. Надання пропозицій щодо застосування додаткових заходів захисту;
- перевірку наявності нормативних документів, які забезпечують функціонування системи захисту інформації;

Аналіз умов функціонування ОІД, його розташування на місцевості

Інформація з обмеженим доступом може бути отримана за допомогою засобів космічної, повітряної, морської та наземної розвідок такими технічними каналами:

- вібро-акустичним, лазерно-акустичним (випромінювання звукового та ультразвукового діапазонів частот);
- радіо-, радіотехнічним (електромагнітні випромінювання в діапазоні радіочастот);
- побічних електромагнітних випромінювань і наводок (електромагнітні випромінювання, що утворюються під час роботи засобів забезпечення інформаційної діяльності під впливом електричних і магнітних полів на випадкові антени у процесі акусто-електричних перетворень, під час виникнення паразитної високочастотної генерації та паразитної модуляції);
- оптичним (електромагнітні випромінювання інфрачервоного, видимого та ультрафіолетового діапазонів частот);
- хімічним (хімічні речовини різної природи, що використовуються як сировина, утворюються в нових технологічних процесах, під час розроблення нових матеріалів, проведення випробувань спеціальної техніки та виробів і містяться у навколишньому середовищі);
- іншими (радіаційним, магнітометричним тощо).

На території України розвідка технічними засобами може проводитися із будинків представництв окремих іноземних держав, місць тимчасового перебування їх представництв, офісів спільних підприємств, а також за допомогою таємно установленої в районі розташування ОІД автоматичної розвідувальної апаратури.

Базові моделі та методи системного аналізу

Невід'ємною складовою системного аналізу є моделювання — процесс дослідження реальної системи, побудова її моделі, дослідження її властивостей, та перенесення отриманих відомостей на систему, що моделюється.

Модель — об'єкт, який має схожість с прототипом и є засобом опису, пояснення, прогнозування його поведінки.

Для адекватного опису складних систем використовують функціональні, інформаційні, поведінкові моделі.

Функціональна модель описує сукупність функцій, що виконуються системою, характеризує морфологію (побудову) системи - склад функціональних підсистем та їх взаємозв'язки.

Інформаційна модель описує відносини між елементами системи в вигляді структур даних (склад та взаємозв'язки).

Поведінкова модель описує інформаційні процеси (динаміку функціонування), та оперує такими поняттями, як стан системи, події, перехід із одного стану в інший, умови переходу, послідовність подій.

Ситуаційний план ОІД

Ситуаційний план підписується відповідальною за технічний захист інформації (ТЗІ) посадовою особою та затверджується керівником.

На плані повинна бути відображена наступна інформація:

- контури будівлі, в якій знаходиться ОІД;
- межі контрольованої зони (КЗ) та відстані від контурів ОІД до меж КЗ;
- контури оточуючих будинків, споруд, місця можливої стоянки автотранспорту, з яких може вестися технічна розвідка (ТР), та відстані до них;
- місця розташування іноземних дипломатичних представництв, установ іноземних держав, місій та відстані до них;
- можливі місця розміщення стаціонарних засобів ТР та знаходження мобільних та переносних засобів ТР;
- напрямок на північ.

В описі ситуаційного плану повинна міститися наступна інформація:

- місце розташування приміщень, в яких знаходиться ОІД (адреса, кількість поверхів будівлі, в якій знаходиться об'єкт, на якому поверсі розміщується, номери приміщень);
- відомості про технічні засоби охорони, перепускний режим, сигналізацію та контроль за переміщенням автотранспорту та осіб в межах КЗ;
- відомості щодо оточення ОІД (будинки, будівлі і споруди, що знаходяться поруч з будівлею, де розташована ОІД);
- адреси іноземних дипломатичних представництв, установ іноземних держав, які показані на ситуаційному плані.

У разі знаходження іноземних дипломатичних представництв поблизу ОІД (до 200 м - в умовах промислового міста та до 500 м - в інших випадках), комісія з категорування повинна розглянути можливість використання стаціонарних засобів ТР і може прийняти рішення про підвищення категорії, що повинна бути встановлена для даного ОІД, на одну ступінь.

План-схема контрольованої території ОІД

Під терміном „контрольована територія" розуміється територія, на якій виключено неконтрольоване перебування осіб та транспортних засобів.

План-схема контрольованої території ОІД повинна бути підписана відповідальною за ТЗІ посадовою особою та затверджена керівником, у веденні якого знаходиться ОІД.

На план-схемі КТ повинна бути відображена наступна інформація:

- контури будівлі, в якій знаходиться ОІД та місце розташування ОІД;
- огорожа навколо будівлі;
- межі КТ та відстані від контурів ОІД до меж КЗ;

- місце розташування та назви вулиць, що знаходяться поруч з ОІД, відстані від ОІД до вказаних вулиць.

В описі план-схеми контрольованої території повинна міститися наступна інформація:

- найменша відстань від ОІД до меж КТ;
- висота огорожі навколо будівлі, в якій знаходиться ОІД, наявність периметрової системи сигналізації, системи відеоспостереження;
- основні характеристики вулиць, що знаходяться поруч з ОІД (ширина частини для проїзду та пішохідної частини, інтенсивність руху автотранспорту, наявність місць неконтрольованого перебування автотранспорту);
- назви вулиць, в бік яких виходять вікна приміщень, в яких розташовано ОІД.

Генеральні плани поверхів будівлі, на яких розташовано ОІД

В додатках до акту обстеження ОІД необхідно привести генеральні плани поверхів будівлі, на яких територіально розташовано ОІД.

В планах показуються розміри виділених та суміжних з ними приміщень, вказується тип будівельних матеріалів, з яких виконані стіни, стелі, підлога, вікна і двері приміщень ОІД, товщина зовнішніх та внутрішніх стін приміщення, висота стелі.

Надається опис суміжних приміщень, які знаходяться з боків, над та під ОІД (призначення приміщень за характером робіт, які в них проводяться), описуються приміщення, де працюють або можливе неконтрольоване перебування іноземних громадян, інших сторонніх осіб (призначення приміщень за характером робіт, які в них проводяться).

ОТЗ, схеми розташування на ОІД, та їх опис

До основних технічних засобів відносяться наступні технічні засоби, які застосовуються для оброблення інформації з обмеженим доступом:

- інформаційно-телекомунікаційні системи, які призначені для формування, пересилання, приймання, перетворення, відображення та зберігання інформації;
- засоби і системи зв`язку;
- засоби і системи звукопідсилення, звукозапису та звуковідтворення;
- пристрої, що утворюють дискретні канали зв`язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна тощо.

ОТЗ можуть бути захищеними і незахищеними.

Канали витоку інформації можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів на ДТЗС у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території.

Рівень наводок визначається відстанню між ОТЗ та ДТЗС, що підпадають під вплив випромінювань ОТЗ, довжиною паралельного пробігу і величиною перехідного затухання ліній, напругою інформативного сигналу в лінії та рівнем шумів (завад).

При проведенні обстеження ОІД необхідно скласти перелік ОТЗ, які знаходяться на ОІД (найменування, тип, заводський номер) та кабелів, що використовуються під час монтажу обладнання.

Необхідно перевірити, що:

- склад ОТЗ відповідає формулярам, всі ОТЗ пройшли спеціальне дослідження на наявність технічних каналів витоку інформації, доопрацьовані та мають приписи на експлуатацію для обробки ІзОД;
- всі ОТЗ, що є у наявності, допущені до обробки ІзОД відповідно до присвоєних категорій;
- ОТЗ іноземного виробництва, що знаходяться на ОІД, пройшли спеціальне дослідження на наявність можливого впровадження радіозакладних пристроїв знімання інформації та мають висновок про можливість їх використання для обробки ІзОД.

Зовнішнім оглядом ОТЗ та виділених приміщень необхідно перевірити наступні питання:

- розміщення та монтаж ОТЗ відповідають вимогам приписів на експлуатацію;

- рознесення між елементами ОТЗ, їх кабельними лініями та ДТЗС відповідає приписам щодо експлуатації ОТЗ;

- усі металеві конструкції ОТЗ (шафи, пульти, корпуси розподільних пристроїв та металеві оболонки кабелів) повинні бути заземлені;

- зайвих дротів та кабелів разом з інформаційними кабелями ОТЗ не прокладено;

- відсутність пошкоджень екранів корпусів, оболонок кабелів та їх з'єднувальних конструкцій із шинами заземлення;

- справність печаток та пломб на ОТЗ та ДТЗС.

ДТЗС, схеми розташування на ОІД, та опис схем

ДТЗС - засоби та системи, що розміщені спільно з ОТЗ або в службових приміщеннях, де циркулює ІОД.

До ДТЗС відносяться:

- засоби і системи спеціальної охоронної та пожежної сигналізації;

- телефонна мережа;

- засоби і системи освітлення, побутового електроживлення та електрообладнання;

- електронна та електрична оргтехніка;

- система заземлення;

- системи опалення, водопостачання та каналізації;

- система автоматизації, контрольно-вимірювальна апаратура;

- засоби і системи кондиціонування;

- засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення;

- засоби і системи годинофікації.

ДТЗС можуть бути захищеними і незахищеними.

При проведенні обстеження ОІД необхідно скласти перелік ДТЗС, які знаходяться на ОІД (найменування, тип, заводський номер) та кабелів, що використовуються під час монтажу обладнання. Привести схеми та надати опис допоміжних систем.

Визначити склад кабельних ліній та комунікацій ДТЗС, будівельні та інженерні конструкції та інші комунікації, які виходять за межі контрольованої території і мають паралельний пробіг з комунікаціями ОТЗ.

Показати на відповідних схемах місця виходу зазначених комунікацій за межі контрольованої території. Місця та відстані взаємного паралельного пробігу між комунікаціями ОТЗ та ДТЗС, які виходять за межі контрольованої території.

На заключному етапі проведення обстеження необхідно визначити на ОІД допоміжні технічні засоби і системи, застосування яких не передбачено службовою та виробничою необхідністю, скласти їх перелік та визначити ДТЗС, які необхідно демонтувати в інтересах забезпечення технічного захисту інформації.

Система електроживлення

До систем електроживлення відносяться трансформаторні підстанції, автономні джерела, засоби захисту, кабелі та інші засоби.

В описі до системи електроживлення вказати, як здійснюється електроживлення ОТЗ, місцезнаходження трансформаторної підстанції, наявність сторонніх споживачів з низьковольтного боку трансформаторної підстанції, схему підключення до трансформаторної підстанції.

На схемі силових кабельних ліній будівлі, в якій розміщено ОІД, показати місця проходження силової кабельної лінії, тип кабелю, місця розташування розподільних щитів.

Система заземлення

В описі до схеми заземлення вказати тип системи заземлення, матеріали, з якого вона виконана, за якою схемою виконана система заземлення („розгалужене дерево", „радіальна схема" або інше) та величину опору заземлення.

Перевірити, що система заземлення не має виходу за межі КЗ, розміщується на відстані не менше 10-15 м. від неї та не має гальванічного контакту з підземними комунікаціями, що виходять за межі КЗ.

Система телефонного зв'язку

При проведенні обстеження ОІД необхідно розглянути та надати опис системи телефонного зв'язку (внутрішнього без виходу на міські АТС та міського з виходом на АТС).

В описах до схем вказати тип телефонних апаратів, до яких телефонних мереж підключені, тип кабелів зв'язку.

Перевірити, що для телефонного зв`язку, не призначеного для пересилання ІзОД, застосовуються апарати вітчизняного виробництва сумісні з пристроями захисту. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку про їх сумісність з пристроями захисту.

На схемі телефонної мережі показати місця проходження кабелів зв'язку, місця розташування телефонних апаратів, захисних пристроїв, розподільчих (комутаційних) елементів, відстані від стін виділених приміщень, висоту, на яких прокладені кабелі зв'язку, місця виходу ліній зв'язку за межі КЗ.

Системи охоронної і пожежної сигналізації

В описах до схем вказати тип сповіщувачів охоронної і пожежної сигналізацій, тип шлейфів зв'язку з пультом-концентратором.

На схемах охоронної і пожежної сигналізацій показати місця проходження шлейфів, відстані від стін виділених приміщень, висоту, на яких прокладені, місце розташування пульта-концентратора. Якщо системи охоронної і пожежної сигналізацій виходять за межі КЗ, показати місця проходження за межами КЗ.

Системи опалення, водопостачання та каналізації

В описах до схем вказати тип систем опалення, водопостачання та каналізації будівлі, в якій розміщено ОІД.

На схемах показати місця проходження комунікацій, відстані від них до стін виділених приміщень, місця виходу за межі КЗ.

На схемі опалення додатково показати місця розташування стояків опалення, напрями подачі теплоносія у систему опалення, тип радіаторів, які знаходяться у виділених приміщеннях, їх розмірі, кількість секцій в радіаторах.

Виявлення незадіяних та транзитних електропровідних кабелів, кіл, дротів

Зовнішнім оглядом виділених приміщень визначити та скласти перелік транзитних та незадіяних (повітряних, настінних, зовнішніх та закладених в каналізацію) електропровідних кабелів, кіл, проводів та інших інженерних комунікацій, які проходять транзитом через виділені приміщення.

З переліку транзитних та незадіяних комунікацій визначити комунікації, застосування яких не обґрунтовано службовою та виробничою необхідністю та які необхідно демонтувати в інтересах забезпечення безпеки ІзОД.

За необхідності, показати незадіяні та транзитні комунікації на схемах приміщень ОІД (генеральних планах приміщення, в якому знаходиться ОІД), вказати висоту, на якій прокладені, та відстані до стін приміщень.

Визначення наявності на ОІД діючих засобів та систем технічного захисту інформації

Спеціальний захист ОТЗ (ДТЗС) є складовою частиною системи заходів з комплексної протидії ТР. Вона забезпечується своєчасним виконанням на ОІД комплексу організаційних та технічних заходів щодо усунення можливих каналів витоку інформації.

До технічних відносяться заходи, призначені для закриття можливих каналів витоку інформації шляхом встановлення захищених ДТЗС або засобів захисту в ОТЗ (ДТЗС).

До засобів технічного захисту відносяться:

- фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;

- фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;

- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;

- генератори лінійного зашумлення;

- генератори просторового зашумлення;

- екрановані камери спеціальної розробки.

До засобів активного спецзахисту відносяться спеціальні пристрої та системи, призначені для електромагнітного зашумлення та акустичного маскування. Вони застосовуються в тих випадках, коли засоби пасивного захисту (фільтри, екрани, діелектричні вставки) не забезпечують попередження витоку інформації.

Перевірка наявності нормативних документів системи ТЗІ

Система документів із забезпечення функціонування системи захисту інформації включає наступні документи:

- закони України із захисту інформації;

- нормативно-правові акти, затверджені Указами Президента України та постановами Кабінету Міністрів України;

- нормативні документи, затверджені ДССЗІ України;

- державні стандарти та інші нормативні документи, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ;

- відомчі нормативні документи, що містять вимоги з захисту інформації в ІТС;

- нормативні, організаційно-розпорядчі та інші документи, чинні у межах організації.

Під час проведення обстеження із приведених переліків необхідно визначити документи, які відсутні і які необхідно придбати для забезпечення всього комплексу робіт з ТЗІ.

1.6. Модель загроз інформації в РКМ

Для того, щоб профіль безпеки міг бути ефективно розроблений і застосований, у процесі його розробки здійснюється виявлення всіх загроз безпеки у відношенні до РКМ , для яких розробляється профіль. У процесі дослідження будуються моделі загроз.

Модель загрози - це формальний чи неформальний опис:

- життєвого циклу загрози;
- спрямованості загрози;
- джерела загрози;
- ресурси РКМ , що вразливі до загроз;
- середовища виробу РКМ;
- ресурси, що вимагають захисту;
- методів, способів і алгоритмів реалізації загрози;
- небажаних подій;
- аналізу ризиків і ряду інших аспектів.

У процесі опису моделі загроз багато спільного з проведенням аналізу ризиків. Так при описі моделі загроз, джерелом яких є навмисна діяльність людини, оцінюється тип джерела за рівнем практичних навичок реалізації загрози (шкала - "низький", "середній", "високий", "невизначений"), і шанси реалізації загрози (шкала - "малоймовірно", "ймовірно", "велика імовірність", "не визначена").

У розгляд вводиться поняття "потенціал нападу". Під цим терміном розуміється прогнозований потенціал для успішного, у випадку реалізації, нападу, виражений у показниках компетентності, ресурсів і мотивації порушника. Існує три рівні потенціалу нападу: низький, помірний і високий.

Загрозою вважається об'єкт або подія, яка, у разі реалізації, може потенційно бути причиною нанесення шкоди інформації, програмним або технічним засобам РКМ .

Вразливими місцями є слабкі місця захисту інформації в РКМ, які можуть використовуватися загрозою для своєї реалізації.

Інформація в РКМ існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. Далі терміни «інформація» і «дані» використовуються як синоніми.

Уся безліч потенційних загроз по природі їхнього виникнення розділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні).

Природні загрози - це загрози, викликані впливами на РКМ (її елементи) об'єктивних фізичних процесів (стихійних природних явищ), що не залежать від людини.

Штучні загрози - це загрози РКМ , які викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна зазначити:

- ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проектуванні РКМ і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.ін.;
- навмисні (навмисні) загрози, зв'язані з корисливими устремліннями людей (зловмисників).

Загальний вигляд моделі загроз інформації

У самому загальному виді модель загроз інформації в РКМ може бути представлена так, як це показано на рис 1.15.

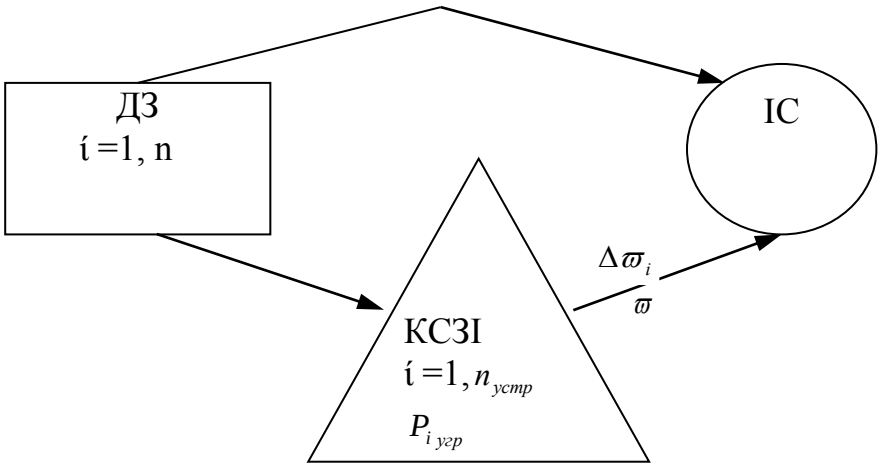


Рис. 1.15. Загальна модель загроз інформації

Зловмисник за допомогою деякого джерела загроз (ДЗ) генерує сукупність загроз РКМ (шлях її буде кінцевим і рахунковим; $i=1,\overline{n}$). Кожна í-а загроза характеризується імовірністю появи $P_{i\,угр}$ і збитком $\Delta q_i^{угр}$, принесеним інформаційній системі. Система захисту інформації (КСЗІ) виконує функцію повної чи часткової компенсації загроз для РКМ . Основною характеристикою засобів захисту є імовірності усунення кожної í-ї загрози $P_{i\,угр}^{устр}$.

За рахунок функціонування КСЗІ забезпечується зменшення збитку W, що здійснюється РКМ впливом загроз. Позначимо загальний відвернений збиток РКМ через $\overline{W}$, а відвернений збиток за рахунок ліквідації впливу і-ї загрози через $\overline{\omega}_i$.

Після введених позначень сформулюємо в загальному виді задачу синтезу засобів захисту інформації в РКМ: необхідно вибрати варіант реалізації КСЗІ, що забезпечує максимум відверненого збитку від впливу загроз при припустимих витратах на КСЗІ.

Формальна постановка задачі має вид:

$$\mathbf{T}^{o} = \omega q \max \overline{W}(\mathbf{T})$$

знайти $$\mathbf{T}^{o} \in \mathbf{T}^{+} \qquad (1.12)$$

при обмеженні $C(\mathrm{T}^0) \le C\partial on$. (1.13)

Де Т- деякий вектор, що характеризує варіант технічної реалізації КСЗІ; T^+T^0 - припустиме й оптимальне значення вектора Т;

Сдоп.- припустимі витрати на КСЗІ.

Для рішення задачі необхідно насамперед сформувати показник якості функціонування КСЗІ $\overline{W}$ (Т).

Очевидно, відвернений збиток у загальному виді виражається співвідношенням:

$$\overline{W} = F(P_{i\,угр}; \Delta q_i^{\,угр}; \mathrm{P}_{i\,угр}^{\,устр}; i = \overline{1,n}). \quad (1.14)$$

Відвернений збиток за рахунок ліквідації впливу і-ї загрози

$$\overline{\omega_i} = \mathrm{P}_{i\,угр} \bullet \Delta q_i^{\,угр} \bullet \mathrm{P}_{i\,угр}^{\,устр}; i = \overline{1,n}. \quad (1.15)$$

За умови незалежності загроз і адитивності їхніх наслідків одержуємо

$$\overline{W} = \sum_{i=1}^{n} \mathrm{P}_{i\,угр} \bullet \Delta q_i^{\,угр} \bullet \mathrm{P}_{i\,угр}^{\,устр}$$

Зупинимося більш докладно на співмножниках, що входять у формулу (1.14).

Імовірність появи і-ї загрози $P_{i\,угр}$ визначається статистично і відповідає відносній частоті її появи

$$\mathrm{P}_{i\,угр} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}_i, \quad (1.16)$$

де λ_i - частота появи і- загрози

Збиток, принесений і-ю загрозою Δq_i, може визначатися в абсолютних одиницях: економічних утратах, тимчасових витратах, обсязі знищеної чи "зіпсованої" інформації і т.д.

Однак, практично це зробити дуже важко, особливо на ранніх етапах проектування КСЗІ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, що по суті справи являє собою ступінь небезпеки і-ї загрози для інформаційно-керуючої системи. Ступінь небезпеки може бути визначена експертним шляхом у припущенні, що всі загрози для РКМ складають повну групу подій, тобто

$$0 \le \Delta q_i \le 1; \sum_{i=1}^{n} \Delta q_i = 1$$

Найбільш складним питанням є визначення імовірності усунення і-ї загрози $\mathrm{P}_{i\,угр}^{\,устр}$ при проектуванні КСЗІ. Зробимо природне допущення, що ця імовірність визначається тим, наскільки повно враховані якісні і кількісні вимоги до КСЗІ при їхньому проектуванні, тобто

$$\mathrm{P}_{i\,угр}^{\,устр} = fi(x_{i1},..,x_{ij},..,x_{im}), \quad (1.17)$$

де x_{ij} - ступінь виконання j-ї вимоги до КСЗІ для усунення і-ї загрози, $i = \overline{1,n}; j = \overline{1,m}$.

Нехай перші "k" вимог будуть кількісними $\left(j = \overline{1,k}\right)$, інші "m-до" – якісними $\left(j = \overline{k+1,m}\right)$.

Ступінь виконання j-ї кількісної вимоги визначається його близькістю до необхідного (оптимальному) значенню. Для оцінки ступеня виконання j-ї кількісної вимоги до КСЗІ зручніше за все використовувати його нормоване значення $\overline{x}_{ij}\,(j = \overline{1,k}), 0 \le x_{ij} < 1$.

Для нормування зручно використовувати функцію виду

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij}^{нх}}{x_{ij}^{нл} - x_{ij}^{нх}}, \tag{1.18}$$

де x_{ij} - поточне значення j-ї вимоги;

$x_{ij}^{нл}, x_{ij}^{нх}$ - найкраще і найгірше значення.

З урахуванням формули (1.18) одержуємо наступні розрахункові співвідношення:

$$x_{ij}^{нл} = x_{ij\ max}; x_{ij}^{нх} = x_{ij\ min}$$

$$\bar{\bar{x}}_{ij} = \frac{x_{ij} - x_{ij\min}}{x_{ij\ max} - x_{ij\min}},$$

при (1.19)

при $x_{ij}^{нл} = x_{ij\min}; x_{ij}^{нх} = x_{ij\max}$

$$\bar{\bar{x}}_{ij} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}}, \tag{1.20}$$

при $x_{ij}^{нл} = x_{ij}opt; x_{ij\ нх} = x_{ij\min}; x_{ij}^{нх} = x_{ij\max}; x_{ij\min} \le x_{ij\ opt} \le x_{ij\max}$

$$\bar{\bar{x}}_{ij} = \begin{cases} 0 & при \quad x_{ij} > x_{ij\min}; x_{ij} < x_{ij\max} \\ 1 & при \quad x_{ij} = x_{ij\ opt} \\ \dfrac{x_{ij} - x_{ij\min}}{x_{ij\ opt} - x_{ij\min}} & при \quad x_{ij\min} \le x_{ij} \le x_{ij\ opt} \\ \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\ opt}} & при \quad x_{ij\ opt} \le x_{ij} \le x_{ij\max} \end{cases} \tag{1.21}$$

Ступінь виконання j-ї якісної вимоги визначається функцією належності до найкращого значення $\mu(x_{ij})$.

Розклавши функцію (1.17) у ряд Макларена й обмежившись лише першими членами ряду, одержимо

$$\mathrm{P}_{i\ угр}^{устр} = \mathrm{P}_{i\ угр}^{устр}(0) + \sum_{\gamma=1}^{m} \frac{\partial \mathrm{P}_{i\ угр}^{устр}}{\partial x_{ij}} \bullet x_{ij} \tag{1.22}$$

де $\mathrm{P}_{i\ угр}^{устр}(0) = 0$ - імовірність усунення і-ї загрози при невиконанні вимог і КСЗІ;

$\frac{\partial \mathbf{P}_{i\ угр}^{устр}}{\partial x_{ij}} = \alpha_{ij}$ - величина, що характеризує ступінь впливу j-ї вимоги на імовірність усунення і-ї загрози (важливість виконання j-ї вимоги для усунення і-ї загрози). Очевидно, що $0 \le \alpha_{ij} \le 1; \sum_{j=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1, n}$.

Після підстановки в (12) відповідних значень, одержуємо

$$P_{i\,угр}^{устр} = \sum_{j=1}^{к} \alpha_{ij} \cdot \overline{x_{ij}} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}) \tag{1.23}$$

Остаточно формула (1.15) для оцінки величини $\overline{W}$ відверненого збитку приймає вид

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \overline{x_{ij}} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu(x_{ij}) \tag{1.24}$$

Таким чином, задача синтезу КСЗІ зводиться до оптимального обґрунтування кількісних і якісних вимог до КСЗІ при припустимих витрат і приймає вид:

$$\text{Знайти } \max \overline{W}(x_{ij}; i = \overline{1,n}; j = \overline{1,m}) \tag{1.25}$$

при обмеженні $C(x_{ij}) \le Cдоп; i = \overline{1,n}; j = \overline{1,m}$.

Відповідно до формулювання задачі (1.25) основними етапами її рішення є:

- збір і обробка експертної інформації про характеристики загроз: частоті появи і-ї загрози $\overline{\lambda_i}$ і збитку Δqi ($i = \overline{1,n}$);

- збір і обробка експертної інформації для визначення важливості виконання j-ї вимоги для усунення і-ї загрози α_{ij} і функції належності μ(xij), ($i = \overline{1,n}$, $j = \overline{1,m}$);

- оцінка вартості КСЗІ для конкретного варіанта її реалізації, що залежить від ступеня виконання вимог З (xij; $i = \overline{1,n}$; $j = \overline{1,m}$);

- розробка математичної моделі й алгоритму вибору раціонального варіанта побудови КСЗІ (раціонального завдання вимог) відповідно до постановки (1.25) як задачі нечіткого математичного програмування.

На закінчення відзначимо, що при відсутності інформації про загрози для рішення задачі (1.25) може бути використаний показник виду

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \alpha_{ij} \cdot \overline{x_{ij}} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}) \tag{1.26}$$

Коротка характеристика моделі загроз

Інформація для свого існування завжди вимагає наявності носія. Як носій інформації виступає поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина.

Втрата інформацією своєї цінності (порушення БІ) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

Загрози оброблюваної в РКМ інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації.

Загрози визначаються як такі, що мають об'єктивну природу (зміна умов фізичного середовища, відмова елементів, пожежі, повені і т. ін.), або суб'єктивну (помилки персоналу чи дії зловмисника).

Загрози, що мають суб'єктивну природу, розглядаються як випадкові або навмисні.

Спроба реалізації загрози вважається атакою.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Загрози, реалізація яких призводить до втрати визначених властивостей інформації, відповідно є загрозами конфіденційності, цілісності або доступності інформації,

Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата керованості може призвести до нездатності КСЗІ забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

Неавторизований доступ до інформаційних ресурсів РКМ - відбувається внаслідок отримання неавторизованим користувачем доступу до засобів РКМ .

Невідповідний доступ до ресурсів РКМ - відбувається внаслідок отримання доступу до ресурсів РКМ авторизованою або неавторизованою людиною неавторизованим способом.

Розкриття даних - відбувається внаслідок отримання несанкціонованого доступу та розкриття інформації випадковим або неавторизованим навмисним чином.

Неавторизована модифікація даних і програм - відбувається внаслідок модифікації, видалення або руйнування людиною даних і програмного забезпечення РКМ неавторизованим або випадковим чином.

Розкриття трафіка каналів зв’язку РКМ - відбувається внаслідок отримання доступу до інформації випадковим або неавторизованим навмисним чином тоді, коли інформація передається через канали зв’язку РКМ .

Неавторизований доступ до інформації в РКМ може відбуватися з використанням наступних типів вразливих місць:

- відсутність або недостатність схеми ідентифікації і аутентифікації,
- наявність паролів, що спільно використовуються,
- погане керування паролями або легкі для вгадування паролі,
- використання відомих системних брешей і вразливих місць, які не були виправлені,
- наявність однокористувальних ПК, що не мають парольного захисту під час загрузки,
- неповне використання механізмів блокування ПК або АРМ,
- наявність паролів доступу, що зберігаються в пакетних файлах на дисках ПК до РКМ ,
- слабкий фізичний контроль за мережевими пристроями,
- незахищені модеми,
- відсутність тайму-ауту при встановленні сеансу і реєстрації невірних спроб,
- відсутність відключення термінала при численних невдалих спробах встановлення сеансу і реєстрації таких спроб,
- відсутність повідомлень “дата/час останнього вдалого сеансу" і “неуспішна спроба встановлення сеансу" на початку сеансу,
- відсутність верифікації користувача в реальному часі (для виявлення “маскараду”).

Невідповідний доступ до ресурсів РКМ може відбуватися при використанні наступних типів вразливих місць:

- використання при призначенні прав користувачам за умовчанням таких системних установок, які є надмірними для користувачів,
- неправильне використання привілеїв адміністратора або менеджера РКМ ,

- дані, що зберігаються з неадекватним рівнем захисту або взагалі без захисту,

- недостатнє або неправильне використання механізму призначення привілеїв для користувачів,

- ПК, на яких не використовують контролю доступу на рівні файлів.

Компрометація даних РКМ може відбуватися при використанні наступних типів вразливих місць:

- неправильні установки управління доступом,

- дані, які вважаються достатньо критичними, щоб треба було використати шифрування, але зберігаються в незашифрованій формі,

- початкові тексти програм, що зберігаються в незашифрованій формі,

- монітори, що знаходяться в приміщеннях, де багато сторонніх людей,

- станції друку, що знаходяться в приміщеннях, де є багато сторонніх людей,

- резервні копії даних і програмного забезпечення, що зберігаються у відкритих приміщеннях.

Неавторизована модифікація даних і програмного забезпечення може відбуватися при використанні наступних типів вразливих місць:

- дозвіл на запис, наданий користувачам, яким потрібний тільки дозвіл на доступ по читанню,

- невиявлені зміни в програмному забезпеченні, включаючи додання коду для створення програми троянського коня,

- відсутність криптографічної контрольної суми критичних даних,

- механізм привілеїв, який дозволяє надмірний дозвіл запису,

- відсутність засобів виявлення і захисту від вірусів,

Компрометація трафіка в каналах зв’язку РКМ може відбуватися при використанні наступних типів вразливих місць:

- неадекватний фізичний захист пристроїв РКМ і середи передачі,

- передача відкритих даних з використанням широкомовних протоколів передачі,

- передача відкритих даних (незашифрованих) по середі РКМ .

Підміна трафіка РКМ включає:

- здатність отримувати повідомлення, маскуючись під легітимне місце призначення,

- здатність маскуватися під об’єкт-відправник

Підміна або модифікація трафіка в каналах зв’язку РКМ може відбуватися при використанні наступних типів вразливих місць:

- передача трафіка РКМ у відкритому вигляді,

- відсутність відмітки дати / часу (показуючи час посилки і час отримання),

- відсутність механізму коду аутентифікації повідомлення або цифрового підпису,

- відсутність механізму аутентифікації в реальному масштабі часу (для захисту від відтворення).

Руйнування функціональних можливостей РКМ можливе при:

- нездатності виявити незвичайний характер трафіка (тобто навмисне переповнення трафіка),

- нездатності перенаправляти трафік, виявити відмови апаратних засобів ЕОМ, і т.ін.,

- наявність конфігурації РКМ , що допускає можливість виходу з ладу через відмову в єдиному місці,

- неавторизованій зміні компонентів апаратних засобів ЕОМ (переконфігуруванні адреси на автоматизованих робочих місцях, зміни конфігурації маршрутизаторів або хабів, і т. ін.),

- неправильному обслуговуванні апаратних засобів РКМ ,

- недостатньому фізичному захисті апаратних засобів РКМ .

Класифікація загроз безпеки

Джерела загроз стосовно РКМ можуть бути зовнішніми чи внутрішніми (компоненти самої РКМ - її апаратура, програми, персонал).

До основних ненавмисних штучних загроз РКМ (дії, чинені людьми випадково, через незнання, неуважності чи недбалості, з цікавості, але без злого наміру) можна віднести:

- ненавмисні дії, що приводять до часткового чи повного відмовлення системи, руйнування апаратних, програмних засобів, інформаційних ресурсів системи (ненавмисне псування устаткування, видалення, перекручування файлів з важливою інформацією чи програм, у тому числі системних і т. ін.);

- неправомірна зміна режимів роботи пристроїв і програм РКМ ;

- ненавмисне псування носіїв інформації;

- запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання, зациклення) чи здійснюючих необоротні зміни в системі (форматування реструктуризацію носіїв інформації, видалення даних і т. ін.);

- нелегальне впровадження і використання неврахованих програм (ігрових, навчальних, технологічних і ін., що не є необхідними для виконання порушником своїх службових обов'язків) з наступною необґрунтованою витратою ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

- зараження комп'ютера вірусами;

- необережні дії, що приводять до розголошення таємної інформації, та роблять її загальнодоступною;

- розголошення, передача чи втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, пропусків і т. ін.);

- проектування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, що представляють небезпеку для працездатності РКМ та системи захисту інформації;

- ігнорування організаційних обмежень (установлених правил) в РКМ ;

- вхід у систему в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв і т. ін.);

- некомпетентне використання, настроювання чи неправомірне відключення засобів захисту персоналом служби безпеки;

- пересилання даних по помилковій адресі абонента (пристрою);

- введення помилкових даних;

- ненавмисне ушкодження каналів зв'язку.

Основні можливі шляхи навмисної дезорганізації роботи РКМ наступні:

- фізичне руйнування системи (шляхом вибуху, підпалу і т ін.) чи вивід з ладу всіх чи окремих найбільш важливих компонентів РКМ (пристроїв, носіїв важливої системної інформації, особи з числа персоналу і т. ін.);

- відключення чи вивід з ладу підсистем забезпечення функціонування РКМ (електроживлення, охолодження і вентиляції, ліній зв'язку і т ін.);

- дії по дезорганізації функціонування РКМ (зміна режимів роботи чи пристроїв програм, страйк, саботаж персоналу, постановка могутніх активних радіоперешкод на частотах роботи пристроїв системи і т. ін.);

- впровадження агентів у число персоналу системи (у тому числі, можливо, і в адміністративну групу, що відповідає за безпеку);

- вербування (шляхом підкупу, шантажу і т. ін.) персоналу чи окремих користувачів, що мають визначені повноваження;

- застосування пристроїв, що підслуховують, дистанційна фото- і відео зйомка і т. ін.;

- перехоплення побічних електромагнітних, акустичних і інших випромінювань пристроїв і ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, що безпосередньо не беруть участь в обробці інформації (телефонні лінії, мережі харчування, опалення і т. ін.);

- перехоплення даних, переданих по каналах зв'язку, і їхній аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача і наступних спроб їхньої імітації для проникнення в систему;

- розкрадання носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, що запам'ятовують пристроїв і цілих ПЕОМ);

- несанкціоноване копіювання носіїв інформації;

- розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації і т. ін.);

- читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;

- читання інформації з областей оперативної пам'яті, використовуваних операційною системою (у тому числі підсистемою захисту) чи іншими користувачами, в асинхронному режимі використовуючи недоліки багаторозрахункових операційних систем і систем програмування;

- незаконне одержання паролів і інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбора, шляхом імітації інтерфейсу системи і т.д.) з наступним маскуванням під зареєстрованого користувача ("маскарад");

- несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т. ін.;

- розкриття шифрів криптографічного захисту інформації;

- впровадження апаратних і програмних "закладок" ("троянських коней" і "жучків"), тобто таких ділянок програм, що не потрібні для здійснення заявлених функцій, але, що дозволяють перебороти систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації і передачі критичної інформації чи дезорганізації функціонування системи;

- незаконне підключення до ліній зв'язку з метою роботи "між рядків", з використанням пауз у діях законного користувача від його імені з наступним введенням помилкових повідомлень чи модифікацією переданих повідомлень;

- незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему й успішної аутентифікації з наступним введенням дезінформації і нав'язуванням помилкових повідомлень.

Варто помітити, що найчастіше для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність з перерахованих вище шляхів.

Класифікація каналів проникнення в систему і витоку інформації

Усі канали проникнення в систему і витоки інформації розділяють на прямі і непрямі. Під непрямими розуміють такі канали, використання яких не вимагає проникнення в приміщення, де розташовані компоненти системи. Для використання прямих каналів таке проникнення необхідне. Прямі канали можуть використовуватися без внесення змін компонентів системи чи зі змінами компонентів.

По типу основного засобу, використовуваного для реалізації загрози, всі можливі канали можна умовно розділити на три групи, де такими засобами є: людина чи програма апаратура.

По способу одержання інформації потенційні канали доступу можна розділити на:

- фізичний;
- електромагнітний (перехоплення випромінювань);
- інформаційний (програмно-математичний).

Специфіка розподілених РКМ , з погляду їхньої уразливості, зв'язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Вразливими є буквально всі основні структурно-функціональні елементи розподілених РКМ: робочі станції, сервери (Host-машини), мережеві мости (шлюзи, центри комутації), канали зв'язку.

Існує ряд варіантів навмисного чи випадкового несанкціонованого доступу до даних і втручання в процеси обробки й обміну інформацією.

Приклад моделі загроз для АС класу 1.

До імовірних загроз для інформаційних ресурсів автоматизованої системи класу 1:

- дії користувачів АС при роботі на ПЕОМ, які можуть призвести до порушення конфіденційності, цілісності, доступності та спостереженості інформаційних ресурсів АС (помилки у роботі або НСД);
- дії персоналу, що обслуговує технічні засоби АС або приміщення де розташовано АС, які можуть призвести до витоку ІзОД шляхом крадіжки носіїв інформації або їх пошкодження;
- дії персоналу, що обслуговує технічні засоби АС або приміщення де розташовано АС, які можуть призвести до порушення доступності та спостереженості інформаційних ресурсів АС (виведення з ладу компонентів АС);
- відвідувачі об'єкта інформаційної діяльності, представники контролюючих органів, які намагаються отримати доступ до приміщення АС з метою здійснення НСД до ІзОД або порушення доступності та спостереженості інформаційних ресурсів АС;
- дії осіб за межами КЗ, які намагаються отримати доступ до приміщення АС з метою здійснення НСД до ІзОД або порушення доступності та спостереженості інформаційних ресурсів АС;
- дії осіб за межами КЗ, які спрямовані на перехоплення інформації технічними засобами розвідки (розвідувальні структури інших країн, протиправні дії фізичних осіб).

Несанкціонований доступ до ІзОД в АС класу 1 може здійснюватися:

1). Сторонніми особами (відвідувачами), які знаходяться на території частини та здійснюють злочинні дії.

2). Співробітниками об’єкту інформаційної діяльності при здійсненні ними ненавмисних дій при виконанні робіт, що пов'язані з виконавчою діяльністю.

Можливі методі та способі здійснення несанкціонованого доступу до ІзОД наведені у таблиці 1.

Для кожної з загроз визначено:

- на порушення яких властивостей інформації або АС вона спрямована (порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);

- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

- можливі способи здійснення загроз.

Таблиця 1.4

Визначення загроз

№	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	С
1	Виведення з ладу технічних засобів	Персонал, користувачі, ТЗ, сторонні особи, які отримали несанкціонований доступ на контрольовану територію (далі - сторонні особи)	Фізичний НСД до обладнання, що захищається		+	+	
2	Порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації)	Персонал, користувачі, сторонні особи, ТЗ	Фізичний НСД до обладнання, що захищається				
3	Порушення режимів функціонування АС (обладнання і ПЗ), та систем життєзабезпечення АС	Персонал, користувачі, сторонні особи, ТЗ, ПЗ	Фізичний НСД до обладнання, що захищається, застосування закладних пристроїв, програм, вкорінення комп’ютерних вірусів				
4	Незаконне підключення: до апаратури, системи електроживлення, заземлення, життєзабезпечення	Персонал, користувачі, сторонні особи, ТЗ	Фізичне підключення	+	+	+	+

№	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	С
5	Читання “сміття” (залишкової інформації з запам’ятовуючих пристроїв)	Персонал, користувачі, сторонні особи, ТЗ, ПЗ	НСД доступу до МНІ або оперативної пам’яті сторонніх осіб, застосування закладних пристроїв, програм	+			
6	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду віддрукованих на принтері документів	Персонал, користувачі, відвідувачі, сторонні особи	Знаходження сторонніх осіб в службових приміщеннях	+			
7	Несанкціоноване використання технічних пристроїв	Персонал, користувачі, відвідувачі, сторонні особи	Фізичний НСД до обладнання	+	+	+	+
8	Несанкціоноване внесення змін (підміни) в КТЗ, в програмне забезпечення, в компоненти інформаційного забезпечення	Персонал, користувачі, відвідувачі, сторонні особи	Фізичний НСД до обладнання та програмного забезпечення, подолання заходів захисту	+			+
9	Несанкціоноване копіювання вихідних документів, магнітних та інших носіїв інформації (у тому числі при проведенні ремонтних та регламентних робіт)	Персонал, користувачі, відвідувачі, сторонні особи	НСД до МНІ, подолання заходів захисту, застосування закладних програм, вкорінення комп’ютерних вірусів	+			
10	Розкрадання магнітних носіїв, документів, чернеток, виробничих	Персонал, користувачі, відвідувачі, сторонні особи	НСД в приміщення, до МНІ та	+		+	

№	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	С
	(оригінали і копії інформаційних матеріалів, ГМД), отримання необлікованих копій		технічних засобів				
11	Використання з корисливою метою персоналу АС	Персонал, користувачі, відвідувачі, сторонні особи	Шантаж, підкуп				
12	Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”)	Персонал, користувачі, відвідувачі, сторонні особи	Застосування закладних програм, підглядування процесу реєстраціївикористання вад системи захисту	+	+	+	+
13	Впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації	Персонал, користувачі, відвідувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та програмного забезпечення, подолання заходів захисту	+	+	+	+
14	Впровадження і використання комп’ютерних вірусів	Персонал, користувачі, відвідувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та програмного забезпечення, подолання заходів захисту	+	+	+	+
15	Включення в програми програмних закладок типу “троянський кінь”, “бомба” тощо	Персонал, користувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та програмного забезпечення,	+	+	+	+

№	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	С
			подолання заходів захисту				
16	Використання вад мов програмування, операційних систем	Персонал, користувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та програмного забезпечення, подолання заходів захисту	+	+	+	+

1.7 Неформальна модель порушника в РКМ

Порушник - це особа, що здійснює спробу виконання заборонених операцій (дій) помилково, чи незнанню усвідомлено зі злим наміром (з корисливих інтересів) чи без такого (заради чи гри задоволення, з метою самоствердження і т. ін.) і, методи, що використають для цього різні можливості, і засоби. Зловмисником будемо називати порушника, що навмисно йде на порушення з корисливих спонукань.

Неформальна модель порушника описує його практичні і теоретичні можливості, апріорні знання, час і місце дії і т. ін. Для досягнення своїх цілей порушник повинний прикласти деякі зусилля, затратити визначені ресурси. Досліджуючи причини порушень, можна або вплинути на самі ці причини (звичайно, якщо це можливо) або точніше визначити вимоги до системи захисту від даного виду порушень чи злочинів.

У кожнім конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, що повинна бути адекватна реальному порушнику для даної РКМ . При розробці моделі порушника визначаються:

- припущення про категорії осіб, до яких може належати порушник;
- припущення про мотиви дій порушника (переслідуваних порушником цілях);
- припущення про кваліфікацію порушника і його технічну оснащеність (про використовувані для здійснення порушення методах і засобах);
- обмеження і припущення про характер можливих дій порушників.

Стосовно РКМ порушники можуть бути внутрішніми (з числа персоналу системи) чи зовнішніми (сторонніми особами). Внутрішнім порушником може бути особа з наступних категорій персоналу:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки і супроводи ПО (прикладні і системні програмісти);
- технічний персонал, що обслуговує будинки (прибиральники, електрики, сантехники й інші співробітники, що мають доступ у будинки і приміщення, де розташовані компоненти РКМ);
- співробітники служби безпеки РКМ;
- керівники різних рівнів посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);
- відвідувачі (запрошені з якого-небудь приводу);
- представники організацій, взаємодіючих з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання і т.ін.);

- представники конкуруючих організацій (іноземних спецслужб) чи особи, що діють по їхньому завданню;

- особи, що випадково чи навмисне порушили пропускний режим (без мети порушити безпеку РКМ);

- будь-які особи за межами контрольованої території.

Можна виділити три основних мотиви порушень: безвідповідальність, самоствердження і корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано чи випадково робить які-небудь дії, що руйнують, не зв'язані проте зі злим наміром. У більшості випадків цей наслідок некомпетентності чи недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних великим успіхом, затіваючи свого роду гру "користувач - проти системи" заради самоствердження або у власних очах або в очах колег.

Порушення безпеки РКМ може бути викликано і корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до збереженої, переданої й оброблюванні у РКМ інформації. Навіть, якщо РКМ має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Класифікація порушників

Усіх порушників можна класифікувати у такий спосіб.

За рівнем знань про РКМ :

- знає функціональні особливості РКМ , основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користатися штатними засобами;

- має високий рівень знань і досвід роботи з технічними засобами системи і їхнього обслуговування;

- має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (використовуваним методам і засобам):

- агентурні методи одержання зведень;

- пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, що можуть бути потай пронесені через охорону;

- методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

За часом дії:

- у процесі функціонування РКМ (під час роботи компонентів системи);

- у період не активності компонентів системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонту і т.п.);

- як у процесі функціонування РКМ , так і в період не активності компонентів системи.

По місцю дії:

- без доступу на контрольовану територію організації;

- з контрольованої території без доступу в будинки і спорудження;

- усередині приміщень, але без доступу до технічних засобів РКМ ;

- з робочих місць кінцевих користувачів (операторів) РКМ ;

- з доступом у зону даних (баз даних, архівів і т.п.):

- з доступом у зону керування засобами забезпечення безпеки РКМ .

Можуть враховуватися наступні обмеження і припущення про характер дій можливих порушників:

- робота з підбору кадрів і спеціальні заходи утрудняють можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій, але подоланню підсистеми захисту двома і більш порушників;

- порушник, плануючи спроби несанкціонованого доступу (НСД), ховає свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, що експлуатує й обслуговує персонал, а також недоліків прийнятої технології обробки інформації і т.д.

Визначення конкретних значень характеристик можливих порушників у значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області і технології обробки інформації, може бути представлена перерахуванням декількох варіантів його виду. Кожен вид порушника повинний бути охарактеризований значеннями характеристик, приведених вище.

Характеристика порушників

Дотепер не склалося єдине розуміння того, хто ж такі порушники. Звичайно зі словом "порушник" асоціюється фахівець, що володіє дуже високою кваліфікацією в області комп'ютерної безпеки. З приводу того, як порушники використовують свої знання, маються серйозні розбіжності. Одні автори називають порушниками тих, хто намагається зламати захищені системи для того, щоб потім сформулювати рекомендації з удосконалювання їхнього захисту. Інші називають порушниками тільки "комп'ютерних асів", що використовують свої знання в злочинних цілях. Іноді порушників у цьому розумінні називають кракерами чи крекерами (від англ. crack – руйнувати).

Будемо розуміти під порушником особу, що намагається подолати захист комп'ютерної системи, неважливо, у яких цілях, будемо мати на увазі найбільш висококваліфікованих порушників, дії яких являють найбільшу загрозу безпеки захищених систем.

У відношенні до системи, що атакується, може виступати в одній з наступних ролей:

- стороння особа, що не має легального доступу до системи. Порушник може атакувати систему тільки з використанням загальнодоступних глобальних мереж;

- співробітник організації, що не має легального доступу до системи, що атакується. Більш ймовірна ситуація, коли в такій ролі виступає не сам порушник, а його агент (прибиральниця, охоронець і т.ін.). Порушник може впроваджувати в систему, що атакується, програмні закладки. Якщо порушник зуміє чи підглянути підібрати пароль легального користувача, він може перейти в роль чи користувача адміністратора;

- користувач системи, що володіє мінімальними повноваженнями. Порушник може атакувати систему, використовуючи помилки в програмному забезпеченні й в адмініструванні системи;

- адміністратор системи. Порушник має легально отримані повноваження, достатні для того, щоб успішно атакувати систему. Для нейтралізації цієї загрози в системі повинні бути передбачені засоби протидії несанкціонованим діям адміністраторів;

- розроблювач системи. Порушник може вбудовувати в код системи "люки", що надалі дозволять йому здійснювати НСД до ресурсів системи.

Професійний рівень порушників варіюється в дуже широких межах. У ролі порушника може виступати як школяр, що випадково знайшов програму злому на одному із серверів Internet. У телеконференціях Internet зустрічалися повідомлення про існування організованих груп порушників, що поставили злом комп'ютерних систем на комерційну основу. Керівництво такими групами здійснюється професіоналами найвищої кваліфікації.

Порушник завжди в курсі останніх новинок науки і техніки в області комп'ютерної безпеки. Він регулярно переглядає матеріали порушників серверів Internet, читає телеконференції (newsgroups) порушників, виписує кілька журналів по комп'ютерній безпеці.

Перед тим, як атакувати систему, порушник збирає максимум інформації про неї. Він заздалегідь з'ясовує, яке програмне забезпечення використовується в системі, намагається познайомиться з її адміністраторами. Знаючи особисті якості адміністратора, простіше шукати помилки в політику безпеки системи.

Характерні риси порушника

Можна виділити наступні характерні риси такого порушника:

Порушник не зневажає оперативно-технічними й агентурними методами. Для проникнення в захищену мережу може бути досить поставити "жучок" у їдальні, де звичайно обідають адміністратори.

Перед тим, як атакувати систему, порушник по можливості випробує засіб атаки на заздалегідь виготовленій моделі. Ця модель являє собою один чи кілька комп'ютерів, на яких установлене те ж програмне забезпечення і дотримується та ж політика безпеки, що й у системі, що атакується.

Порушник не атакує систему, поки не буде упевнений (чи майже упевнений) в успіху.

При першій атаці системи порушник звичайно намагається впровадити в систему, що атакується, програмну закладку. Якщо впровадження закладки проходить успішно, друга атака вже не потрібна.

Атака системи відбувається швидко. Адміністратори звичайно довідаються про атаку тільки після її закінчення.

Порушник не використовує особливо витончених алгоритмів атаки системи – чим складніше алгоритм атаки, тим більше імовірність помилок і збоїв при його реалізації.

Порушник не здійснює атаку вручну – він пише необхідні програми. При атаці системи надзвичайно важлива швидкість дій.

Порушник ніколи не атакує систему під своїм ім'ям чи зі своєї мережної адреси.

Порушник заздалегідь продумує порядок дій у випадку невдачі. Якщо атака не удалася, порушник намагається замести сліди. Якщо це неможливо, він намагається залишити помилковий слід. Якщо, наприклад, атака виробляється через Internet, помилковий слід можна залишити, провівши дуже грубу і свідомо невдалу атаку системи з іншої адреси. При аналізі журналу аудита адміністратору буде важко помітити сліди основної атаки серед величезної кількості зареєстрованих подій.

Якщо в системі, що атакується, передбачений аудит, порушник намагається його відключити.

Програмна закладка, впроваджена в систему, помітна тільки порушнику. З погляду інших користувачів система працює як звичайно.

При виявленні програмна закладка само знищується. Крім того, часто закладка програмується так, що її самознищення відбувається, коли нею довго ніхто не користується. У цьому випадку порушнику не потрібно турбуватися про знищення речовинних доказів.

1.8. Аналіз ризику функціонування автоматизованих систем

В загалі, послідовність проведення робіт з аналізу ризику передбачає:

- аналіз цінних ресурсів;
- аналіз загроз;
- аналіз порушника (можливих дій потенційного порушника);
- аналіз ризику;

Методики аналізу цінності інформаційних ресурсів

На початку наведемо один із прагматичних підходів до практичного аналізу цінності інформації. Відповідно до нього виділяються наступні чотири види методик аналізу цінності інформації:

"Тотальний" — у цьому випадку організація робить комерційною таємницею абсолютно все. Природно, окрім відомостей, які не можуть бути закриті. На думку спеціалістів, цей метод є найменш ефективним, оскільки адже фірма не зможе захистити інформацію повністю. До того ж із-за режиму тотальної секретності буде значно ускладнена її робота.

"Плагіаторський" — фірма дізнається, яку саме інформацію партнери і контрагенти вважають комерційною таємницею на своїх підприємствах, а потім поступають аналогічно у себе. Мінуси цього способу є наочними: універсальних положень для будь-яких фірм практично не

існує. Що добре для однієї компанії, може не працювати в іншій. Проте це досить популярний спосіб у невеликих компаніях.

“Аналітичний” — керівництво фірми ставлять себе на місце конкурентів і недоброзичливців та аналізують, яка саме інформація могла би їх зацікавити.

“Експертний” — у даному випадку фірма запрошує незалежних спеціалістів для оцінки інформації. Як правило, це найбільш ефективний, але у цей же час і дорогий спосіб.

Зрозуміло, що для проведення детального аналізу та визначення цінності ресурсів доцільним є використання більш деталізованих методів (методик). їх основою, як правило є певний підхід до групування (класифікації) цінної інформації за певною ознакою.

Прикладом застосування такого підходу є формування і використання державами різного роду переліків цінної інформації, їх зазначенням ознак таких відомостей та режиму обмеження доступу до них. В Україні до таких переліків відносяться, наприклад: Зведений перелік відомостей, що становлять державну таємницю (ЗВДТ) та Перелік конфіденційної інформації. Приклади цінної інформації, що визначені законодавчими актами України: секретна, конфіденційна, службова, персональні дані и т. ін.

За своєю сутністю процес класифікація інформації це поділ наявних інформаційних активів організації за деякою ознакою, який виконується відповідно до ступеня тяжкості наслідків від втрати ними певних властивостей, які є важливими з точки зору інформаційної безпеки (як правило доступності, конфіденційності, цілісності).

Так, відповідно до ISO/IEC TR 13569:2005 (Фінансові послуги - Рекомендації по інформаційній безпеці), класифікація класифікація це схема, що поділяє інформацію на категорії, такі як: можливість шахрайства, конфіденційність або критичність інформації, з метою застосування до неї відповідних захисних мір.

Класифікація об’єктів захисту виконується з метою забезпечення диференційованого підходу до організації її захисту з урахуванням рівня критичності, що визначаєтсь впливом на діяльність та репутацію організації, її ділових партнерів та працівників. Класифікація дозволяє визначити пріоритетність та економічну обґрунтованість проведення подальших заходів по забезпеченню інформаційної безпеки об’єкта захисту.

Крім національних документів, обов’язковість проведення класифікації інформації зазначається наприклад в ISO/IEC 27002:2005.

Помилки в класифікації інформації призводять до неадекватного визначання завдань з захисту цінних ресурсів і, відповідно, до недостатньо ефективних заходів з їх захисту.

Можливі підходи до класифікації:

- однофакторна (наприклад за потенційною шкодою: до $1000, $10000, $1000000);
- багатофакторна зі зведенням до єдиної шкали класів інформації ({К, Ц, Д} -> Гриф);
- багатофакторна зі зведенням до груп (решітки) цінності ({К, Ц, Д} -> Актив 1, Актив 2, ..., Актив N);

Зрозуміло, що властивості інформації (К,Ц,Д) доцільно оцінювати за окремими шкалами.

Також можуть використовуватися шкали, що відображають вплив на:

- репутацію,
- ефективність технологій оброблення інформації,
- порушення вимог нормативних документів,
- економічні збитки,
- вплив на стратегію розвитку організації.

Особливості класифікації інформації для організацій:

- має цінність для організації;
- має цінність для організації;
- впливає на прийняття рішень;
- впливає на поведінку людей, що призводить до економічних наслідків;
- має власну вартість;
- не має цінності для організації, але має для когось іншого;

Основні проблеми класифікації інформації:

- врахування всіх цінних ресурсів,
- складність формалізації процесів оброблення інформації,
- визначення показників за якими проводиться класифікація інформації, їх шкал вимірювання,
- класифікація компильованих матеріалів (проблема агрегації),
- класифікація відомостей, що передаються з використанням сучасних комунікаційних служб (ICQ, IP-телефонія, відеоконференції),
- класифікація відомостей, що визначають режими роботи ІКС, в тому числі роботу її механізмів захисту,
- перегляд властивостей інформації та його наслідки.

Вимоги до політики класифікації інформації:

- відповідати нормативній базі,
- практичною (визначати не більше 3-4 класифікацій),
- враховувати гнучкість та динамічність технологій оброблення цінної інформації,
- економічна обґрунтованість,
- враховувати життєвий цикл оброблення інформації,
- дозволяти підрозділам уточнювати класифікацію,
- не повинна залежить від конкретних технологій оброблення інформації та організаційної структури компанії.

Класифікація може визначати безпосередні обмеження на оброблення цінної інформацій, наприклад:

- обмеження доступу (тільки співробітники, керівництво, визначені посадові особи),
- обмеження способу оброблення (вимоги до ЕОМ, вимоги до способу захисту при передаванні каналами зв'язку),
- обмеження на спосіб зберігання (носій, обов’язковість шифрування).
- обмеження на терміни зберігання.
- побудову актуальних (зміну існуючих) моделей порушника та загроз.

Загрози класифікуються за базовими ознаками:

- природою походження (природні, штучні);
- ступенем навмисності (випадкові, навмисні);
- безпосереднім джерелом загроз (природне середовище, людина, санкціоновані програмно-апаратні засоби, несанкціоновані програмно-апаратні засоби);
- місце знаходження джерела загроз (за межами контрольованої зони, в межах контрольованої зони, джерело має доступ до засобів АС, джерело знаходиться в АС);
- ступенем залежності від активності АС (не залежать від активності, виявляються тільки під час активності АС);
- ступенем впливу на АС (активні, пасивні);
- етапами доступу до ресурсів (в ході прийняття рішення на доступ, після надання доступу);
- способом доступу до ресурсів АС (використання безпосереднього стандартного шляху доступу, використання прихованого нестандартного шляху доступу);
- поточним місце знаходженням інформації, що є об’єктом загрози (зовнішні запам’ятовуючі пристрої, оперативна пам’ять, канали зв’язку, монітори, принтери, активне мережне обладнання та ін.).

Наведемо ще один приклад формування класифікації загроз, орієнтованої на розподілені ІТС:

А) за характером впливу:

- пасивні;
- активні.

Б) по цілі впливу:

- порушення конфіденційності інформації або ресурсів системи;
- порушення цілісності інформації;
- порушення працездатності (доступності) системи.

В) за умовами початку виконання впливу:

- після запиту від об’єкту, який атакується;
- після очікуваної події на об’єкті, що атакується;
- безумовий вплив.

Г) за наявністю зворотного зв’язку з об’єктом, який атакується:

- із зворотнім зв’язком;
- без зворотного зв’язку чи одно направлений вплив.

Д) за розміщенням суб’єкту впливу по відношенню до об’єкту, стосовно якого здійснюється вплив:

- внутрішньо сегментний;
- між сегментний.

Е) за рівнем еталонно моделі ISO/OSI, на якому виконується вплив:

- фізичний;
- канальний;
- мережний;
- транспортний;
- сеансовий;
- представницький;
- прикладень.

Можливі підходи:

- за НД ТЗІ 1.1-002-99;
- за міжнародними, промисловими, інших держав стандартами та методиками (наприклад BSI);
- за іншими відомими класифікаціями.

Для поглибленого огляду можливих підходів до формування моделей загроз та порушника можна рекомендувати.

Приклад класифікації, яка може бути використана для формування моделі порушника:

- за рівнем кваліфікації (наприклад, користувачі, фахівці, експерти);
- за наявними ресурсами для проведення атак (наявність комп’ютерів, масивів даних, каналів і т. ін.);
- за рівнем поінформованості по побудову АС;
- за метою проведення атак;
- за мотивом проведення атак;
- за прийнятним рівнем ризику проведення атак;
- за місцеположенням по відношенню до периметру АС.

Відповідно до НД ТЗІ 1.1-002-99, як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу комп’ютерної системи (КС) засобами. Порушники класифікуються за **рівнем можливостей**, що надаються їм штатними засобами КС. Виділяються **чотири** рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з КС - можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- **третій рівень** визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- **четвертий рівень** визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації. Припускається, що в своєму рівні порушник - це **фахівець вищої кваліфікації**, який має повної інформації про КС і її КЗЗ.

Контрольні запитання для самооцінки рівня знань

1. Що в себе включає опис інформаційно-телекомунікаційної системи та середовища її функціонування?
2. Загальна класифікація цілей захисту інформації.
3. Визначення і аналіз поняття загрози безпеці інформації
4. Класифікація сучасних кібератак.
5. Особливості реалізації атак та заходи послаблення їх деструктивного впливу.
6. Система показників уразливості інформації і вимоги до первинних даних
7. Основні етапи оцінки дій загроз в інформаційних системах обробки інформації.
8. Аналіз організації функціонування автоматизованої системи
9. Модель загроз інформації в РКМ.
10. Класифікація загроз безпеки інформації.
11. Класифікація каналів проникнення в систему і витоку інформації.
12. Неформальна модель порушника в РКМ.
13. Класифікація порушників.
14. Характерні риси порушника.
15. Можливі атаки на автоматизовані системи.
16. Аналіз ризику функціонування. Управління ризиком.
17. Витрати на розробку систем захисту інформації.

Розділ 2

ОСНОВИ АНАЛІЗУ І СИНТЕЗУ ПОЛІТИК БЕЗПЕКИ

2.1. Політика безпеки інформації

Заходи щодо забезпечення інформаційної безпеки (ІБ), як відомо, не приносять фінансової вигоди тому хто захищається. Їх впровадження лише зменшує збиток від можливих інцидентів. Відомо, що оцінювати можливий збиток доцільно окремо для порушень доступності, конфіденційності й цілісності за трирівневою якісною шкалою на низькому, помірному (середньому) та високому рівнях (рис. 2.1).

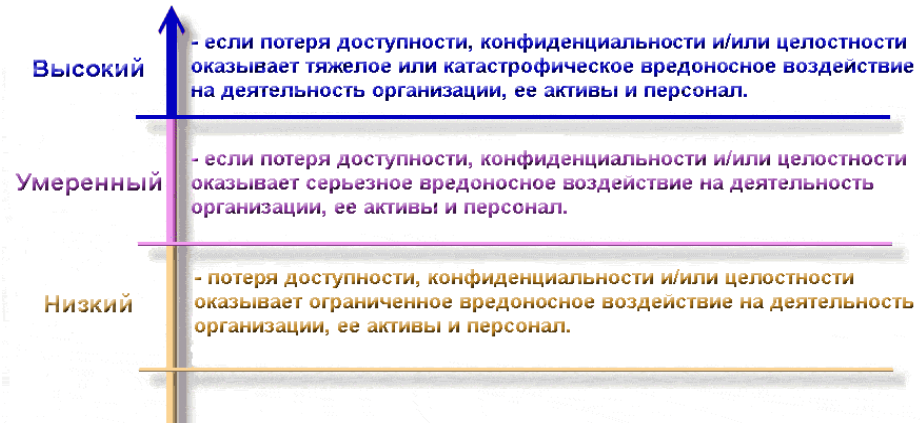


Рис.2. 1. Шкала оцінювання збитку при порушенні інформаційної безпеки

При цьому потенційний збиток для організації оцінюється як низький якщо втрата доступності, конфіденційності та/або цілісності завдає обмежений шкідливий вплив на діяльність організації, її активи й персонал, тобто:

- організація залишається здатною виконувати покладену на неї місію, але ефективність основних функцій виявляється помітно зниженою;
- активам організації наноситься незначний збиток;
- організація несе незначні фінансові втрати;
- персоналу наноситься незначна шкода.

Потенційний збиток для компанії оцінюється як помірний (середній), якщо втрата доступності, конфіденційності та/або цілісності завдає серйозного шкідливого впливу на діяльність організації, її активи й персонал, тобто:

- компанія залишається здатною виконувати покладену на неї місію, але ефективність основних функцій виявляється істотно зниженою;
- активам організації заподіюється значний збиток;
- компанія несе значні фінансові втрати;
- персоналу наноситься значна шкода, що не створює загрози життю або здоров'ю.

Потенційний збиток для організації оцінюється як високий, якщо втрата доступності, конфіденційності та/або цілісності завдає суттєвого або катастрофічного шкідливого впливу на діяльність організації, її активи й персонал, тобто:

- компанія втрачає здатність виконувати всі або деякі зі своїх основних функцій;
- активам організації заподіюється великий збиток;
- організація несе великі фінансові втрати;
- персоналу наноситься важка або катастрофічна шкода, що створює можливу загрозу життю або здоров'ю.

Виходячи із цього дуже важливо, щоб витрати на створення й підтримку ІБ були на належному рівні співвимірні цінності активів організації, пов'язаних з її ІС.

Співвимірність може бути забезпечена вибором відповідних адміністративних, процедурних, а також програмно-технічних регуляторів безпеки (рис. 2.2)

Рис. 2.2. Регулятори інформаційної безпеки

з використанням базового і детального підходу до оцінювання можливих ризиків (рис. 2.3).

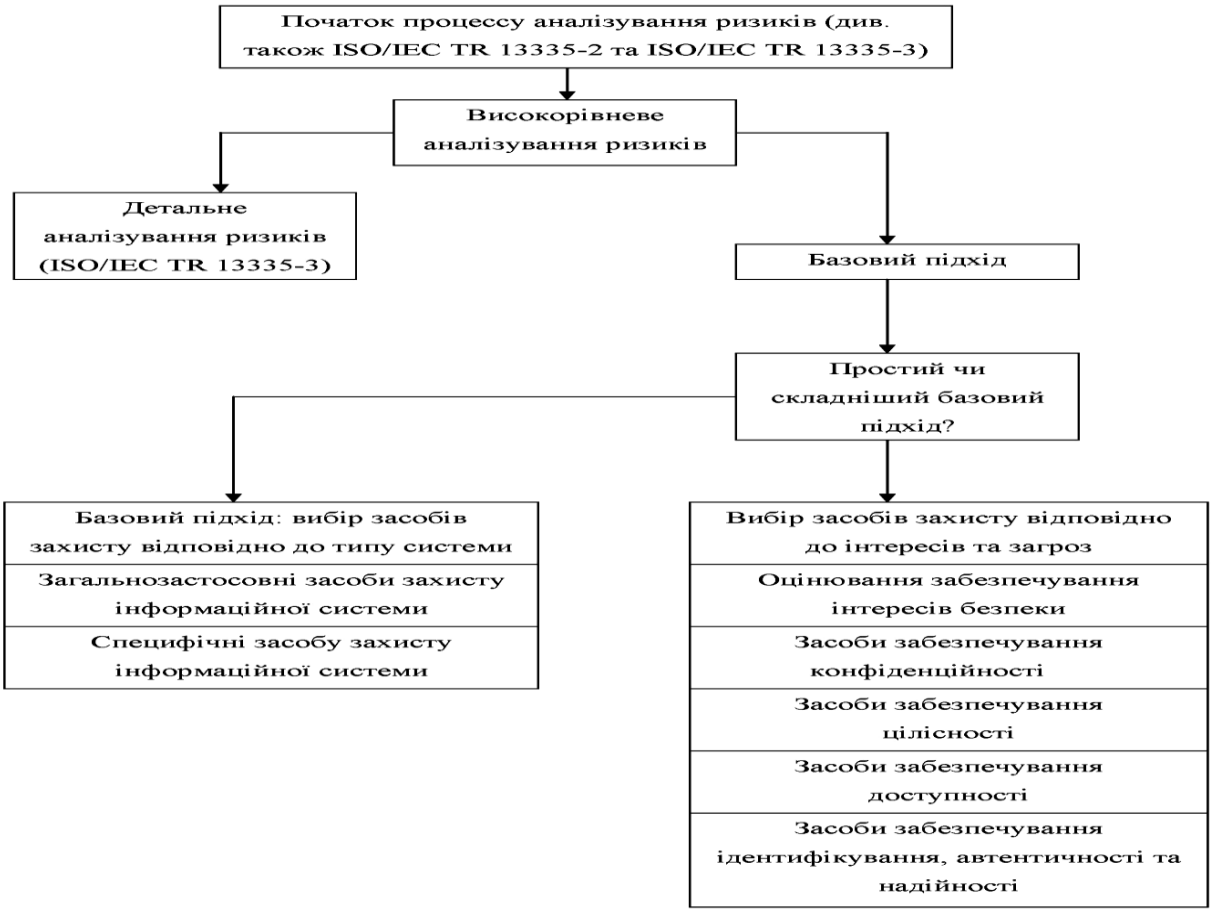


Рис. 2.3. Способи вибору засобів безпеки інформаційної системи

Категоріями загального застосування засобів безпеки при базовому підході є управління ІБ та політикою безпеки, перевірка узгодженості безпеки, реагування на порушення, питання експлуатації, планування неперервності бізнесу та фізична безпека. Засоби безпеки, які належать до цих категорій формують основу успішного управління ІБ. Важливою умовою є забезпечення взаємодії цих засобів з більш технічними засобами. Наряду з ними, для кожного відповідного типу системного компонента треба вибирати специфічні засоби безпеки. Таблиця, що наведена нижче, дає приклад того, як починати процес вибору специфічних засобів системи. В цьому прикладі «Х» означає засоби, що

мають реалізуватись за нормальних обставинах, та «(X)» означає засоби, які можуть стати у нагоді за деяких обставин (табл. 2.1).

Таблиця 2.1

Критерії вибору специфічних засобів системи

	Автономна робоча станція	Робоча станція (клієнт без спільних ресурсів), під'єдна на до мережі	Сервер чи робоча станція з спільними ресурсами, під'єднана до мережі
Автентифікація			
Автентифікація на основі інформації, якою володіє користувач	X	X	X
Автентифікація на основі дечого, чим володіє користувач	X	X	X
Автентифікація на основі того, ким є користувач	(X)	(X)	(X)
Контроль логічного доступу та аудит			
Політика контролю доступу			X
Доступ користувачів до інформаційних систем	X	X	X
Доступ користувачів до даних, служб та програм	X	X	X
Перегляд і оновлення прав доступу			X
Журнали аудиту	X	X	X
Зловмисний код			
Сканери	X	X	X
Програми перевіряння цілісності	X	X	X
Контроль за обігом переносних носіїв інформації	X	X	X
Процедурні засоби безпеки	X	X	X
Управління мережею			
Методика експлуатації			X
Планування системи			X
Конфігурація мережі			X
Відокремлення мережі			X
Моніторинг мережі			X
Виявлення вторгнень			X
Криптографія			
Безпека конфіденційності даних	(X)	(X)	(X)
Безпека цілісності даних	(X)	(X)	(X)
Неспростовність		(X)	(X)
Автентичність даних	(X)	(X)	(X)
Управління ключами	(X)	(X)	(X)

Першим кроком на цьому шляху є визначення й оцінювання проблем безпеки, що можуть призвести до втрати конфіденційності, цілісності, доступності, спостережності, автентичності та надійності. Другим – визначення для кожної проблеми безпеки типових загроз, а для кожної загрози певних засобів ІБ. У такий спосіб можливо задовольнити специфічні потреби безпеки та досягнути безпеки там, де вона дійсно необхідна.

Втрата конфіденційності може призвести до:

- втрати суспільної довіри чи погіршення репутації;
- судової відповідальності, включаючи відповідальність за порушення законодавства про безпеку даних;
- несприятливі наслідки організаційної політики;
- загрози власній безпеці;
- фінансових втрат.

Втрата цілісності може призвести до:

- прийняття невірних рішень;
- обману;
- порушення ділових функцій;
- втрати суспільної довіри чи погіршення репутації;
- фінансових втрат та судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних.

Втрата доступності до критичних програм чи доступності до критичної інформації може призвести до:

- прийняття невірних рішень;
- неможливості виконувати ризиковані задачі;
- втрати суспільної довіри чи погіршення репутації;
- фінансових втрат;
- судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних, недотримання строків виконання, вказаних в контракті, та суттєвих затрат на відновлення.

Втрата спостережності може призвести до:

- маніпуляції системою з боку користувачів;
- обману;
- індустріального шпіонажу;
- дій, що не прослідковуються;
- помилкових обвинувачень, та судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних.

Втрата автентичності може призвести до:

- обману;
- використання в правильному процесі неправильних даних, що призводить до неправильного результату;
- маніпуляції організацією з боку сторонніх осіб;
- індустріального шпіонажу;
- помилкових обвинувачень та судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних.

Вибір засобів безпеки відповідно до детальних оцінок здійснюють згідно з принципами, наведеними вище. Детальне аналізування ризиків дозволяє враховувати спеціальні вимоги до ІС та її цінності. Відмінність від базового підходу обумовлюється обсягом робіт та подробицями, які можуть бути зібрані протягом процесу оцінювання. Нині є чотири основних аспекти, на які спрямований засіб безпеки: впливи, загрози, вразливості та ризики самі по собі. Способи, якими засоби безпеки можна направляти на ці аспекти, такі:

1) загрози – засоби безпеки можуть зменшити ймовірність виникнення загрози (наприклад, розглянемо загрозу втрати даних через помилки користувача, тоді навчальний курс для користувачів зменшить кількість цих помилок), чи, у випадку зловмисного нападу, вони можуть спинити його через збільшення технічної складності успішної атаки;

2) вразливість – засоби безпеки можуть усунути вразливість чи зробити її менш серйозною приклад, якщо внутрішня мережа, що з’єднана із зовнішньою мережею,

вразлива до несанкціонованого доступу, то реалізація відповідного брандмауера зробить з'єднання менш вразливим, а роз'єднання усуне цю вразливість);

3) вплив – засоби безпеки можуть зменшити чи усунути вплив (якщо зловмисний вплив являє собою недоступність інформації, він зменшується через створення копій інформації, які надійно зберігаються в іншому місці, та готовність до активування плану неперервності бізнесу). Добре організований облік і аналізування журналів аудиту та засобів сигналізації може допомогти ранньому виявленню інциденту та знизити зловмисний вплив на бізнес.

Як і де використовують засіб безпеки, може бути суттєва різниця від тієї користі, яку отримано завдяки його запровадженню. Дуже часто, загрози можуть використовувати більше ніж одну вразливість. Тому, якщо засіб безпеки використовують, щоб запобігти виникненню такої загрози, він може бути спрямованим на декілька вразливостей одночасно. Також вірно і зворотне – засіб безпеки, що захищає вразливість, може бути спрямованим на декілька безпек. Ці переваги слід розглядати, за можливості, під час вибору засобів безпеки передусім при детальному підході. Отримані переваги потрібно документувати з тим, щоб мати повноту вимог безпеки, яким задовольняє будь-який засіб безпеки.

Політика безпеки – це якісний або якісно-кількісний опис властивостей захищеності в термінах, що представляють ІС (рис. 2.4). Опис ПБ повинен включати або враховувати властивості загрози, об'єкта атаки та каналу дії.

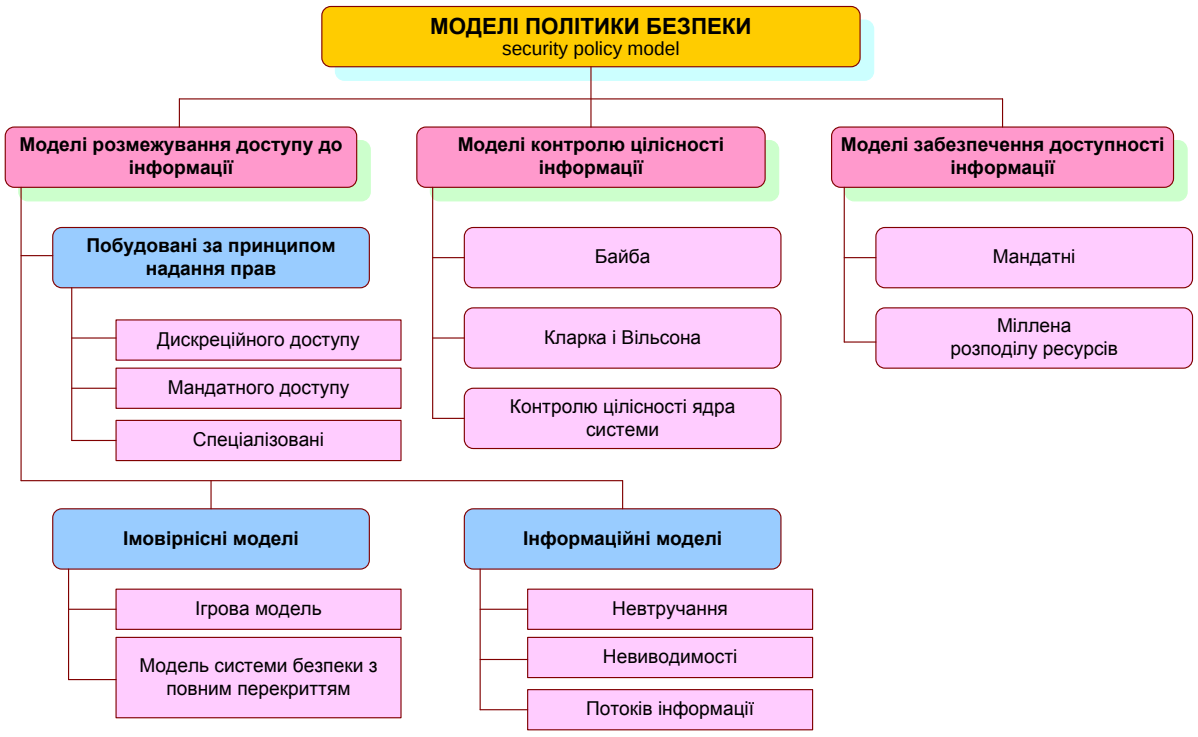


Рис. 2.4. Класифікація моделей безпеки за типами загроз

Політика безпеки є базовим документом в організації. Для забезпечення зручності формування та змін в організаційно-нормативній базі компанії, як правило формується система ієрархічно підпорядкованих документів (рис. 2.5).

Термін «політика безпеки» може бути застосований до організації, ІС, операційної системи (ОС), послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз тощо. Чим менший об'єкт, щодо якого вживається цей термін, тим конкретніші й формальніші стають правила.

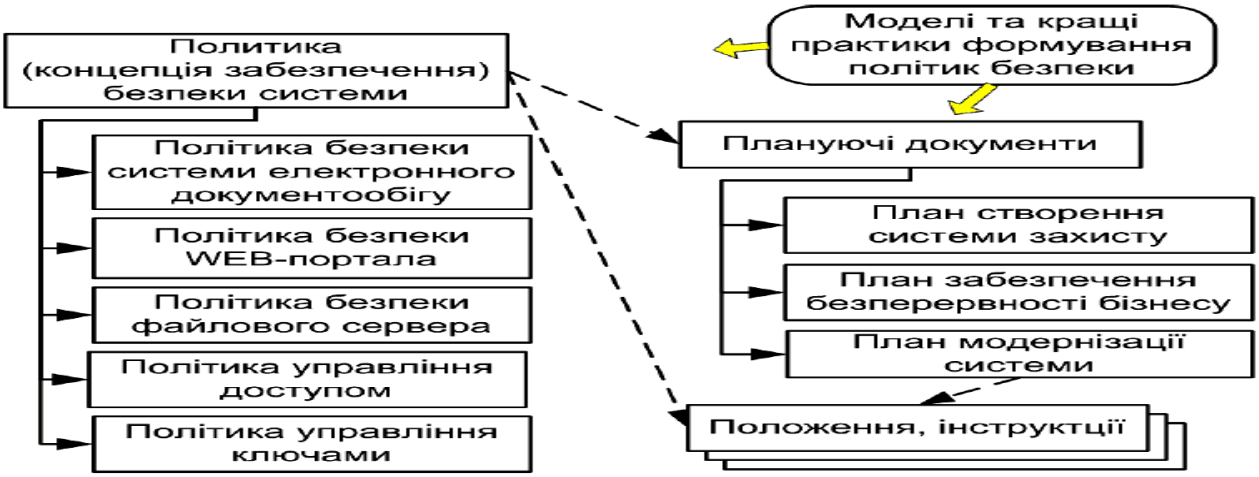


Рис. 2.5. Система документів, що забезпечують реалізацію політики безпеки

Політика інформаційної безпеки є частиною загальної ПБ організації і може успадковувати, зокрема, положення державної політики у сфері захисту інформації. Під нею слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації та спрямовані на захист такої інформації від певних внутрішніх і зовнішніх загроз. Побудова ПІБ передбачає виконання таких кроків:

- визначення структури цінностей і проведення аналіз ризику інформації;
- визначення правил для будь-якого процесу користування певним видом доступу до елементів інформації, які мають певну оцінку цінностей.

ПІБ може бути викладена як на описовому рівні, так і за допомогою певної формальної мови. Вона є необхідною (а іноді й достатньою) умовою безпеки системи. Формальний вираз політики безпеки називають моделлю ПІБ. Основна мета створення ПІБ й опису її у вигляді формальної моделі – визначення умов, яким має підпорядковуватися поведінка системи, вироблення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при додержанні встановлених правил і обмежень. Серед моделей ПІБ найвідомішими є дискреційна, мандатна та рольова моделі. Загальний підхід щодо їх формування полягає в поділі множини сутностей, що становлять систему, на множини суб'єктів і об'єктів (у різних моделях визначення понять «об'єкт» і «суб'єкт» можуть істотно відрізнятися). Взаємодії в системі моделюються встановленням відношень певного типу між суб'єктами та об'єктами. Множина типів відношень визначається у вигляді набору операцій, які суб'єкти можуть здійснювати над об'єктами.

Усі операції в системі контролюються і забороняються або дозволяються відповідно до правил ПІБ. При цьому власне сама ПІБ задається у вигляді правил, відповідно до яких мають виконуватися всі взаємодії між суб'єктами та об'єктами. Взаємодії, що призводять до порушень цих правил, припиняються засобами контролю доступу й не можуть бути здійснені.

Дискреційна модель політики інформаційної безпеки

Основою дискреційної політики інформаційної безпеки (ДПІБ) є дискреційний механізм управління доступом (Discretionary Access Control - DAC). Він визначається такими властивостями:

- усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на основі деякого зовнішнього відносно системи правила і реалізуються шляхом безпосереднього звертання суб'єктів до об'єктів на основі певних атрибутів доступу.

Для реалізації такого механізму в системі має бути:

- забезпечено контрольований доступ ідентифікованих суб'єктів до об'єктів;
- задано явне і однозначне перерахування допустимих типів доступів;
- реалізовано механізм управління, який втілює дискреційні правила доступу та обмежує розповсюдження прав на доступ;
- забезпечено управління доступом для кожної пари суб'єкт-об'єкт;
- забезпечено можливість санкціонованої зміни як правил та прав розмежування доступу, так і списків користувачів та об'єктів.

Дискреційна політика інформаційної безпеки реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту. Матриця доступів (рис. 2.6) – це матриця розмірності S*O, у котрій рядки відповідають суб'єктам, а стовпці – об'єктам. При цьому кожен елемент матриці доступів M[s,o] визначає права доступу суб'єкта до об'єкту.

Рис. 2.6. Матриця доступу дискреційної політики безпеки

Існує декілька варіантів завдання матриці доступу:

- листи можливостей (privilege list, profile): для кожного суб'єкта створюється лист (файл) усіх об'єктів, до якого він має доступ;
- листи контролю доступу (access control list – ACE): для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до нього.

Найбільш відомими модель ДПІБ є модель Харрісона-Руссо-Ульмана (рис. 2.7) та модель Take-Grant.

У першій з них ІС з дискреційним управлінням доступом описується певною кількістю матриць доступів, кожна з яких відповідає стану системи, і командами перетворення матриць доступів. Кожна з команд задається певною кількістю параметрів, умовою виконання і кінцевої послідовністю примітивних операторів, перетворюючих матрицю доступів. Застосування команди переводить систему із стану в подальший стан. У моделі ХРУ аналізуються умови, при виконанні яких можлива перевірка безпеки системи. Методом представлення даних є матриця доступу. Метою моделювання є представлення прав доступу.

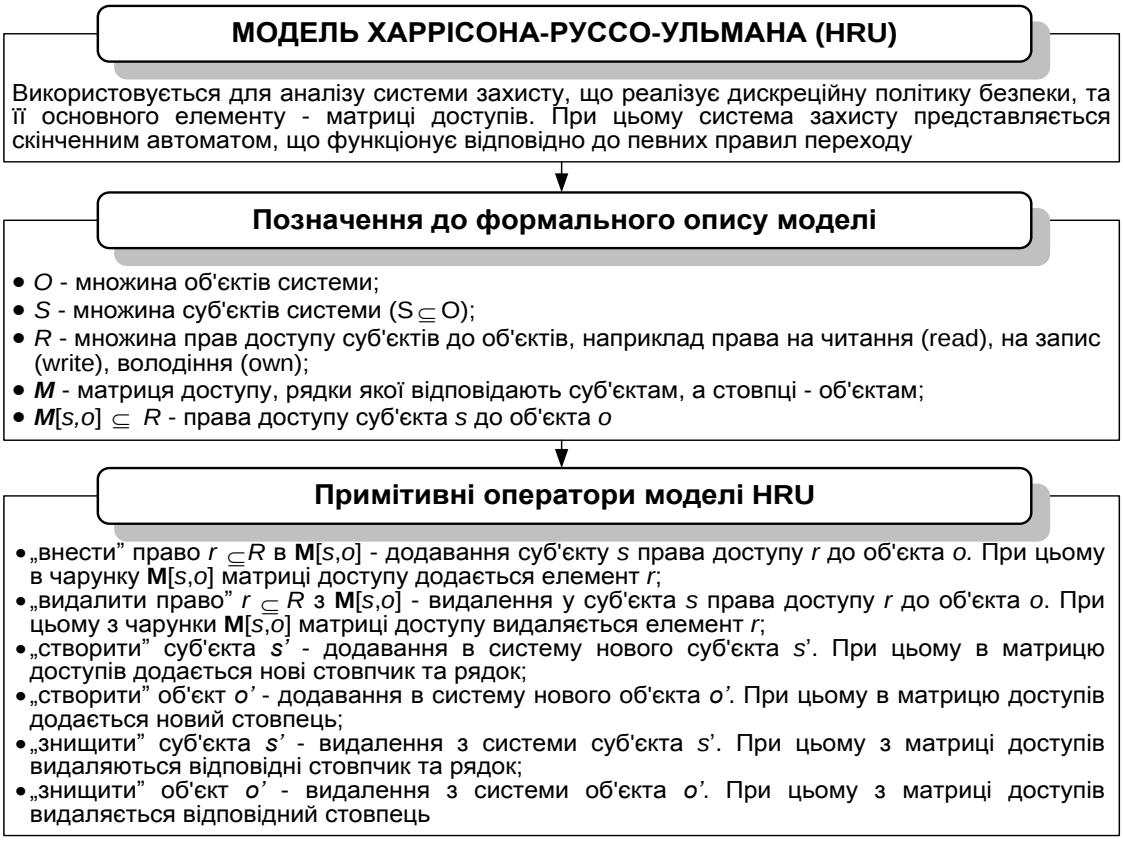


Рис. 2.7. Модель Харрісона-Руссо-Ульмана –модель дискреціного доступу

У моделі Take-Grant (рис. 2.8) умови передачі прав доступу та реалізації інформаційних потоків розглядаються з використанням графів доступів, що дозволяє домогтися більшої наочності досліджуваних положень моделі.

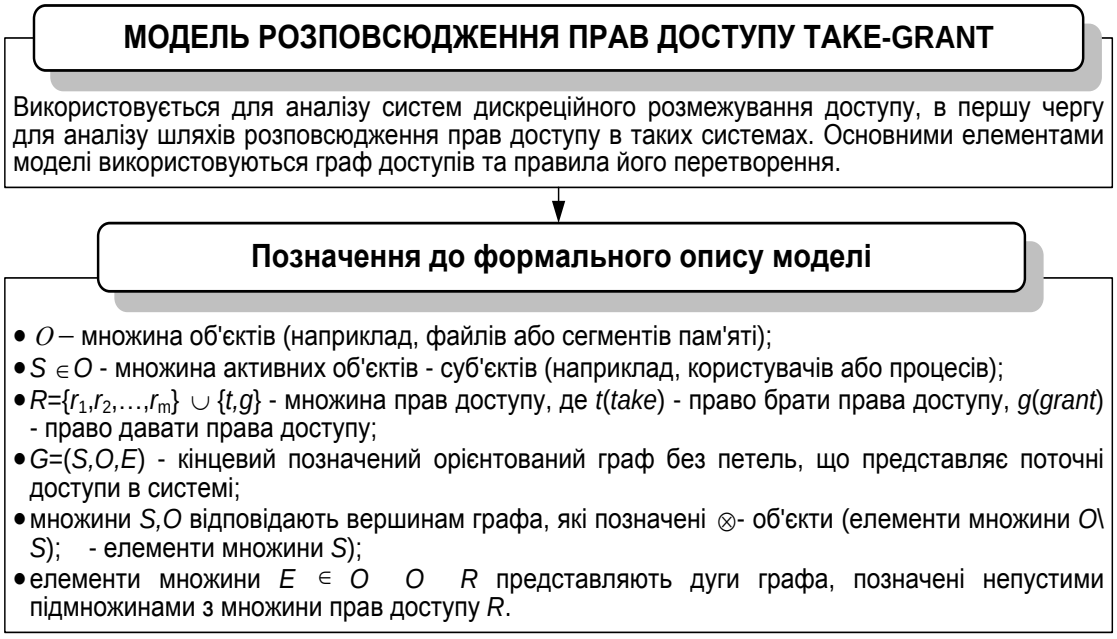


Рис. 2.8. Модель *Take-Grant* –модель розповсюдження прав доступу

Модель Take-Grant вивчається в два етапи. На першому етапі розглядається класична модель Take-Grant, в якій аналізуються алгоритмічно перевіряються умови передачі прав доступу. На другому етапі розглядається розширена модель Take-Grant, в якій аналізуються умови реалізації в комп'ютерних системах інформаційних потоків. Ціль

моделі - дати відповідь на питання про можливості одержання прав доступу суб'єктом системи на об'єкт у стані, описаному графом доступів. У цей час модель Take-Grant одержала продовження як розширена модель Take-Grant , у якій розглядаються шляхи виникнення інформаційних потоків у системах з дискреційним розмежуванням доступу. Позначимо елементи моделі: O – множина об'єктів, S – множина суб'єктів, R = {r1, r2, r3, r4, ..., rn } U {t,g} – множина прав доступу, де t – право брати, g – право давати. G = (S, O, E) – кінцевий граф. У класичній моделі Take-Grant описуються чотири де-юре правила перетворень графів доступів (табл. 2.2). Методом представлення даних для даної моделі є граф доступу. Метою моделювання є аналіз шляхів поширення прав доступу.

Таблиця 2.2

Правила перетворень прав доступу

Правила де-юре Take-Grant	**Умови**	**Результативний стан системи G'=(S',O',E')**
"брати" take(б,x,y,z)	$x \in S$, $(x,y,t) \in E$, $(y,x,в) \in E$, $x \neq z$, $б \subseteq в$	S'=S, O'=O, E'=E $\cup$ {(x,z,б)}
"давати" grant(б,x,y,z)	$x \in S$, (x,y,g) E, $(x,z,в) \in E$, $x \neq z$, $б \subseteq в$	S'=S, O'=O, E'=E $\cup$ {(y,z,б)}
"створити" create(в,x,y)	$x \in S$, $y \notin O$	O'=O $\cup$ {y}, S'=S $\cup$ {y} , якщо y суб'єкт, E'=E $\cup$ {(x,y,в)}
"видалити" remote (б,x,y)	$x \in S$, $y \in O$, $(x,y,в) \in E$, $б \subseteq в$	S'=S, O'=O, E'=E\{(x,z,б)}

До переваг цих та інших моделей ДПІБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлений той факт, що більшість поширених сьогодні захищених ІС забезпечують виконання положень ДПІБ. Крім того, при її реалізації досягається велика економія пам'яті, оскільки матриця доступів звичайно буває дуже розрядженою. Однак багатьох проблем захисту ця політика розв'язати не може. Найбільш суттєвими серед них є:

- нездатність витримати атаки із застосуванням "троянського коня";
- неспроможність заздалегідь задати перелік усіх суб'єктів і об'єктів з метою автоматичного визначення прав;
- неспроможність забезпечити контроль розповсюдження прав доступу;
- нездатність визначити правила розповсюдження прав доступу та провести аналіз їх впливу на безпеку ІС.

Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати якісну і чітку систему захисту інформації в інформаційній системі.

Мандатна модель політики інформаційної безпеки

Основу мандатної (повноважної) політики інформаційної безпеки (МПІБ) становить мандатне управління доступом (Mandatory Access Control – MAC). Принципи мандатного управління:

- всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
- у системі має бути визначено лінійно упорядкований набір міток чутливості;
- кожному об'єкту системи має бути присвоєна мітку чутливості (секретності), яка визначає цінність інформації, що міститься в ньому;
- кожному суб'єкту системи має бути присвоєна мітка чутливості (секретності), яка визначає рівень довіри до нього в ІС й дорівнює максимальному рівню чутливості об'єктів, до яких цьому суб'єкту дозволений доступ (називається рівнем допуску);
- право доступу суб'єкта до об'єкта визначається шляхом порівняння їхніх міток.

Для цього в системі повинен бути реалізований:

- процес запиту і отримання класифікаційних міток;
- мандатний принцип контролю зчитування і записування
- механізм санкціонованої зміни як правил та прав розмежування доступу, так і списків користувачів та об'єктів;
- диспетчер доступу (звернень), тобто засіб, що контролює усі звернення, а також розмежовує доступ відповідно до заданого принципу розмежування.

Основна **мета** МПІБ – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в ІС інформаційних каналів згори вниз. Саме поняття решітки цінностей L і поняття інформаційного потоку є основою мандатної політики інформаційної безпеки.

Цінність інформаційних об'єктів (або їх мітки рівня секретності) часто дуже важко визначити. Однак досвід показує, що в будь-якій ІС майже завжди для будь-якої пари об'єктів X та Y можна сказати, який з них більш цінний. Визначення цінності об'єктів для МПІБ можна здійснювати шляхом їх порівняння. Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція c(X) (тобто, відображення $\{c: O \to L\}$), яка дозволяє для будь-яких об'єктів X і Y сказати, що коли Y більш цінний об'єкт, ніж X, то $c(Y) > c(X)$. І навпаки, якщо $c(Y) > c(X)$, то Y - більш цінний об'єкт, ніж X.

Означення. МПІБ вважає інформаційний потік $X \to Y$ дозволеним тоді і тільки тоді, коли $c(Y) > c(X)$ в решітці L. Тобто, потік інформації від X до Y дозволяється, якщо $c(X) < c(Y)$, і не дозволяється, якщо $c(X) > c(Y)$.

Визначення. У системі з двома доступами r і w МПІБ визначається такими

правилами доступу: $X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y)$, та $X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y)$.

Отже, МПІБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені за дуже простою умовою ─ значенням наведеної функції. МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю.

Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, організується так: монітор звернень порівнює мітки рівня секретності кожного об'єкта з мітками рівня доступу суб'єкта. За результатом порівняння міток приймається рішення про допуск. Найчастіше МПІБ описують у термінах, поняттях і визначеннях властивостей моделі Bell-LaPadula (рис. 2.9).

Модель призначена для управління суб'єктами, тобто активними процесами, що запитують доступ до інформації, і об'єктами, тобто файлами, поданнями, записами, полями або іншими сутностями даної інформаційної моделі. В моделі об'єкти піддаються класифікації, а кожен суб'єкт зараховується до одного з рівнів допуску до класів об'єктів. Класи й рівні допуску спільно називаються класами або рівнями доступу.

Клас доступу складається з двох компонентів. Перший з них – це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій, які можуть ставитися до будь-якого рівня ієрархії, своєрідний опис рівня ієрархії. Так, наприклад, у військових відомствах США застосовується наступна ієрархія класів (зверху вниз): абсолютно секретно; секретно; конфіденційно; без грифа таємності. Другий компонент міг би, наприклад, приймати значення з наступного списку: тільки з опуском по ядерній зброї; не для іноземних урядів; – не для підрядників.

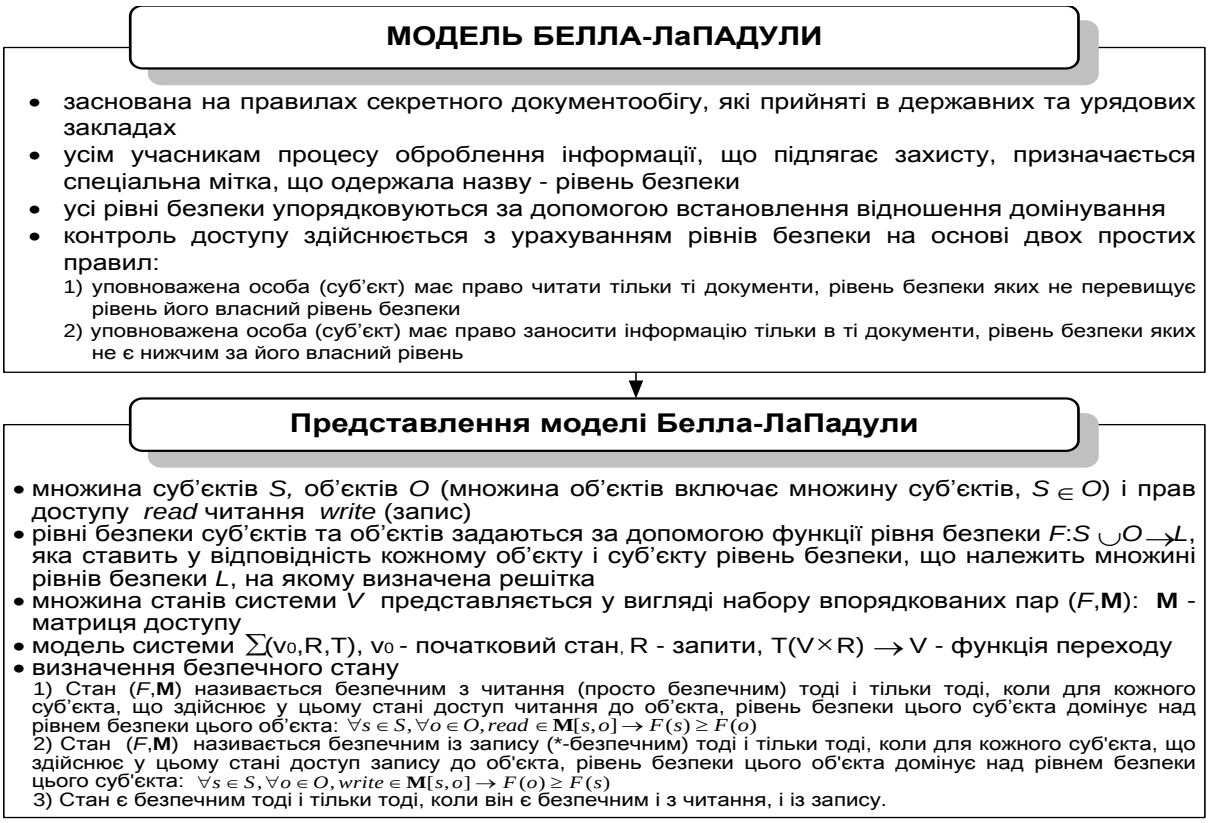


Рис. 2.9. Мандатна модель управління доступом – модель Белла-ЛаПадули

Інший приклад відноситься до приватної компанії, де можливі такі рівні ієрархії (зверху вниз): секретно; для обмеженого поширення; конфіденційно; для службового користування; для необмеженого поширення. Другий компонент для тієї ж компанії міг би включати такі категорії:не для субпідрядників; фінансові дані корпорації; дані по зарплаті.

Ясно, що можна визначити матрицю взаємозв'язків між ієрархічними й неієрархічними компонентами. Наприклад, якщо деякий об'єкт класифікований як зовсім секретний, але йому не приписаний ніякий неієрархічний компонент, то він може надаватися іноземним урядам. У той же час секретний об'єкт може мати категорію "не для іноземних урядів", отже не повинен їм надаватися. Однак у моделі Белла-ЛаПадули створюються "ґрати", де неієрархічні компоненти кожного рівня ієрархії автоматично приписуються до наступного більш високого рівня ієрархії (так назване "зворотне спадкування"). Також існує правило що дозволяє суб'єктові мати доступ на запис до об'єкта тільки в тому випадку, якщо рівень допуску цього суб'єкта такий же або більше низький, чим клас об'єкта - операнда операції запису. Це означає, що інформація, що належить якому-небудь рівню, ніколи не може бути записана в який-небудь об'єкт, що має більше низький рівень, ніж її джерело, оскільки це могло б потенційно привести по необережності до руйнування класифікації інформації в розглянутій системі. Методом представлення даних є визначення двох компонентів. Перший з них – це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій. Мета моделювання є управління суб'єктами, тобто активними процесами, що запитують доступ до інформації. Основна теорема безпеки Белла-ЛаПадули приведена на рис. 2.10.

Система $\sum(v_0, R, T)$ є безпечною тоді і тільки тоді, коли:
а) початковий стан v_0 безпечний і
б) для будь-якого стану v, який досягається з v_0 шляхом застосування скінченної послідовності запитів з R таких, що $T(v,r)=v^*$, $v=(F,M)$ і $v^*=(F^*,M^*)$для кожного $s \in S$ і $o \in O$ виконуються наступні умови:

1) якщо $read \in \mathbf{M}^*[s,o]$ і $read \notin \mathbf{M}[s,o]$, то $F^*(s) \geq F^*(o)$;
2) якщо $read \in \mathbf{M}[s,o]$ і $F^*(s) < F^*(o)$, то $read \notin \mathbf{M}^*[s,o]$;
3) якщо $write \in \mathbf{M}^*[s,o]$ і $write \notin \mathbf{M}[s,o]$, то $F^*(o) \geq F^*(s)$;
4) якщо $write \in \mathbf{M}[s,o]$ і $F^*(o) < F^*(s)$, то $write \notin \mathbf{M}^*[s,o]$.

Рис. 2.10. Основна теорема безпеки Белла-ЛаПадули

До переваг цієї та інших моделей МПІБ можна віднести високий ступінь надійності, прості та ясні для розуміння розробниками і користувачами правила, стійкість до атак типу «троянський кінь», можливість точного математичного доказу того, що дана система в заданих умовах підтримує ПІБ. Недоліком мандатної (повноважної) політики інформаційної безпеки є виняткова складність для практичної реалізації і значні вимоги до ресурсів обчислювальної системи. Тим не менш МПІБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не розв'язуються або розв'язуються частково, як побічний результат захисту секретності.

Рольова модель політики інформаційної безпеки

Рольову політику інформаційної безпеки (РПІБ - Role Base Access Control) не можна віднести ані до дискреційної, ані до мандатної, тому що управління доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель (рис. 8) є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПІБ, і жорсткістю правил контролю доступу, що притаманна МПІБ.

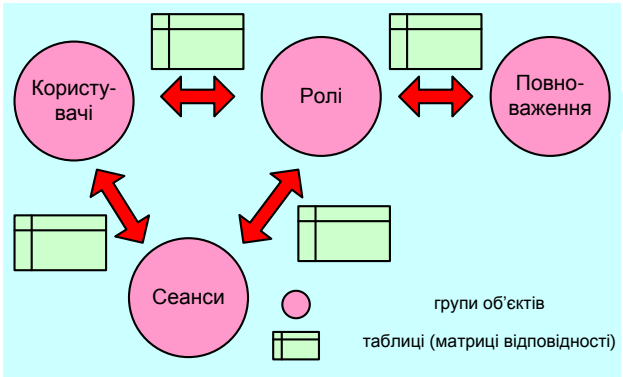


Рис. 2.11. Рольова політика безпеки

У РПІБ класичне поняття суб'єкт заміщується поняттями користувач і роль. Користувач – це людина, яка працює з системою і виконує певні службові обов'язки. Роль – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності. РПІБ застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя. Справді, по суті, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди виконують певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю. Тому цілком логічно здійснювати управління доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати

розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Наприклад, у реальній системі обробки інформації системний адміністратор, менеджер баз даних і прості користувачі. У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів - один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу.

Принципи рольового управління:

- усі суб'єкти і об'єкти повинні бути однозначно ідентифікованими;
- у системі має бути визначено набір ролей у системі;
- кожній ролі має бути встановлено певний обсяг повноважень;
- доступ суб'єктів до об'єктів має здійснюватися на підставі певних правил в рамках певної ролі.

Введення ролей призводить до двоетапної організації системи розмежування доступу. Перш за все створення ролей і визначення їх повноважень (прав доступу до об'єктів) й, по-друге, призначення ролей користувачам системи. Відповідно формальні специфікації рольових моделей повинні регламентувати тим чи іншим способом, точніше в рамках тієї чи іншої політики, і визначення повноважень ролям і призначення ролей користувачам. Управління доступом в рольових системах вимагає розбиття процесу функціонування системи та роботи користувача на сеанси, в кожному з яких, у свою чергу, виділяється дві фази:

- авторизація в даному сеансі користувача з однієї або декількома дозволеними (призначеними на другому етапі організації доступу) для нього ролями;
- дозвіл або заборона суб'єктам користувача доступу до об'єктів системи в рамках повноважень відповідних ролей, з котрими авторизований в даному сеансі користувач.

Неважко побачити, що рольові моделі поєднують мандатний підхід до організації доступу через певну агрегацію суб'єктів та об'єктів доступу, і тим самим забезпечують жорсткість правил розмежування доступу, і дискреційний підхід, що забезпечує гнучкість в налаштуванні системи розмежування доступу на конкретні функціонально-організаційні процеси предметної області ІС. Дані особливості рольової політики дозволяють будувати системи розмежування доступу з хорошою керованістю в складних системах з великою кількістю користувачів та об'єктів, і тому знаходять широке застосування в практичних системах.

У базовій моделі рольового розмежування прав доступу визначаються такі множини: U – множина користувачів, R – множина ролей, P – множина повноважень на доступ до об'єктів, що може бути подана у вигляді матриці доступу, S – множина сеансів роботи користувача із системою. Множина повноважень P у загальному вигляді задається спеціальними механізмами, що об'єднують операції доступу та об'єкти доступу, наприклад, запитами на обробку даних у СУБД, або іншими іменованими процедурами обробки даних, в тому числі можливо високого логічного рівня.

Для названих множин визначають такі відношення:

- $PA \subseteq P \times R$ – відображає множину повноважень на множину ролей, встановлюючи для кожної ролі набір наданих їй повноважень
- $UA \subseteq U \times R$ – відображає множину користувачів на множину ролей, встановлюючи

для кожного користувача набір доступних йому ролей.

Відображення P*R і U*R забезпечують перший і другий етапи процесів організації системи рольового доступу. При цьому відображення U*R може реалізовуватися механізмами однією з базових політик розмежування доступу - матрицею "Користувачі-Ролі", або на основі співвідношення ступенів допуску користувачів і грифів конфіденційності ролей, або на основі співвідношення дозволених тематик користувача і тематики ролей.

Управління доступом в ІС здійснюється на основі введення таких функцій:

- user: $S \rightarrow U$ – значенням функції $u = user(s)$ є користувач $u \in U$, що здійснює даний сеанс роботи з системою;

- roles : $S \rightarrow R$ – значенням функції $r = roles(s)$ є набір ролей $r \in R$ з доступних користувачеві u, по яких користувач працює (здійснює доступ) у даному сеансі $s \in S$;

- permissions: $S \rightarrow P$ – значенням функції $p = Fpermissions(s)$ є набір повноважень $p \in P$, доступних за всіма ролям, задіяним користувачем у даному сеансі $s \in S$.

Основне правило (критерій безпеки) рольового доступу визначається наступним чином: система функціонує безпечно, тоді і тільки тоді, коли будь-який користувач $u \in U$, що працює в сеансі $s \in S$, може здійснювати дії (операції, процедури) в рамках повноваження $p \in P$ за умови

$$p \in P, \text{ де } P = permissions(s).$$

З формулювання критерію безпеки моделі РПІБ виходить, що управління доступом здійснюється головним чином не за допомогою призначення повноважень ролям, а шляхом задання відношення UA, яке призначає ролі користувачам, і функції roles, що визначає доступний в сеансі набір ролей. Тому числені інтерпретації рольової моделі відрізняються видом функцій user, roles і permission, а також обмеженнями, що накладаються на відношення PA та UA.

Виходячи з такого можна сформулювати такі основні питання організації рольового доступу:

- скільки і яких ролей може бути призначено для роботи з системою одному користувачеві?

- скільки і які ролі може одночасно задіяти один користувач в одному сеансі роботи з системою?

Ще однією суттєвою обставиною є можливі відносини між ролями, в тому, числі можлива передача (делегування) повноважень і прав від одних ролей іншим ролям. Залежно від особливостей вирішення даних питань виділяють кілька різновидів рольових моделей: з ієрархічною організацією системи ролей; з взаємовиключними на будь-які (всі) сеанси ролями (модель статичного розподілу обов’язків); з взаємовиключними на один сеанс ролями (модель динамічного розподілу обов’язків); з кількісними обмеженнями за ролями; з групуванням ролей і повноважень.

Завдяки гнучкості та широким можливостям РПІБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так вона практично не гарантує безпеку за допомогою формального доказу, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості і зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, але позбавляє систему теоретичної доказової бази (вада). У деяких ситуаціях ця обставина утруднює використання РПІБ, однак, в будь-якому разі, оперувати ролями набагато зручніше ніж суб’єктами (знову перевага), оскільки це більш відповідає розповсюдженим технологіям обробки інформації, які передбачають розподіл обов’язків і сфер відповідальності між користувачами.

Крім того, РПІБ може використовуватися одночасно з іншими ПІБ, коли повноваження ролей, що призначаються користувачам, контролюється ДПІБ або МПІБ,

що дозволяє будувати багаторівневі схеми контролю доступу. Результати порівняння ДПІБ, МПІД та РПІБ наведені у таблиці 2.3.

Таблиця 2.3

Порівняння ДПІБ, МПІД та РПІБ

Характеристика	ДПБ	МПБ	РПБ
Орієнтація	Безпосередній доступ суб'єктів до об'єктів	Інформаційні потоки	Організаційні ролі
Підтримка системою захисту	Децентралізована	Централізована	Централізована
Адміністративна модель	Орієнтована на об'єкти і ресурси	Утруднення при відображенні на адміністративну модель управління доступом	Відносно легко відображається на адміністративну модель управління доступом
Розуміння розробниками	Складна	Проста	Проста
Ступінь надійності	Низька	Висока	Висока
Реалізація	Проста	Складна	Проста
Можливість формального доведення	Дає можливість доведення нерозв'язуваності задачі захищеності	Дає можливість доведення задачі захищеності	Не дає можливості доведення задачі захищеності

2.2. Документи, що забезпечують реалізацію політику безпеки інформації

Основні документи, які враховуються під час формування політики безпеки:

- НД ТЗІ: 1.1-002-99 "Загальні положення", 1.4-001-00 "Методичні вказівки щодо розроблення ТЗ на КСЗІ", 2.5-004-99 "Критерії оцінки", 2.5-005-99 "Класифікація АС та стандартні ФП", 3.7-001-99 "Положення про службу захисту".

- Міжнародні стандарти: ISO/IEC 13335 "Management of information and communications technology security", ISO/IEC "17799 Code of Practice for information security management", ISO/IEC 15408 "Common criteria for Information Technology Security Evaluation".

- Документи інших держав: NIST 800-12 "An Introduction to Computer Security: The NIST Handbook", NIST 800-14 "Generally Accepted Principles and Practices for Securing Information Technology Systems", NIST 800-18 "Guide for Developing Security Plans for Information Technology Systems".

Основні розділи, які можуть входити до складу політики інформаційної безпеки:

- загальний, у якому визначається відношення керівництва АС (організації) до проблеми безпеки інформації;

- організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки та ін.);

- класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в АС, та необхідний рівень їхнього захисту;

- розділ, у якому визначаються ПРД до інформації;
- розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;
- розділ, у якому висвітлюються питання фізичного захисту;
- розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;
- розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;
- розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування АС;
- юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

Система документів, що забезпечують реалізацію політики безпеки

Політика безпеки є базовим документом в організації. Для забезпечення зручності формування та змін в організаційно-нормативній базі компанії, як правило формується **система** ієрархічно підпорядкованих документів (рис. 2.12):

- різного рангу політик;
- планів;
- інструкцій та правил;
- кодексів;
- та ін.

Приклад формування системи документів для ІС в США, розроблений NIST наведений на рис. 2.13.

План захисту (security plan) — документ, що визначає порядок побудови та експлуатації СЗ. Основними питаннями, що розглядаються в ньому є (в тому числі з урахуванням існуючих документів):

1) завдання захисту інформації в АС;
2) класифікація критичної інформації;
3) опис компонентів АС та технологій оброблення інформації;
4) опис загроз;
5) порядок формування та коригування ПБ;
6) порядок та шляхи створення КСЗІ;
7) порядок введення в дію КСЗІ;
8) порядок та основні заходи з підтримки КСЗІ;
9) відповідальність персоналу.

2.3. Гарантії правильності забезпечення політики безпеки інформації

Гарантії — друга складова оцінки ефективності реалізації захисних функцій.

Рівень гарантій свідчить про ступень впевненості в правильності реалізації в СЗ встановленої для обчислювальної (автоматизованої) системи політики безпеки.

Необхідність підвищення рівня гарантій призводить до необхідності більш глибокого та детального аналізу системи, що створюється чи створена.

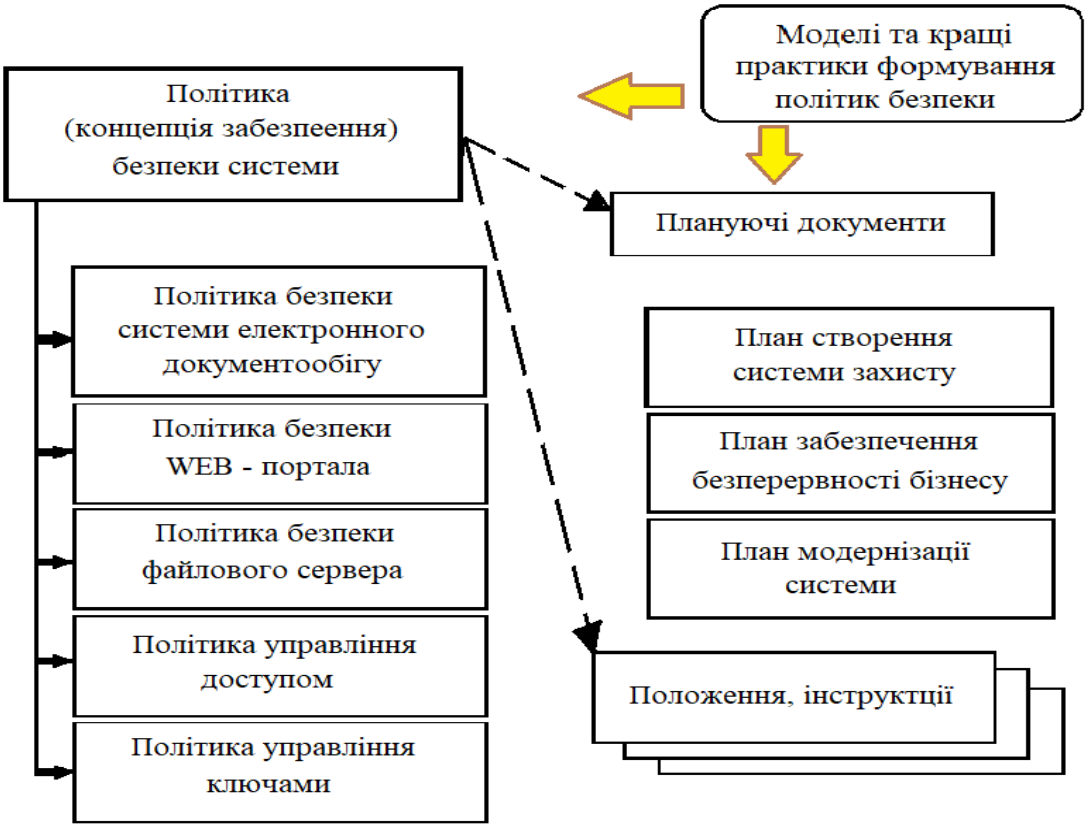


Рис. 2.12. Структура організаційно-нормативних документів з забезпечення захисту

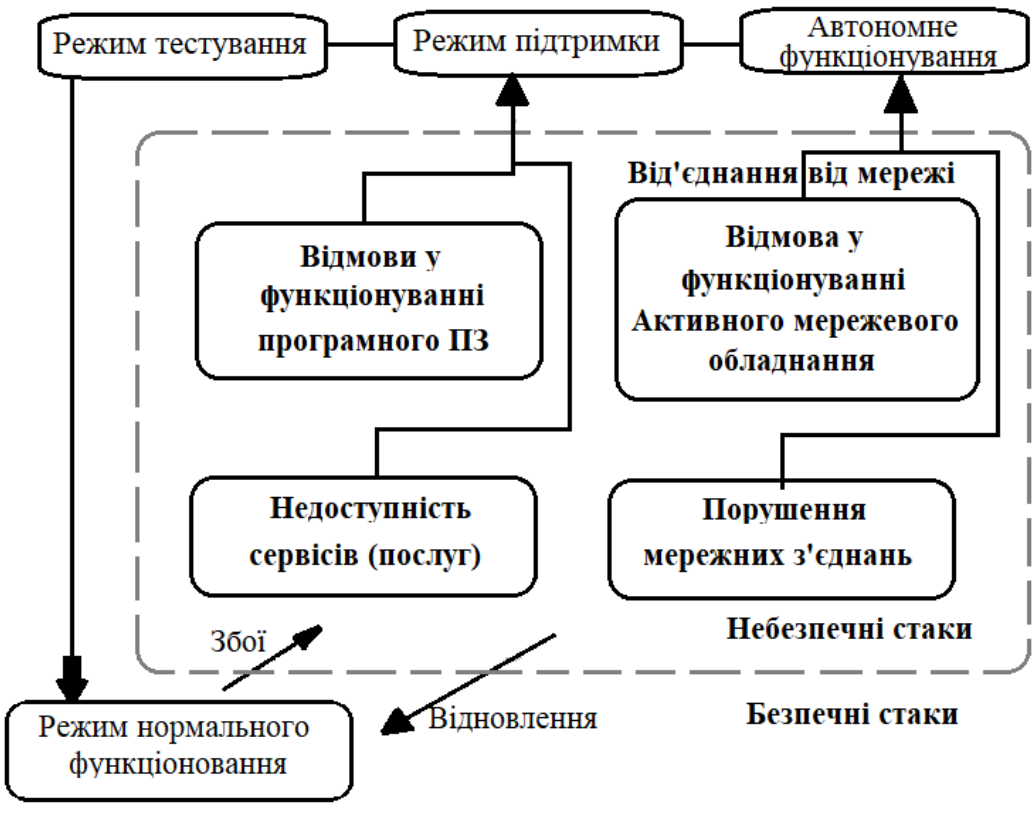


Рис. 2.13. Приклад визначення станів функціонування системи

Контрольні запитання для самооцінки рівня знань

1. Яким чином доцільно оцінювати можливий збиток від інцидентів ІБ?
2. Назвіть регулятори інформаційної безпеки.
3. Класифікація моделей безпеки за типами загроз.
4. Визначення терміну «політика інформаційної безпеки».
5. Система документів, що забезпечують реалізацію політики безпеки.
6. Сутність дискреційної моделі політики інформаційної безпеки.
7. Які найбільш відомі моделі дискреційної політики інформаційної безпеки Ви знаєте?
8. Сутність мандатної моделі політики інформаційної безпеки.
9. Яку найбільш відому модель мандатної політики інформаційної безпеки Ви знаєте?
10. Сутність рольової моделі політики інформаційної безпеки.
11. Порівняння дискреційної, мандатної та рольової політик інформаційної безпеки.
12. Які документи забезпечують реалізацію політику безпеки інформації?
13. Які основні розділи можуть входити до складу політики інформаційної безпеки?
14. Структура організаційно-нормативних документів з забезпечення захисту інформації.
15. Гарантії правильності забезпечення політики безпеки інформації.

Розділ 3

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ПОЛІТИК БЕЗПЕКИ

3.1. Концепція розроблення захищених систем компанії IBM

На думку фахівців IBM, розробка корпоративних керівних документів в області безпеки повинна починатися зі створення політики інформаційної безпеки. При цьому рекомендується використати міжнародний стандарт ISO 17799:2005 і розглядати політику безпеки компанії як складову частину процесу управління інформаційними ризиками (рис. 3.1). Уважається, що розробка політики безпеки відноситься до стратегічних завдань менеджменту компанії, що здатний адекватно оцінити вартість її інформаційних активів і прийняти обґрунтовані рішення зі захисту інформації з урахуванням цілей і завдань бізнесу.

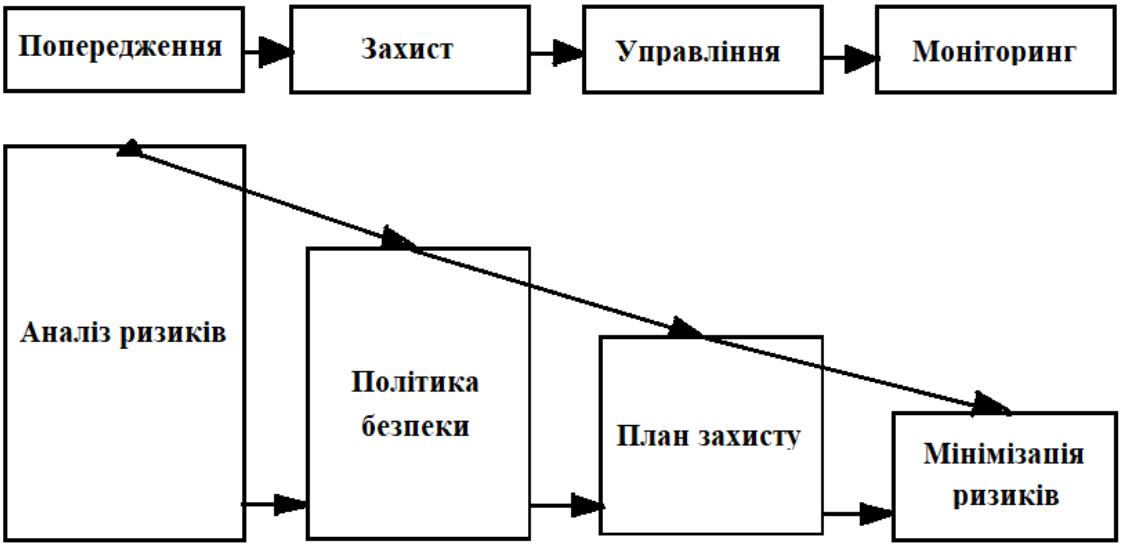


Рис. 3.1. Процес розробки політики безпеки компанії

Компанія IBM виділяє наступні основні етапи розробки політики безпеки:

- визначення інформаційних ризиків компанії, здатних завдати максимальної шкоди, для подальшої розробки процедур і заходів із попередження їхнього виникнення;
- розробка політики безпеки, що описує заходи захисту інформаційних активів, адекватні цілям і завданням бізнесу;
- прийняття планів дій у надзвичайних ситуаціях для зменшення збитку у випадках, коли обрані заходи захисту не змогли запобігти інцидентам в області безпеки;
- оцінка залишкових інформаційних ризиків й ухвалення рішення про додаткові інвестиції в засоби й заходи безпеки. Рішення приймає керівництво на основі аналізу залишкових ризиків.

Політика безпеки компанії, з погляду IBM, повинна містити явну відповідь на питання "Що потрібно захистити?". Дійсно, якщо керівництво компанії розуміє, що необхідно захистити, які інформаційні ризики й загрози інформаційним активам компанії існують, тоді можна приступати до створення ефективної політики інформаційної безпеки. При цьому політика безпеки є першим стратегічним документом, якому необхідно створити і який містить мінімум технічних деталей, будучи настільки статичним (незмінним), наскільки можливо. Передбачається, що політика безпеки компанії буде містити:

- визначення інформаційної безпеки з описом позиції й намірів керівництва компанії по її забезпеченню;

• опис вимог по безпеці, у які входить:
  - відповідність вимогам законодавства й контрактних зобов'язань;
  - навчання питанням інформаційної безпеки;
  - попередження й виявлення вірусних атак;
  - планування безперервності бізнесу;
  - визначення ролей й обов'язків по різних аспектах загальної програми інформаційної безпеки;
  - опис вимог і процесу звітності по інцидентах, пов'язаним з інформаційною безпекою;
  - опис процесу підтримки політики безпеки.

• компанія IBM рекомендує виконати наступні дії для розробки ефективної політики безпеки компанії:
  - аналіз бізнесу-стратегії компанії й визначення вимог по інформаційній безпеці;
  - аналіз IT-стратегії, яка витікає з проблем інформаційної безпеки й визначення вимог по інформаційній безпеці;
  - створення політики безпеки, взаємно ув'язаної з бізнес- і IT-стратегіями.

У цьому випадку рекомендується структура, яка керується документами по забезпеченню інформаційної безпеки компанії та може бути представлена в такий спосіб (рис. 3.2).

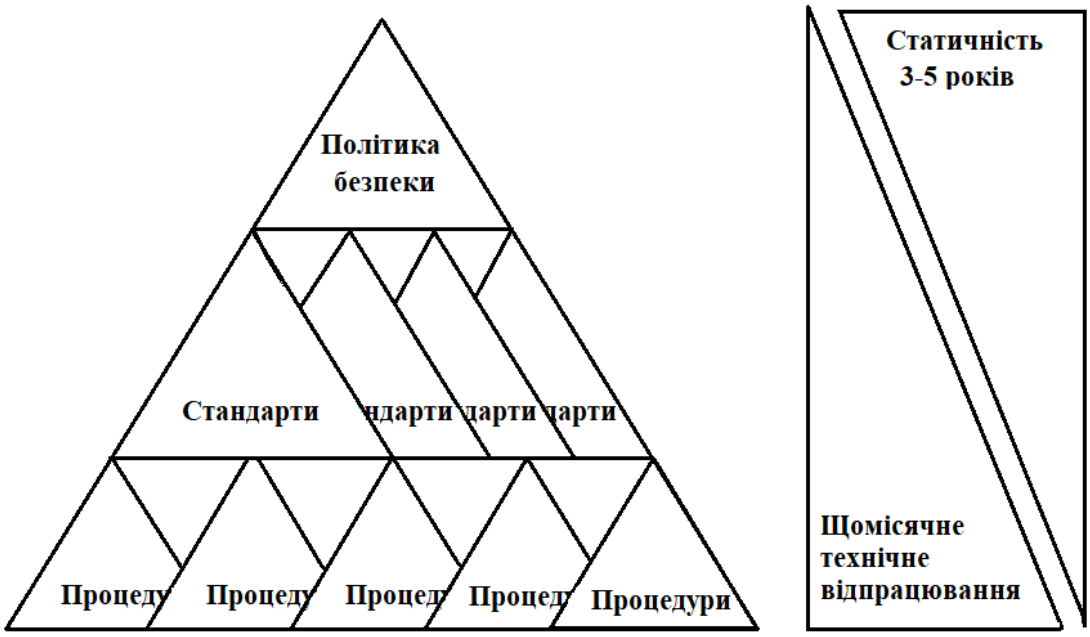


Рис. 3.2. Структура керівних документів по забезпеченню інформаційної безпеки

Після створення корпоративної політики створюється серія стандартів. Під стандартами IBM розуміє документи, які описують порядок застосування корпоративної політики безпеки в термінах автентифікації, авторизації, ідентифікації, контролю доступу й т. ін. Стандарти можуть вимагати частих змін, тому що на них впливають поточні загрози й уразливості інформаційних технологій.

У поданні IBM політики й стандарти безпеки створюються для:
- розробки правил і норм безпеки рівня компанії;
- аналізу інформаційних ризиків і способів їхнього зменшення;
- формалізації способів захисту, які повинні бути реалізовані;
- визначення очікувань із боку компанії й співробітників;

- чіткого визначення процедур безпеки, яким потрібно випливати;
- забезпечення юридичної підтримки у випадку виникнення проблем в області безпеки.

Стандарти реалізуються за допомогою практик й/або процедур. Практики є реалізацією стандартів в операційних системах, додатках й інформаційних системах. У них деталізуються сервиси, установлювані на операційних системах, порядок створення облікових записів і т. ін. Процедури документують процеси запиту й підтвердження доступу до певних сервісів, наприклад VPN.

Розглянемо особливості пропонованого підходу IBM (рис. 3.3) на наступному прикладі:

- проблемна ситуація — співробітники завантажують програмне забезпечення з мережі Інтернет, що приводить до зараження вірусами, а в остаточному підсумку до зменшення продуктивності роботи співробітників компанії;
- у політику безпеки додається рядок — інформаційні ресурси компанії можуть бути використані тільки для виконання службових обов'язків. Політика безпеки доступна для ознайомлення всім співробітникам компанії;
- створюється стандарт безпеки, у якому описується, які сервіси й програмне забезпечення дозволені для використання співробітниками; практика безпеки описує, як настроїти операційну систему відповідно до вимог стандарту безпеки;
- процедура безпеки описує процес запиту й одержання дозволу на використання додаткових сервісів або установку додаткового програмного забезпечення співробітниками;
- установлюються додаткові сервіси для контролю виконання вимог політики безпеки.

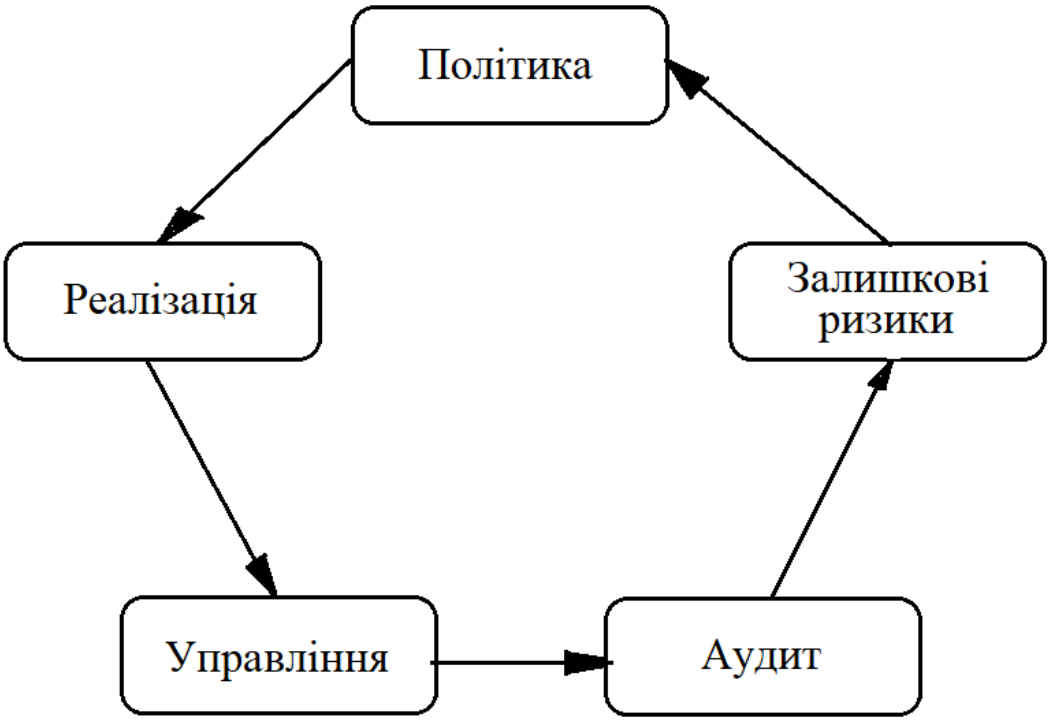


Рис. 3.3. Підхід IBM до розробки документів інформаційної безпеки

3.2. Концепція розроблення захищених систем компанії Microsoft

Компанія Microsoft має складну корпоративну інфраструктуру, що складається з 6 тис. серверів Windows Server 2003 (з них 800 серверів додатків). У штаті компанії працює більше 55 тис. співробітників. Співробітники дуже добре готові технічно, і 95% з них мають адміністраторські права на своїх комп'ютерах. Більш ніж 300 тис. комп'ютерів

компанії розташовані в 400 представництвах по усьому світі, використовується більше 1,6 тис. додатків.

У мережу компанії щодня надходить приблизно 8 млн. поштових повідомлень ззовні, і приблизно 6,5 млн. поштових повідомлень циркулює щодня в мережі самої компанії. У мережу компанії мають доступ 30 тис. партнерів. Унікальна інфраструктура по розробці продуктів, тестуванню й підтримці, вихідний код продуктів вимагають особливого захисту. Щомісяця на мережу компанії здійснюється понад 100 тис. спроби вторгнення. У поштову систему щомісяця надходить понад 125 тис. поштові повідомлення, заражених вірусами (у день приблизно 800 нових вірусів), і 2,4 млн. поштових повідомлень Зі спамом у день.

Обов'язок по забезпеченню інформаційної безпеки в компанії Microsoft покладена на дві групи — Corporate Security Group й Operations and Technology Group.

Компанія Microsoft розробила стратегію безпеки, що складає з 4 основних компонентів:

- місія корпоративної безпеки,
- принципи операційної безпеки,
- модель прийняття рішень, заснована на аналізі ризиків,
- тактичне визначення пріоритетності дій по зменшенню ризиків.

Фундаментом для дизайну, розробки й нормального функціонування захищених систем є принципи безпеки, розділені на кілька категорій (див. табл. 3.1).

Для забезпечення інформаційної безпеки Corporate Security Group використає підхід по управлінню інформаційними ризиками. Під управлінням ризиками тут розуміється процес визначення, оцінки й зменшення ризиків на постійній основі: управління ризиками

Табл. 3.1

Принципи безпеки захищених систем

Категорія	Принцип безпеки
Організаційна Спрямована на отримання підтримки керівництва з управління ризиками та ознайомлення з питаннями безпеки	Управління ризиками відповідно до завдань бізнесу Визначення ролей і обов'язків Інвестиції в дизайн захищеності Забезпечення безпеки операцій
Користувачі і дані Включає автентифікацію, захист даних користувачів, авторизацію	Управління принципом найменших привілеїв Класифікація даних і користувачів Впровадження захисту даних і користувача ідентичності Захист інформації Гарантії цілісності даних Моніторинг гарантій ідентичності Доступність
Розробка додатків і систем Виділена для дизайну і розробки захищених систем	Убудовування безпеки в життєвий цикл Дизайн "багаторівневого захисту" Зменшення поверхні атаки Збереження простоти
Операції і супроводження Об'єднання людей, процесів і технологій для побудови. підтримки і використання захищених систем	План підтримки систем Впровадження захищених конфігурацій Моніторинг і журналізація Практика реагування на інциденти Перевірка процедур відновлення на випадок аварії

безпеки дозволяє знайти розумний баланс між вартістю засобів і мер захисту й вимогами бізнесу.

Модель управління ризиками Corporate Security Group являє собою комбінацію різних підходів, таких, як кількісний аналіз ризиків, аналіз повернення інвестицій у безпеку, якісний аналіз ризиків, а також підходи кращих практик.

Інвестування в процес управління ризиками — із цільною структурою й певними ролями й обов'язками — готовить організацію до визначення пріоритетів, плануванню зменшення загрози й переходу до відбивання або нейтралізації наступної загрози або уразливості. Для найкращого управління ризиками Corporate Security Group треба традиційному підходу по управлінню ризиками, що складається із чотирьох етапів:

- оцінка інформаційних ризиків — виконання методології оцінки ризику для визначення його величини;
- розробка політики безпеки — розробка політики безпеки по зменшенню, відхиленню й попередженню ризиків;
- впровадження засобів захисту — об'єднання співробітників, процесів і технологій для зменшення ризиків, пов'язаних з аналізом співвідношення "ціна — якість";
- аудит безпеки й вимір поточної захищеності — моніторинг, аудит безпеки й вимір захищеності інформаційних систем компанії.

Методологія, використовувана при розробці політики, базується на стандарті ISO 17799:2005 (BS 7799).

Етапи управління інформаційними ризиками

Рекомендована компанією Microsoft політика безпеки містить у собі:

- визначення цілей безпеки;
- важливість забезпечення безпеки;
- визначення необхідного рівня безпеки;
- стандарти безпеки, включаючи стратегії їхнього моніторингу й аудита;
- ролі й відповідальність по забезпеченню безпеки;
- мети й завдання офіцера по безпеці;
- визначення процесів по захисту індивідуальних компонентів архітектури;
- визначення програм навчання питанням безпеки.

Прикладами цілей безпеки, що декларуються, є:

- досягнення максимально можливого рівня якості, надійності й конфіденційності інформації;
- збереження репутації компанії;
- недопущення ушкодження або втрати інформації, процесів,
- власності компанії й забезпечення в такий спосіб безперервної роботи компанії;
- збереження ЦІННОСТІ інформації, інтелектуальної власності й технологічних ресурсів.

Для розробки цілей безпеки створюється комітет з інформаційній безпеці. Комітет складається зі співробітників з досвідом роботи в області безпеки, технічних співробітників і представників інших підрозділів під керівництвом офіцера по безпеці. Комітет вирішує наступні завдання:

- розробка й управління життєвим циклом політики безпеки;
- створення процесів, що забезпечують досягнення цілей безпеки;
- створення процесів і планів по реалізації стандартів, описаних у політику;
- допомога в організації програм ознайомлення з питаннями безпеки;
- консультування персоналу з питань безпеки;
- визначення бюджету й необхідних ресурсів по забезпеченню безпеки.

3.3. Концепція розроблення захищених систем компанії Sun Microsystems

Як уважають в Sun, політика безпеки є необхідною для ефективної організації режиму інформаційної безпеки компанії. Тут під політикою безпеки розуміється стратегічний документ, у якому очікування й вимоги керівництва компанії до організації режиму інформаційної безпеки виражаються в певних вимірних і контрольованих цілях і завданнях. При цьому Sun рекомендує реалізувати підхід "униз", тобто спочатку розробити політику безпеки, а потім приступати до побудови відповідної архітектури корпоративної системи захисту інформації. У противному випадку політика безпеки буде створена співробітниками служби автоматизації довільно. При цьому архітектура корпоративної системи захисту інформації буде розрізненої, витратної й далеко не оптимальною.

Визначення ролей й обов'язків. До розробки політики безпеки рекомендується залучити співробітників таких підрозділів компанії, як:

- управління бізнесом,
- технічне управління,
- відділ захисту інформації,
- департамент управління ризиками,
- департамент системних операцій,
- департамент розробки додатків,

- відділ мережного адміністрування,
- відділ системного адміністрування,
- служба внутрішнього аудита і якості,
- юридичний відділ,
- відділ кадрів.

Структура документів, що рекомендує політика безпеки:

- опис основних цілей і завдань захисту інформації,
- визначення відносини керівництва компанії до політики безпеки,
- обґрунтування шляхів реалізації політики безпеки,
- визначення ролей й обов'язків відповідальних за організацію режиму інформаційної безпеки в компанії,
- визначення необхідних правил і норм безпеки,
- визначення відповідальності за порушення політики,
- визначення порядку перегляду й контролю положень політики безпеки.

Основне призначення політики безпеки

Основне призначення політики безпеки — інформування співробітників і керівництва компанії про існуючі вимоги по захисту інформаційних активів компанії. Політика також визначає механізми й способи, використовувані для досягнення виконання цих вимог. Для цього в політику безпеки повинні бути визначені показники й критерії захищеності активів компанії, відповідно до яких повинні установлюватися й настроюватися засобу захисту. Політика також є основою для наступної розробки стандартів, процедур, регламентів безпеки.

Зв'язок зі стандартами й процедурами безпеки

Політика безпеки містить очікування посібника із забезпечення безпеки, мети й завдання організації режиму інформаційної безпеки. Для того щоб бути практична й здійсненної, політика безпеки повинна реалізовуватися в процедурах, руководствах і стандартах, що забезпечують детальну інтерпретацію положень політики безпеки для співробітників, партнерів і клієнтів компанії. При цьому рекомендується починати розробку стандартів, процедур і руководств безпеки після прийняття політики безпеки й впровадження відповідних механізмів контролю виконання її вимог.

Основні ідеї політики безпеки.

До основних ідей політики безпеки відносяться:

- визначення цінності інформаційних активів; розробка політики безпеки компанії заснована на необхідності захисту коштовних інформаційних активів компанії. Це означає, що потрібно приділити пильна увага категорированию інформаційних ресурсів, визначенню їхніх власників, визначенню критично важливих для компанії інформаційних потоків;
- управління залишковими ризиками; для створення реалістичної політики безпеки компанії необхідно, щоб вона була адекватної цілям і завданням розвитку бізнесу компанії. Для цього потрібно скористатися концепцією управління інформаційними ризиками. У теорії управління фінансами категорія ризику визначається в такий спосіб:

$R = H \times P$,

де H — грошова оцінка збитку в результаті інциденту;

P — імовірність інциденту.

Представимо, наприклад, захист джерела живлення сховища даних деякого комерційного банку. Джерело живлення коштує 10 млн. доларів. Якщо прийняти ймовірність повного руйнування джерела живлення, наприклад, у результаті теракту, як 1:1 000 000 000, то ризик буде дорівнює добутку цих величин і складе всього 1 цент.

Тепер представимо персональний рахунок клієнта, який захищений лише 4-значним PIN-кодом. Імовірність підбора такого коду дорівнює 0,001. Якщо представити, що середня сума на балансі становить 3 тис. доларів, то ризик складе 30 центів. Тобто ризик злому банківського рахунку може бути в 30 разів вище ризику втрати джерела

живлення вартістю 10 млн. доларів.

Варто сказати, що завдання управління ризиками складається не в тім, щоб визначати ризик винятково кількісно з високою точністю й вірогідністю. Тут досить просто розуміння природи ризику й визначення такої метрики ризику, що дозволяє вимірювати, порівнювати, спостерігати й оптимизировать залишкові ризики компанії й тим самим установлювати, наскільки політика безпеки відповідає вимогам бізнесу.

• управління інформаційною безпекою;

Необхідно чітко представляти, що тільки один компонент корпоративної системи захисту інформації (нехай навіть найважливіша) не забезпечить прийнятну безпеку інформаційних активів компанії. Політики безпеки будуть ефективні тільки в контексті цілісної архітектури безпеки, тобто всі системи контролю доступу, межсетевые екрани, криптосистемы, системи управління ключами й інші засоби захисту інформації повинні працювати як єдине ціле.

• обґрунтована довіра, довіра — основа всіх декларацій безпеки компанії. Для довіри потрібно розуміти й приймати основні положення політики безпеки й мати впевненість у тім, що вони відповідають заявленим очікуванням керівництва компанії.

Принципи безпеки

Формулювання принципів забезпечення інформаційної безпеки є першим важливим кроком при розробці політики безпеки, тому що вони визначають сутність організації режиму інформаційної безпеки компанії. До них відносяться принципи:

• відповідальності — відповідальність за забезпечення безпеки інформаційних систем компанії повинна бути явно визначена;

• ознайомлення — власники інформації, користувачі інформаційних систем, а також клієнти й партнери по бізнесі повинні бути проінформовані про правила затвердженої політики безпеки компанії, а також про ступінь відповідальності при роботі з конфіденційною інформацією компанії;

• етики — забезпечення інформаційної безпеки компанії повинне здійснюватися у відповідності зі стандартами етики, застосовними до діяльності компанії;

• комплексності — політики, стандарти, практики й процедури безпеки повинні охоплювати всі рівні забезпечення безпеки: нормативно-методичний, економічний, технологічний, технічний й організаційно-управлінський;

• економічної виправданості — забезпечення безпеки компанії повинне бути економічно виправданим;

• інтеграції — політики, стандарти, практики й процедури безпеки повинні бути скоординовані й інтегровані між собою;

• своєчасності — забезпечення безпеки компанії повинне дозволяти вчасно реагувати на загрози безпеки й парирувати їх;

• перегляду — регулюючі документи в області безпеки компанії повинні періодично переглядатися й доповнюватися;

• демократичності — забезпечення безпеки інформаційних активів компанії повинне здійснюватися відповідно до прийнятих норм демократії;

• сертифікації й акредитації — інформаційні системи компанії й компанія в цілому повинні бути сертифіковані на відповідність вимогам безпеки. Співробітники компанії, відповідальні за організацію режиму інформаційної безпеки, повинні бути сертифіковані й внутрішні накази керівництва компанії допущені до виконання своїх посадових обов'язків;

• відбивання нападу зловмисника — стратегії й тактики забезпечення безпеки, а також відповідні технічні рішення повинні бути адекватні рівню нападу різного роду зловмисників;

• найменших привілеїв — співробітникам компанії повинні бути надані привілеї, необхідні для виконання службових обов'язків, і не більше того;

• поділу привілеїв — привілею співробітників компанії повинні бути розподілені

таким чином, щоб попередити можливість нанесення ними навмисного або ненавмисного збитку критично важливим інформаційним системам компанії;

• безперервності — повинна бути забезпечена необхідна безперервність бізнесу компанії у випадку надзвичайних ситуацій;

• простоти — повинне бути віддане перевага більше простим засобам і технологіям забезпечення безпеки.

Простота політики безпеки

Ключ до успіху політики безпеки — її простота. У зв'язку з тим, що сучасні інформаційні технології, програмне забезпечення й устаткування швидке й постійно вдосконалюються й змінюються, політика безпеки повинна бути незалежна від певних програмних й апаратних рішень. У додавання до цього повинні бути явно описані механізми зміни політики безпеки.

Доведення політики безпеки

Після створення політики безпеки вона повинна бути доведена до відомості співробітників компанії, її партнерів і клієнтів. При цьому бажано доводити політику безпеки через підпис, що підтверджує сам факт ознайомлення з політикою безпеки, а також означаючу, що всі вимоги політики безпеки зрозумілі і їх зобов'язуються виконувати.

Перегляд політики безпеки

Необхідно організувати процес періодичного перегляду політики безпеки для того, щоб її положення не застарівали. У цей процес повинен бути включений механізм внесення змін. Компанія Sun рекомендує створити експертну групу зі співробітників компанії, які будуть відповідати за регулярний перегляд політики безпеки, перевірку положень політики безпеки на практиці, а також, при необхідності, внесення змін.

Реалізація в інформаційних системах

Після створення політики безпеки, а також відповідних процедур безпеки ці процедури можуть бути реалізовані в інформаційних системах компанії. Наприклад, у системах, заснованих на технології Java, деякі вимоги політики безпеки можуть обумовити необхідність установки додаткових криптопровайдерів сторонніх виробників, у той час як інші вимоги політики безпеки можуть бути реалізовані убудованої в Java бібліотекою Security API. Варто підкреслити, що виконання вимог політики безпеки в системах обробки даних не є достатнім для підтримки довіри клієнтів: не можна гарантувати безпека без правильної організації обробки даних.

Етапи розробки політики безпеки

Компанія Sun рекомендує розробляти політику безпеки компанії на основі кращих практик, описаних у відомих стандартах безпеки, наприклад ISO 17799:2005. При цьому рекомендуються наступні етапи розробки політики безпеки:

• визначення основних цілей і завдань розвитку бізнесу компанії;

Визначення основних цілей і завдань розвитку бізнесу компанії важливо для визначення області застосування політики безпеки. Необхідний відповідний рівень згоди усередині компанії, що гарантує, що політика безпеки належним чином відображає вимоги безпеки, адекватні цілям і завданням розвитку бізнесу компанії. Тут важливо розуміти, хто буде визначати політикові безпеки компанії й хто буде займатися її реалізацією й підтримкою. Команда розроблювачів політики безпеки повинна бути представницької й, як мінімум, включати співробітників відділу захисту інформації, юридичного відділу, відділу кадрів, відділу внутрішнього аудита і якості, відділу системних операцій і відділу програмних розробок.

• опис основних принципів безпеки;

Опис основних принципів забезпечення інформаційної безпеки компанії дозволяє простою й зрозумілою мовою, не вдаючись у технічні деталі, сформулювати основні цінності компанії й необхідність їхнього захисту.

• класифікація й категорирование інформаційних ресурсів;

В основі будь-якої політики безпеки лежить визначення цінності інформаційних активів компанії. Класифікація й категорирование інформаційних ресурсів компанії дозволяє швидко і якісно ухвалити рішення щодо необхідному ступені захищеності цих ресурсів.

- аналіз інформаційних потоків;

Ціль аналізу інформаційних потоків — визначити всі критичні крапки обробки дані компанії. Наприклад, у системі обробки транзакцій дані можуть переміщатися через Web-браузери, сервери даних і межсетевые екрани й можуть зберігатися в базах даних, на магнітних носіях і на папері. Відслідковуючи інформаційні потоки, можна визначити склад і структуру відповідних засобів захисту інформації.

- визначення основних загроз і моделі порушника;

Розробка моделі загроз і моделі порушника дозволяє вирішити, які типи загроз існують в інформаційних системах компанії, яка ймовірність реалізації загроз й які їхні наслідки, а також вартість відновлення.

- визначення сервісів безпеки;

Визначення сірвісів безпеки компанії, наприклад журналізація, авторизації, ідентифікації, автентифікації й ін., дозволяє правильно виробити політику безпеки.

- створення шаблона політики безпеки;

Структура політики безпеки може бути різна. Цей крок використовується для чіткого визначення розділів політики безпеки компанії.

- визначення області дії політики безпеки.

Останній етап перед створенням перших чорнових варіантів політики безпеки — визначення всіх областей, на яких фокусируєтся політика безпеки. Наприклад, можуть бути визначені політики безпеки:

- категорування інформаційних ресурсів,
- доступу до інформаційних ресурсів,
- використання паролів,
- використання шифрування й управління ключами,
- мережної безпеки,
- фізичної безпеки,
- роботи з електронною поштою,
- реагування на інциденти в області безпеки,
- моніторингу й аудита безпеки,
- межсетевого екранування,
- антивірусного захисту,
- управління системами й мережами,
- контролю дій співробітників,
- резервного копіювання,
- допуску сторонніх організацій,
- розробки й впровадження додатків,
- управління конфігураціями,
- виявлення вторгнень й ін.

Шаблон політики безпеки

Компанія Sun рекомендує використати наступний шаблон політики безпеки:

- розділи: робиться короткий огляд основних розділів політики безпеки; заява про призначення: чому потрібна політика безпеки;
- область дії: яка область дії політики безпеки;
- заява політики**:** які специфічні особливості політики безпеки;
- обов’язки: хто й що повинен робити;
- аудиторія: на кого орієнтована політика безпеки;
- впровадження: хто відповідає за впровадження політики безпеки; хто відповідає за порушення політики безпеки;

- виключення: опис можливих виключень;
- інші угоди: опис додаткових угод;
- доведення: хто відповідає за доведення політики безпеки до співробітників; який процес доведення;
- процес перегляду й відновлення: хто відповідає за перегляд і відновлення політики безпеки; що являє собою процес перегляду; з яких причин це відбувається; періодичність перегляду політики безпеки (наприклад, щорічно або при виникненні проблеми);
- здійснення політики: хто відповідає за здійснення політики безпеки; як це виконується;
- моніторинг відповідності: як виконується моніторинг відповідності політики безпеки вимогам бізнесу.

3.4. Архітектура безпеки SAFE компанії Cisco Systems

З погляду фахівців Cisco, відсутність мережної політики безпеки може привести до серйозних інцидентів в області безпеки. Розробку політики безпеки компанії рекомендується починати з оцінки ризиків мережі й створення робочої групи по реагуванню на інциденти.

Компанія Cisco рекомендує створити політики використання, які описують ролі й обов'язки співробітників компанії для належного захисту конфіденційної інформації. При цьому можна почати з розробки головної політики безпеки, у якій чітко прописати загальні цілі й завдання організації режиму інформаційної безпеки компанії.

Наступний крок — створення політики припустимого використання для партнерів, щоб проінформувати партнерів компанії про те, яка інформація їм доступна. Варто чітко описати будь-які дії, які будуть сприйматися як ворожі, а також можливі способи реагування при виявленні таких дій.

На закінчення необхідно створити політику припустимого використання для адміністраторів, щоб описати процедури адміністрування облікових записів співробітників і перевірки привілеїв. При цьому якщо компанія має певну політику щодо використання паролів або категорування інформації, те потрібно її тут згадати. Далі необхідно перевірити названі політики на несуперечність і повноту, а також переконатися в тім, що сформульовані вимоги до адміністраторів знайшли своє відображення в планах по навчанню.

Проведення аналізу ризиків

Призначення аналізу ризиків полягає в тому, щоб категорувати інформаційні активи компанії, визначити найбільш значимі загрози й уразливості активів й обґрунтовано вибрати відповідні контрзаходи безпеки. Мається на увазі, що це дозволить знайти й підтримувати прийнятний баланс між безпекою й необхідним рівнем доступу до мережі. Розрізняють наступні рівні інформаційних ризиків:

- низький рівень — інформаційні системи й дані, будучи скомпрометованими (доступні для вивчення неавторизованими особами, ушкоджені або загублені), не приведуть до серйозного збитку, фінансовим проблемам або до проблем із правоохоронними органами;
- середній рівень — інформаційні системи й дані, будучи скомпрометованими (доступні для вивчення неавторизованими особами, ушкоджені або загублені), приведуть до помірного збитку або до невеликих проблем із правоохоронними органами, або до помірних фінансових проблем, а також до одержання подальшого доступу до інших систем. Порушені системи й інформація вимагають помірних зусиль по відновленню;
- високий рівень — інформаційні системи й дані, будучи скомпрометованими (доступні для вивчення неавторизованими особами, ушкоджені або загублені), приведуть до значного збитку або до серйозних проблем із правоохоронними органами, або до фінансових проблем, завданню збитків здоров'ю й безпеці співробітників. Системи й

інформація вимагають істотних зусиль по відновленню.

Рекомендується визначити рівень ризику для кожного з перерахованих пристроїв: мережні пристрої, пристрої моніторингу мережу сервери автентифікації (TACACS+ й RADIUS), поштові сервери, файлові сервери, сервери мережних додатків (DNS й DHCP), сервери баз даних (Oracle, MS SQL Server), персональні комп'ютери й інші пристрої.

При цьому вважається, що мережне встаткування, таке, як комутатори, маршрутизатори, DNS- і DHCP-сервери у випадку компрометації можуть бути використані для подальшого проникнення в мережу й тому повинні ставитися до групи середнього або високого ризику. Можливе ушкодження цих пристроїв може привести до припинення роботи всієї мережі. Такі інциденти завдають серйозної шкоди компанії.

Після визначення рівнів ризику необхідно визначити ролі користувачів у цих системах. Рекомендується виділяти наступні п'ять найбільш загальних типів користувачів:

- адміністратори — внутрішні користувачі, відповідальні за мережні ресурси;
- привілейовані користувачі — внутрішні користувачі з необхідністю більшого рівня доступу;
- рядові користувачі — внутрішні користувачі зі звичайним рівнем доступу;
- партнери — зовнішні користувачі з необхідністю доступу до деяких ресурсів;
- інші — зовнішні користувачі або клієнти.

Визначення рівнів ризику й типів доступу, необхідних для кожної мережі, дозволяє сформувати деяку матрицю безпеки (див. табл. 3.2). Ця матриця безпеки є стартовою крапкою для подальших кроків по забезпеченню безпеки, наприклад таких, як створення відповідної стратегії по обмеженню доступу до мережних ресурсів.

Визначення складу й структури групи мережної безпеки. Рекомендується створити групу мережної безпеки під керівництвом менеджера по безпеці із представниками з кожної значимої бізнесу-одиниці компанії (мінімум із представників одиниць розвитку,

Табл. 3.2

Матриця безпеки Cisco

Система	Опис	Рівень ризику	Типи користувачів
ATM-комутатори	Основні мережні пристрої	Високий	Мережні адміністратори
Мережні маршрутизатори	Мережні пристрої розподілу	Високий	Мережні адміністратори
Комутатори доступу	Мережні пристрої доступу	Середній	Мережні адміністратори
ISDN- або dial up-серверы	Мережні пристрої доступу	Середній	Мережні і системні адміністратори
Міжмережні екрани	Мережні пристрої доступу	Високий	Адміністратори безпеки
Сервери DNS і DHCP	Мережні додатки	Середній	Мережні і системні адміністратори
Зовнішні поштові сервери	Мережні додатки	Низький	Адміністратори і користувачі
Внутрішні поштові сервери	Мережні додатки	Середній	Адміністратори і користувачі
Сервери баз даних Oracle	Мережні додатки	Середній або високий	Адміністратори баз даних і користувачі

виконання й виробництва й/або продажів). Члени групи повинні добре знати політику безпеки й технічні аспекти систем, що захищають, і мереж. Часто це вимагає додаткового навчання співробітників названої групи. Група безпеки повинна брати участь у розробці політики безпеки, організації режиму інформаційної безпеки, а також вчасно реагувати на інциденти в області інформаційної безпеки компанії. Процес супроводу політик безпеки полягає в контролі й, при необхідності, перегляді політик безпеки компанії. Необхідний як мінімум щорічний перегляд політики безпеки й проведення аналізу ризиків.

На практиці група мережної безпеки повинна проводити аналіз ризиків,

підтверджувати запити на проведення змін у системі безпеки, проводити моніторинг оповіщень про появу нових уразливостей з використанням списків розсилань вендорів і незалежних аналітичних центрів, наприклад CERT або SANS, а також підтримувати відповідність вимогам політики безпеки за допомогою певних технічних й організаційних заходів.

Тому що порушення безпеки часто виявляються під час проведення моніторингу мережі, то члени групи мережної безпеки повинні брати участь у розслідуванні інцидентів і попередженні подібних порушень надалі. Кожен член групи безпеки повинен мати гарні знання в області прикладного, системного й мережного програмного й апаратного забезпечення систем безпеки. При цьому рекомендується визначити індивідуальні ролі й обов'язки кожного члена групи мережної безпеки.

Попередження. Під попередженням порушень компанія Cisco розуміє підтвердження змін у системах безпеки й моніторинг безпеки мережі.

Підтвердження змін у системах безпеки. Зміни в системах безпеки можуть бути визначені як зміни в мережному встаткуванні, які здатні зробити потенційний вплив на стан безпеки мережі. Політика безпеки компанії повинна визначати специфічні вимоги конфігурації безпеки й містити мінімум технічних деталей. Інакше кажучи, замість такого визначення вимоги, як "не дозволені зовнішні FTP-з'єднання у внутрішню мережу", потрібно визначити цю вимогу так — "зовнішні з'єднання не повинні бути здатні одержувати файли із внутрішньої мережі". При цьому бажано прагнути до визначення унікальних вимог компанії. Використання стандартних шаблонів забезпечення безпеки й настроювань за замовчуванням у підході компанії Cisco настійно не рекомендується.

Група мережної безпеки переглядає описані загальнодоступною мовою вимоги й визначає відповідність технічного дизайну й настроювань елементів мережі цим вимогам. Якщо виявляються невідповідності, група безпеки створює необхідні зміни мережної конфігурації для виконання вимог політики безпеки й застосовує їх надалі. При цьому групою мережної безпеки можуть контролюватися не всі зміни. Тут важливо переглянути зміни, найбільш значимі й істотні для мережі компанії в плані безпеки. Наприклад, до них ставляться зміни:

- у конфігурації міжмережних екранів,
- у списках контролю доступу,
- у конфігурації SNMP,
- версій програмного забезпечення.

Компанія Cisco рекомендує додержуватися наступних правил:

- регулярно змінювати паролі на мережних пристроях;
- обмежити доступ до мережних пристроїв відповідно до затвердженого списку співробітників;
- гарантувати, що поточна версія програмного забезпечення мережного й серверного встаткування відповідає вимогам безпеки.

У додавання до цих правил необхідно включити представника групи мережної безпеки в постійно діючу комісію компанії за твердженням змін для відстеження всіх змін, що відбуваються в мережі компанії. Представник групи безпеки може заборонити реалізацію будь-якої зміни, пов'язаного з безпекою, доти , поки ця зміна не буде дозволено керівником групи мережної безпеки.

Моніторинг мережної безпеки. Моніторинг мережної безпеки зосереджується на виявленні змін у мережі, що дозволяють визначити порушення безпеки. Відправною точкою моніторингу безпеки є визначення поняття "порушення безпеки". Аналіз загроз й інформаційних ризиків дозволяє визначити необхідний рівень повноти моніторингу безпеки мережі компанії. Надалі при твердженні змін безпеки щораз перевіряється значимість виявлених загроз мережі. Оцінкою цих загроз визначається об'єкт і частота моніторингу.

Наприклад, у матриці аналізу ризиків міжмережний екран визначений як пристрій з

високим рівнем ризику. Це означає, що моніторинг міжмережного екрана повинен виконуватися постійно в режимі реального часу. З розділу підтвердження змін безпеки треба, що необхідно виявляти всі зміни в настроюваннях конфігурації міжмережного екрана. Тобто SNMP-агент повинен відслідковувати такі події, як відкинуті спроби реєстрації, незвичайний трафік, зміни на міжмережному екрані, надання доступу до міжмережного екрана й установлення з'єднань через міжмережний екран.

У такий спосіб можна створити політикові моніторингу для кожного компонента мережі, певної при проведенні аналізу ризиків. Рекомендується проводити моніторинг компонентів мережі з низьким рівнем ризику — щотижня, із середнім рівнем ризику — щодня, з високим рівнем ризику — раз у годину. При цьому якщо потрібно більше швидкий час реагування, то необхідно зменшити названі тимчасові проміжки.

Важливо також визначити в політику безпеки порядок повідомлення членів групи мережної безпеки про порушення. Як правило, засобу моніторингу безпеки мережі будуть першими автономно виявляти порушення. Повинна бути передбачена можливість відправлення по будь-яких доступних каналах зв'язку повідомлень у центр реагування на інциденти в області безпеки для оперативного оповіщення членів групи мережної безпеки.

Реагування на порушення. Під реагуванням на порушення в безпеці тут розуміється визначення порушень безпеки, порядку відновлення й перегляду правил безпеки.

Порушення безпеки. При виявленні порушення безпеки важливо вчасно відреагувати й оперативно відновити нормальне функціонування сервисів мережі. Тут головне правило — своєчасне оповіщення групи мережної безпеки після виявлення порушення. Якщо це правило не виконується, то реагування буде вповільнено, а отже, вторгнення й наслідки більше важкими. Тому необхідно розробити відповідну процедуру реагування й оповіщення, діючу 24 години на день 7 днів у тиждень.

Далі необхідно чітко визначити рівень привілеїв по внесенню змін, а також порядок внесення змін. Тут можливі наступні коригувальні дії:

- реалізація змін для попередження подальшого поширення порушення,
- ізолювання ушкоджених систем,
- взаємодія із провайдером для відстеження джерела атаки,
- використання записуючих пристроїв для збору доказів,
- відключення ушкоджених систем або джерел атаки,
- звернення до правоохоронних органів або федеральних агентств,
- вимикання ушкоджених систем,
- відновлення систем у відповідності зі списком пріоритетності,
- повідомлення керівництва і юристів компанії.

Необхідно деталізувати будь-які зміни в політику безпеки, які можуть бути зроблені без обов'язкового одержання дозволу від керівництва.

Відзначимо, що існують дві основні причини для збору й зберігання інформації про атаки: визначення наслідків реалізації атаки й розслідування й переслідування зловмисників. Тип інформації, спосіб збору й обробка інформації обумовлені цілями реагування на порушення безпеки.

Для визначення наслідків порушення безпеки рекомендується здійснити наступні кроки:

- зафіксувати інцидент за допомогою запису мережного трафіка, зняття копій файлів журналів, активних облікових записів і мережних підключєнь;
- обмежити подальші порушення шляхом відключення облікових записів, від'єднання мережного встаткування від мережі й від Інтернету;
- провести резервне копіювання скомпрометованих систем для проведення детального аналізу ушкоджень і методу атаки;
- спробувати знайти інші підтвердження компрометації. Часто при компрометації системи виявляються порушеними інші системи й облікові записи;

• переглядати збережені файли журналів пристроїв безпеки й мережного моніторингу, тому що вони часто є ключем для визначення методу атаки.

Якщо необхідно зробити юридичні дії, варто повідомити керівництво й залучити юристів компанії для збору відповідних доказів. Якщо порушення було внутрішнім, то буде потрібно залучити співробітників відділу кадрів компанії.

Відновлення. Відновлення працездатності сервісів мережі компанії є кінцевою метою процедури реагування на порушення в області безпеки. Тут необхідно визначити порядок відновлення доступності сервісів, наприклад за допомогою процедур резервного копіювання. При цьому треба враховувати, що кожна система має свої власні механізми резервного копіювання. Тому політика безпеки, будучи загальної для всіх елементів мережі, при необхідності повинна дозволяти деталізувати умови відновлення конкретного елемента. Якщо потрібно одержати з на відновлення, потрібно описати порядок одержання дозволу в політику безпеки.

Перегляд політики безпеки. Перегляд політики безпеки із заключним етапом життєвого циклу політики безпеки. Тут важливо звернути увагу на наступне. Політика безпеки повинна з "життєздатним" документом, адаптованим до умов, що змінюються. Порівняння існуючої політики безпеки із кращими практиками в цій області й наступний перегляд політики повинні підтримувати в актуальному стані захищеність активів мережі. Необхідно регулярно звертатися на Web-сайти різних незалежних аналітичних центрів, наприклад CERT або SANS, за корисними радами й рекомендаціями із забезпечення безпеки й ураховувати їх у підтримуваній політиці безпеки компанії.

Також рекомендується проводити аудит безпеки мережі шляхом обігу у відповідні консалтингові компанії, що спеціалізуються на наданні подібних послуг. Для мереж з високими вимогами до доступності інформаційних ресурсів рекомендується проведення незалежного аудита безпеки як мінімум раз у рік. Крім того, досить ефективні й внутрішні тренування для відпрацьовування дій у надзвичайних ситуаціях.

3.5. Концепція розроблення захищених систем компанії Symantec

Керівні документи в області безпеки (політики, стандарти, процедури й метрики безпеки), як думають в Symatec, є основою будь-якої успішної програми забезпечення інформаційної безпеки компанії.

Політика інформаційної безпеки визначає, чому компанія захищає свою інформацію. Стандарти — що компанія має намір уживати для реалізації й управління безпекою інформації. Процедури описують, як компанія буде виконувати вимоги, описані у документах високого рівня (політики й керівництва). Керівництва являють собою рекомендації, яким бажано випливати.

Основні етапи розробки політики безпеки. Компанія Symantec виділяє наступні основні етапи розробки політики бепеки:

• визначення й оцінка інформаційних активів — які активи необхідно захищати і як їх захищати з урахуванням цілєй і завдань бізнесу;

• визначення загроз безпеки — виявлення потенційних джерел проблем в області безпеки компанії. Оцінка ймовірності реалізації загрози й оцінка можливого збитку. При цьому виділяють зовнішні й внутрішні загрози безпеки;

• оцінка інформаційних ризиків — являє собою один із самих складних етапів процесу розробки політики безпеки. На тратегічно важливими клієнтами й партнерами;

• визначення відповідальності — вибір команди з, здатної визначити потенційні загрози у всіх областях діяльності компанії. В ідеалі в процесі розробки політики безпеки повинні брати участь представники всіх ключових підрозділів компанії. Ключові члени команди — представники керівництва, відділу кадрів, юридичного відділу, відділу по зв’язках із громадськістю, мережні адміністратори, експерти в області інформаційної безпеки;

• створення комплексного документа — створення політики з посиланнями на такі додаткові документи, як процедури, керівництва, стандарти й контракти співробітників. Ці документи повинні містити вимоги до конкретних інформаційних систем, технологіям, а також визначати ступінь відповідальності співробітників. У результаті стає можливим

робити зміни в документах, не торкаючись самої політики інформаційної безпеки. Політика інформаційної безпеки підписується керівником компанії;

- реалізація — політика безпеки повинна чітко визначати відповідальність за забезпечення інформаційної безпеки й відповідальних за інформаційні системи й захист інформації. Компанія може зажадати від співробітників підпису в тім, що вони ознайомлені з політикою безпеки й зобов'язуються дотримувати її вимоги. Відповідальність реалізується за допомогою визначення:
- процедури відповідності — для визначення відповідальності за виконання вимог політики безпеки;
- складу й структури підрозділу офіцерів безпеки — визначає співробітників, які відповідають за забезпечення режиму інформаційної безпеки. Тут необхідно передбачити проблеми, пов'язані з конфліктом інтересів;
- процедури виділення необхідних ресурсів — гарантує виділення необхідних ресурсів для відповідності вимогам політики інформаційної безпеки;
- управління програмою безпеки — визначає внутрішні процедури для реалізації вимог політики.

Рекомендований склад політики безпеки. Ключовими аспектами політики інформаційної безпеки є:

- область застосування,
- необхідність строгого дотримання політики,
- основна частина політики,
- відповідальність,
- наслідки за невідповідність до вимог політики.

Істотними твердженнями політики безпеки є наступні:

- компанія є власником всіх даних і систем;
- співробітник зобов'язується не робити копій даних і програмного забезпечення без одержання відповідного дозволу;
- співробітник зобов'язується виконувати вимоги по парольному захисту;
- співробітник зобов'язується одержувати доступ до систем й інформації тільки легальним способом, після авторизації;
- співробітник підтверджує право компанії здійснювати моніторинг його діяльності.

Обсяг політики інформаційної безпеки, що рекомендується, не повинен перевищувати двох сторінок.

Реалізація політики досягається використанням стандартів, процедур, керівництв.

Що приймається до уваги? Для ефективності політики безпеки необхідно, щоб політика:

- була простою для розуміння,
- ґрунтувалася на вимогах бізнесу,
- була реалізованої,
- підтримувала баланс між безпекою й продуктивністю,
- була доступна всім співробітникам для ознайомлення,
- не суперечила іншим політикам компанії,
- не суперечила вимогам законодавства,
- ясно визначала відповідальність співробітників за її порушення,
- регулярно обновлювалася.

Стандарти. Вимоги до стандартів:

- кожен стандарт повинен підтримувати виконання мет компанії, відповідати вимогам існуючого законодавства й діючої в компанії політикам;
- стандарт повинен бути розроблений для захисту інформації, у той же час він не повинен утруднять одержання доступу до інформації співробітникам компанії; стандарт повинен розроблятися спільними зусиллями менеджерів і технічних експертів;
- стандарт не повинен суперечити вимогам політики інформаційної безпеки.

За основу при розробці стандартів компанія Symantec рекомендує використати стандарт ISO 17799:2005.

Процедури. Наступним рівнем документів є процедури. Роль процедури — визначити, як реалізуються й адмініструються засоби безпеки. Процедури є свого роду "біблією" для співробітників компанії, їхнім щоденним керівництвом до дії. Процедури, на відміну від

політики й стандартів, є часто, що змінюються документами, тому важливо мати в компанії гарну процедуру управління змінами документів. Кожна процедура повинна бути написана відповідно до загального шаблона, розробленим для процедур, бути доступної співробітникам як в електронному, так й у паперовому виді. Тому що деякі процедури можуть містити конфіденційну інформацію, то доступ до них може бути обмежений, що регулюється окремим стандартом.

Елементами процедур безпеки, що рекомендуються, є:

- ціль процедури:
- для відповідності якому стандарту вона розроблена;
- для чого потрібна процедура;
- область дії процедури:
- до яких систем, мереж, додатків, категорій персоналу, приміщень застосовується процедура;
- яка роль необхідна для виконання процесу;
- що потрібно знати для виконання процесу;
- визначення процесу:
- введення в процес (опис);
- детальний опис процесу (як, коли, що, критерії успіху, види звітів, взаємодія з іншими процесами);
- контрольний список процесу;
- проблеми процесу (дії при виникненні проблем).

3.6. Підхід SANS

Організація SANS виробила свій підхід у розумінні політики інформаційної безпеки і її складових. У термінології SANS політика інформаційної безпеки — багаторівневий документований план забезпечення інформаційної безпеки компанії:

- верхній рівень — політики;
- середній рівень — стандарти й керівництва;
- нижчий рівень — процедури.

Далі документи розбиваються на наступні основні категорії:

- твердження керівництва про підтримку політики інформаційної безпеки;
- основні політики компанії;
- функціональні політики;
- обов'язкові стандарти (базові);
- рекомендовані керівництва;
- деталізовані процедури.

Стандарти деталізують розходження по настроюванню безпеки в окремих операційних системах, додатках і базах даних.

Керівництва представляють із себе що рекомендують, необов'язкові до виконання дії по попередженню проблем, пов'язаних з різними аспектами інформаційної безпеки.

Процедури — детальні покрокові інструкції, які співробітники зобов'язані неухильно виконувати.

При розробці політик дуже важливим є коректний розподіл ролей й обов'язків. Дуже важливо дотримувати принципу найменших привілеїв, принцип "знати тільки те, що необхідно для виконання службових обов'язків" і використати поділ обов'язків на критичних системах.

Розрізняють наступні типи політик безпеки:

- спрямовані на рішення конкретної проблеми — прикладами таких політик можуть служити політика по найманню персоналу, політика використання паролів, політика використання Інтернету;
- програмні — політики високого рівня, що визначають загальний підхід компанії до забезпечення режиму інформаційної безпеки. Ці політики визначають напрямок розробки інших політик і відповідність із вимогами законодавства й галузевих стандартів;
- застосовувані до конкретного середовища — наприклад, кожна операційна система вимагає окремого стандарту по її настроюванню.

Рекомендовані компоненти політики безпеки:

- ціль,

- область дії,
- твердження політики,
- історія документа,
- необхідність політики,
- які політики скасовує,
- дії по виконанню політики,
- відповідальність,
- виключення,
- порядок і періодичність перегляду.

Організація SANS розробила ряд шаблонів політик безпеки:

- політика припустимого шифрування,
- політика припустимого використання, посібник з антивірусного захисту,
- політика аудита уразливостей,
- політика зберігання електронної пошти,
- політика використання електронної пошти компанії,
- політика використання паролів,
- політика оцінки ризиків,
- політика безпеки маршрутизатора ,
- політика забезпечення безпеки серверів,
- політика віртуальних приватних мереж,
- політика бездротового доступу в мережу компанії,
- політика автоматичного перенаправлення електронної пошти компанії,
- політика класифікації інформації,
- політика відносно паролів для доступу до баз даних,
- політика безпеки лабораторії демілітаризованої зони,
- політика безпеки внутрішньої лабораторії,
- політика екстранет,
- політика етики,
- політика лабораторії антивірусного захисту.

3.7. Сервіси безпеки

Забезпечення безпеки відкритих систем являє собою комплексне багаторівневе й багатопланове завдання. Вона підрозділяється на напрямки, які розрізняються між собою по об'єктах захисту, характеру загроз, способам протидії їм і критеріям оцінки ефективності систем безпеки.

Окремо зупинимося на сучасних сервісах безпеки. Якими би потужними і стійкими вони не були, самі по собі вони не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки єдина архітектура безпеки здатна зробити ефективним об'єднання цих сервісів, забезпечити керованість ІС, її здатність розвиватися й протистояти новим загрозам ІБ.

Сервіси безпеки повинні забезпечувати чотири рівні захисту:

- запобігання, або профілактика — тільки авторизований персонал має доступ до інформації, ресурсам і процесам;
- виявлення й реєстрація — забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;
- обмеження — зменшується розмір втрат, якщо злочин все-таки відбувся, незважаючи на заходи для його запобігання й виявлення;
- відновлення — забезпечується ефективне відновлення всіх мережних ресурсів при наявності документованих і пєрєвірєних планів по відновлєнню.

До необхідного мінімуму для захисту Інтранету варто віднести реалізацію сервісів безпеки на мережному й транспортному рівнях стека протоколів TCP/IP і підтримку механізмів автентифікації, стійких до мережних загроз.

Для сервісів безпеки повинен дотримуватися принцип простоти їхнього використання. Він націлений на те, щоб зробити роботу сервісів безпеки прозорої для користувачів. Повністю домогтися цього, звичайно, неможливо (наприклад, без автентифікації за участю користувача не обійтися), але якийсь поріг складності перевищувати не можна. Користувачі — сама слабка ланка будь-якої системи, і чим менше вони повинні (і можуть) зробити, тим краще. Важливість цього принципу доведена всім ходом розвитку

інформаційних технологій, кризами програмування, невдачами при створенні більших систем. Повною мірою принцип ставиться й до підсистеми безпеки, причому на всіх рівнях — від реалізації окремих функцій до об'єднання сервісів. Варто прагнути до мінімізації числа зв'язків між компонентами ІС, оскільки саме воно визначає складність. Загалом кажучи, із принципом простоти конфлікту є необхідність внесення в систему певної надмірності, що забезпечує стійкість стосовно збоїв і відмов. По цілому ряді причин реальний захист ресурсів Інтранет виявляється результатом численних компромісів.

Відповімо два важливих питання: як об'єднати сервіси безпеки для створення ешелонованої оборони і яке їхнє місце в загальній архітектурі ІС. На зовнішньому рубежі розташовуються засоби виявлення злочинної активності й контролю захищеності. Далі йдуть МЕ, що захищають зовнішні підключення. Вони разом із засобами підтримки віртуальних приватних мереж утворять периметр безпеки, що відокремлює корпоративну ІС від зовнішнього миру. Для швидкого виявлення атак, навіть уже успішно минулих, сервіс активного аудиту повинен бути присутнім у всіх критично важливих компонентах, і зокрема в захисті управління доступом також повинне бути присутнім на всіх сервісах. Доступу повинна передувати ідентифікація й автентифікація суб'єктів.

Криптографічні засоби доцільно виносити на спеціальні шлюзи, якими управляє кваліфікований адміністратор. Застосування криптографії користувачами краще мінімізувати. Останній рубіж утворять засобу пасивного аудита, що допомагають оцінити наслідки порушення безпеки, знайти винного, з'ясувати, чому успіх атаки став можливим.

Розташування засобів забезпечення високої доступності визначається критичністю відповідних сервісів або їхніх компонентів.

Ідентифікація/автентифікація

Дана функція забезпечує автентифікацію партнерів по спілкуванню й автентифікацію джерела даних. Автентифікація партнерів по спілкуванню використається при встановленні з'єднання або іноді періодично під час сеансу. Вона служить для запобігання таких загроз, як спуфінг, або "маскарад", і повтор попереднього сеансу зв'язку. Автентифікація джерела даних — це підтвердження дійсності джерела окремої порції даних. Автентифікація буває однобічної, коли клієнт звичайно доводить свою дійсність серверу, і двосторонньої, або взаємної.

Сучасні засоби ідентифікації/автентифікації повинні задовольняти двом умовам: бути стійкими до мережних загроз (пасивному й активному прослуховуванню мережі) і підтримувати концепцію єдиного входу в мережу (так називані системи з однократною ре-єстрацією — від англ. Smgle Slgn-On, SSO).

Перша вимога можна виконати, використовуючи криптографічні методи. У цей час загальноприйнятими є підходи, засновані на системі Kerberos або службі каталогів із сертифікатами в стандарті X.509.

Починаючи з Wmdows 2000 в ОС Microsoft підтримується Kerberos — відкритий протокол автентифікації (визначений в RFC 1510, випущеному Internet Engmeermg Task Force), за допомогою якого комп'ютер, що збирається встановити зв'язок з іншим комп'ютером, може підтвердити свою "особистість". Після підтвердження Kerberos постачаються обидва комп'ютери ключами шифрування для проведення захищеного сеансу зв'язку. Автентифікація за допомогою Kerberos являє собою тристоронній процес, у якому роль посередника виконує сервіс за назвою Key Distribution Center (KDC), що підтверджує особистість комп'ютера по запиту іншого комп'ютера й поставляющих ключів для встановлення між ними захищеного з'єднання. Кожний з комп'ютерів, що бере участь у сеансі зв'язку, "ділить секрет"з KDC, що складається із двох компонентів: сервера автентифікації й сервера видачі квитків. Якщо KDC одержує запит про невідомому йому сервері призначення, він перенаправляє автентифікаційну транзакцію на інший KDC, що розташовує потрібними відомостями.

Обмінюючись із клієнтом серією шифрованих повідомлень, називаних квитками, KDC генерує нові ключі шифрування для кожного етапу процесу автентифікації. Він може успішно підтвердити особистість одного комп'ютера по запиту іншого, не видаючи секретних ключів ні однієї зі сторін і не вимагаючи ні від однієї з них постійного зберігання ключів доступу до всіх комп'ютерів, з якими вони коли-небудь, установлять з'єднання. Квиток дійсний протягом заданого періоду часу й може використатися тільки одним певним комп'ютером для підключення до іншого певного комп'ютера. Після видачі

квитка клієнт може використати його для одержання доступу до цільового сервера необмежене число раз, але тільки в період дії квитка. Ні клієнт, ні хтось інший не можуть уважати або модифікувати квиток, не зробивши його недійсним.

В Kerberos реалізовано багато корисних функцій захисту, у тому числі взаємна автентифікація й реєстрація за допомогою смарт-карт. Kerberos функціонує на багатьох платформах, так що його можна використати для процедури єдиної реєстрації. Даний протокол підтримує делегування або переадресацію автентифікації.

Єдиний вхід у мережу з однократною реєстрацією (SSO) — це в першу чергу вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежний обіг, то багаторазова ідентифікація/автентифікація стає занадто обтяжною. Завдяки системі SSO користувач, лише один раз пройшовши процедуру реєстрації, одержує доступ одночасно до ресурсів своєї робочої станції й всієї мережі відповідно до своїх посадових обов'язків. Супровід численних облікових записів і паролів для кожного користувача збільшує витрати й на системне адміністрування.

На багатьох підприємствах значна частина часу системних адміністраторів витрачається на РІШЄННЯ завдань, пов'язаних з обліковими записами й паролями, включаючи первісне створення користувальницьких облікових записів при прийомі користувачів на роботу, видалення облікових записів при звільненні користувачів або зміни їхніх ролей, переустановку паролів, коли вони забуваються. Наявність декількох облікових записів у кожного користувача збільшує відповідне навантаження на системних адміністраторів. На жаль, поки не можна сказати, що SSO-системи стали нормою, що домінують рішення поки не сформувалися.

Додаткові зручності створює застосування біометричних методів автентифікації, заснованих на аналізі відбитків (точніше, результатів сканування) пальців. На відміну від спеціальних карт, які потрібно зберігати, пальці "завжди під рукою" (правда, під рукою повинен бути й сканер). Підкреслимо, що й тут захист від порушення цілісності й перехоплення з наступним відтворенням здійснюється методами криптографії.

Розмежування доступу

Управління доступом забезпечує захист від несанкціонованого використання ресурсів, доступних по мережі. Із традиційної точки зору засобу управління доступом дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі й процеси) можуть виконувати над об'єктами (інформацією й іншими комп'ютерними ресурсами).

Розмежування доступу, імовірно, є самою дослідженою областю ІБ, особливо те, що здійснюється по імені й паролю користувача. Дискреційне й мандатне управління ввійшли в усі теоретичні курси й критерії оцінки. Хоча в цей час розмежування доступу не завжди ефективно бореться зі злочинними користувачами. Сучасні ІС характеризуються надзвичайною складністю, і їхні внутрішні помилки представляють не меншу небезпеку. Динамічність сучасного програмного середовища й складність окремих її компонєнтів істотно звужують область застосовності дискреційної моделі управління доступом (що називається також моделлю з довільним управлінням). При визначенні допустимості доступу важливо не тільки (і не стільки) те, хто звернувся до об'єкта, але й те, яка семантика дії. Без залучення семантики не можна виявити "троянські" програми, протистояти яким довільне управління доступом, як відомо, не в змозі. Нові моделі управління доступом (наприклад, модель "пісочниці" в Java-технології) також, на жаль, не враховують семантику програм, що є однією з основних причин слабостей, що виявляють, у системі безпеки. Активно рольове управління, що розвиває, доступом (Role-Based Access Control, RBAC) (між користувачами і їхніми привілеями містяться проміжні сутності — ролі, можливо кілька од- почасово для кожного користувача) вирішує не стільки проблеми безпеки, скільки поліпшує керованість систем (рис. 3.4).

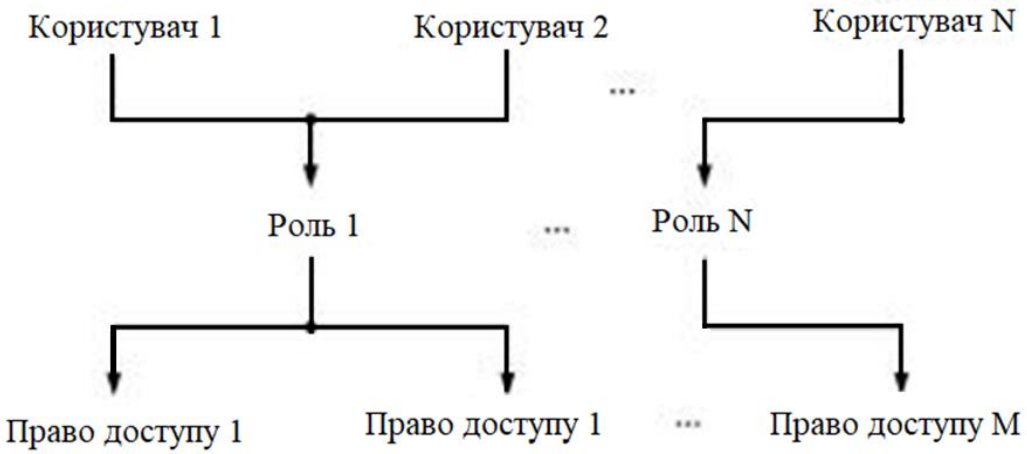


Рис. 3.4. Користувачі і ролі

На підставі цієї моделі можна реалізувати такі важливі принципи, як поділ обов'язків. Між ролями можуть бути визначені статичні або динамічні відносини несумісності (неможливості одному суб'єктові одночасно або по черзі активізувати обидві ролі), що й забезпечує необхідний захист. Ще одна специфічна й методологічно важлива мета безпеки — організація ієрархії ролей зі спадкуванням прав доступу. Для деяких сервісів типу WWW рольове управління доступом може бути реалізоване відносно просто (у випадку WWW — на основі CGi-процедур).

В IP-мережах відомо й розмежування доступу на основі IP-адреси, підмережі або домена.

Окремі документи або цілі директорії можуть бути зроблені доступними тільки для браузерів, що мають конкретний IP-адрес, або належать до певної підмережи, бо прилежних до певного домену. Обмеження доступу із IP-адреси ефективно проти випадкових спроб доступу, але не проти зловмисника, що діє цілеспрямовано. Існують різні способи обходу такого роду обмежень. Маючи необхідні апаратури й ПЗ, що атакує може підмінювати свою IP-адресу (атаки IP spoofing), імітуючи з'єднання не з того місця в мережі, де дійсно розташований його комп'ютер, а з якого-небудь іншого. Крім того, немає ніякої гарантії того, що людина, що звертається до сервера з комп'ютера, доступ з якого дозволений, є саме тою людиною, яку мали на увазі. Комп'ютер міг бути зламаний і використаний зловмисником. Обмеження по мережній адресі повинні для надійності доповнюватися якими-небудь перевірками користувача (його імені й пароля) або застосуванням ME, здатним визначати й запобігати спроби використання фіктивних IP-адресов на основі фільтрації. Простіше всього перехоплюються пакети, що приходять із зовнішнього миру, але складені так, начебто вони послані з комп'ютера локальної мережі. Варто розуміти, що якщо браузер настроєний на використання проксі-сервера, то веб-сервер одержить тільки IP-адресу представника, але не тієї машини, на якій працює користувач. Це значить, що при наявності проксі-сервера в домене, якому довіряють, будь-яка людина може використати його для доступу до іншого сервера.

Обмеження доступу по імені комп'ютера або домена, що володіють тими ж слабостями, якими володіють й обмеження по IP-адресам, чутливі, крім того, до підміни імен DN3 (DN8 spoofing) — атаці, при якій сервер переконують на час у тім, що дозволене ім'я відповідає іншому (потрібному зловмисникові) IP-адресу. Для зменшення подібного ризику деякі сервери можуть бути настроєні на додаткову перевірку імені DNS для кожного клієнта. Після перетворення IP-адреси, з якого прийшов запит, в ім'я комп'ютера, сервер використовує систему DNS для зворотного перетворення імені в IP-адреси. Якщо дві IP-адреси не збігаються, то доступ не надається.

Для контролю доступу до серверів в Ітранеті, крім імєн і паролів організації, що служить, можна використати видавані їм особисті сертифікати (Personal Certificates) (наприклад, вони застосовуються при настроюванні протоколу SSL для ідентифікації користувача). Для цього необхідно встановити відповідний сервер сертифікатів.

Механізми управління доступом можуть розташовуватися в кожної зі сторін, що

спілкуються, або в проміжній крапці.

Протоколювання й аудит

Формула “захищати, виявляти, реагувати” (protect, detect, react) є класичною. Тільки ешелонована, активна оборона, що містить різноманітні елементи, дає шанс на успішне виявлення й відбиття атак.

Активний аудит доповнює ідентифікацію/автентифікацію й розмежування доступу. Подібне доповнення необхідно по двох причинах. По-перше, що існують засоби розмежування доступу не здатні реалізувати всі вимоги ПБ, якщо останні мають більше складний вид, чим дозвіл-заборона атомарних операцій з ресурсами. Розвинена ПБ може накладати обмеження на сумарний обсяг прочитаної інформації, забороняти доступ до другого ресурсу, якщо раніше мав місце доступ до першого, і т.ін. По-друге, у самих захисних засобах є уразливості.

Протоколювання/аудит традиційно були останнім рубежем оборони, що забезпечує аналіз наслідків порушення і виявлення зловмисників. Такий аудит можна назвати пасивним. Узагальненням пасивного аудита для мережного середовища є спільний аналіз реєстраційних журналів окремих компонентів на предмет виявлення протиріч, що важливо у випадках, коли зловмисникові вдалося відключити протоколювання або модифікувати журнали. У сучасний арсенал захисних засобів увійшов активний аудит, спрямований на виявлення підозрілих (злочинних й/або аномальних) дій компонентів у реальному масштабі часу з метою оперативного вживання відповідних заходів. Призначення активного аудиту — виявляти й реагувати. Тепер такі засоби стали першим й останнім рубежем. До першого рубежу можна віднести також і сканери безпеки, що допомагають виявляти й усувати слабкі місця в захисті. На останньому рубежі для виявлення порушень можуть використовуватися засоби контролю цілісності.

Активний аудит включає два види:

- виявлення нетипового поводження (користувачів, програм або апаратури);
- виявлення початку злочинної активності.

Нетипове поводження виявляється статистичними методами, шляхом зіставлення з попередньо отриманими зразками. Початок злочинної активності виявляється по збігу із сигнатурами відомих атак. За виявленням треба заздалегідь запрограмована реакція (як мінімум — інформування системного адміністратора, як максимум — контратака на систему передбачуваного зловмисника).

Важливим елементом сучасного трактування протоколювання/аудита є протокол автоматизованого обміну інформацією про порушення безпеки між корпоративними системами, підключеними до однієї зовнішньої мережі. Робота над цим протоколом ведеться під егідою IETF.

Екранування

Екранування як сервіс безпеки виконує такі функції, як:

- розмежування міжмережного доступу суб’єктів однієї мережі (фрагмента мережі, автоматизованої системи) до об’єктів іншої мережі шляхом фільтрації переданих даних;
- контроль інформаційних потоків між мережами й перетворення переданих даних;
- іноді реєстрація подій, пов’язаних із процесами розмежування доступу, зокрема фіксація всіх "незаконних" спроб доступу до інформації й, додатково, сигналізація про ситуації, що вимагають негайної реакції.

Інформація, що надходить у мережеві екрани (МЕ), може призначатися для фільтрації або для зміни параметрів самого МЕ.

Як критерії аналізу інформаційного потоку можуть використовуватися наступні параметри:

- службові поля пакетів повідомлень, що містять мережні адреси, ідентифікатори, адреси інтерфейсів, номера портів й інші значимі дані;
- безпосередній зміст пакетів повідомлень, що перевіряє, наприклад на наявність комп’ютерних вірусів;

зовнішні характеристики потоку інформації, наприклад тимчасові, частотні характеристики, обсяг даних і т.ін.

Сучасні МЕ фільтрують дані на основі заздалегідь заданої бази правил, що дозволяє реалізовувати набагато більше гнучку політику безпеки, чим в ОС. При комплексній фільтрації, що охоплює мережний, транспортний і прикладний рівні, у правилах можуть фігурувати мережні адреси, кількість переданих даних, операції прикладного рівня,

параметри оточення (наприклад, час) і т. ін. МЕ класифікуються на підставі рівнів еталонної моделі ВВС, на яких здійснюється фільтрація потоків даних.

У процесі фільтрації може виконуватися додатковий контроль (наприклад, антивірусний). Можливі й додаткові перетворення, найбільш актуальним з яких є виправлення заголовків або іншої служебной інформації.

Перетворення переданих даних може зачіпати як службові поля пакетів, так і прикладні дані. У першому випадку звичайно мається на увазі мережна трансляція адрес (Network Address Translation, NAT), що допомагає сховати топологію захищеної системи. Це унікальна властивість сервісу екранування, що дозволяє приховувати існування деяких об'єктів доступу, Перетворення даних може складатися, наприклад, у їхньому шифруванні.

МЕ може використатися й для захисту окремого комп'ютера. У цьому випадку МЕ встановлюється на захищений компьютер, що і називається персональним. Він контролює весь вихідний і вхідний трафик, незалежно від всіх інших системних захисних засобів. При екрануванні окремого комп'ютера зменшується або взагалі ліквідується навантаження, породжуване зовнішньою активністю, у результаті чого знижується уразливість внутрішніх сервісів комп'ютера.

Тунелювання

Тунелювання (tunneling), або інкапсуляція (encapsulation) — це метод вирішення завдання узгодження мереж, що застосовується тільки для узгодження транспортних протоколів і тільки при певних обмеженнях. Інкапсуляція може бути використана, коли дві мережі з однією транспортною технологією необхідно з'єднати через мережу, що застосовує іншу транспортну технологію (рис. 3.5) [85].

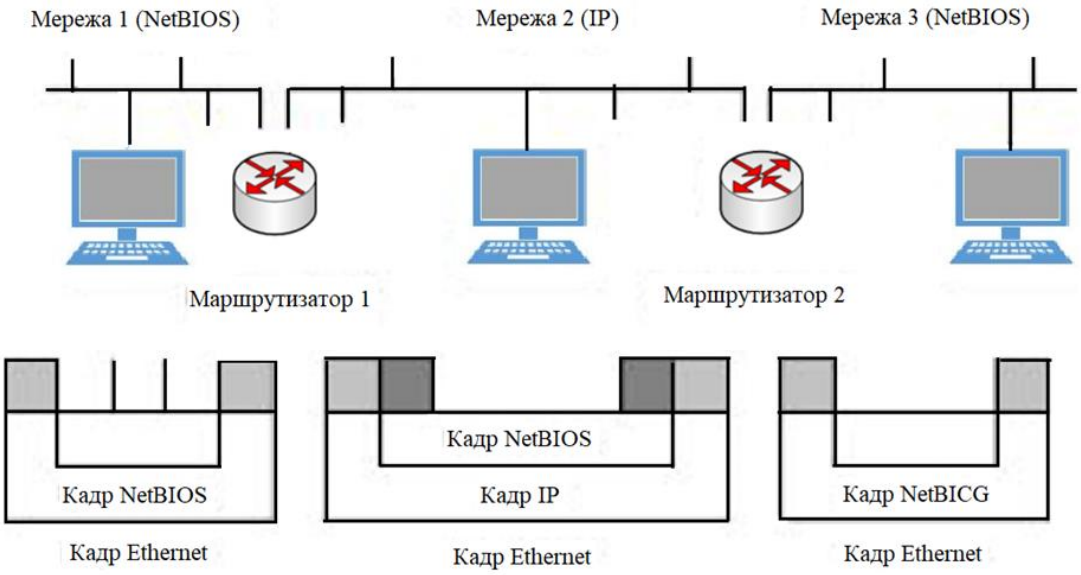


Рис. 3.5. Інкапсуляція протоколів мережного рівня

Суть туннелирования як самостійного сервісу безпеки полягає в тому, щоб "упакувати" передану порцію даних, разом зі службовими полями, у новий "конверт". Метод полягає в тім, що прикордонні маршрутизатори, які підключають поєднувані мережі до транзитного, упаковують пакети транспортного протоколу поєднуваних мереж у пакети транспортного протоколу транзитної мережі. Туннелирование може бути використане для транспортних протоколів будь-якого рівня. Наприклад, протокол мережного рівня X.25 може бути інкапсульований до протоколу транспортного рівня TCP або ж протокол мережного рівня IP може бути інкапсульований до протоколу мережного рівня X.25. Для узгодження мереж на мережному рівні можуть бути використані багатопротокольні й інкасулюючі маршрутизатори, а також програмні й апаратні шлюзи. Даний сервіс може застосовуватися для декількох цілей:

- для здійснення переходу між мережами з різними протоколами

(наприклад, IPv4 й IPv6);

- забезпечення конфіденційності й цілісності всієї переданої порції інформації, включаючи службові поля.

Звичайно тунелювання приводить до більше простих і швидких рішень у порівнянні із трансляцією, тому що вирішує більше приватне завдання, не забезпечуючи взаємодії з вузлами транзитної мережі.

Тунелювання може застосовуватися як на мережному, так і на прикладному рівні. Наприклад, стандартизоване туннелювання для IP і подвійне конвертування для пошти X.400.

Комбінація туннелирования й шифрування (з необхідною криптографічною інфраструктурою) на виділених шлюзах дозволяє реалізувати таке важливий в сучасних умовах захисний засіб, як віртуальні частки мережі. Такі мережі, накладені звичайно поверх Інтернету, істотно дешевше й набагато безпечніше, ніж дійсно власні мережі організації, побудовані на виділених каналах. Комунікації на всьому їхньому протязі фізично захистити неможливо, тому краще споконвічно виходити із припущення про уразливість і відповідно забезпечувати захист. Сучасні протоколи, спрямовані на підтримку класів обслуговування, допоможуть гарантувати для віртуальних приватних мереж задану пропускну здатність, величину затримок і т.ін., ліквідуючи тим самим єдину на сьогоднішній день реальну перевагу власних мереж.

Шифрування

Шифрування — найважливіший засіб забезпечення конфіденційності. У комп'ютерної криптографії дві сторони — властиво криптографічна й интерфейсная, що дозволяє сполучатися з іншими частинами IC. Наприклад, інтерфейс GSS-API (Generic Security Service Application Program Interface, RFC 2078) захищає комунікації між компонентами програмних систем, побудованих по архітектурі клієнт-сєрвєр, надаючи їм послуги по взаємної автенти- фікації й по забезпеченню цілісності й конфіденційності повідомлень, що пересилають. Важливо, щоб було забезпечене достатнє функціональне багатство інтерфейсів й їхня стандартизація.

У сучасного шифрування є й внутрішні проблеми, як технічні, так і нормативні. З технічних найбільш гострої є проблема продуктивності. Програмна реалізація на універсальних процесорах не є адекватним засобом (можна провести аналогію з компресією відеозображень). Ще одне технічне завдання — розробка широкого спектра продуктів, призначених для використання у всіх видах комп'ютерного й мережного устаткування — від персональних коммунікаторів до потужних шлюзів. З нормативних проблем відзначимо необхідність офіційного визнання допустимості використання закордонних засобів й алгоритмів (оскільки це пропонується, наприклад, специфікаціями протоколу IPSec).

Контроль цілісності

У керівних документах цілісність інформації визначається як здатність засобу обчислювальної техніки або автоматизованої системи забезпечувати незмінність інформації в умовах випадкового й/або навмисного перекручування (руйнування). Також поширене визначення цілісності інформації як відсутність неналежних змін.

Контроль цілісності ставиться до числа тих сервісів, для яких проблема продуктивності коштує не так гостро, як у випадку шифрування, і вітчизняні стандарти краще погодяться з міжнародними.

Будь-які внесені в оригінальні файли програми-закладки (як відомі сьогодні, так і ті, що з'являться в майбутньому) можуть бути виявлені в ході перевірок цілісності. Вони будуть виявлені по зміні довжини, контрольної суми й інших параметрів оригінального файлу, що виконує.

У сучасних системах контроль цілісності повинен поширюватися не тільки на окремі порції даних (файли, ключі й т.ін.), апаратні або програмні компоненти. Він зобов'язаний охоплювати розподілені конфігурації, захищати від несанкціонованої модифікації потоки даних. Ще надійніше здійснювати подвійний контроль цілісності — безперервний контроль списку критичних подій і контроль файлів, що запускаються при спробах несанкціонованої підміни списку критичних подій (крім того, періодичний контроль файлів).

У цей час існує досить рішень для контролю цілісності й із системної, і з мережною спрямованістю (звичайно контроль виконується прозорим для додатків образом як частина загальної протокольної активності). Найбільш простим й одним з найперших методів забезпечення цілісності даних є метод контрольних сум. Пізніше розроблений спосіб контролю цілісності даних так званий метод циклічної перевірки надмірності (Cycliic Redundancy Check, CRC). Даний алгоритм широко використовується в апаратних пристроях (дискові контролери, мережні адаптери й т. ін.) для верифікації незмінності вхідної й вихідної інформації, а також у багатьох програмних продуктах для виявлення помилок при передачі даних по каналах зв'язку. Істотно більше високої надійності можна досягти, використовуючи односпрямовані функції гешування. І найсучаснішим методом є застосування ЕЦП як реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий у результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису й що дозволяє ідентифікувати власника сертифіката ключа підпису, а також установити відсутність перекручування інформації в електронному документі.

Процедура контролю цілісності окремого повідомлення, або поля, містить у собі два процеси: один на передавальній стороні, інший — на приймаючій. На передавальній стороні до повідомлення додається надлишкова інформація, що є функцією від повідомлення (тей або інший різновид контрольної суми). На приймаючій стороні незалежно генерується контрольна сума отриманого повідомлення з наступним порівнянням результатів. Але даний механізм не захищає від дублювання повідомлень (це робить, наприклад, протокол IPsec).

Для перевірки цілісності потоку повідомлень, захисту від крадіжки, дублювання й вставки повідомлень — використовуються порядкові номери, тимчасові штампи, криптографічне зв'язування, при якому результат шифрування чергового повідомлення залежить від попереднього, або інші аналогічні прийоми. При спілкуванні в режимі без установлення з'єднання використання тимчасових штампів може забезпечити обмежену форму захисту від дублювання повідомлень. Стандартизовано програмний інтерфейс до цього сервісу (як частина раніше згаданого загального інтерфейсу служби безпеки).

Цікаві рішення, що пропонують мережну реалізацію системи контролю цілісності з метою підвищення надійності захисту списків критичних процесів і підвищення ефективності функціонування системи захисту. Ці рішення розподіляють завдання контролю між клієнтською й серверною частинами мережної системи захисту. Клієнтська частина, установлювана на робочу станцію, запобігає можливим порушенням цілісності інформації (програм і даних). Із цією метою виділяються події, зміна яких може привести до наступного перекручування даних, створюються списки дозволених подій і здійснюється контроль правильності (неспотвореності) даних списків. До таких подій можуть бути віднесені ім'я користувача, ім'я процесу, що запускає, і т. ін. (може почати роботу тільки зареєстрований користувач, при цьому в системі може бути запущений тільки дозволений процес, тобто виконана тільки дозволена команда й т. ін.). У випадку виявлення спроби підміни даних у таблицях відповідна подія знищується засобами ОС, про що інформується сервер безпеки (передача інформації на серверну частину). При одержанні команди від серверної частини клієнтська частина виконує контроль файлової системи. Серверна частина, установлювана на виділеному сервері безпеки, крім функції централізованої реєстрації подій, пов'язаних зі спробами НСД до файлів, і ухвалення рішення про доцільність перевірки файлової системи з видачею відповідної команди на клієнтську частину, здійснює контроль схоронності списків дозволених подій. З метою захисту списків дозволених подій клієнтська частина здійснює їхнє періодичне копіювання на серверну частину, де зберігаються еталонні списки, і порівняння списків, що надійшли, з еталоном. Крім того, серверна частина здійснює ті ж перевірки, які проводить і клієнтська, на устаткуванні, на якому вона сама встановлюється.

Контроль захищеності

Контроль захищеності, по суті, являє собою спробу злому ІС, яка здійснюється силами самої організації або уповноваженими особами. Ідея даного сервісу в тім, щоб протестувати реакцію ІС на відомі уразливості в захисті й виявити їх раніше зловмисників. У першу чергу маються на увазі не архітектурні (їх ліквідувати складно), а "оперативні" проломи, що з'явилися в результаті помилок конфігурування й адміністрування або через неуважність до відновлення версій ПЗ.

Засоби контролю захищеності дозволяють накопичувати й бааторазово використовувати знання про відомі атаки. Очевидна їхня схожість із антивірусними засобами; формально останні можна вважати їхньою підмножиною. Очевидний і реактивний, запізнілий характер подібного контролю (він не захищає від нових атак).

Відзначимо також, що переважна більшість атак носить рутинний характер: вони можливі тільки тому, що відомі слабості роками залишаються неусунутими.

Існує кілька типових варіантів застосування систем аналізу захищеності.

Інвентаризація корпоративної мережі з метою одержання інформації про її компоненти. Найчастіше карта мережі створюється (якщо взагалі створюється) на етапі проектування ІС. Потім вона вже не підтримується в актуальному стані й не може бути основою для контролю й виявлення несанкціонованих змін. Крім того, подібна інформація перебуває тільки в управліннях інформатизації і є недоступною для відділів захисту. Для побудови мережної складової цієї карти можна використовувати різні наявні на ринку системи мережного управління типу HP OpenView, SPECTRUM, Vivio, Internet Scanner і т.ін.

Такого роду інструменти містять у собі функцію, що дозволяє автоматично підтримувати актуальність мережної карти, відслідковувати всі несанкціоновані зміни в мережній конфігурації й ідентифікувати на вузлах мережі мережні сервіси, заголовки активних сервісів, типи й версії використовуваних ОС і прикладного ПЗ, поділювані ресурси NetBiOS (NetBiOS Share) і загальні параметри ПБ (політика аудита, використання паролів й облікових записів і т.ін.).

Зловмисники можуть підключати свої комп'ютери до критичних сегментів мережі з метою одержання доступу до переданої конфіденційної інформації. Тоді вони одержують доступ до паролів користувачів й адміністраторів, переданим по більшості протоколів, побудованих на базі стека TCP/IP. Тут же можна виділити й виявлення модемів. Комп'ютери, до яких підключені модеми, ніяк не захищені, і будь-який зловмисник, що виявив такий "чорний хід", може скористатися ним для НСД до ресурсів, що вимагають захисту.

Аналіз настроювань мережного устаткування й засобів захисту (наприклад, маршрутизаторів або більше складних МЕ). Вихід з ладу хоча б одного маршрутизатора або комутатора може надовго порушити функціонування всієї мережі. Метою аналізу є перевірка захищеності комунікаційного устаткування і його схильності різним атакам типу "відмова в обслуговуванні", що порушує функціонування устаткування, або підбор пароля, що дозволяє встановити контроль над цим устаткуванням.

Адміністратори безпеки, як правило, захищають ті комп'ютери, на яких обробляється критична інформація (сервери додатків, веб-серверы, комп'ютери платіжної системи й т.ін.). Однак загальний рівень безпеки мережі дорівнює рівню безпеки самої слабкої її ланки. Як відзначалося вище при розгляді типових уразливостей ОС, для рідко використовуваних сервісів не встановлюють "латок", що усувають виявлені уразливості. Тому недооцінка в захисті рідко використовуваних сервісів, таких, як сервіс мережної печатки або мережного факсу, може бути використана зловмисниками для проникнення в Інтранет або з її інформаційних ресурсів.

Користувачі, не маючи відповідну кваліфікацію в області ІБ, піддають всі ресурси великому ризику, завантажуючи з Інтернету, і встановлюючи неперевірене ПЗ або підключаючи до свого комп'ютера модем. Також більшу небезпеку представляє електронна пошта, за допомогою якої зловмисники можуть впроваджувати на робочі станції користувачів "троянські коні", що дозволяють уживати ці комп'ютери як базові площадки для атаки на інші комп'ютери мережі.

Інтерес зловмисника спрямований, як правило, до тих крапків Інтранету, що не представляє для них інтересу інформації, імовірно, не із захищеної, тобто до вузлів або мереж, з якими встановлені довірені відносини. А вилучені офіси ставляться саме до цієї категорії вузлів.

Аналіз захищеності доступу в Інтернет. Метою даного аналізу є виявлення всіх відомих уразивостей і неправильних конфігурацій, у першу чергу веб-сервера, а також будь-яких інших пристроїв, що перебувають у ДМЗ (FTP-, DNS-сервера, поштового сервера й т.ін.).

Аналіз захищеності специфічних типів мереж. У зв'язку з появою й поширенням

нових мережних технологій виникає необхідність аналізу їхньої уразливості до типових мережних атак, наприклад можливості несанкціонованого підключення пристроїв доступу, до DoS-атак, підбору пароля до крапок доступу, неправильному конфігуруванню й т.ін. Для специфічних мереж типу бездротових (WTeless LAN), побудованих на основі стандарту 802.11b, потрібно перевіряти й характерні тільки для них уразливості (у нашому випадку це слабості WTed Equivalent Privacy, WEP).

Проведення детальних регулярних обстежень із метою аналізу захищеності корпоративних ресурсів і самих засобів захисту.

Існують як комерційні, так і вільно розповсюджувані продукти для здійснення автоматизованого контролю захищеності. Важливо не просто один раз установити їх, але й постійно обновлювати БД типових уразивостей.

Виявлення відмов й оперативне відновлення

Одна з основних проблем побудови мереж є завдання забезпечення їхнього тривалого функціонування, що означає усунення несправностей системи, породжуваних відмовами (faults) і збоями в її роботи Виявлення відмов й оперативне відновлення ставиться до числа сєрвісів, що забезпечують надійність і високу доступність (готовність) (high availability). Його робота опирається на елементи архітектурної безпеки, а саме на існування надмірності в апаратно-програмній конфігурації.

Сучасні мережні технології вимагають усунення крапок, вихід яких з ладу може привести до відмови всієї мережі. Сьогодні при створенні мереж характерне використання складних мережних пристроїв від різних постачальників, таких, як маршрутизатори й мережні інтелектуальні комутатори (hubs). Маршрутизатори, які визначають шлях даних у мережах, можуть обчислити новий шлях у випадку відмови зв'язку. Інтелектуальні комутатори можуть мати конфігурації з надлишковими пристроями й можуть ізолювати відмови у фізичній мережі для запобігання відмови всієї мережі. Важливу роль у підтримці оптимального функціонування систем грають також мережні аналізатори, що дозволяють викликати системного менеджера при будь-якому симптомі, що може потенційно привести до простою. Як правило, системні компоненти типу драйверів, файлових систем і мережних засобів у випадку якої-небудь відмови просто повертають додатку код помилки. В ОС із засобами забезпечення високої готовності є можливість генерувати сигнали тривоги, ідентифікувати їхні джерела й передавати інформацію про їх централізованому процесу обробки подій.

Підвищення надійності засноване на принципі запобігання несправностей шляхом зниження інтенсивності відмов і збоїв за рахунок застосування компонентів з високим і надвисоким ступенем інтеграції, зниження рівня перешкод, полегшених режимів роботи, а також за рахунок удосконалювання методів зборки апаратури. Одиницею виміру надійності є середній час наробітку на відмову (Mean Time Between Failure, MTBF). Підвищення готовності припускає придушення в певних межах впливу відмов і збоїв на роботу системи за допомогою засобів контролю й корекції помилок, а також засобів автоматичного відновлення процесів після прояву несправності включаючи апаратурну й програмну надмірність, на основі яких реалізуються різні варіанти стійких до відмов архітектур. Підвищення готовності — це спосіб боротьби за зниження часу простою системи. Одиницею виміру тут є коефіцієнт готовності, що визначає ймовірність перебування системи в працездатному стані в будь-який довільний момент часу. Статистично коефіцієнт готовності визначається як MTBF/(MTBF+MTTR), де MTTR (Mean Trne To RepaF) — середній час відновлення (ремонту), тобто середній час між моментом виявлення несправності й моментом повернення системи до повноцінного функціонування.

У цей час спектр програмних й апаратних засобів даного класу можна вважати сформованими. На програмному рівні відповідні функції бере на себе ПЗ проміжного шару. Серед апаратно-програмних продуктів стандартом стали кластерні конфігурації (пристрої, що кластеризовані разом, можуть при відмові одного процесора перерозподілити роботу на інші процесори усередині кластера, причому відновлення виробляється оперативно — десятки секунд, у крайньому випадку хвилини, прозорим для

додатків образом).

Відзначимо, що виявлення відмов й оперативне відновлення може грати стосовно інших засобів безпеки інфраструктурну роль, забезпечуючи високу готовність останніх. Це особливо важливо для МЕ, засобів підтримки віртуальних мереж, серверів автентифікації, нормальне функціонування яких критично для ІС у цілому. Такі комбіновані засоби одержують усе більше широке поширення.

Управління

Основними завданнями управління мережею є:

- виявлення й локалізація несправностей у мережному устаткуванні й мєрєжі в цілому в інтересах мінімізації часу відновлення;
- облік мережних й інформаційних ресурсів в інтересах забезпечення функцій управління й планування;
- контроль і управління продуктивністю мережі і її елементів в інтересах підтримки її працездатності й раціонального використання мережних ресурсів.

Управління можна віднести до числа інфраструктурних сервісів, що забезпечують нормальну роботу функціонально корисних компонентів і засобів безпеки. Складність сучасних систем така, що без правильно організованого управління вони поступово деградують як у плані ефективності, так й у плані захищеності. Особливо важливою функцією управління є контроль погодженості конфігурацій різних компонентів (у змісті семантичної погодженості, що ставиться, наприклад, до наборів правил декількох МЕ), постійне адміністрування й перевірка на відповідність політиці безпеки.

Розроблено протоколи мережного управління, що визначають стандартний метод контролю якого-небудь пристрою зі станції управління з метою визначення його стану, настроювань й іншої інформації, а також його модифікації. Основним протоколом управління, використовуваним у сімействі TCP/IP, є протокол SNMP. Сам протокол дуже простий: він визначає тільки ієрархічний простір імен об'єктів управління й спосіб читання/запису даних цих об'єктів на кожному вузлі. Основна перевага цього протоколу полягає в тім, що він дозволяє однаковим образом управляти всіма типами апаратних засобів, незалежно від їхнього призначення й особливостей. Він надає вилучений поточний контроль і настроювання маршрутизаторів, мостів, мережних плат, комутаторів і т. ін.

Для управління звичайно застосовуються так називані платформи мережного управління, що дозволяють здійснювати виявлення пристроїв у мережі, поєднувати модулі управління устаткуванням різних виробників, виконувати загальні функції управління й оповіщення. Сьогодні на ринку вже представлені продукти, що володіють достатньою інтелектуальністю, відкритістю, розширюваністю, масштабованістю, продукти, прийнятні за ціною й по споживаних ресурсах. У число найбільш відомих платформ мережного управління входять HP OpenView, Solstice Domain Manager (Sun Microsystems), CA Unicenter, ШМ Tivoli, SNMPc (Castle Rock) і ін. Вони надають через зручні інтерфейси такі функціональні можливості, як швидке конфігурування настроювань мережі, виявлення пристроїв і каналів зв’язку, складання карт мережі, виявлення виникаючих проблем, управління портами мережних пристроїв, контроль завантаження зі складанням звітів, що набудовують, і відправленням попереджувальних повідомлень, спостереження за мережними подіями, запуск програм настроювання устаткування, а також надання графічної й статистичної інформації про роботу мережі в масштабі реального часу.

3.8. Нормативно-правова основа створення політик безпеки

У сучасних стандартах з організації менеджменту інформаційної безпеки наголошується, що з метою протидії загрозам ІБ, зниження ризиків ІБ та ефективної обробки інцидентів ІБ необхідно забезпечувати й протягом тривалого часу підтримувати достатній для організації рівень безпеки. При цьому головне призначення діяльності з організації управління безпекою ІТ полягатиме у створенні таких умов, за яких мінімізуватимуться ризики ІБ, що, як наслідок, сприятиме стабільному розвитку бізнесу.

Національні стандарти

Вся база національних стандартів ТЗІ наведена на сайті Державної служби спеціального звязку та захисту інформації (http://www.dsszzi.gov.ua).

Міжнародні стандарти

Таблиця 3.3

Перелік чинних та перспективних стандаргів ISO/IEC 27000

Стандарт	Призначення
ISO/IEC 27000:2009	**Системи управління Інформаційною безпекою — Основні положення і терміни**
ISO/IEC 27001:2005	**Системи управління інформаційною безпекою — Вимоги (також відомий, як BS 7799-2:2005)**
ISO/IEC 27002:2005	**Практичні правила управління інформаційною безпекою (також відомий, як BS 7799-1:2005, BS ISO/IEC 17799:2005)**
ISO/IEC 27003:2010	**Керівництво з упровадження системи управління інформаційною безпекою**
ISO/IEC 27004:2010	**Управління інформаційною безпекою — Оцінювання**
ISO/IEC 27005:2008	**Управління ризиками інформаційної безпеки (поєднує вимоги ISO/IEC TR 13335-3:1998 та ISO/IEC TR 13335-4:2000)**
ISO/IEC 27006:2007	**Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою**
ISO/IEC 27007	**Настанови по аудиту систем управління шформацшною безпекою (в розробці)**
ISO/IEC 27008	**Кєрівництво аудиторів заходів керування системами управління інформаційною безпекою (в розробці)**
ISO/IEC 27010	**Управління інформаційною безпекою міжсегментної взаємодії (в розробці, складається з 2-х частин) - Part 1: Керівництво із управління інформаціною безпекою для міжсегментної взаємодії промисловості та уряду, Part 2: Протоколи взаємодії та оповіщення та механізми.**
ISO/IEC 27011:2008	**Настанови по аудиту систем управління інформаційною безпекою для телекомунікаційних організацій засновані на ISO/IEC 27002 (також відомий, як ITU X.1051)**
ISO/IEC 27013	**Керівництво з сумісного впровадження ISO/IEC 20000-1 та ISO/IEC 27001 (в розробці)**
ISO/IEC 27014	**Керівництво інформаційною безпекою (в розробці)**
ISO/IEC 27015	**Керівництво з управління системами інформаційної безпеки для фінансових організацій (в розробці)**
ISO/IEC 27031	**Готовність інформаційно-комунікаційних технологій до забезпечення безперервності бізнесу (в розробці)**
ISO/IEC 27032	**Настанови по кібербезпеці (в розробці)**
ISO/IEC 27033	**Мережева безпека (заснований на ISO/IEC 18028, на даний час передбачено 7 частин, частини 2-7 в розробці) — Part 1: Огляд та концепції (виданий в 2009 р.), Part 2: Настанови по проектуванню та впровадженню мережевої безпеки, Part 3: Довідник по мережевим сценаріям - Загрози, методики проектування та об'єкти контролю, Part 4: Використання шлюзів безвеки для захисту міжмережевої взаємодії - Загрози, методики проектування та об'єкти контролю, Part 5: Захист виртуальних приватних мереж - Загрози, методики проектування та об'єкти контролю, Part 6: Конвергенція IP, Part 7: Настанови по утезпеченню бездротових мереж - Загрози, методики проектування та об'єкти контролю.**
ISO/IEC 27034	**Безпека прикладних програм (складається з 5 частин, в розробці): Part 1: Огляд та концепції, Part 2: Організація системи нормативних документів, Part 3: Процес управління безпекою прикладних програм, Part 4: Перевірка безпекою прикладних програм, Part 5: Структура даних протоколів та мєтодів убезпечення прикладних програм.**
ISO/IEC 27035	**Керівництво інцидентами з інформаційної безпеки (на заміну ISO/IEC TR 18044)**
ISO/IEC 27036	**Настанови із аутсорсінгу в галузі безпеки**
ISO/IEC 27037	**Настанови із ідентифікації, вимявлення, збору та збереження цифрових доказів**
ISO/IEC 27799	**Керівництво із впровадження систем управління інформаційною безпекою в галузі охорони здоров'я засноване на ISO/IEC 27002**

Міжнародний стандарт ISO/IEC 17799:2005. Призначення та особливості

Міжнародний стандарт ISO/IEC 17799:2005 (BS 7799-1:2002) «Управління інформаційною безпекою – Інформаційні технології» («Information Technology – Information Security Management») є найбільш відомим стандартом в області захисту інформації. Він призначений для використання будь-якою організацією, котра планує встановити систему ефективного інформаційного захисту або покращувати існуючі методи інформаційного захисту. Однак, це не свідчить, що всі рекомендації стандарту повинні бути обов'язково прийняті. Все залежить від конкретних місцевих інформаційних ризиків та вимог. Враховуючи таке узагальнений алгоритм застосування стандарту може бути поданий схемою, наведеною на рис. 3.6.

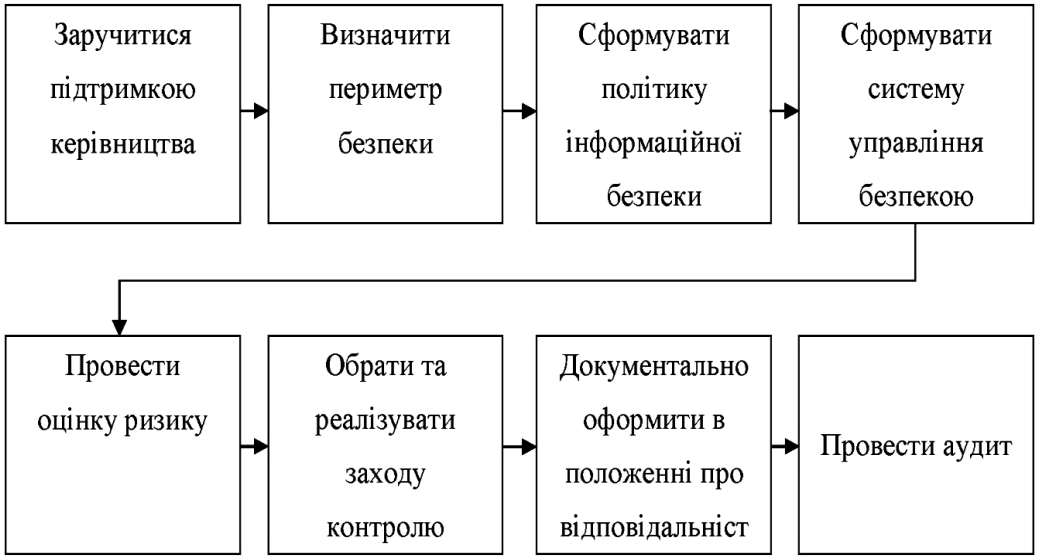


Рис. 3.6. Алгоритм застосування стандарту ISO/IEC 17799:2005

Стандарт відноситься до нового покоління стандартів ІБ. Його розроблено на основі першої частини британського стандарту BS 7799-1:1995 «Практичні рекомендації по управлінню інформаційною безпекою» («Information Security Management – Part 1: Code of Practice for Information Security Management»). Стандарт складається з 13 розділів (рис. 3.7):

1. Загальна частина
2. Терміни та визначення
3. Політика безпеки
4. Організовані методи забезпечення інформаційної безпеки
5. Управління ресурсами
6. Користувачі інформаційної системи
7. Фізична безпека
8. Управління комунікаціями та процесами
9. Контроль доступу
10. Придбання та розробка інформаційних систем
11. Управління інцидентами інформаційної безпеки
12. Управління безперервністю ведення бізнесу
13. Відповідність вимогам.

Рис. 3.7. Основні області застосування стандарту ISO/IEC 17799:2005

Кожен з розділів стандарту має таку структуру:

- мета – вказує, яка мета повинна бути досягнута;
- управління – вказує, як визначені цілі можуть бути досягнуті;
- керівництво – вказує, як управління може бути реалізовано та Додатки.

Зокрема в термінах і визначеннях позиціонуються такі поняття, як інформаційна безпека (збереження конфіденційності, цілісності й доступності інформації), конфіденційність (забезпечення доступу до інформації тільки для авторизованих користувачів, що мають право на доступ до неї), цілісність (захист точності й повноти інформації й методів її обробки), доступність (забезпечення доступності інформації й пов'язаних з нею ресурсів авторизованим користувачам за необхідності) тощо. Також визначається політика безпеки.

Документ, що містить опис політики інформаційної безпеки повинен бути схвалений керівництвом, опублікований й відповідно розповсюджений серед всіх співробітників. Цей документ повинен виражати підтримку керівництва компанії й визначати підхід до УІБ, що буде застосовуватися в організації. Як мінімум даний документ повинен включати такі відомості:

- визначення ІБ, її загальні цілі й галузь дії, а також відомості про важливість безпеки як механізм, що робить можливим спільне використання інформації;
- заява про наміри керівництва, яка висвітлює цілі й принципи УІБ;
- короткий опис політики безпеки, принципів, стандартів і нормативних вимог, що мають певне значення для організації, наприклад: відповідність вимогам законодавства й умовам контрактів; вимоги до освітньої підготовки в галузі безпеки; захист від вірусів й інших зловмисних програм; підтримка безперервності бізнесу; наслідки порушення політики безпеки;
- визначення загальних і приватних обов'язків з управління інформаційною безпекою, у тому числі надання відомостей про інциденти;

- посилання на документацію, що може доповнювати опис політики, наприклад, більш докладні описи політик й інструкцій для Конкретних інформаційних систем або правила безпеки, які повинні дотримуватися користувачами. Цей опис політики необхідно поширити серед користувачів у всій організації в придатному для них вигляді.

Для цього необхідно призначити співробітника, відповідального за підтримку політику ІБ та її оновлення відповідно до прийнятої процедури. Ця процедура повинна гарантувати перегляд політики у відповідь на будь-які зміни, що впливають на основу вихідної оцінки ризиків – наприклад, великі інциденти, пов'язані з безпекою, нові вразливості або зміни в організаційній або технічній інфраструктурі. Крім того, необхідно створити графік періодичної переоцінки таких критеріїв:

- ефективність політики, яка демонструється на основі типів, кількості й збитку від зареєстрованих інцидентів;
- вартість і вплив заходів безпеки на ефективність діяльності організації;
- вплив технологічних змін.

Відповідно до положень стандарту регламентується процедура аудиту безпеки інформаційних систем (рис. 3.8).

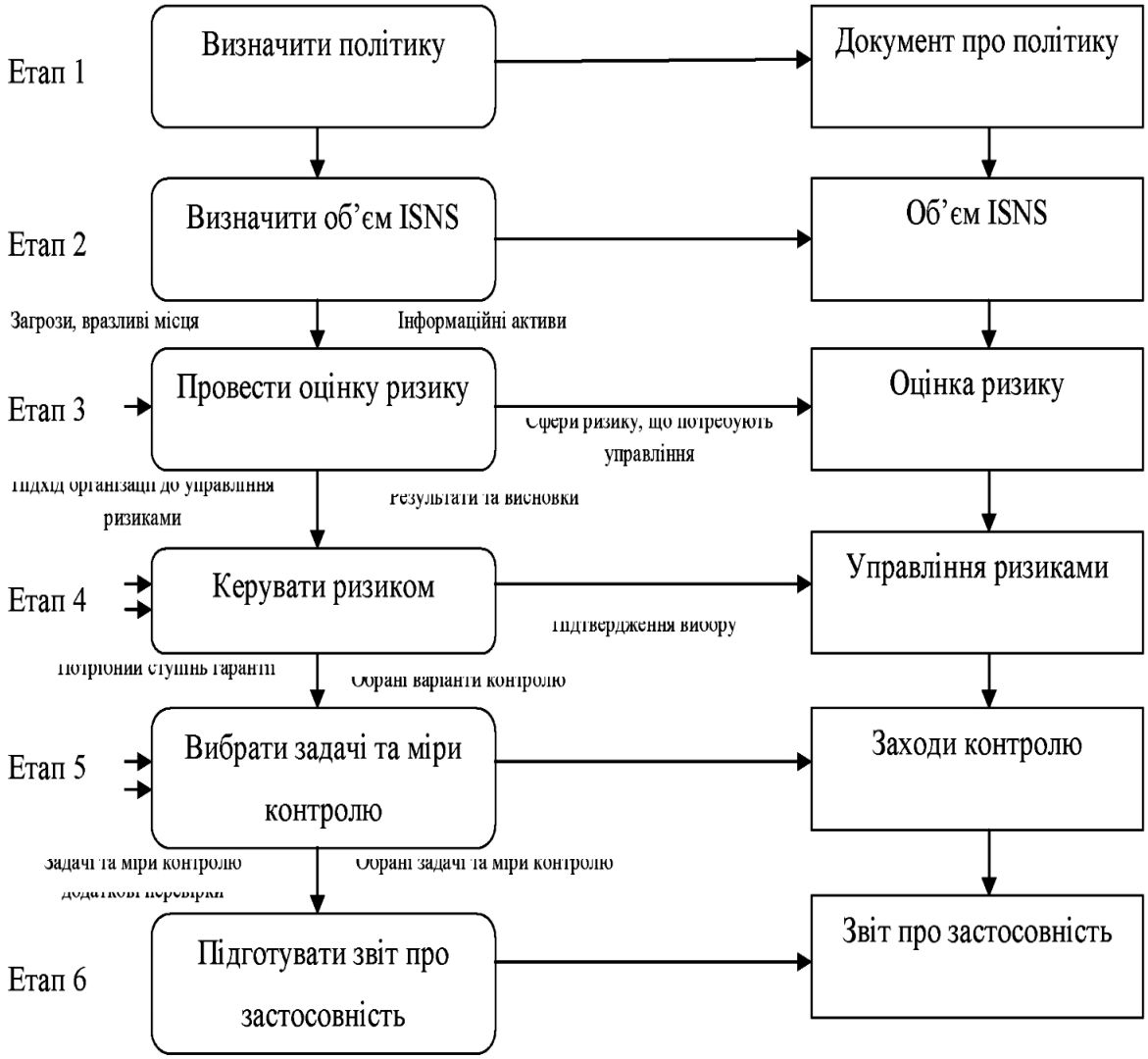


Рис. 3.8. Рекомендовані етапи перевірки режиму інформаційної безпеки

Правила по управлінню ІБ розбиті у стандарті на десять розділів:

- політика безпеки;
- організація безпеки;
- класифікація ресурсів і їх контроль;
- безпека персоналу;
- фізична безпека;
- адміністрування інформаційних систем і мереж;
- управління доступом;
- розробка і супровід інформаційних систем;
- планування безперервної роботи організації;
- контроль виконання вимог політики безпеки.

Ключові засоби контролю представляють або обов'язкові вимоги (наприклад, вимоги діючого законодавства), або рахуються основними структурними елементами інформаційної безпеки (наприклад, навчання правилам безпеки). Ці засоби актуальні для всіх організацій і складають основу системи УІБ. Вони служать в якості основи для організації, що приступає до реалізації засобів управління інформаційною безпекою. До ключових відносяться наступні засоби контролю:

- документ про політику інформаційної безпеки;
- розподіл обов'язків по забезпеченню інформаційної безпеки;
- навчання і підготовка працівників до підтримування режиму ІБ;
- повідомлення про випадки порушення безпеки;
- засоби безпеки від вірусів;
- планування безперервної роботи організації;
- контроль над копіюванням програмного забезпечення, захищеного законом про авторські права;
- захист документації і даних організації;
- контроль відповідності політики безпеки.

Стандарт ISO 17799 (BS 7799) дозволяє задати правила безпеки і визначити політику безпеки. Так, наприклад, представлені контрольні запитання згідно стандарту BS 7799-2, які дозволяють оцінити систему управління інформаційною безпекою та задати правила безпеки.

Додаткові рекомендації по вибору політики безпеки мають керівництва Британського інституту стандартів (www.bsi-glbal.com) у вигляді серій:

«Можливості сертифікації на відповідність вимог стандарту BS 7799-2»;

«Керівництво з вибору засобів забезпечення інформаційної безпеки у відповідності із BS 7799-2» тощо.

Таким чином, для побудови збалансованої системи БІТ організаії потрібно спочатку провести аналіз ризиків у сфері ІБ. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему БІТ (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику.

Міжнародний стандарт ISO/IEC 27001. Призначення та особливості

ISO/IEC 27001 – міжнародний стандарт з інформаційної безпеки розроблений спільно Міжнародною Організацією по Стандартизації (ISO) та Міжнародною електротехнічної комісією (IEC). Стандарт містить вимоги в області ІБ для створення, розвитку і підтримки Системи менеджменту інформаційної безпеки (СМІБ). Поняття "захисту інформації" трактується в стандарті як забезпечення конфіденційності, цілісності та доступності інформації (рис. 3.9). Основа стандарту ICO 27001 – система управління ризиками, пов'язаними з інформацією. Система управління ризиками дозволяє отримувати відповіді на наступні питання:

- на якому напрямку ІБ потрібно зосередити увагу?
- скільки часу і коштів можна витратити для захисту інформації?

Процес сертифікації організації акредитованими агентствами згідно з цим стандартом складається з трьох стадій:

- стадія 1: вивчення аудитором ключових документів Системи Менеджменту Інформаційної Безпеки (положення про застосування (SoA).

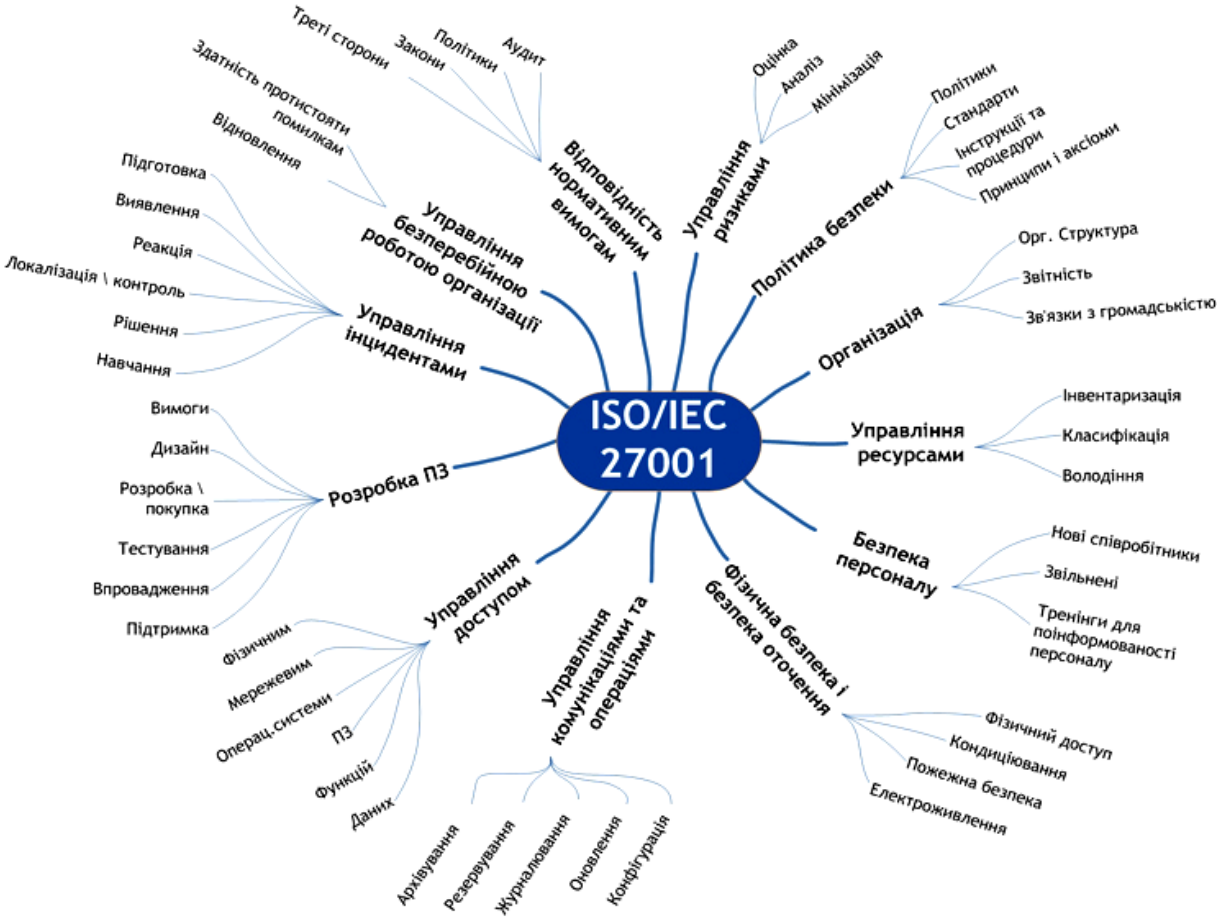


Рис.3.9. Структура стандарту ISO/IEC 27001

Зазначені заходи можуть виконуватися як на території організації, так і шляхом висилки цих документів зовнішньому аудитору;

- стадія 2: детальний, глибокий аудит включаючи тестування впроваджених заходів та оцінювання їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

- стадія 3: виконання інспекційного аудиту для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується періодично.

Алгоритм впровадження системи менеджменту інформаційної безпеки відповідно до вимог міжнародного стандарту ISO/IEC 27001 передбачає послідовне виконання таких основних етапів:

- перший етап – управлінський, полягає в усвідомленні цілей і вигоди впровадження СМІБ, отриманні підтримки керівництва на впровадження та введення в експлуатацію СМІБ, розподіленні відповідальності за СМІБ;

- другий етап – організаційний, полягає у створенні груп з впровадження та підтримки СМІБ, навчанні групи з впровадження та підтримки СМІБ, визначення області дії СМІБ;

- третій етап – початковий аналіз СМІБ, полягає у проведенні аналізу існуючої СМІБ, визначенні переліку робіт з доопрацювання існуючої СМІБ;

- четвертий етап – визначення політики і цілей СМІБ, полягає у визначенні політики СМІБ, визначенні цілей СМІБ по кожному процесу СМІБ;

- п’ятий етап – порівняння поточної ситуації зі стандартом, полягає у проведенні навчання відповідальних за СМІБ вимогам стандарту, опрацюванні вимог стандарту, порівнянні вимог стандарту з існуючим станом справ;

- шостий етап – планування впровадження СМІБ, полягає у визначенні переліку заходів для досягнення вимог стандарту, розробці керівництва з ІБ;

- сьомий етап – впровадження системи управління ризиками, полягає в розробці процедури з ідентифікації ризиків, ідентифікуванні і ранжуванні активів, визначенні відповідальних за активи, оцінюванні активів, ідентифікуванні загроз та вразливостей активів, проведенні розрахунків і ранжуванні ризиків, розробці плану по зниженню ризиків, визначенні непридатних напрямів безпеки, розробці положення про застосування контролів;

- восьмий етап – розробка документації СМІБ, полягає у визначенні переліку документів (процедур, записів, інструкцій), а також у розробці управлінських процедур (стандарт на розробку документів, управління документацією, записами; коригувальні і попереджуючі заходи; внутрішній аудит; управління персоналом та ін); технічних процедур (придбання, розвиток і підтримка інформаційних систем; управління доступом; реєстрація та аналіз інцидентів; резервне копіювання; управління знімними носіями та ін); управлінських записів (звіти про внутрішні аудити, аналіз СМІБ з боку вищого керівництва; звіт про аналіз ризиків; звіт про роботу комітету з інформаційної безпеки; звіт про стан коригувальних і запобіжних дій; договору; особисті справи співробітників та ін); технічних записів (реєстр активів; план підприємства; план фізичного розміщення активів; план комп’ютерної мережі; журнал реєстрації резервного копіювання; журнал реєстрації факту технічного контролю після змін в операційній системі; логи ІС; логи системного адміністратора; журнал реєстрації інцидентів; журнал реєстрації тестів з безперервності бізнесу та ін); інструкцій, положень (правила роботи з ПК, правила роботи з інформаційною системою, правила поводження з паролями, інструкція з відновлення даних з резервних копій, політика віддаленого доступу, правила роботи з переносним обладнанням та ін.);

- дев’ятий етап – навчання персоналу, полягає у навчанні керівників підрозділів, а також всього персоналу вимогам ІБ;

- десятий етап – розробка та прийняття заходів щодо забезпечення роботи СМІБ, полягає у впровадженні засобів захисту (адміністративних, навчальних і технічних);

- одинадцятий етап – внутрішній аудит СМІБ, полягає у підборі команди внутрішнього аудиту СМІБ, плануванні внутрішнього аудиту СМІБ, проведенні внутрішнього аудиту СМІБ;

- дванадцятий етап – аналіз СМІБ з боку вищого керівництва, полягає у проведенні аналізу СМІБ з боку вищого керівництва;

- тринадцятий етап – офіційний запуск СМІБ, полягає в підписанні наказу про введення СМІБ в дію;

- чотирнадцятий етап - оповіщення зацікавлених сторін (клієнтів, партнерів, ЗМІ тощо) про запуск СМІБ.

Отже, впровадження стандарту ISO/IEC 27001 дозволить дати відповіді на наступні питання:

1) які на сьогоднішній день інформаційні ризики підприємства і як вони впливають на бізнес-процеси? Як ці ризики мінімізувати?;

2) які інформаційні активи є в компанії, і що захищати в першу чергу?;

3) що робити, якщо трапиться непередбачена ситуація?

3.9. Управління безпекою інформаційних технологій

Управління безпекою інформаційних технологій (БІТ) в організації – це цілеспрямований процес, який здійснюється з метою досягнення і забезпечення

необхідних рівнів конфіденційності, цілісності, доступності, достовірності і надійності інформації, яка в ній циркулює (рис. 3.10).

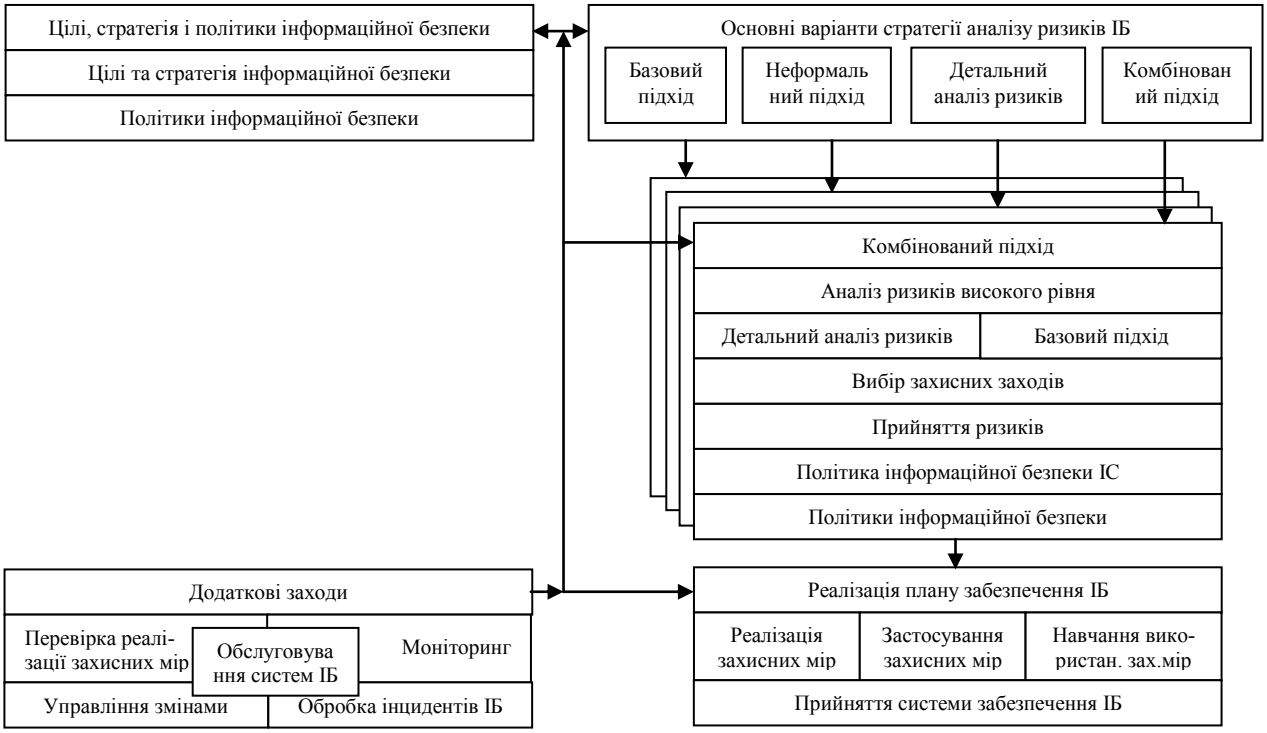


Рис. 3.10. Етапи процесу управління інформаційною безпекою

Сутність процесу управління БІТ зводиться до аналізу вимог захисту, створенні плану з дотримання цих вимог, виконанні цього плану, а також підтриманні й управлінні здійсненим захистом (див. рис. 3.10). Починається процес з визначання організацією цілей і стратегій захисту в інформаційних технологіях й має своє логічне продовження у методиках захисту інформаційних технологій.

Відправною точкою початку такої діяльності в організації є встановлення чітких цілей безпеки, які повинні задовольнити її потреби. Щоб визначити такі цілі, необхідно розглянути активи організації та їхню цінність. Для цього бажано знайти відповіді на такі питання:

- наскільки важливою є та частина бізнесової діяльності організації, яка не може виконуватися без підтримки інформаційних технологій;
- які задачі організації можуть бути виконані її співробітниками лише з використанням інформаційних технологій;
- які важливі рішення залежать від точності, цілісності, доступності чи актуальності інформації, оброблюваної за допомогою інформаційної технології;
- яка оброблювана конфіденційна інформація потребує захисту;
- які можуть бути приховані передумови небажаних інцидентів безпеки для організації при впровадженні інформаційних технологій тощо.

Кінцевою метою створення системи безпеки інформаційних технологій є попередження або мінімізація збитку (прямого або опосередкованого, матеріального, морального або іншого), що завдається суб'єктам інформаційних відносин завдяки небажаного впливу на інформацію, її носіїв та процеси обробки.

Практичний досвід з управління БІТ показує, що даний процес є довготривалим. Головний зміст даного процесу становить управління: управління людьми, ризиками, ресурсами, засобами захисту тощо. Він складається з багатьох взаємопов'язаних підпроцесів. Деякі з них, такі як управління конфігурацією настроювання, управління змінами та ризиками застосовувані не тільки до питань безпеки. Так, наприклад,

підпроцес настроювання системи полягає у фіксації тенденції можливих змін. Метою управління настроюванням, з погляду безпеки, є розпізнання змін та дослідження ступеня їх можливого впливу на загальну безпеку організації, а також гарантування того, що зміни в системі не знизять ефективність засобів захисту і загальну безпеку організації.

Управління змінами – процес визначання потреб в нових засобах безпеки у випадках, коли відбуваються зміни в системі ІТ. Такі зміни можуть спровокувати нові процедури та нові можливості ІТ, модернізоване програмне та перероблене апаратне забезпечення. Вони можуть виникнути при появі нових користувачів у зовнішніх або анонімних групах, а також при роботі користувачів з мережами і зв'язками. Якщо такі факти фіксуються або стає відомо про можливе внесення змін в систему інформаційних технологій важливо визначити ступень ураження в захисті системи, якщо зміни мали місце або спланувати комплекс заходів щодо попередження таких змін. При цьому має бути оцінена величина ризику, виходячи з користі і витрат.

Управління ризиком – процес визначання, регулювання і виокремлення чи мінімізації сумнівних подій, що можуть впливати на ресурси системи ІТ. Він передбачає порівняння оцінки ризиків з вигодами і (або) витратами на засоби безпеки і забезпечення стратегії їхнього застосування. Дії з управління ризиками найбільш ефективні, якщо вони виконуються в процесі всього життєвого циклу системи. Процедура аналізу ризику ідентифікує ризики, що вимагають управління ними або врахування (прийняття до уваги) в подальшій роботі ІС. Вона може бути реалізована без додаткових витрат часу і ресурсів після оглядового і короткого аналізу всіх підсистем ІС. При цьому власне самі ризики з погляду безпеки оцінюють відносно потенційного ураження, що може бути викликано порушенням конфіденційності, цілісності, доступності, облікованості, достовірності чи надійності інформації. Результатом оглядового аналізу ризику є положення про найбільш ймовірні ризики стосовно активів. Його наявність дозволить установити, які підсистеми можуть бути захищені за допомогою практичних вказівок або базовими засобами управління, а також ті, які можна використати після детальнішого аналізування ризику. Це питання практично охоплює комплект інструкцій і базових настанов, які можуть бути використані як базис для домовленості щодо задоволення основних потреб захисту.

Забезпечення ефективної безпеки інформаційних технологій вимагає обліковості (звітності) точно визначених завдань і розподілу обов'язків у питаннях безпеки. Обов'язки і обліковість мають бути доручені власникам активів, постачальникам і користувачам ресурсів систем інформаційних технологій. Отже, володіння активами і пов'язані з ними обов'язки щодо безпеки з подальшим перевірянням реалізованої безпеки є важливими чинниками для ефективної безпеки. Відсутність компетентності і недостатність досвіду персоналу також може призвести до значного зниження ефективності загальної системи безпеки організації. Щоб бути упевненим у належному рівні компетентності в безпеці організації, необхідно дотримуватись і розвивати програму компетентності безпеки, метою якої є пояснення робітникам, компаньйонам і компаніям-постачальникам цілей, стратегій і методик безпеки, а також потреб у безпеці і зв'язаних з ними функцій і обов'язків. Її реалізація передбачається у декілька етапів, одним із яких є розроблення і розподіл документації щодо компетентності в безпеці (наприклад плакатів, бюлетенів, брошур чи брифінгів). Призначення цих матеріалів – збільшити загальну компетенцію службовців і контрактників. Наступний етап – організація курсів для навчання службовців з питань безпеки. Також необхідні поглиблені курси професійного рівня для специфічних аспектів безпеки. У деяких випадках ефективним є об'єднання всіх повідомлень з безпеки в окремі навчальні програми. Цей підхід може бути альтернативою або повноцінною заміною до програми компетентності безпеки. Для розвитку програми компетентності безпеки, що взаємозалежна з необхідними мікрополітичними й адміністративними умовами організації, увага має бути зосереджена на таких аспектах: аналізу потреб; забезпеченні контролю та змісті програми компетентності. Крім того, має бути розроблена

програма забезпечення ІБ , що гарантуватиме розподіл обов'язків із безпеки між співробітниками, компаньйонами і компаніями-постачальниками.

Після затвердження цілей безпеки ІТ організації необхідно розробити стратегію їх захисту, яка стане основою для розробки відповідних методів захисту. Обрана стратегія має відповідати важливості активів, які підлягають захисту. Якщо, наприклад, відповідь на одне або кілька питань, що були наведені вище буде стверджувальною, то найімовірніше організація має важливі потреби в захисті і необхідно порекомендувати обрати стратегію разом з необхідними заходами для реалізації цих потреб.

Стратегія управління БІТ тезисна і в загальних рисах описує способи досягнення організацією заданого рівня безпеки. Положення, яких має стосуватися стратегія, будуть залежати як від кількості, типу і важливості цих цілей, так і тих цілей, які організація розглядає як важливі для усіх своїх підрозділів. Положення можуть бути або цілком конкретними або дуже загальними. Приклад першого: організація, яка може мати таку первинну мету безпеки інформаційних технологій, що через вид її ділової активності всі системи повинні підтримувати високий рівень доступності. У цьому випадку одне положення стратегії може бути спрямоване на зменшення зараження вірусами через впровадження антивірусного програмного забезпечення для всієї організації (чи визначенням вибіркових ділянок для перевірки на наявність вірусу, необхідної для всього отриманого програмного забезпечення). Приклад останнього, щодо загального рівня: організація може мати мету безпеки інформаційної технології, тому що її ділова активність щодо надання послуг інформаційних технологій і захист її систем, повинні бути продемонстровані потенційним замовникам. У цьому випадку положення стратегії можуть полягати в тому, що всі системи затверджують як такі, безпечність яких визначає третя особа.

Інші можливі положення стратегії безпеки інформаційних технологій, згідно з визначеними цілями чи їхніми комбінаціями, можуть включати:

- стратегію аналізу ризику і методи, що будуть прийняті для всієї організації;
- вимоги методів забезпечення БІТ для кожної системи;
- вимоги механізмів захисту для кожної системи;
- схему класифікації критичної інформації для всієї організації;
- вимоги щодо захисту засобів зв'язку; це повинно бути визначено і перевірено до установлення відносин з іншими організаціями;
- схему обробки інцидентів, універсальну у використанні.

Після визначення стратегії безпеки її положення мають міститися в методиці безпеки інформаційних технологій організації, яка має базуватися на вагомих твердженнях на користь захисту, особливо якщо є необхідність узгодження захисту і стратегії. Методика безпеки повинна охоплювати такі розділи:

- інфраструктуру організації і розподіл обов'язків;
- інтеграцію захисту в розробці і реалізації системи;
- класи класифікації інформації, стратегії управління ризиком;
- планування непередбачених обставин, юридичні і регуляторні зобов'язання;
- зовнішнє управління розробкою й забезпечення інформаційної взаємодії;
- вимоги безпеки інформаційних технологій (умови конфіденційності, цілісності, доступності, обліковості, достовірності і надійності, особливо з урахуванням уявлень власників активів);
- заходи з підготовки персоналу (особлива увага повинна приділятися службовцям, що займають відповідальні посади, наприклад, технічному персоналу й адміністраторам системи) тощо.

Діяльність із забезпечення БІТ організації здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від тину діяльності, в якій вони

використовуються, а також сфери застосування. Так, наприклад, важливими методами аналізу стану забезпечення БІТ організації є методи опису та класифікації, а також методи дослідження причинних зв'язків. За допомогою останніх виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. Серед них найбільшого застосування отримали: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану забезпечення БІТ залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери БІТ, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський та технологічний рівні, рівень користувача, мережний і процедурний рівні. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному – здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності. На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання роботоздатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Нині можна виокремити декілька типів методів забезпечення БІТ:

- однорівневі методи (будуються на підставі одного принципу управління БІТ);
- багаторівневі методи (будуються на основі декількох принципів управління БІТ, кожний з яких слугує для вирішення власного завдання);
- комплексні методи (багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення безпеки інформаційних технологій виходячи з аналізу сукупності чинників небезпеки);
- інтегровані високоінтелектуальні методи (багаторівневі, багатокомпонентні технології, які побудовані на підставі потужних автоматизованих інтелектуальних засобів із організаційним управлінням).

Вони активно використовуються на будь-якій стадії управління загрозами. При цьому специфіка методів, які використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. У цілому ж слід зазначити, що обрання цілей, стратегій і методів протидії конкретним загрозам та небезпекам безпеці інформаційних технологій становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності. Для цього цілі (які мають бути досягнуті), стратегії (як досягнути цих цілей) і методи (які визначають правила для досягнення цілей) доцільно визначати для кожного рівня організації і для

кожного ділового підрозділу чи відділу. Для досягнення необхідного рівня ефективності безпеки різні цілі, стратегії і методики для кожного організаційного рівня і ділового підрозділу мають бути впорядковані та узгоджені між собою. Це досягається шляхом перевірки (контролювання) вихідних даних на наявність вагомих для безпеки подій.

До функцій управління безпекою інформаційних технологій належать:

- визначення цілей, стратегій і методик організації БІТ;
- визначення необхідних умов під час організації БІТ;
- ідентифікація та аналіз загроз безпеки для активів ІТ організації;
- ідентифікація та аналіз ризиків;
- визначення відповідних засобів безпеки;
- контроль за застосуванням і функціонуванням засобів безпеки;
- розроблення і реалізація програми компетентності в безпеці;
- виявлення і реагування на інциденти.

Для повноцінної реалізації цих функцій як на стратегічному, так й на тактичному та оперативному рівнях (рис. 3.11) БІТ повинна стати невід'ємною частиною загального плану управління організацією (ДСТУ ISO/IEC TR 13335-1:2003). Самий верхній рівень БІТ – адміністративний. На ньому приймаються суто стратегічні рішення.

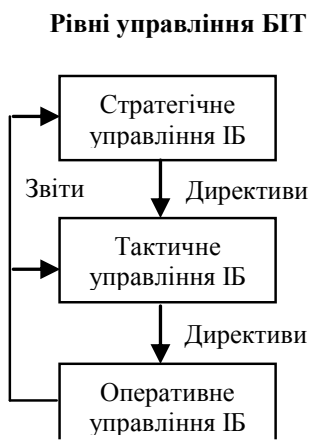


Рис. 3.11. Рівні управління безпекою інформаційних технологій

Середній рівень ІБ – тактичний. Його ключовою ланкою є центр управління ІБ, головне призначення якого полягає у формуванні й контролюванні ПІБ організації (рис. 3.12).

На нижньому – тактичному рівні сформована ПІБ знаходить свою практичну реалізацію. Аналіз стану ІБ проводиться на підставі порівняння визначеної політики ІБ даним моніторингу і аудита ІБ рівня оперативного управління. Кваліфікація осіб, відповідальних за безпеку інформаційних технологій повинна бути при цьому достатньою для адаптування матеріалів до конкретних потреб організацій.

Головними елементами, задіяними в процесі управління безпекою інформаційних технологій в організації є її активи.

До активів організації належать:

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

Активи є об'єктами для багатьох видів загроз (табл. 3.4).

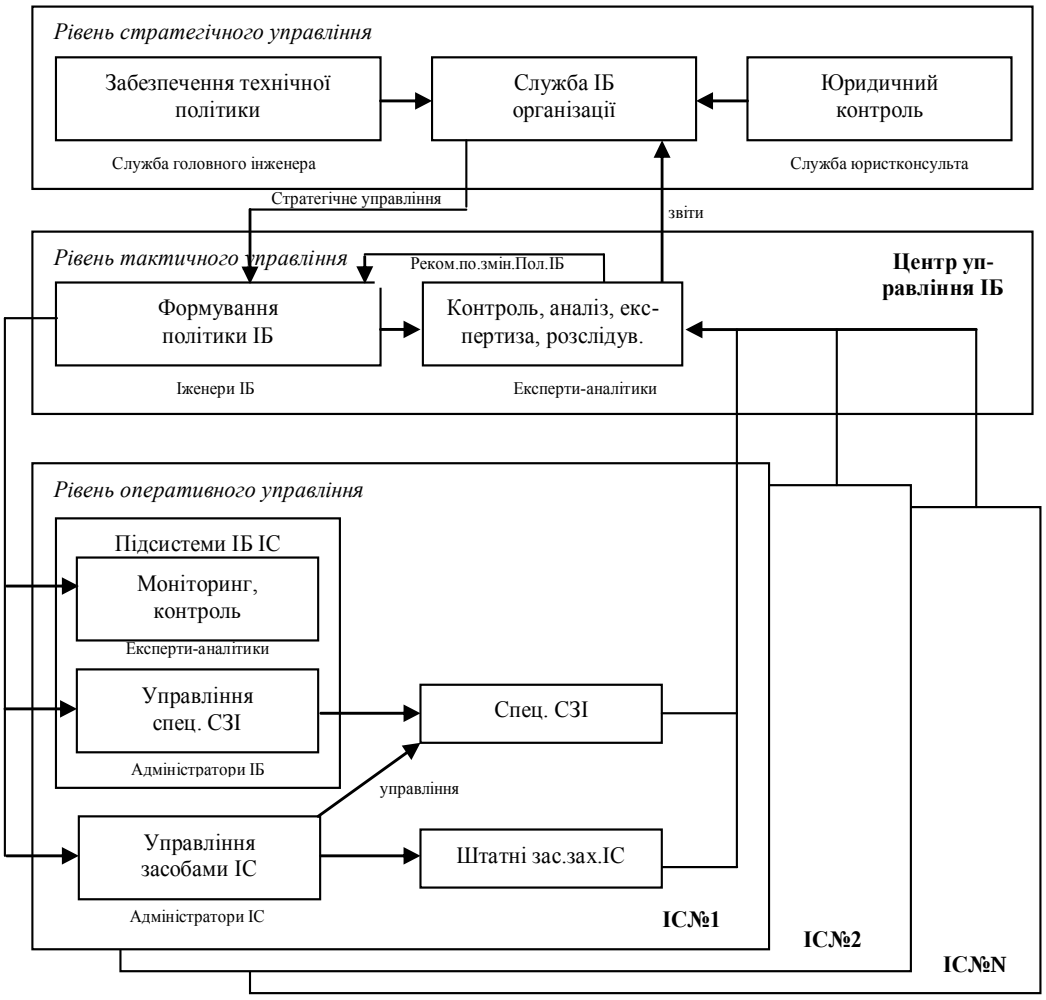


Рис. 3.12. Функціональна структура управління політикою безпеки інформаційних технологій

Таблиця 3.4

Приклади загроз

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

Загроза потенційно є причиною небажаного інциденту, що здатний заподіяти шкоду системі чи організації та її активам. Ця шкода є результатом прямої чи непрямої атаки, спрямованої на інформацію, якою оперує система чи служба інформаційних технологій, і являє собою, наприклад, її несанкціоноване знищення, розкриття, зміну, перекручування, втрату доступності чи втрату. Загроза може здійснитися, заподіяти шкоду у випадку наявності в активах уразливих місць. Загрози, причиною яких є людина, розділяють на випадкові й навмисні.

Деякі загрози мають спрямовану дію на окремі елементи організації, наприклад викликають збої інформаційних систем. Загрози можуть мати специфічне територіальне

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

Обсяги шкоди заподіяні загрозою, можуть варіювати в широких межах для кожного конкретного випадку. Наприклад:

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

Такі загрози часто характеризуються обсягами заподіюваної ними шкоди. Наприклад, вірус можна охарактеризувати як такий, що руйнує чи не руйнує, а силу землетрусу можна відобразити за шкалою Ріхтера.

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

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

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

Оточення й мікрополітика організації можуть мати істотне значення й обумовлювати вплив загроз на організацію. У критичних ситуаціях деякі загрози в певних мікрополітичних середовищах не розглядають і вважають безпечними.

Вразливості звичайно пов’язані зі слабкими місцями в активах, а саме у розташуванні організації, процесах, персоналі, управлінні, адмініструванні, апаратному та програмному забезпеченні, в інформації. Їх використовують як потенційну загрозу для заподіяння шкоди системі інформаційних технологій чи діловій активності в цілому. Вразливість сама по собі не є причиною шкоди. Вона є умовою чи множиною умов, які можуть допустити вплив загрози на активи.

Вразливість послабляє експлуатовану систему і може призводити до небажаних наслідків. Наприклад, відсутність механізмів контролювання за доступом до службових і гостьових приміщень – вразливість, що може дати змогу загрозі з легкістю впливати на активи і призводити до їхньої втрати. Специфіка конкретної системи чи організації спричинює те, що не всі вразливості чутливі до загроз. Треба негайно приділяти увагу вразливості, що має відповідну загрозу. Оскільки оточення може змінюватися динамічно, усі вразливості потрібно постійно перевіряти щодо відкритості до старих і нових загроз. Аналіз вразливості – це експертиза слабких місць, вразливих до ідентифікованих загроз. Цей аналіз повинен брати до уваги середовище й наявні засоби захисту. Вразливість специфічної системи чи активів до загрози описує способи, якими система чи активи можуть бути ушкоджені.

Ураження – наслідок небажаного інциденту, спричинений навмисним чи випадковим впливом на активи. Наслідки можуть бути згубними для деяких активів, нанести ушкодження системі інформаційних технологій, призвести до втрати

конфіденційності, цілісності, доступності, обліковості, достовірності чи надійності ІС. Можливі також і побічні наслідки, наприклад, іміджу компанії. Уведення кількісних характеристик уражень дає можливість знаходити компромісне рішення між втратами в результаті небажаного інциденту і витратами на засоби захисту, які страхують від небажаного інциденту. Необхідно враховувати також і частоту появи небажаних інцидентів. Це особливо важливо, коли заподіяна шкода в кожному окремому випадку незначна, проте сумарні втрати як наслідок багатьох випадків протягом періоду часу будуть дуже великими. Запобігання ураженням є важливим складником у зменшенні ризику і виборі засобів безпеки.

Кількісні і якісні характеристики ураження можна отримати через:

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

Ризик – ймовірність того, що активи чи група активів є уразливими до загроз, що, як результат, може спричинити їхнє ушкодження чи знищення. Разові або численні загрози, що повторюються, можуть скористатися окремою чи множинною вразливістю. Сценарій ризику описує як специфічна загроза чи група загроз може скористатися конкретною вразливістю чи групою вразливостей, що шкодять активам. Ризик характеризується комбінацією двох чинників: ймовірністю появи небажаного інциденту і його ураженням. Будь-яка зміна стану активів, загроз, вразливостей і засобів захисту може вплинути на ризики. Чим раніше будуть виявлені зміни в оточенні чи в самій системі, тим більше можливостей для дій, що зменшують ризик.

Засоби безпеки – засоби, процедури або механізми, що можуть захистити від загроз, зменшити вразливість, обмежити ураження внаслідок небажаного інциденту, знайти небажані інциденти і полегшити процес відновлення. Ефективна безпека звичайно потребує комбінації різних засобів безпеки для забезпечення багаторівної безпеки активів. Наприклад, механізми контролювання доступу, які застосовуються в ІС, повинні супроводжуватися засобами управління аудитом, увагою персоналу, навчанням і безпекою фізичних засобів.

Засоби безпеки можуть виконувати одну або декілька таких функцій: виявляння, стримування, запобігання, обмеження, корекція, відновлювання, контролювання й усвідомлення. Відповідний добір засобів безпеки – невід’ємна частина правильно виконаної програми безпеки. Часто вигідніше і дешевше вибрати засоби безпеки, що реалізують декілька функцій аніж боротися з наслідками. Засоби безпеки використовуються фізичним і технічним оточенням (апаратні засоби, програмне забезпечення і зв’язок), персоналом та адміністрацією.

Приклади засобів безпеки:

- фаєрволи в мережі;
- моніторинг і аналіз мережі;
- шифрування з метою забезпечення конфіденційності;
- цифрові підписи;
- програми антивірусів;
- резервні копії інформації;
- безперебійні джерела живлення;
- механізми контролювання доступу.

Обмеження звичайно установлює чи визнає керівництво організації з урахуванням чинників оточення, в якому діє організація. Розглядають, наприклад, організаційні, фінансові, навколишні, персональні, часові, юридичні, технічні та мікрополітичні/соціальні обмеження:

Усі ці чинники треба враховувати під час вибору і застосування засобів безпеки. Періодично наявні та нові обмеження треба переглядати, фіксуючи будь-які зміни.

Необхідно також відзначити, що обмеження можуть змінюватися з часом, географією і соціальним еволюціонуванням, а також з мікро політикою організації. Оточення і мікрополітика, у яких діє організація, можуть негативно впливати на різні елементи безпеки, особливо на загрози, ризики і засоби безпеки.

Відомо, що нині існує багато моделей, спрямованих на забезпечення управління безпекою інформаційних технологій. Вони здебільшого представляють концепції, необхідні для розуміння процесів управління, описують залежності елементів безпеки і управління ризиком, а також власне управління процесом безпеки інформаційних технологій. Один з можливих варіантів структури концепції БІТ подано на рис. 3.13.

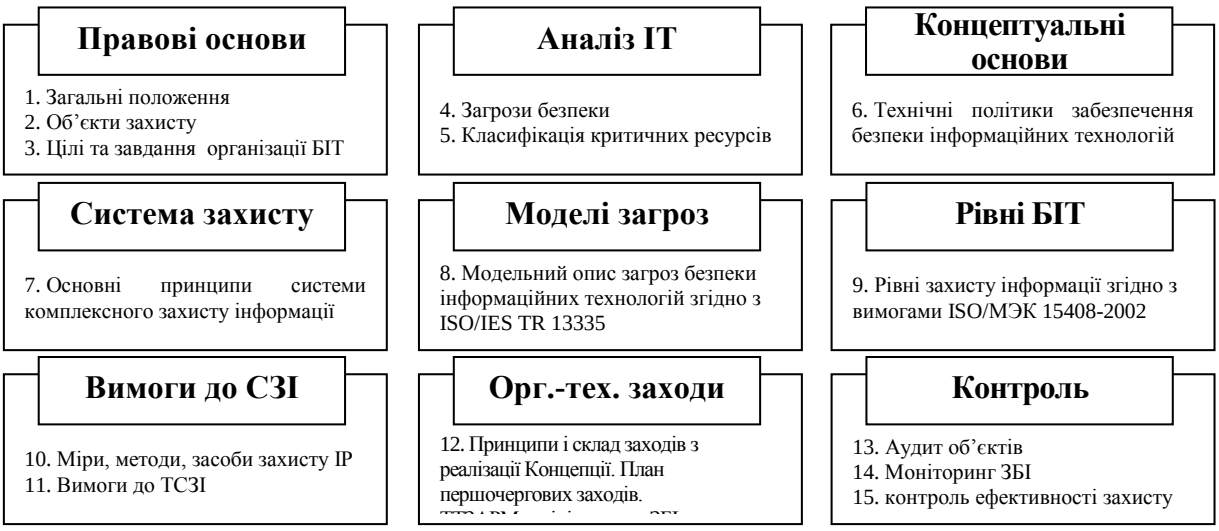


Рис. 3.13. Варіант структури концепції безпеки інформаційних технологій

Виходячи з того, що забезпечення БІТ фактично є процесом управління ризиками – систему захисту будемо вважати системою управління, яка реалізує технологію забезпечення безпеки. При цьому рівні по управлінню ІБ організації можуть поділятися на:

1) рівень прийняття рішень. Керівництво організації приймає стратегічні рішення з питань створення системи управління ІБ, затверджує основні документи, що регламентують порядок функціонування і розвитку ІС. Керівники і фахівці ІТ-підрозділів, технічного захисту інформації, начальники служб безпеки, керівники й фахівці служб економічної безпеки визначають критичність процесів, ресурсів і необхідний ступінь їхнього захисту, а також координують управління і розподіл обов'язків служб ІБ та ІТ;

2) рівень підготовки інформації для прийняття рішень. Аналітики підрозділів ІБ та ІТ відповідають за аналіз стану безпеки ІТ, визначення вимог до захищеності різних підсистем ІС й вибір методів і засобів захисту, розробляють регламенти (політику ІБ);

3) рівень організації й контролю виконання рішень. Системні й мережні адміністратори, адміністратори серверів, додатків, баз даних і т.п. відповідають за ефективне застосування штатних засобів захисту й розмежування доступу всіх використовуваних ОС і СУБД. Адміністратори додаткових засобів захисту, контролю і управління безпекою відповідають за ефективне застосування спеціалізованих засобів захисту (впливають на безпеку й персонал через засоби захисту);

4) рівень підтримки виконання політики ІБ. Відповідальні за забезпечення безпеки ІТ у підрозділах (на технологічних ділянках) – це посередники між нечисленним підрозділом безпеки й численними користувачами (це «представники ІБ» на місцях). Основні функції відповідальних за забезпечення безпеки ІТ – ефективна підтримка реалізації розроблених підрозділом безпеки й затверджених керівництвом регламентів;

5) рівень виконання політики ІБ (співробітники структурних підрозділів: кінцеві користувачі системи й обслуговуючий персонал, що працюють із засобами

автоматизованої обробки інформації), які вирішують свої функціональні завдання із застосуванням засобів автоматизації тощо).

Подана на рис. 3.14 модель системи БІТ відображує сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних або інформаційних ресурсів. Вона дає змогу повністю проаналізувати і документально оформити вимоги щодо гарантування послуг, що надаються, і гарантій безпеки майнових прав та інтересів клієнтів. Цього можна досягти при вирішенні таких основних завдань:

- віднесення інформації до категорії обмеженого доступу;

На нижньому – тактичному рівні сформована ПІБ знаходить свою практичну реалізацію. Аналіз стану ІБ проводиться на підставі порівняння визначеної політики ІБ даним моніторингу і аудита ІБ рівня оперативного управління. Кваліфікація осіб, відповідальних за безпеку інформаційних технологій повинна бути при цьому достатньою для адаптування матеріалів до конкретних потреб організацій.

Головними елементами, задіяними в процесі управління безпекою інформаційних технологій в організації є її активи.

До активів організації належать:

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

Активи є об'єктами для багатьох видів загроз (табл. 3.4).

Рис. 3.14. Модель системи безпеки інформаційних технологій в організації

- прогнозування і своєчасного виявлення загроз БІТ, а також причин і умов, що сприяють фінансовим, матеріальним і моральним збиткам, порушенню нормального функціонування і розвитку об'єкта;

- створення умов функціонування з найменшою ймовірністю реалізації загроз безпеці інформаційних ресурсів і зумовлення різних видів збитку;

- створення механізму і умов оперативного реагування на загрози БІТ та прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних заходів, засобів гарантування безпеки;

- створення умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей.

- уникнути витрат на зайві заходи безпеки, що можливі у разі суб'єктивної оцінки ризиків;

- надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;

- забезпечити проведення робіт в короткі терміни;

- подати обґрунтування вибору заходів протидії;

- оцінити ефективність контрзаходів, порівняти їх різні варіанти тощо.

Об'єктивними чинниками моделі є:

- загрози БІТ, що характеризуються вірогідністю реалізації;

- вразливі місця ІС або системи контрзаходів (системи БІТ);

- ризик – чинник, що відображує можливий збиток організації в результаті реалізації БІТ: просочування інформації та її неправомірного використання.

Концепції і бізнесові цілі організації формують плани, стратегії і методики для забезпечення безпеки інформаційних технологій організації. Змінювання цілей має гарантувати, що організація буде здатна до ділової активності з допустимими рівнями ризику. Щоб визначити і реалізувати загальну й чітку стратегію та методи забезпечення БІТ, організація повинна врахувати усі можливі аспекти (рис. 3.15).

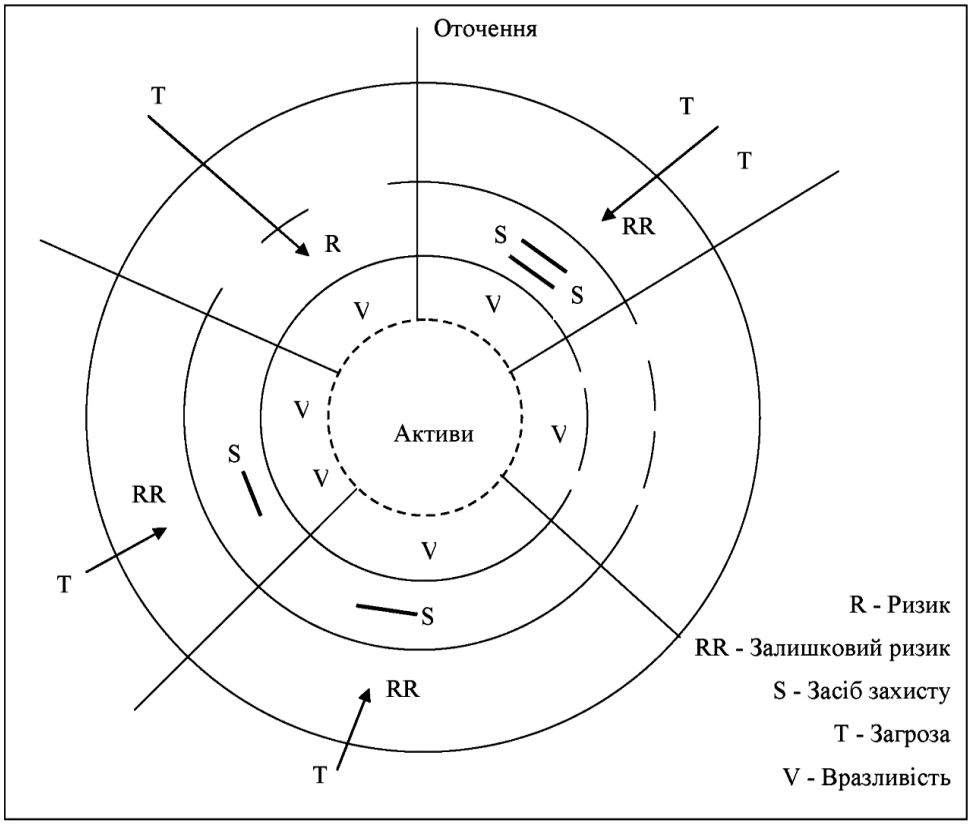


Рис. 3.15. Залежності елементів безпеки

З рис. 3.15 видно, що деякі засоби безпеки можуть бути ефективними для зменшення ризиків, пов'язаних із множинними загрозами і (або) множинними вразливостями. Іноді потрібні декілька засобів безпеки, щоб звести залишковий ризик до допустимого рівня. У деяких випадках, коли ризик допустимий, немає потреби застосовувати засоби безпеки, навіть якщо є загрози. В інших випадках уразливість може існувати, але не обов'язкова

наявність відомих загроз щодо неї. Засоби безпеки можуть забезпечувати контролювання наявності загроз в оточенні, щоб запобігти ураженню у разі прояву загрози.

На рис. 3.16 подано залежність між елементами безпеки, тісно пов'язаними з управлінням ризиком. Для ясності відображені тільки основні залежності.

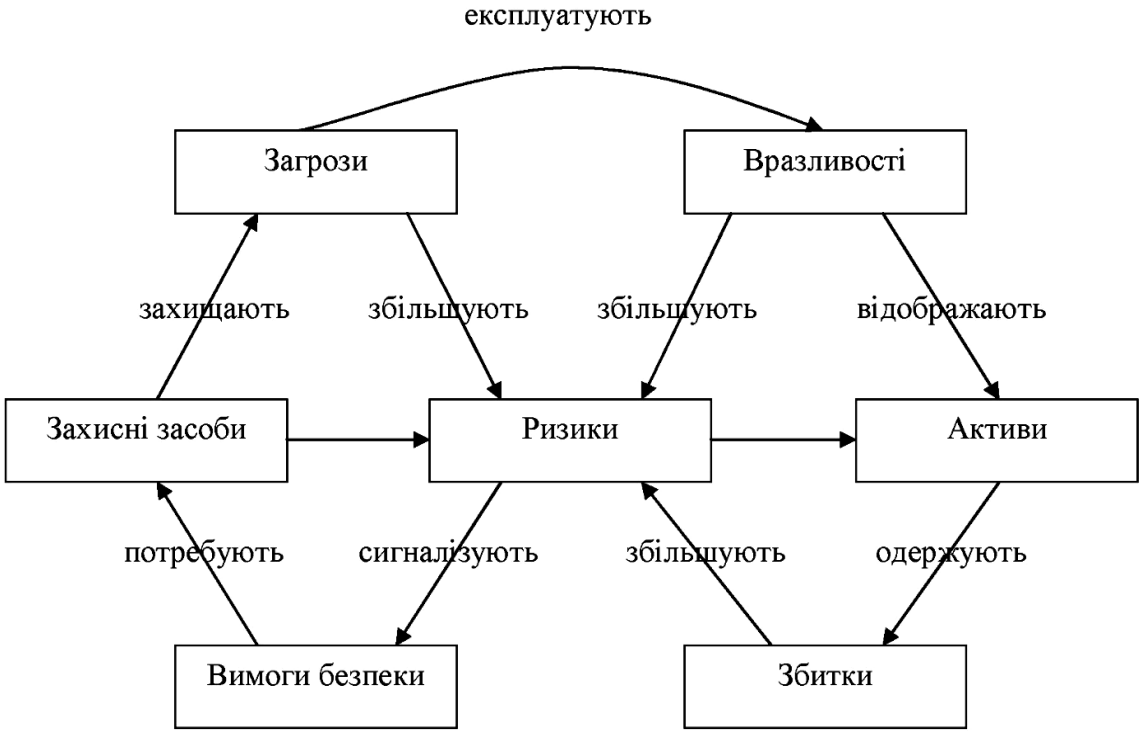


Рис. 3.16. Залежність в управлінні ризиком

Ризик – це небезпека, якій може піддаватися система і організація, що використовує її. Він залежить від: показників цінності ресурсів; вірогідності завдання збитку ресурсам (що виражається через вірогідність реалізації загроз для ресурсів); ступеня легкості, від якого системи захисту вразливості можуть бути використані при виникненні загроз; існуючих або планованих засобів забезпечення інформаційної безпеки. Обчислюють ці показники математичними методами, що мають такі характеристики, як обґрунтування і параметри точності.

Процес оцінювання ризиків складається з ряду послідовних етапів:

- опис об'єкта і заходів захисту;
- ідентифікація ресурсу та оцінювання його кількісних показників;
- аналіз загроз безпеці інформаційних технологій;
- оцінювання слабких місць;
- оцінювання існуючих і перспективних засобів гарантування БІТ;
- оцінювання ризиків.

На рис. 3.17, 3.18 та 3.19 подано залежності між необхідними умовами безпеки і загрозами, уразливостями і вартістю активів відповідно.

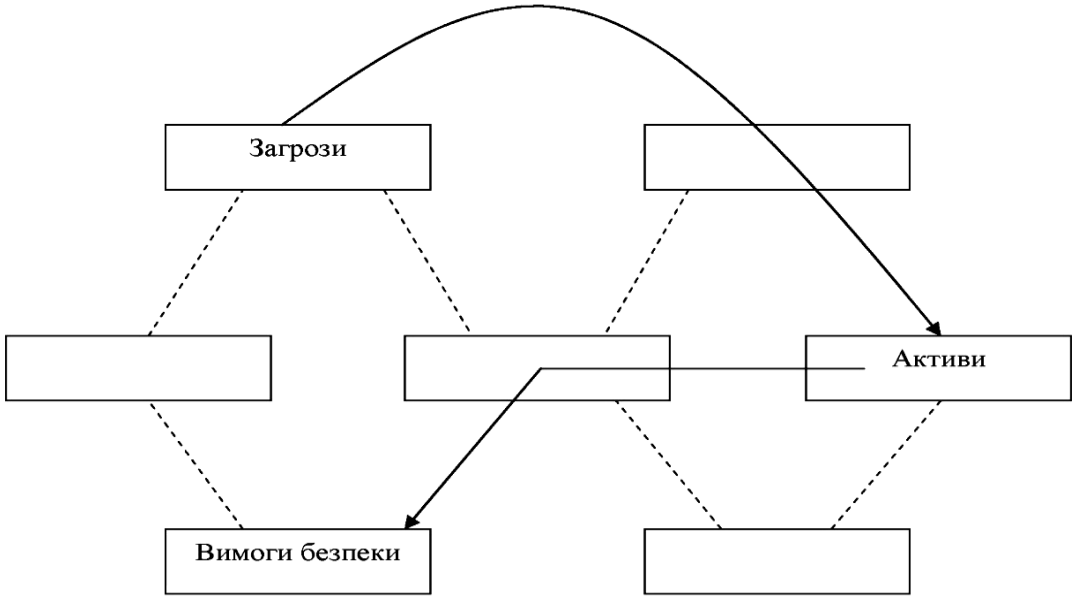


Рис. 3.17. Залежність в управлінні ризиком у аспекті загроз

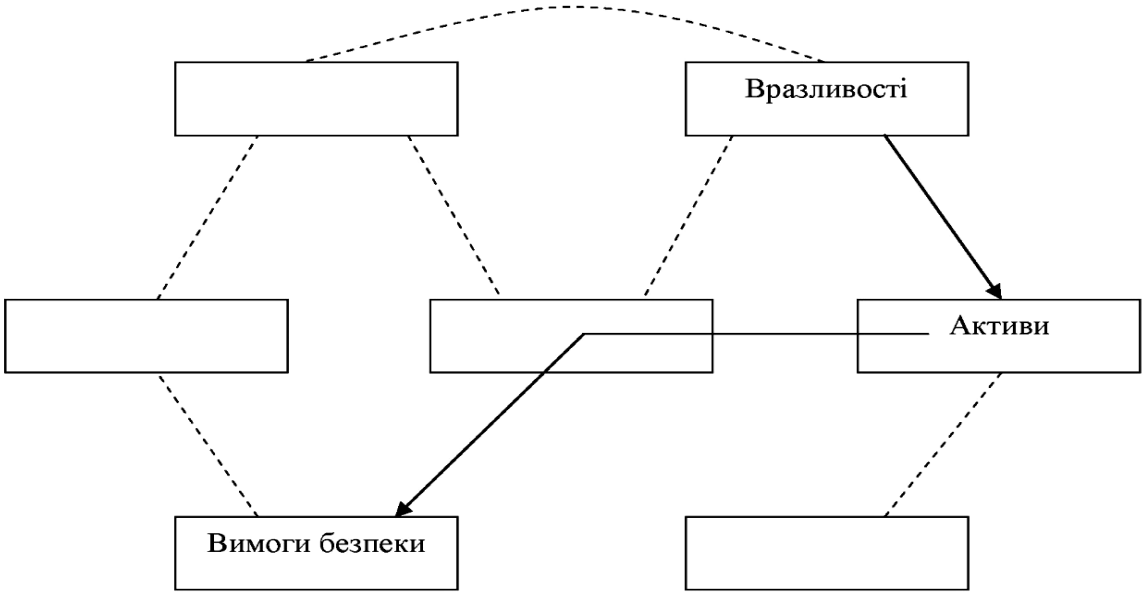


Рис. 3.18. Залежність в управлінні ризиком у аспекті вразливостей

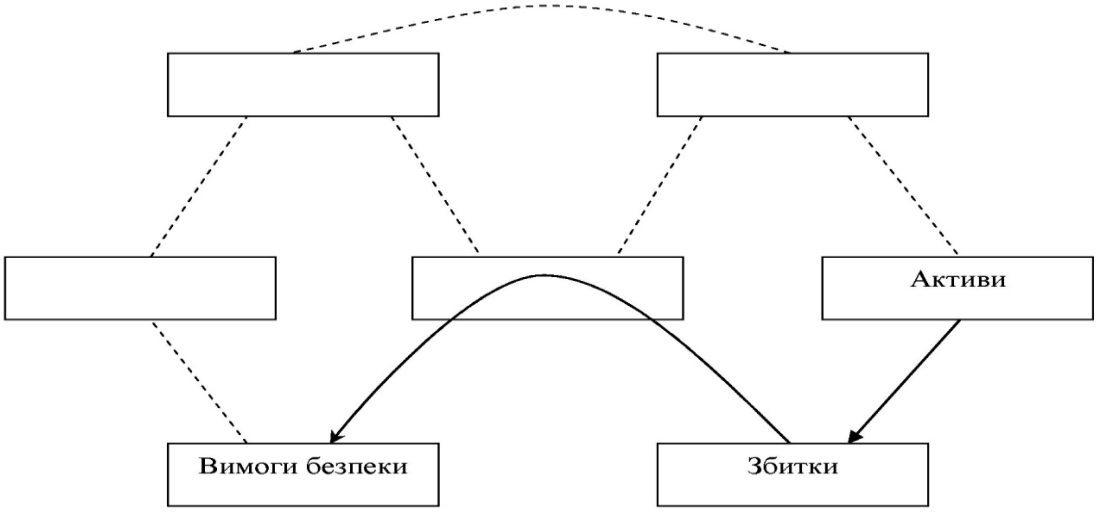


Рис. 3.19. Залежності в управлінні ризиком у аспекті ураження

На цих рисунках проілюстровано перспективи деяких підходів до управління безпекою інформаційних технологій. Однак такі підходи можуть не враховувати деякі важливі аспекти.

Контрольні запитання для самооцінки рівня знань

1. Які основні етапи розробки політики безпеки виділяє компанія IBM?
2. Зміст політики безпеки компанії IBM.
3. Структура керівних документів по забезпеченню інформаційної безпеки компанії IBM.
4. Основні компоненти стратегії безпеки компанії Microsoft.
5. Етапи управління інформаційними ризиками, рекомендовані політикою безпеки компанії Microsoft.
6. Принципи безпеки захищених систем з погляду компанії Microsoft.
7. Зміст політики безпеки, яка рекомендована компанією Microsoft.
8. Структура документів, що рекомендує політика безпеки компанії Sun Microsystems.
9. Основне призначення політики безпеки компанії Sun Microsystems та її зв'язок зі стандартами й процедурами безпеки.
10. Основні ідеї політики безпеки компанії Sun Microsystems.
11. Принципи безпеки компанії Sun Microsystems.
12. Етапи розробки політики безпеки компанії Sun Microsystems.
13. Архітектура безпеки SAFE компанії Cisco Systems.
14. Концепція розроблення захищених систем компанії Symantec.
15. Підхід до політики безпеки компанії SANS.
16. Які рівні захисту повинні забезпечувати сервіси безпеки інформації?
17. Які Ви знаєте основні сервіси безпеки інформації?
18. Сутність сервісу «ідентифікація/автентифікація».
19. Сутність сервісу «розмежування доступу».
20. Сутність сервісу «протоколювання й аудит».
21. Сутність сервісу «екранування».
22. Сутність сервісу «тунелювання».
23. Сутність сервісу «шифрування».
24. Сутність сервісу «контроль цілісності».
25. Сутність сервісу «контроль захищеності».
26. Сутність сервісу «виявлення відмов й оперативне відновлення».
27. Сутність сервісу «управління».
28. Національні стандарти зі створення політики безпеки інформації.
29. Перелік міжнародних стандартів зі створення політики безпеки інформації.
30. Міжнародний стандарт ISO/IEC 17799:2005. Призначення та особливості.
31. Алгоритм застосування стандарту ISO/IEC 17799:2005.
32. Основні області застосування стандарту ISO/IEC 17799:2005.
33. Рекомендовані етапи перевірки режиму інформаційної безпеки згідно стандарту ISO/IEC 17799:2005.
34. Міжнародний стандарт ISO/IEC 27001. Призначення та особливості.
35. Структура стандарту ISO/IEC 27001.
36. Етапи процесу управління інформаційною безпекою.
37. Рівні управління безпекою інформаційних технологій.
38. Функціональна структура управління політикою безпеки інформаційних технологій.
39. Варіант структури концепції безпеки інформаційних технологій.
40. Модель системи безпеки інформаційних технологій в організації.

Розділ 4

ОЦІНКА ПОЛІТИКИ БЕЗПЕКИ

4.1. Забезпечення гарантій виконання політики безпеки на основі методу генерації ізольованих програмних середовищ

Розглянемо забезпечення гарантій виконання політики безпеки на основі аналізу можливих шляхів її порушення (рис. 4.1).

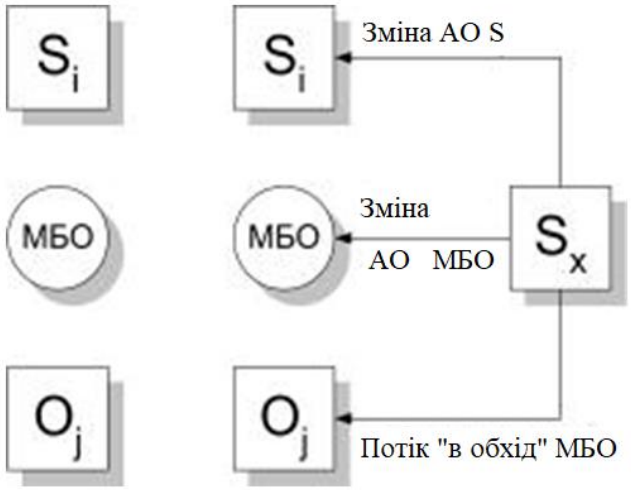


Рис. 4.1. Можливі шляхи порушення політики безпеки

Очевидно, що при зміні об’єктів (АО), які функціонально асоційовані з суб’єктом реалізації політики безпеки, що визначаються монітором безпеки об’єкта (МБО), можуть змінюватися і властивості самого монітора безпеки об’єкта, що полягають у фільтрації потоків, і як наслідок можуть виникати потоки, що належать до заборонених потоків множини N. У зв’язку з цим вводиться поняття коректності суб’єктів.

Пара суб’єктів Si і Sj називаються такими, що не впливають один на одного (або коректними відносно один одного), якщо у будь-який момент часу відсутній потік (що змінює стан об’єкта) між асоційованим об’єктом суб’єкта Si(Osi) і Sj(Osj), причому Osj не є асоційованим об’єктом Si, а Osi не є асоційованим об’єктом Sj

Можна дати наступне пояснення до визначення: “зміна стану об’єкта” трактується в даному визначенні як нетотожність об’єктів у відповідні моменти часу, але при цьому підкреслюється, що операція зміни об’єкта локалізована в суб’єкті, з яким цей об’єкт не асоційований. Суть поняття коректності пояснюється наступним чином: програми, що існують в єдиному просторі програмного забезпечення, не повинні мати функціональних можливостей для зміни “чужого” вектору коду та стану змінних.

Абсолютна коректність легко досягається у випадку віртуального адресного простору.

Визначення абсолютної коректності дозволяє сформулювати достатні умови гарантованого здійснення тільки дозволеного доступу.

Твердження 1 або достатня умова гарантованого виконання політики безпеки в комп’ютерній системі. Монітор безпеки об’єктів дозволяє породження потоків тільки з дозволеної множини L, якщо усі існуючі в системі суб’єкти абсолютно коректні відносно нього та один одного.

Доведення. Умова абсолютної коректності (жорстким визначенням) передбачає незмінність функціонально асоційованих об’єктів монітора безпеки об’єктів (оскільки потоків, що змінюють асоційовані об’єкти монітора безпеки об’єктів, не існує). З іншої сторони, такі потоки можуть з’явитися при зміні асоційованих об’єктів, що належать іншим суб’єктам комп’ютерної системи (змінюються властивості суб’єкта, у тому числі

(можливо) і з породження потоків до монітора безпеки об’єктів.). Умова коректності суб’єктів відносно одни одного роблять це неможливим (за визначенням абсолютної коректності). Це у свою чергу, означає, що монітор безпеки об’єктів реалізує тільки потоки з множини L. Твердження доведене.

Проте сформульоване твердження накладає вельми жорсткі та важкорозв’язні умови на властивості суб’єктів в комп’ютерній системі. Крім того, неможливо гарантувати коректність будь-якого суб’єкта, що активізується в комп’ютерній системі, відносно монітора безпеки суб’єктів. У зв’язку з цим логічно обмежити множину породжуваних суб’єктів, які апріорно коректні відносно монітора безпеки об’єктів. У зв’язку з цим можна ввести визначення монітора породження суб’єктів (за аналогією з монітором звернень) та монітора безпеки суб’єктів.

Монітор породження суб’єктів — це суб’єкт, що активізується при будь-якому породженні суб’єктів.

За аналогією з переходом від монітора звернень до монітора безпеки об’єктів можна ввести поняття монітора безпеки суб’єктів.

Монітор безпеки суб’єктів — це суб’єкт, який дозволяє породження суб’єктів тільки для фіксованої підмножини пар суб’єктів, що активізуються, і об’єктів, що породжуються.

Вплив монітора безпеки суб’єктів виділяє в усій множині суб’єктів S підмножину дозволених E. Звичайно зазначають, що якщо У підмножині суб’єктів у момент часу t включається суб’єкт монітора безпеки суб’єктів, то першим аргументом операції create може бути тільки суб’єкт, що входить до множини суб’єктів, а аргумент — будь-який об’єкт.

Можна також сформулювати тепер ряд базових визначень які у подальшому можна використати.

Комп’ютерна система називається замкнутою з породження суб’єктів, якщо в ній діє монітор безпеки суб’єктів, що дозволяє породження тільки фіксованої скінченної підмножини суб’єктів для будь-яких об’єктів-джерел, що розглядаються для фіксованої де- композиції комп’ютерної системи на суб’єкти та об’єкти.

При розгляді питань реалізації захищених середовищ буде використовуватися термін “захищене програмне середовище”, який по суті є еквівалентним наведеному вище визначенню.

Проте замкнутості комп’ютерної системи з породження суб’єктів недостатньо для опису властивостей системи у частині захищеності, оскільки необхідно забезпечити коректність породжуваних монітором безпеки суб’єктів суб’єктів відносно його самого та монітора безпеки об’єктів. Механізм замкнутого програмного середовища скорочує множину можливих суб’єктів до деякої множини фіксованої потужності, але при цьому припускає існування некоректних суб’єктів, включених у замкнуте середовище.

Сформулюємо визначення ізольованості комп’ютерної системи. Множина суб’єктів комп’ютерної системи називається ізольованою (абсолютно ізольованою), якщо в ній діє монітор безпеки суб’єктів та суб’єкти з породжуваної множини коректні (абсолютно коректні) відносно один одного та монітора безпеки суб’єктів.

Виходячи з визначення ізольованості комп’ютерної системи можна сформулювати два основні наслідки:

- будь-яка підмножина суб’єктів ізольованої (абсолютно ізольованої) комп’ютерної системи, що включає монітор безпеки суб’єктів, також складає ізольоване (абсолютно ізольоване) середовище;

- системи суб’єктом, коректним (абсолютно коректним) відносно будь-якого з числа тих, що входять до ізольованого (абсолютно ізольованого) середовища, залишають його ізольованим (абсолютно ізольованим).

Тепер можна переформулювати достатню умову гарантованого виконання політики безпеки наступним чином.

Твердження 2 або достатня умова гарантованого виконання політики безпеки в комп'ютерній системі. Якщо в абсолютно ізольованій комп'ютерній системі існує монітор безпеки об'єктів та породжувані суб'єкти абсолютно коректні відносно монітора безпеки об'єктів, а також монітор безпеки суб'єктів абсолютно коректний відносно монітора безпеки об'єктів, то у такій комп'ютерній системі реалізується тільки доступ, описаний в правилах розмежування доступу.

Доведення. З доведення абсолютної ізольованості виходить можливість існування в комп'ютерній системі тільки скінченної множини суб'єктів, які, у свою чергу, коректні відносно монітора безпеки суб'єктів.

Дальше за умовою твердження (коректність монітора безпеки об'єктів відносно будь-якого з породжуваних суб'єктів і монітора безпеки суб'єктів) асоційовані об'єкти можуть змінюватися тільки самим монітором безпеки об'єктів, отже, в комп'ютерній системі реалізуються тільки потоки, що належать множині L. Твердження доведене.

Легко бачити, що дане твердження є більш конструктивним відносно попередньої достатньої умови гарантованої захищеності, оскільки раніше вимагалася коректність монітора безпеки об'єктів відносно довільного суб'єкта, що практично є неможливим. У даному ж випадку множина суб'єктів обмежена за рахунок застосування механізму монітора безпеки суб'єктів і є можливість упевнитися у попарній коректності породжуваних суб'єктів.

При розгляді технічної реалізації ізольованості суб'єктів в комп'ютерній системі застосовується термін "ізольоване програмне середовище" (ІПС), який описує механізм реалізації ізольованості для конкретної програмно-апаратної реалізації комп'ютерної системи і при відповідній декомпозиції на суб'єкти та об'єкти.

При розгляді операції породження суб'єкта виникає вельми важлива проблема, повязана з тим, що в реальних комп'ютерних системах однаково пойменовані об'єкти можуть мати різні стани у просторі (наприклад, можуть бути розташованими в різних каталогах) або у часі.

Припустимо, що зафіксований стан об'єкта Om у деякий момент часу to. Будемо позначати стан об'єкта Om у момент часу t як Om[t].

Операція породження суб'єкта create(Sj. ,Om) ^ Si називається породженням з контролем незмінності об'єкта, якщо для будь-якого моменту часу t > to, в який активізована операція породження create, породження суб'єкта Si можлива тільки про тотожності об'єктів Om[t0] і Om[t].

При даних умовах породжені суб'єкти Si[ti] і Si[t2] є тотожними, якщо ti > to і t2 > to. При ti = t2 породжується один і той же суб'єкт. При породженні суб'єктів з контролем незмінності об'єкта в комп'ютерній системі допустимі потоки від суб'єктів до об'єктів-джерел, що беруть участь в породженні суб'єктів, із зміною їх стану.

Твердження 3 або базова теорема ізольованого програмного простору формулюється наступним чином. Якщо у момент часу to в ізольованій комп'ютерній системі діє тільки породження суб'єктів з контролем незмінності об'єкта та існують потоки від будь-якого суб'єкта до будь-якого об'єкта, що не суперечить умові коректності (абсолютної коректності) суб'єктів, то ц будь-який момент часу t > to комп'ютерна система залишається ізольованою (абсолютно ізольованою).

Доведення теореми. За умовою твердження в комп'ютерній системі є можливим існування потоків, що змінюють стан об'єктів, не асоційованих у цей момент часу з будь-яким суб'єктом. Якщо об'єкт із зміненим станом не є джерелом для породження суб'єкта, то множина суб'єктів ізольованого середовища не є розширюваною, у протилежному випадку (змінюваний об'єкт є джерелом для породження суб'єкта) за умовами твердження (породження суб'єкта з контролем) породження суб'єкта є неможливим. Отже, потужність множини суб'єктів не може перевищувати тієї, яка була зафіксована до зміни етану будь-якого об'єкта. Відповідно до наслідку з визначення операції породження суб'єкта з контролем незмінності об'єкта (про замкнутість множини суб'єктів в ізольованому

програмному просторі з незроетаючою потужністю множини суб'єктів) одержимо, що множина суб'єктів комп'ютерної системи є ізольованою. Твердження доведене.

Можна сформулювати методологію проектування гарантовано захищених комп'ютерних систем. Сутність даної методології полягає у тому, що при проектуванні захисних механізмів комп'ютерної системи необхідно опиратися на сукупність достатніх умов, які повинні бути реалізовані для суб'єктів, що гарантують захисні властивості, визначені для реалізації монітора безпеки об'єктів в комп'ютерній системі (тобто гарантоване виконання заданої монітором безпеки об'єкта політики безпеки).

Концепцію ізольованого програмного середовища звичайно розглядають як розширення підходів до реалізації ядра безпеки.

Модель функціонування ядра безпеки відображається у вигляді наступної схеми, представленої на рис. 4.2.

Рис. 4.2. Класична модель ядра безпеки

На рис. 4.2 "база даних захисту" означає об'єкт, що містить у собі інформацію про потоки множини L (захист за "білим списком" — дозволи на потоки) або N (захист за "чорним списком" — заборону на потоки).

Для урахування впливу суб'єктів в комп'ютерній системі необхідно розглядати розширену схему взаємодії елементів системи реалізації та гарантування політики безпеки.

Тепер можна перейти до опису практичних методів побудови ізольованого програмного середовища. Метою розгляду є ілюстрація твердження про те, що достатні умови гарантованої захищеності можуть бути практично виконані в реальних комп'ютерних системах

Метод генерації ізольованого програмного середовища при проектуванні механізмів гарантованої підтримки політики безпеки.

Опираючись на базову теорему ізольованого програмного середовища можна описати метод суб'єктно-об'єктної взаємодії в рамках ізольованого програмного середовища для більш конкретної архітектури комп'ютерної системи.

З твердження 3 виходить, що для створення гарантовано захищеної комп'ютерної системи (стосовно виконання заданої політики безпеки) необхідно:

Упевнитися у попарній коректності суб'єктів, що входять до ізольованого програмного середовища (або впевнитися у коректності будь-якого суб'єкта відносно монітора безпеки суб'єктів та монітора безпеки об'єктів).

Спроектувати або реалізувати програмно (або програмно-апаратно) монітор безпеки суб'єктів так, щоб:

• для будь-якого суб'єкта та будь-якого об'єкта здійснювався би контроль породження суб'єктів (тобто, щоб реалізація монітора безпеки суб'єктів відповідала його визначенню);

• породження будь-якого суб'єкта відбувалося би з контролем незмінності об'єкта-джерела.

Реалізувати монітор безпеки об'єктів в рамках апріорно сформульованої політики безпеки.

Треба відзначити, що наведені вище твердження є вірними тільки тоді, коли описана та реалізована політика безпеки не порушує їх умов (перевірка даного факту залежить від моделі політики безпеки та є окремим вельми важливим завдання).

Крім того, необхідно звернути увагу на наступне. Об'єкт управління, який є асоційованим об'єктом монітора безпеки суб'єктів, відіграє вирішальну роль у проектуванні ізольованого програмного середовища. При можливості зміни стану об'єкта управління потенційно можливе "розмикання" програмного середовища, тобто додавання до множини дозволених суб'єктів додаткових, які реалізують зловмисні функції. З іншої сторони, процес управління безпекою припускає можливість зміни об'єкта. Можливість зміни етану об'єкта управління (реалізація потоку stream) повинна бути присутньою для виділених суб'єктів (можливо з додатковими умовами активізації цього суб'єкта виділеним користувачем або користувачами).

Важливу роль при проектуванні ізольованого програмного середовища відіграє властивість комп'ютерної системи, що полягає у поетапній активізації суб'єктів із об'єктів різного рівня представлення інформації. У табл. 4.1 можна розглянути ієрархію рівнів при завантаженні операційної системи.

У таблиці виділений термін "сектор" для позначення представлення об'єкта апаратно-програмного рівня. Він позначає безперервну послідовність елементів зберігання (байт) на матеріальному носії, що характеризується місцем знаходження.

Термін "файл" позначає абстрактний об'єкт, побудований за обліковою структурою з об'єктів "сектор". Об'єкти тину "файл" і "сектор" виділені виключно виходячи з типової структури об'єктів комп'ютерної системи.

У загальному вигляді можна говорити про рекурсивну структуру об'єктів деякого рівня, що вміщують об'єкти попереднього рівня. На нульовому рівні первинний об'єкт (елементарна структура нижнвої'о рівня) в табл. 4.1 відповідають терміну "сектор".

Таблиця 4.1

Ієрархія рівнів при завантаженні операційної системи

Рівень	Суб'єкт	Локалізація	Представ лення інформації	Через які функції реалізуються потоки
0	Суб'єкт апарат-но-програмного рівня	ПЗП (BIOS)	сектори	через мікропрограми ПЗП
1	Суб'єкт рівня первинного завантаження	Завантажник операційної системи	сектори	через BIOS або первинний завантажник
2	Суб'єкт рівня вторинного завантажника	драйвери операційної системи	сектори	через BIOS або первинний завантажник
3	Суб'єкт рівня операційної системи	ядро операційної системи	файли	через драйвери
4	Суб'єкт користуваль-ницького рівня	прикладні додатки	файли	через ядро операційної системи

З урахуванням ієрархічної структури представлення об'єктів можна говорити про те, що у початкові стани активізації комп'ютерної системи декомнозиція на об'єкти та суб'єкти динамічно змінюється. Отже, основна теорема ізольованого програмного простору може бути застосовною тільки на окремих інтервалах часу, коли рівень представлення об'єктів постійний а декомнозиція фіксована. Можна стверджувати, що ізольований програмний простір, який діє від моменту активізації до моменту закінчення роботи комп'ютерної системи, неможливо сформувати у початковий момент активізації комп'ютерної системи.

Нехай у комп'ютерній системі відділяється скінченне число рівнів представлення об'єктів U = {0,..., R}, де R — максимальний рівень представлення об'єктів.

З точки зору виконання умов твердження 3 мало би смисл говорити про деякий "стаціонарний" стан комп'ютерної системи, коли у відображеннях stream і create беруть участь тільки об'єкти рівня R. Тоді реалізація монітора безпеки суб'єктів може бути значно спрощеною (у тому смислі, що усі аргументи-об'єкти операції create мають такий же рівень). Необхідно звернути увагу на те, що така вимога, з однієї сторони, може накладати обмежувальні умови на властивості прикладного програмного забезпечення (неможливість ініціювання потоків, що включають об'єкти рівня R) та бути наслідком проектувальних рішень реалізації суб'єкта, локалізованого в ядрі операційної системи (прикладом є операційна система Windows NT 4.0, що забороняє операції вище рівня "файл" зі сторони суб'єктів прикладного рівня).

Звичайно, необхідно зробити застереження, що стосується можливості реалізації потоків до об'єктів нижнього рівня (операційні системи типу DOS, в яких можлива операція з будь-яким об'єктом нижнього рівня (сектор) з програмами прикладного рівня).

Тут звичайно вводять поняття послідовності активізації компонент комп'ютерної системи. Смисл введених понять та сформульованих нижче тверджень полягає у необхідності приведення суб'єктів комп'ютерної системи в один і той же стан після активізації первинного суб'єкта програмно-апаратного рівня, або, інакше кажучи, у завданні наперед визначеної послідовності активізації суб'єктів комп'ютерної системи.

Позначимо, що ZI — послідовність пар (i, j)t (t = 0,1, 2,..., l — 1 — моменти часу) довжини I, такі, що create(Si,Oj[t] ^ Sm[t + I].

Позначимо також:

sz — множина всіх суб'єктів, включених до послідовності Zp;

Oz — множина всіх об'єктів, включених до послідовності Zp. Для багатопотокових комп'ютерних систем можна розглядати декілька (можливо залежних один від одного) послідовностей Zp.

Визначимо, що станом комп'ютерної системи у момент часу t називаєтся упорядкована сукупніств станів об'єктів, і, що кожний об'єкт є словом на апріорно визначеній мові, а поняття стану суб'єкта сформулвоване вище.

Твердження 4 або умова однакового стану комп'ютерної системи. Стан комп'ютерної системи у моменти часу t x l і t x 2 (t x 1 і t x 2 обчислюються для двох відрізків активності комп'ютерної системи від нульового моменту активізації комп'ютерної системи tol і to2 (наприклад, вмикання живлення апаратурної частини) однаково, якщо:

- t x 1= t x 2;
- тотожні суб' єкти Si [tol] і Si[t0 2];
- незмінна послідовніств Zp.

Доведення за принципом математичної індукції. Вірність твердження при t = 1 випливає з визначення тотожності суб'єктів.

Нехай твердження є вірним для t = k < 1.

Тоді у момент часу k + 1 можуть бути породженими тільки тотожні суб'єкти. Оскільки тотожні активізуючі суб'єкти (за припущенням індукції) і за умовою твердження є незмінними елементами Oz.

Довжина l послідовності Zi визначається:

- множиною Sz, зі сторони користувача (у протилежному випадку послідовність активізації суб'єктів може бути зміненою);

- з множини Oz;

- в іншому випадку мається на увазі, що існує момент часу tx такий, що для будь-якого t > tx об'єкт-аргумент Oj операції stream(Si,Oj)t належить до одного рівня представлення). Необхідно зазначити, що послідовність Zx локалізується в деякому об'єкті або сукупності об'єктів (наприклад, для DOS послідовність активізації суб'єктів наперед визначена змістом файлів autoexec.bat та config.svs) і незмінність послідовності Zx тотожна незмінності вказаних об'єктів, для операційної системи Windows NT послідовність активізації компонент визначена змістом відповідних ключів реєстру (registry).

Нехай в послідовності Zx можна виділити Zi таке, що для будь-якого Zk: к>і відображень create і stream використовують тільки об'єкти рівня R. іншими словами, з моменту часу і наступає стаціонарна фаза функціонування комп'ютерної системи.

За цих умов, а також при попарній коректності суб'єктів та дій монітора безпеки суб'єктів з контролем незмінності об'єктів - джерел на рівні R з моменту часу m > к є вірним.

Твердження 5 або достатня умова ізольованості програмного середовища при східчастому завантаженні. За умови незмінності Zx та незмінності об'єктів Oz в комп'ютерній системі з моменту часу встановлення незмінності Zx та Oz діє ізольоване програмне середовище.

Доведення. Необхідно зазначити, що всі умови твердження 5 відповідають твердженню 4. уточнення стосуються структури по Zx

Відповідно до твердження 4 з моменту часу t=0 до моменту t=l діє ізольоване (в рамках) Sz програмне середовище.

Для доведення твердження необхідно переконатися у тому, що:

- монітор безпеки суб'єктів у момент часу t = m гарантовано активізується;

- у будь-який мо мент t > m програмне середовище є ізольованим.

Використовуючи твердження 3, 4 та 5, розглянемо процес практичного проектування захищеного фрагменту комп'ютерної системи.

Спочатку необхідно впевнитися у виконанні умов коректності або абсолютної коректності для суб'єктів, що беруть участь у породженні ізольованого програмного середовища. Указані суб'єкти в основному можуть бути локалізовані на рівні програмно-апаратної компоненти ЕОМ (програми постійного запам'ятовуючого пристрою, завантажувальники операційних середовищ), тобто працювати на рівні, що є близьким до взаємодії з обладнанням комп'ютерної системи, або на рівні операційного середовища. Доведення коректності суб'єктів програмно-апаратного рівня значно відрізняєтвся від відповідних доведень для суб'єктів прикладного рівня. У зв'язку з цим можна виділити перевірку умов коректності суб'єктів у два кроки. Кроком 1 називаютв доведення коректності суб'єктів програмно-апаратного рівня. Поняття модуль означає реалізацію об'єкта-джерела, а сукупність суб'єкта, породженого з об'єкта-джерела та усієї множини асоційованих з цим суб'єктом об'єктів протягом усього часу існування суб'єкта, що називається, як правило, процесом (або задачею, завданням).

Дальше необхідно визначити склад програмних засобів базового обчислювального середовища, тобто визначити конкретне операційне середовище, додаткові програмні засоби сервісу (наприклад, програмні оболонки та засоби телекомунікацій) і програмні засоби підтримки додаткового обладнання (програми управління принтером і т.ін.). Після цього наступає найбільш трудомісткий етап (крок 2), на якому необхідно впевнитися у коректності суб'єктів описаного базового набору програмних засобів. При цьому важливо відзначити наступне.

У складі програмного забезпечення комп’ютерної системи не повинно бути цілого класу можливостей — які можна назвати інструментальними. Насамперед це можливість зміни стану асоційованих об’єктів зі сторони суб’єкта (наприклад, зміна вмісту оперативної пам’яті), інших суб’єктів (зміна змісту припускає існування операцій stream типу запис), можливість ініціювання та припинення виконання процесів нестандартним чином (окрім механізмів операційного середовища). Крім того, при реалізації монітора безпеки суб’єктів та монітора безпеки об’єктів на стаціонарній фазі функціонування комп’ютерної системи необхідна відсутніств у будь-яких суб’єктах, замкнутих в ізолвоване програмне середовище. операцій породження потоків stream до об’єктів рівня k > R.

У загальному вигляді достатні умови до базового набору програмного забезпечення можна сформулювати наступним твердженням.

Твердження 6 або вимоги до суб’єктного наповнення ізольованого програмного середовища. Для того щоб ізольоване програмне середовище підтримувалося протягом усього часу активності комп’ютерної системи, достатньо, щоб у складі програмного забезпечення, яке може бути ініційованим в ізольованому програмному середовищі, не було функцій породження суб’єктів і припинення їх роботи, крім раніше визначених при реалізації монітора безпеки суб’єктів, і не існувало можливостей впливу на середовище виконання (під середовищем виконання розуміють множину асоційованих об’єктів) будь-якого процесу, а також ініціювання потоків R.

Легко бачити, що дане твердження - зібрані воєдино умови виконання приведених вище тверджень.

Вимогу неможливості припинення виконання суб’єкта будь-яким іншим чином, крім призначеного пояснимо наступним чином. У даному випадку необхідно враховувати, що у множині суб’єктів, замкнутих в ізольованому програмному просторі, два особливих випадки — монітор безпеки суб’єктів і монітор безпеки об’єктів, припинення існування монітора безпеки суб’єктів означає порушення умови замкнутості середовища, а припинення існування монітора безпеки суб’єктів означає допустимість потоків множини N, тобто несанкціонований доступ.

Крок 3 полягає у проектуванні та розробці програмних або програмно-апаратних засобів захисту в комп’ютерній системі, а потім їхньому тестуванні. Він припускає проектування та реалізацію у заданій множині суб’єктів монітора безпеки суб’єктів або монітора безпеки об’єктів.

Практичні кроки 1-3 можуть бути виконані виходячи з методик розробки та тестування програмного забезпечення.

Крок 4 полягає у “замиканні” всього комплексу нрограмного забезпечення, включаючи і засоби захисту, в ізольоване програмне середовище.

Отже, показано, що основними елементами підтримки ізольованості нроі'рамного середовища є контроль цілісності та контроль породження процесів.

Вище уже були сформульовані поняття монітора безпеки суб’єктів та породження суб’єктів з контролем їх незмінності. Необхідно відзначити, що для достовірного контролю незмінності об’єкта (тобто з ймовірністю помилки, що є рівною 0) необхідно впевнитися у повній тотожності об’єкта, що перевіряється, та зразка. З цього виходить, що еталон повинен містити не менше інформації, ніж об’єкт, що піддається перевірці. З цього у свою чергу випливає, що еталонний обєкт повинен бути як мінімум однакової довжини з тим. що перевіряється. На практиці такий підхід може бути застосованим із серйозними обмеженнями (наприклад, для об’єктів невеликого об’єму тину програм постійних запам’ятовуючих пристроїв або завантажувальників операційних систем).

У зв’язку з цим для контролю цілісності застосовують об’єкти, що містять інформацію, яка не залежить від усього змісту об’єкта, але тим не менше значно меншого об’єму, обчислену за допомогою класу функцій тину “геш-функцій” . Очевидно, що у цьому випадку процес встановлення незмінності об’єкта стає ймовірнісним.

Виходячи з даного факту неможливо говорити про гарантовані (детерміновані) властивості системи (оскільки незмінність об'єкта гарантується лише з деякою ймовірністю, що не є рівною 1). Отже, всі умови тверджень виконуються з деякою ймовірністю, що залежить від властивостей геш-функцій, що застосовуються для контролю цілісності. Для підкреслювання умов, що змінилися, дальше можна говорити не про контроль незмінності об'єкта, а про контроль цілісності об'єкта.

Необхідно також відзначити, що у процедурі контролю незмінності (яка тепер приймає ймовірнісний характер) беруть участь мінімум два об'єкти: об'єкт контролю та еталонний об'єкт (геш-значення), а також суб'єкт, що реалізує геш-функцію та здійснює порівняння.

Тому для суб'єкта контролю цілісності важливим є виконання наступних умов:

- якісний алгоритм контролю цілісності (термін "якісний" буде пояснений нижче);
- що підлягає контролю, та еталонного об'єкта в асоційовані об'єкти-дані суб'єкта контролю цілісності, що співпадаютв з тотожним).

Можна пояснити більш докладно другий пункт. Контроль цілісності завжди сполучений з читанням даних (тобто з ініціюванням потоків від об'єктів до асоційованих об'єктів-даних суб'єкта контролю цілісності, причому потоки можуть відповідати різному рівню представлення інформації — читання за секторами, читання за файлами і т.ін.). Наприклад, вбудований в BIOS ПЕОМ суб'єкт (практично це програмна закладка) може нав'язувати при читанні замість одного сектора інший або редагувати безпосереднво буфер, у який були прочитані дані. Аналогічний ефект може бути викликаний суб'єктами операційного середовища, наприклад, суб'єктами, що локалізовані в первинних завантажниках операційної системи. З іншої сторони, навітв контроль BIOS може здійснюватися "під спостереженням" будь-якої додаткової апаратури і не показувати його зміни. Аналогічні ефекти можуть виникнути і при обробці файлу. Мета організації режиму читання реальних даних полягає у тотожному відображенні параметрів читання на асоційованому об'єкті суб'єкта читання (потік від асоційованого суб'єкта контролю цілісності до асоційованого об'єкта суб'єкта читання) і тотожному відображення об'єкта, що зчитується (відповідно до параметрів, що які передані суб'єкту читання) до асоційованих об'єктів-даних суб'єкта контролю цілісності.

При ввімкненні живлення ПЕОМ відбуваєтвся тестування операційної системи, ініціалізація таблиці векторів переривань та пошук розширень BIOS. При їх наявності управління передається на них. Після обробки розширень BIOS у памяти зчитується перший сектор дискети або вінчестера та управління передаєтвся на нього (утворюєтвся код завантажника), потім код завантажника зчитує драйвери операційної системи, потім інтепретуються файли конфігурації, підвантажується командний інтерпретатор та виконується файл автозапуску.

При реалізації ізольованого програмного середовища на нього повинна бути покладена функція запусків програм та контролю цілісності.

При описуванні методології проектування ізольованого програмного середовища згадувалася проблема контролю реальних даних. Ця проблема полягає у тому, що контрольована на цілісність інформація може по-різному представлятися на різних рівнях.

Упроваджений у систему об'єкт може вплинути на процес читання-запису даних на рівні файлів (або на рівні секторів) та пред'являти системі контролю деякі інші замість реально існуючих даних. Цей механізм неодноразово реалізовувався в stels-вірусах. Проте є вірним наступне твердження.

Твердження 7 або достатня умова читання реальних даних. Якщо суб'єкт, який обслуговує процес читання даних (тобто вказаний суб'єкт ініціюється суб'єктом, що запитує дані, та бере участь у потоці), містив тільки функції тотожного відображення даних на асоційовані об'єкти-дані будь-якого суб'єкта, що ініціює потік читання, і цілісність об'єкта-джерела а для цього суб'єкта зафіксована, то при його наступній

незмінності читання з використанням породженого суб'єкта буде читанням реальних даних.

Доведення. Вірність твердження випливає з визначення тотожності суб'єкта та з умови твердження, що гарантує незмінність об'єкта-джерела.

Необхідно і тут зробити застереження про імовірнісний характер установлення незмінності та говорити, що читання реальних даних можливе з імовірністю, що визначається алгоритмом контролю цілісності.

Метод східчастого контролю не суперечить твердженням 4 і 5 та передбачає розділення послідовності активізації компонент на підпослідовності з однаковим рівнем представлення інформації.

Реалізація методу східчастого контролю цілісності повинна задовольняти умовам твердження 4.

Тепер можна описати практичну реалізацію сформульованих методів.

Реалізація гарантій виконання заданої політики безпеки. Вище було сказано про те, що суб'єкт контролю незмінності об'єктів, що входять у процедури активізації комп'ютерної системи та об'єктів, що описують послідовність активізації компонент, повинен бути активним уже на етапі роботи суб'єктів апаратно- програмного рівня, але його об'єкт-джерело не може бути перевіреним на незмінність. У зв'язку з цим можна підкреслити надзвичайно важливий факт для будь-яких реалізації ізольованого програмного середовища.

Аксіома. Генерація ізольованого програмного середовища розглядається в умовах незмінності конфігурації тих суб'єктів комп'ютерної системи, які активізуються до старту процедур контролю цілісності об'єктів Oz та послідовності Zl. Незмінність даних суб'єктів забезпечується зовнішніми по відношенню до власне комп'ютерної системи методами та засобами. При аналізі або синтезі захисних механізмів властивості вказаних суб'єктів є апріорно заданими.

При вирішенні практичних питань генерації ізольованого програмного середовища можна виділити три самостійних напрямки.

Перший з них пов'язаний з використанням зовнішніх по відношенню до комп'ютерної системи суб'єктів (як правило, розташованих на зовнішньому носії), цілісність яких гарантується методами зберігання або періодичного контролю. Зумовленість активізації суб'єктів, локалізованих на зовнішніх носіях, забезпечується властивостями суб'єктів програмно-апаратного рівня (наприклад, можна встановити таку апаратну конфігурацію ПЕОМ, при якій буде відбуватися завантаження операційної системи з гнучкого магнітного диску).

Другий напрямок пов'язаний з локалізацією ізолвованого програмного середовища в межах обмеженого робочого місця (як правило, ПЕОМ) і використовує апаратну підтримку для завдання передвизначеної послідовності активізації суб'єктів. Даний напрямок, як правило, включає апаратну підтримку автентифікації користувачів.

Третій напрямок пов'язаний з реалізацією методу довіреного завантаження операційного середовища з використанням уже наявних в нвому механізмів реалізації та гарантування політики безпеки.

Необхідно зазначити, що у різноманітні інтервали активності комп'ютерної системи суб'єктами можуть управляти різні користувачі, для яких множина дозволених суб'єктів E різна, у зв'язку з цим можна говорити про множину Ej для j-того користувача комп'ютерної системи.

Також необхідно розуміти, що перед встановленням однозначної відповідності множини Ej користувачеві і відбуваєтвся процедура його автентифікації.

Говорячи про перший спосіб реалізації ізолmованого програмного середовища слід відзначити, що в його рамках можна розглядати конфігурацію ізольованого програмного середовища у двох варіантах:

- при локалізації всіх об’єктів-джерел для породження ізолвованого програмного середовищ в рамках одного або декількох зовнішніх носіїв;

- у зовнішній пам’яті робочого місця.

Друга конфігурація характеризуєтвся потенційною можливістю порушення ізольованості, що полягає у тому, що активізація суб’єктів із об’єктів-джерел, що не належать зовнішнвому носію, може здійснюватися поза рамками ізольованого програмного середовища. Як приклад можна розглядати ситуацію, коли програми запускаються в рамках операційного середовища, що завантажується з дискети. З іншої сторони, запуск вказаних програм можливий і при завантаженні операційної системи з іншого носія (зокрема, з носіїв робочого місця), і при цьому можлива активація і тих модулів, які знаходяться на дискеті.

Отже, основною задачею при використанні зовнішнього носія для генерації ізольованого програмного середовища є забезпечення неможливості активізації будь-якого суб’єкта з об’єкта-джерела зовнішнього носія поза рамок зафіксованої для цього носія послідовності активізації компонент ізольованого програмного середовища.

Найбільш ранній спосіб проектування ізольованого програмного середовища в рамках підходу з використанням зовнішнього носія одержав назву невидимої дискети. Цей спосіб полягає у тому, що всі об’єкти, які належать множині Oz, і об’єкти, що описують послідовність Zl, поміщаються на зовнішній носій, з якого може відбуватися завантаження операційної системи (звичайно дискета). Незмінність об’єктів забезпечується фізичним захистом носія від запису.

Крім того, використання спеціальної технології не дозволяє використовувати об’єкти (у тому числі і забезпечити виконання програм) без завантаження операційної системи саме з цієї дискети. Практично така дискета виглядає достатньо нетривіально: будучи поміщеною в дисковод ПЕОМ вона як неформатована (або, в іншому варіанті, пуста). Після завантаження з такої “пустої” дискети користувач відразу “пірнає” в задану програму та працює з нею, звертаючись у тому числі і до даних на вінчестері та запускаючи програми з локально незмінних носіїв робочого місця з попереднім контролем незмінності відповідних їм об’єктів-джерел (виконуваних файлів).

Запропонований спосіб дозволяє виключити використання виготовленої дискети без завантаження з неї. Доповнивши завантажуване з такої дискети операційне середовище програмами перевірки цілісності можна досягнути дотримання усіх вимог ізольованості програмно-апаратного середовища.

Як видно із твердження 5, однією з найважливіших умов підтримування ізольованого програмного середовища є втрата неможливості змін послідовності активізації компонент.

У даному випадку цілісність об’єктів, що містять послідовність активізації компонент, гарантується фізичною забороною запису на дискету.

Важливою проблемою є неможливість переривання процесу активізації компонент. В ряді операційних середовищ для цього існують штатні можливості, передбачені для забезпечення захисту від помилок користувача, що сформовують некоректну послідовність активізації компонент операційної системи. У зв’язку з цим повинні бути прийняті заходи, що гарантують пасивність органів управління в період оброблення послідовності Zp (наприклад, апаратне блокування клавіатури з моменту активізації модифікованого boot до моменту закінчення активізації суб’єктів множини Sz).

Описаний метод пізніше був реалізований у зовнішніх носіях типу CD-ROM, які дозволили значно (на два порядки) збільшити інформаційну ємність носія та завантажувати з нього розвинені операційні середовища типу OS/2. Проте однократність запису суттєво знижує гнучкість побудови ізольованого програмного середовища таким методом.

Незручність використання завантажувальної дискети та їх швидке зношення обумовили виникнення наступного способу проектування ізольованого програмного середовища.

Можна відмовитися від завантажувальної дискети та розглянути ПЕОМ із завантаженням операційної системи з пристрою зберігання (вінчестера) та додатковим апаратним пристроєм ізольованого середовища.

Твердження 8 або умови генерації ізольованого програм,ного середовища при реалізації методу довіреного завантаження.

Нехай ядро операційної системи містить монітор безпеки об'єктів та монітор безпеки суб'єктів, ініційовані в операційній системі суб'єкти попарно коректні, їх об'єкти-джерела належать множині перевірюваних на незмінність в ході довіреного завантаження, монітор безпеки об'єктів забороняє зміну будь-якого об'єкта-джерела і виконана процедура довіреного завантаження операційної системи. Тоді після ініціювання ядра операційної системи генерується ізольоване програмне середовище.

Доведення. Процедура довіреного завантаження за побудовою забезпечує незмінність Oz і Zl, за умовою твердження про породження суб'єктів є дозволеними тільки об'єкти-джерела, що Oz належать Oz, незмінність об'єктів-джерел за умовою гарантується властивостями монітора безпеки об'єктів. Отже, виконанні умови твердження 5 та генерується ізольоване програмне середовище. Твердження доведене.

4.2. Стандартизовані моделі та методи оцінки ефективності захисту інформації

Модель, що покладена в основу міжнародного стандарту ISO 7498-2. Ієрархічна декомпозиція в моделі OSI/ISO

Одним з розповсюджених прикладів ієрархічної структури мов для опису складних систем є розроблена Міжнародною організацією зі стандартизації (ISO) Еталонна модель взаємодії відкритих систем (Open Systems Interconnection (OSI) model). Вона відіграє важливу роль як методологічна, концептуальна і термінологічна основа побудови обчислювальних мереж. Описана в стандарті ISO/IEC 7498-2 (рис. 4.3).

Модель складається із семи рівнів фізичного, канального, мережного, сеансового, представницького та прикладного, для кожного з яких створені свої стандарти і загальні моделі.

Верхні рівні вирішують завдання подання даних користувачеві у такій формі, яку він може розпізнати та використати. Нижні рівні служать для організації передавання даних.

Ієрархія полягає у наступному. Усю інформацію у процесі передавання повідомлення від одного користувача (процесу) до іншого можна розбити на рівні; кожний рівень є виразом деякої мови, яка описує інформацію свого рівня. У термінах мови даного рівня виражається перетворення інформації і "послуги", які на цьому рівні надаються наступному рівню. При цьому, сама мова опирається на основні елементи, які є "послугами" мови більш низького рівня. У моделі взаємодії відкритих систем мова кожного рівня разом з порядком його використання називається протоколом цього рівня.

Розглянемо призначення кожного рівня, та представлення кожного рівня.

Прикладний рівень [application level] має відношення до семантики інформації, якою обмінюються, (тобто до її смислу). Мова прикладного рівня забезпечує взаєморозуміння двох прикладних процесів у різних точках, що сприяє здійсненню бажаного оброблення інформації.

Одним з важливих протоколів прикладного рівня є електронна пошта (протокол X.400), тобто транспортування повідомленв між незалежними системами з різноманітними технологіями передавання та доставки повідомленв.

Представницький рівень (presentation level] вирішує ті проблеми взаємодії прикладних процесів, які зв'язані з різноманіттям представлення цих процесів. Представницький рівень надає послуги для двох користувачів, які бажають зв'язатися на прикладному рівні, забезпечуючи обмін інформацією відносно синтаксису даних, що передаються між ними. Це можна зробити або у формі імен, якщо обом системам, що зв'язуються, відомий синтаксис, яким будуть користуватися, або у формі опису синтаксису, який буде використовуватися, якщо він є невідомим. Якщо синтаксис інформації, що передається, відрізняється від синтаксису, яка використовується

приймальною системою, то представницький рівень повинен забезпечити відповідне перетворення.

Крім того, представницький рівень забезпечує відкривання та закривання зв'язку, управління станом представницького рівня та контролем помилок.

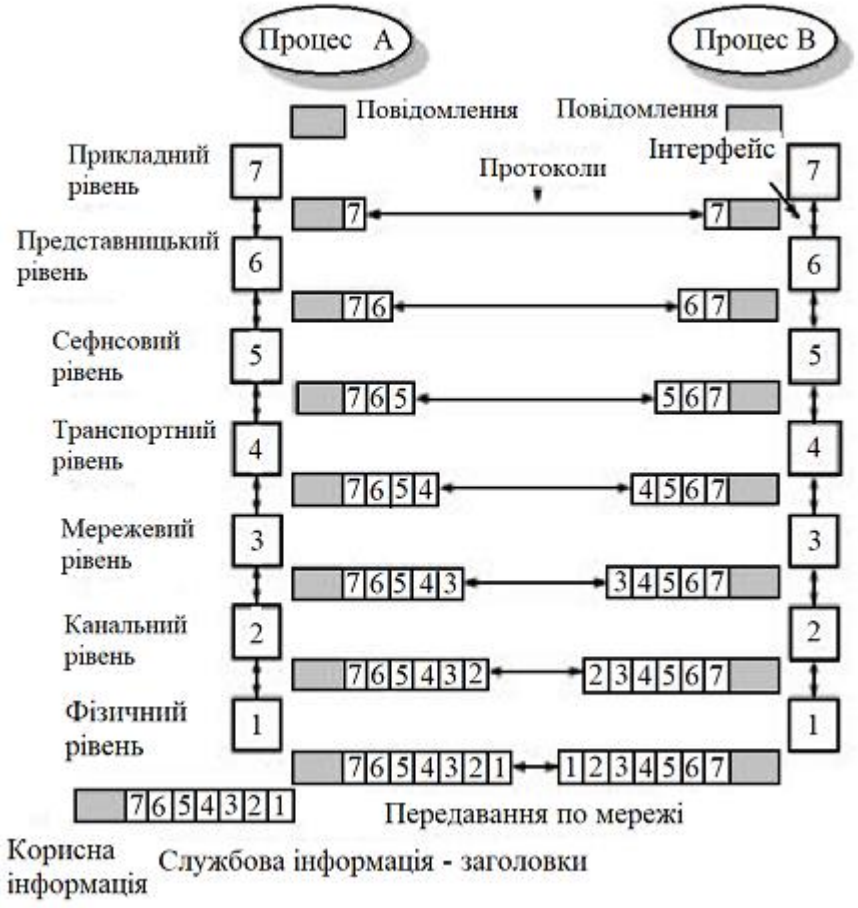


Рис. 4.3. Модель взаємодії відкритих систем

Сеансовий рівень (session level] забезпечує управління діалогом між обслуговуваними процесами на представницькому рівні. Сеансове з'єднання спочатку повинно бути встановлене, а параметри з'єднання обговорені шляхом обміну інформацією управління. Сеансів рівень надає послугу синхронізації для подолання будь- яких виявлених помилок.

Це здійснюється наступним чином: мітки синхронізації вставляються у потік даних користувачами послуги сеансу. Якщо виявлена помилка, сеансове з'єднання повинно повернутися у встановлену точку діалогового потоку інформації, скинути частину переданих даних а потім відновити передачу, починаючи з цієї точки.

Транспортний рівень [transport level] представляє сеансовому рівневі послугу у вигляді надійного та прозорого механізму передавання даних (незалежно від виду реальної мережі) між вершинами мережі.

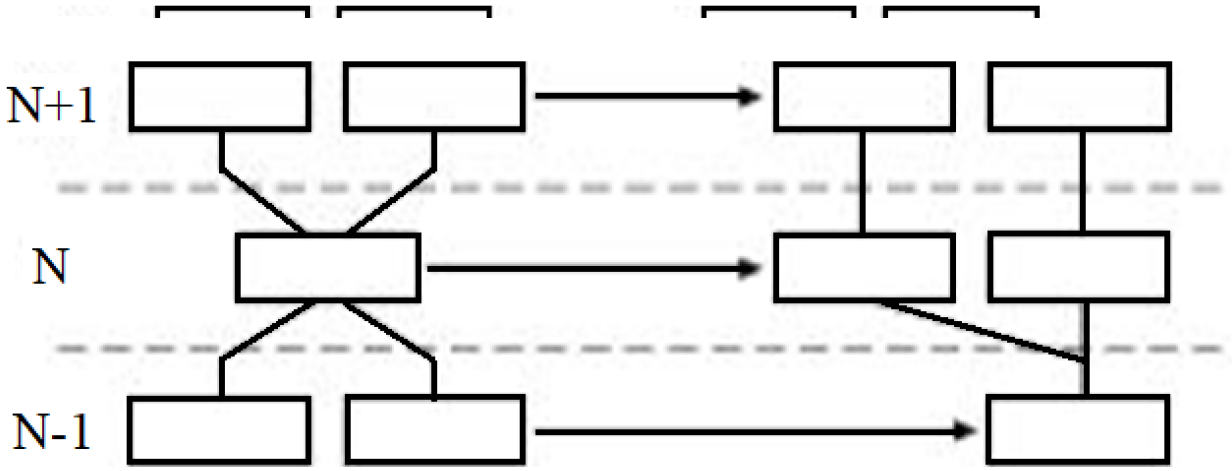
Мережний рівень [network level] надає транспортному рівневі послуги зв'язку. Мережний рівень визначає маршрут у мережі. Організовує мережний обмін (протокол IP). Управляє потоками в мережі.

Канальний рівень [link level] надає мережному рівневі послуги каналу. Ця послуга полягає у безпомилковій послідовного передавання блоків даних каналом у мережі. На цьому рівні реалізується синхронізація, порядок блоків, виявлення та виправлення помилок, лінійне шифрування.

Фізичний рівень [physical level] забезпечує те, що символи, які поступають у фізичне

середовище передавання на одному кінці, досягали другого кінця.

Для реалізації функції обміну інформацією на кожному рівні до вхідного блоку даних додається інформація у виді вираження мови відповідного рівня (як правило у вигляді додаткового заголовка).



Рівні функціонально взаємодіють, по-перше, як однакові рівні у різних абонентів, по-друге, як суміжні рівні в одній ієрархії.

Якщо важливі інформаційні елементи кожного рівня назвати об'єктами, то зв'язок (N-l)-го, N-го і (N+l)-го рівнів виглядає наступним чином (рис. 4.4) кожний рівень містить набір об'єктів, які взаємодіють між собою у різних системах на одному рівні. На різних рівнях об'єкти взаємодіють через ключі доступу послуг.

Запит подається користувачем послуги на (N+1) рівні системи А для того, щоб звернутися до послуги протоколу постачальника послуги на N-му рівні. Це призводить до посилки повідомлення N-го рівня в систему В. У системі В запит на рівні N викликає появу примітивної "ознаки", що випускається постачальником послуги на рівні N у В на (N+1) рівень.

Примітивна "відповідь" випускаєтвся користувачем послуги на рівні (N+1) у В у відповідь на ознаку, що з'явилася у точці доступу до послуги між рівнями N і (N+1) системи В. Примітивна "відповідь" є директивою протоколу рівня N завершити процедуру звернення примітивної "ознаки". Протокол на рівні N у системі В генерує повідомлення, яке передаєтвся у мережі та повторюється на рівні N системи А. Це викликає посилання примітива "підтвердження", який випускається постачальником послуги в системі А на рівні N у точці доступу до послуги між рівнями N і (N+1). Ця процедура, розпочата запитом у точці доступу до послуги між рівнями N і (N+1) в системі А завершуєтвся.

Процедури захисту

Архітектура захисту інформації в мережах телекомунікації — концепція захисту інформації в мережах телекомунікації, що використовує міжнародні стандарти, яка розроблена і розвиваєтвся Міжнародною організацією зі стандартизації (**ISO**) у відповідності до ідеології моделі взаємодії відкритих систем.

Рекомендації МСЕ для захисту інформації у телекомунікаціях (ITU-T Recommendations) — це процедури, рекомендовані Міжнародною організацією зі стандартизації (ISO) для створення сервісних служб захисту інформації у мережах телекомунікації.

Процедура шифрування даних у телекомунікаційних системах призначена для "закриття" всіх даних абонента або декількох полів повідомлення. Може мати два рівні: шифрування в каналі зв'язку (лінійне) і міжкінцеве (абонентське) шифрування.

Процедура цифрового підпису в телекомунікаційних системах служить для підтвердження правильності змісту повідомлення. Вона засвідчує факт його відправлення

власне тим абонентом, який вказаний у заголовкові як джерело даних. Цифровий підпис є функцією від змісту таємної інформації, відомої тільки абоненту-джерелу, і загальної інформації, відомої всім абонентам системи.

Процедура керування доступом до ресурсів телекомунікаційної системи виконуєтвся на основі множини правил і формальних моделей, що використовуються як аргумент доступу до інформації - інформацію про ресурси (класифікацію) та ідентифікатори абонентів. Службова інформація для керування доступом (паролі абонентів, списки дозволених операцій, персональні ідентифікатори, часові обмежувачі і т. ін.) містяться в локальних базах даних забезпечення безпеки мережі.

Процедура забезпечення цілісності даних у телекомунікаційних системах передбачає введення в кожне повідомлення деякої додаткової інформації, яка є функцією від змісту повідомлення. В рекомендаціях МСЕ розглядаються методи забезпечення цілісності двох типів: перші забезпечують цілісність поодинокого блока даних, інші — цілісність потоку блоків даних або окремих полів цих блоків. При цьому забезпечення цілісності потоку блоків даних не має сенсу без забезпечення цілісності окремих блоків. Ці методи застосовуються у двох режимах — при передаванні даних по віртуальному з'єднанню і при використанні дейтаграмного передавання. В першому випадку виявляються невпорядкованість, утрати, повтори, вставки даних за допомогою спеціальної нумерації блоків або введенням міток часу. У дейтаграмному режимі мітки часу можуть забезпечити тільки обмежений захист цілісності послідовності блоків даних і запобігти переадресації окремих блоків.

Процедура автентифікації у телекомунікаційних системах призначена для захисту при передаванні в мережі паролів, автентифікаторів логічних об'єктів і т. ін. Для цього використовуються криптографічні методи і протоколи, засновані, наприклад, на процедурі "трикратного рукостискання". Метою таких протоколів є захист від установлення з'єднання з логічним об'єктом, утвореним порушником або діючим під його керуванням із метою імітації роботи справжнього об'єкта.

Процедура заповнення потоку в телекомунікаційних системах призначена для запобігання аналізу трафіка. Ефективність застосування цієї процедури підвищуєтвся, якщо одночасно з нею передбачене лінійне шифрування всього потоку даних, тобто потоки інформації й заповнення стають нерозбірливими.

Процедура керування маршрутом у телекомунікаційній системі призначена для організації передавання тільки маршрутами, утвореними за допомогою надійних і безпечних технічних засобів і систем. При цвому може бути організований контроль із боку одержувача, який у випадку виникнення підозри про компрометацію використовуваної системи захисту може вимагати зміну маршруту.

Процедура підтвердження характеристик даних у телекомунікаційних системах передбачає наявність арбітра, який є довіреною особою взаємодіючих абонентів і може підтвердити цілісність, час передавання документів, а також запобігти можливості відмови джерела від видавання будь-якого повідомлення, а споживача — від його приймання, тобто підтвердження причетності.

Спільне використання процедур захисту дозволяє організувати п'ять базових сервісів: **автентифікація** [authentication], **контроль доступу** [access control], **засекречування** (конфіденційність) [confidentiality], **цілісність** [integrity], **інформування** (причетність) [nonrepudiation]. Для всіх цих сервісів визначені також варіанти, як наприклад, для комунікацій з установленням з'єднань і (установлення з'єднань або забезпечення безпеки на рівнях комунікації, пакетів або окремих полів.

Сервісні служби захисту інформації.

Сервісні служби захисту інформації в мережах телекомунікації це сукупність заходів захисту інформації у мережах телекомунікації, які у відповідності до рекомендацій МСЕ реалізуються за допомогою процедур захисту.

Автентифікація

Сервісна служба автентифікації однорівневих об'єктів реалізує свої функції за допомогою процедур автентифікації (на мережному, транспортному та прикладному

рівнях моделі взаємодії відкритих систем) та (або) шифрування даних і цифрового підпису (на мережному та транспортному рівнях МВВС).

Сервісна служба автентифікації джерела даних реалізує свої функції за допомогою процедур шифрування даних (на мережному й транспортному рівнях МВВС) та цифрового підпису (на мережному, транспортному та прикладному рівнях МВВС).

Контроль доступу

Сервісна служба контролю доступу реалізує свої функції за допомогою процедури керування доступом до ресурсів телекомунікаційної системи на мережному, транспортному і прикладному рівнях МВВС.

Конфіденційність

Сервісна служба засекречування з'єднання реалізує свої функції за допомогою процедур шифрування даних (на фізичному, канальному, мережному, транспортному, представницькому та прикладному рівнях МВВС) та керування маршрутом (на мережному рівні МВВС).

Сервісна служба засекречування в режимі без з'єднання реалізує свої функції за допомогою процедур шифрування даних (на **канальному,** мережному, транспортному, представницькому і прикладному рівнях МВВС) та керування маршрутом (на мережному рівні МВВС).

Сервісна служба засекречування вибіркових полів реалізує свої функції за допомогою процедури шифрування даних на представницькому та прикладному рівнях моделі взаємодії відкритих систем.

Сервісна служба засекречування потоку даних реалізує свої функції за допомогою процедур шифрування даних (на фізичному і представницькому рівнях МВВС), заповнення потоку (на мережному і прикладному рівні МВВС) та керування маршрутом (на мережному рівні МВВС).

Цілісність

Сервісна служба забезпечення цілісності з'єднання реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на транспортному і прикладному рівнях МВВС.

Сервісна служба забезпечення цілісності з'єднання без відновлення реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на мережному, транспортному і прикладному рівнях МВВС.

Сервісна служба забезпечення цілісності вибіркових полів даних реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на прикладному рівні моделі взаємодії відкритих систем.

Сервісна служба забезпечення цілісності даних без установлення з'єднання реалізує свої функції за допомогою процедур забезпечення цілісності даних, шифрування даних (на мережному, транспортному і прикладному рівнях МВВС) та цифрового підпису (на транспортному рівні МВВС).

Сервісна служба забезпечення цілісності вибіркових полів без з'єднання реалізує свої функції за допомогою процедур забезпечення цілісності даних, шифрування даних (на прикладному рівні моделі взаємодії відкритих систем) та цифрового підпису (на мережному, транспортному та прикладному рівнях МВВС).

Інформування

Сервісна служба інформування про відправлення реалізує свої функції за допомогою процедур підтвердження характеристик даних, забезпечення цілісності даних та цифрового підпису на прикладному рівні МВВС.

Сервісна служба інформування про доставку реалізує свої функції за допомогою процедур підтвердження характеристик даних, забезпечення цілісності даних та цифрового підпису на прикладному рівні моделі взаємодії відкритих систем.

Кожна із сервісних служб може самостійно вирішувати відповідне завдання із забезпечення інформаційної безпеки за допомогою тих чи інших механізмів захисту. При цвому один і той же механізм захисту може бути використаний в інтересах різних служб інформаційної безпеки.

Реалізація захисту

На фізичному та каналвному рівнях основний механізм захисту — шифрування з'єднання або трафіка (зашифровуватися може як весь трафік, так і його частина), що забезпечує конфіденційність інформації, яка передається. Для захисту інформації на фізичному рівні застосовують скремблювання, шифрувальні модеми, спеціалізовані адаптери.

Достоїнство реалізації засобів захисту: апаратна реалізація.

Недоліки застосування засобів захисту:

- фіксована продуктивність;
- висока вартість.

Адміністрування засобів безпеки

Адміністрування засобів безпеки включає в себе розповсюдження інформації, необхідної для роботи сервісів і механізмів безпеки, а також збирання і аналіз інформації про їх функціонування. Прикладами можуть служити розповсюдження криптографічних ключів, установка значень параметрів захисту, ведення інформаційного журналу і т.ін.

Концептуальною основою адміністрування є інформаційна база **управління безпекою.** Ця база може не існувати як єдине розподілене сховище, але кожна з кінцевих систем повинна мати інформацію, необхідну для реалізації вибраної політики безпеки.

Серед дій, що відносяться до системи у цілому, відзначають забезпечення актуальності політики безпеки, взаємодія з іншими адміністративними службами, реагування на події, що відбуваються, аудит та безпечне відновлення.

Адміністрування сервісів безпеки включає в себе визначення об'єктів, що підлягають захисту, вироблення правил підбору механізмів безпеки (при наявності альтернатив), комбінування механізмів для реалізації сервісів, взаємодія з іншими адміністраторами для забезпечення узгодження роботи.

Обов'язки адміністратора безпеки визначаються переліком задіяних механізмів.

Модель, що покладена в основу НД ТЗІ 2.5-005-99

Комп'ютерна система представляється множиною компонентів. Частина компонентів призначаються для реалізації політики безпеки (наприклад, засоби ізоляції процесів або керування потоками інформації). Інші виливають на безпеку опосередковано, наприклад, забезпечують функціонування компонентів першого тину. Треті не задіяні під час вирішення завдань забезпечення безпеки. Множина всіх компонентів перших двох типів називається комплексом засобів захисту.

У НД ТЗІ 2.5-005-99 усі ресурси комп'ютерної системи, що знаходяться під управлінням комплексу засобів захисту називаються об'єктами. Як об'єкти вони характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поводженням, яке визначає способи зміни стану. Для різних комп'ютерних систем об'єкти можуть бути різні. Наприклад, для системи управління базами даних в якості об'єктів можна розглядати записи баз даних, а для операційної системи процеси, файли, кластери, сектори дисків, сегменти нам'яті і т.ін. Все, що підлягає захисту відповідно до політики безпеки, має бути визначено як об'єкт.

При розгляді взаємодії двох об'єктів комп'ютерної системи, що виступають як приймальники або джерела інформації, виділяють пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. Розглядаються такі тини об'єктів КС: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-кориетувача і об'єкта-нроцееу (рис. 4.5).

Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини. В інших доменах об'єкти залишаються в пасивному стані. Цс дозволяє одному об'єкту-процееу керувати іншим об'єктом-процсеом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Іншими словами, об'єкти можуть

знаходитись в одному з трьох різних станів: об’єкт-користувач, об’єкт-процее і пасивний. Перехід між станами означає, що об’єкт просто розглядається в іншому контексті.

Пасивний об’єкт переходить в стан об’єкта-користувача, коли особа (фізична особа-користувач) “входить” в систему. Цей об’єкт- користувач виступає для комплексу засобів захисту як образ фізичного користувача. Звичайно, за цим процесом іде активізація об’єкта-процесу за ініціативою користувача. Цей об’єкт-процес є керуючим для пасивних об’єктів всередині домену користувача. Об’єкти-користувачі, об’єкти-процеси і пасивні об’єкти далі позначаються просто як користувачі, процеси і об’єкти, відповідно.

Взаємодія двох об’єктів комп’ютерної системи (звернення активного об’єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об’єктами і/або зміни стану системи. Як потік інформації розглядається будь-яка порція інформації, що передається між об’єктами комп’ютерної системи.

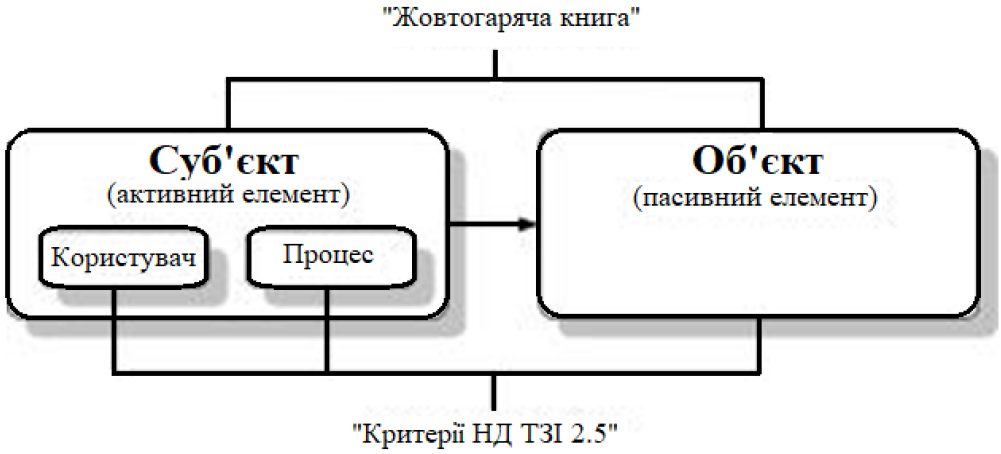


Рис. 4.5. Відповідність понять “Критеріїв НД ТЗІ 2.5-005-99” та “Жовтогарячої книги”

Основні принципи керування доступом Принцип безперервності захисту

Захист інформації повинен забезпечується протягом всього періоду її існування. З моменту створення об’єкта комп’ютерної системи або його імпорту до системи і аж до його знищення або експорту з системи всі запити на доступ до об’єкта і об’єкта на доступ до інших об’єктів мають контролюватися комплексом засобів захисту.

Перший аспект, що випливає з цього принципу, - це необхідність того, щоб абсолютно всі запити на доступ до об’єктів контролювалися комплексом засобів захисту і не існувало можливості обминути цей контроль (одержати доступ в обхід комплексу засобів захисту). Для захисту об’єктів комплекс засобів захисту повинен в першу чергу забезпечувати свою цілісність і керованість.

Другим аспектом є те, що особливе значення набуває визначення діючих за умовчанням правил, які визначають початкові умови, за яких починається існування об’єкта всередині комп’ютерної системи.

Принцип використання атрибутів доступу

Для реалізації політики безпеки комплекс засобів захисту повинен забезпечити ізоляцію об’єктів всередині сфери управління і гарантувати розмежування запитів доступу і керування потоками інформації між об’єктами. Для цього з об’єктами комп’ютерної системи має бути пов’язана інформація, що дозволяла б комплексу засобів захисту ідентифікувати об’єкти і перевіряти легальність запитів доступу. Як така інформація є атрибути доступу.

Кожний об’єкт комп’ютерної системи повинен мати певний набір атрибутів доступу, який включає унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього. Атрибут доступу — термін, що використовується для опису будь-якої інформації, яка використовується при керуванні доступом і зв’язана з

користувачами, процесами або пасивними об’єктами. Відповідність атрибутів доступу і об’єкта може бути як явною, так і неявною. Атрибути доступу об’єкта є частиною його подання в комп’ютерній системі.

Коли користувачі або процеси намагаються одержати доступ до пасивних об’єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть “прийняти рішення” про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати довірче керування доступом, адміністративне, контроль та цілісністю та інші види керування доступом.

Для відображення функціональності комп’ютерної системи у простір, в якому не розглядаються нрава власності, використовується концепція матриці доступу. Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об’єктів комп’ютерної системи, а в якості елементів матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двомірною (наприклад, кориетувачі/паеивні об’єкти або нроцееи/наеивні об’єкти) або тримірною (користувачі/процеси/пасивні об’єкти). Матриця доступу може бути иовною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих на даний час об’єктів комп’ютерної системи даного тину, або частковою. Повна тримірна матриця доступу дозволяє точно описати, хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чої'о (ідентифікатор пасивного об’єкта), який вид доступу може одержати.

Принципи довірчого і адміністративного керування доступом

У даному випадку створення додаткових потоків інформації може бути зумовлене: модифікацією атрибутів доступу користувача, процесу або пасивного об’єкта; створенням нових об’єктів (включаючи копіювання існуючих); експортом або імпортом об’єктів.

Функціональні критерії НД ТЗІ 2.5-005-99

Загальні відомості про функціональні критерії НД ТЗІ 2.5-005-99

В критеріях НД ТЗІ 2.5-005-99 комп’ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов’язково являють собою точну підмножину один одного. Рівні починаються з першого і зростають до значення n, де n — унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі **“Критерії конфіденційності”.**

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі **“Критерії цілісності”.**

Доступність. Загрози, що відносяться до порушення можливості використання комп’ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі **“Критерії доступності”.**

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп’ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі **“Критерії спостереженості”.**

У табл.4.2 наведені ідентифікатори рівнів функціональних критеріїв.

Таблиця 4.2

Ідентифікатори рівнів функціональних критеріїв

Ідентифікатор	Найменування	Рівні
Критерії конфіденційності		
КД	Довірча конфіденційність	КД-1 КД-4
КА	Адміністративна конфіденційність	КА-1 КА-4
КО	Повторне використання об´єктів	КО-1
КК	Аналіз прихованих каналів	КК-1 КК-3
КВ	Конфіденційність при обміні	КВ-1 КВ-4
Критерії цілісності		
ДД	Довірча цілісність	ЦД-1 ЦД-4
ЦА	Адміністративна цілісність	ЦА-1 ЦА-4
ДО	Відкат	ЦВ-1 ЦВ-3
ДВ	Цілісність при обміні	ЦО-1 ЦО-2
Критерії доступності		
ДР	Використання ресурсів	ДР-1 ДР-3
ДЕ	Стійкість до відмов	ДС-1 ДС-3
ДЗ	Гаряча заміна	ДЗ-1 ДЗ-3
ДВ	Відновлення після збоїв	ДВ-1 ДВ-3
Критерії спостережності		
НР	Реєстрація	НР-1 НР-5
НИ	Ідентифікація і автептифікація	НИ-1 НИ-3
НО	Розподіл обов’язків	НО-1 НО-3
НВ	Автептифікація при обміні	НВ-1 НВ-3
НП	Автептифікація отримувача	НП-1 НП-2
НК	Достовірний капал	НК-1 НК-2
НЦ	Цілісність комплексу засобів захисту	НЦ-1 НЦ-3
НТ	Самотестувашія	НТ-1 НТ-3
НА	Автептифікація відправника	НА-1 НА-2

Ранжирування вимог критеріїв конфіденційності

Для того, щоб комп’ютерна система могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної комп’ютерної системи повинен надавати послуги з захисту об’єктів від несанкціонованого ознайомлення з їх змістом (компрометації).

Загальні відомості про критерії гарантій безпеки НД ТЗІ 2.5-005-99

Критерії гарантій дозволяють оцінити коректність реалізації послуг. Вони включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. Таксономія критеріїв гарантій наведена на рис. 4.6.

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної комп’ютерної системи є повністю керованими з боку розробника.

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис комп’ютерної системи і реалізація комп’ютерної системи точно відповідає вихідним вимогам (політиці безпеки).

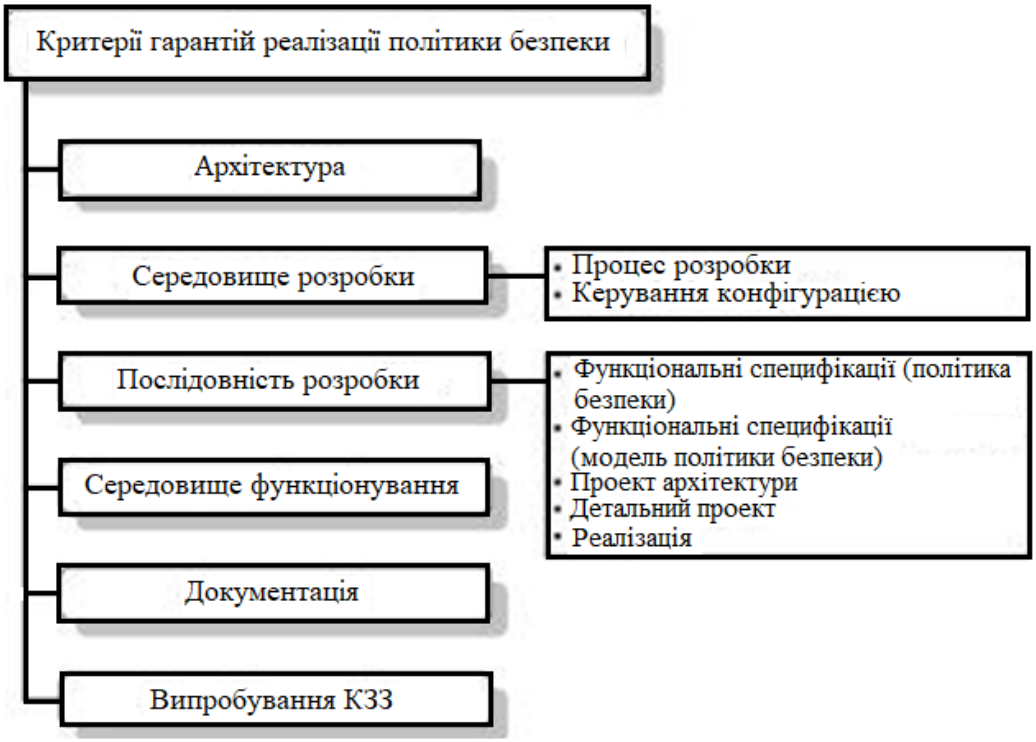


Рис. 4.6. Таксономія критеріїв гарантій реалізації політики безпеки НД ТЗІ 2.5-005-99

Вимоги до середовища функціонування забезпечують гарантії того, що комп'ютерна система поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється замовником так, як це передбачається розробником.

В критеріях НД ТЗІ 2.5-005-99 вводиться сім рівнів гарантій (Г-1,...,Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру впевненості в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Гарантії повинні забезпечуватися як в процесі розробки, так і в процесі оцінки. В процесі розробки гарантії забезпечуються діями розробника щодо забезпечення правильності (коректності) розробки. В процесі оцінки гарантії забезпечуються шляхом перевірки додержання розробником вимог критеріїв, аналізу документації, процедур розробки і постачання, а також іншими діями експертів, які проводять оцінку.

Функціональні профілі захищеності інформації НД ТЗІ 2.5-005-99

Необхідність створення методики, за якою можна було би створити класи безпеки комп'ютерних систем, як в "Жовтогарячій книзі" призвела до втілення концепції функціональних профілів безпеки в більш пізніх стандартах безпеки.

У НД ТЗІ 2.5-005-99 встановлюються принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Мета введення класифікації АС і стандартних функціональних профілів захищеності - полегшення задачі вставлення вимог до КЗЗ обчислювальної системи АС з характеристиками АС.

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і

призначенням АС.

В цьому документі за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас 1 - одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка обробляєтвся;
- технічні засоби (носії інформації і засоби вводу/виводу) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і/або вводу/виводу всієї інформації.

Приклад — автономна персоналвна ЕОМ, доступ до якої контролюєтвся з використанням організаційних заходів.

Клас 2 — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад — ЛОМ.

Клас 3 — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад — глобальна мережа.

Для кожного з підкласів кожного класу вводиться деяка кілвкість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Стандартний функціоналвний профіль захищеності являє собою перелік мінімалвно необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювалвної системи АС, щоб задоволвняти певні вимоги щодо захищеності інформації, яка обробляєтвся в даній АС. Стандартні функціональні профілі будуютвся на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред’являються.

Для стандартних функціональних профілів захищеності не вимагається ні зв’язаної з ними політики безпеки, ні рівня гарантій, хоч їх наявність і допускається в разі необхідності. Політика безпеки КС, що реалізує певний стандартний профіль, має бути "успадкована" з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в АС. Так, один і той же профіль захищеності може використовуватись для опису функціональних вимог з захисту оброблюваної інформації і для ОС, і для

СУБД, в той час, як їх політика безпеки, зокрема визначення об'єктів, буде різною.

Єдина вимога, якої слід дотримуватися при утворенні нових профілів, — це додержання описаних в НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" необхідних умов для кожної із послуг, що включаються до профілю.

Функціональні профілі можуть використовуватись також для зрівняння оцінки функціональності КС за критеріями інших держав з оцінкою за національними критеріями.

Семантика профілю

Опис профілю складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад, 2.К.4 — функціональний профіль номер чотири, що визначає вимоги до АС класу 2, призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності.

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостсй реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу АС.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

Стандартні профілі

Наведені профілі відповідають тим видам КС, потреба в яких найактуальніша.

Даний розділ являє собою довідник щодо функціональних профілів захищеності для різних класів АС. Багато профілів наведені лише для повноти класифікації, а не для практичного використання. Особливо це стосується профілів, що містять послуги, які забезпечують захист тільки від одного тину загроз.

До всіх профілів включені послуги сностереженості, оскільки, з одного боку, реалізація багатьох з них є необхідною умовою для реалізації інших послуг, а з іншого, спостереженість та керованість важливі для будь-якої системи, що реалізує будь-які функції захисту інформації.

Модель, що покладена в основу міжнародного стандарту ISO/IEC 15408. Основні положення загальних критеріїв безпеки інформаційних технологій

Загальні критерії безпеки інформаційних технологій (Common Criteria for Information Technology Security Evaluation (CCITSE)) стандарт інформаційної безпеки, що узагальнює зміст і досвід використання "Жовтогарячої книги".

В ньому розвинені " Європейські критерії'', втілена в реальні структури концепція типових профілів захисту "Федеральних критеріїв" США і відповідно до "Канадських критеріїв" представлена однакова основа для формулювання розробниками, користувачами та оцінювачами інформаційних технологій (експертами з кваліфікації) вимог, метрик і гарантій безпеки.

Матеріали стандарту являють собою енциклопедію вимог і гарантій з інформаційної безпеки, які можуть відбиратися та реалізовуватися у функціональні стандарти (профілі захисту) забезпечення інформаційної безпеки для конкретних систем, мереж і засобів як користувачами (по відношенню до того, що вони хочуть одержати в продукті, який пропонується), так і розробниками й операторами мереж (по відношенню до того, що вони гарантують у продукті, який реалізується).

До складу "Загальних критеріїв" входять три основні частини (рис. 4.7):

- частина 1 "Уявлення та загальна модель" [Part 1: Introduction and general model];

- частина 2 “Вимоги до функцій безпеки” [Part 1: Security functional requirements];
- частина 3 “Вимоги гарантій безпеки” [Part 1: Security assurance requirements].

За межі стандарту винесена частина 4 “Наперед визначені профілі захисту”, із-за необхідності постійного поповнення каталогу профілів захисту.

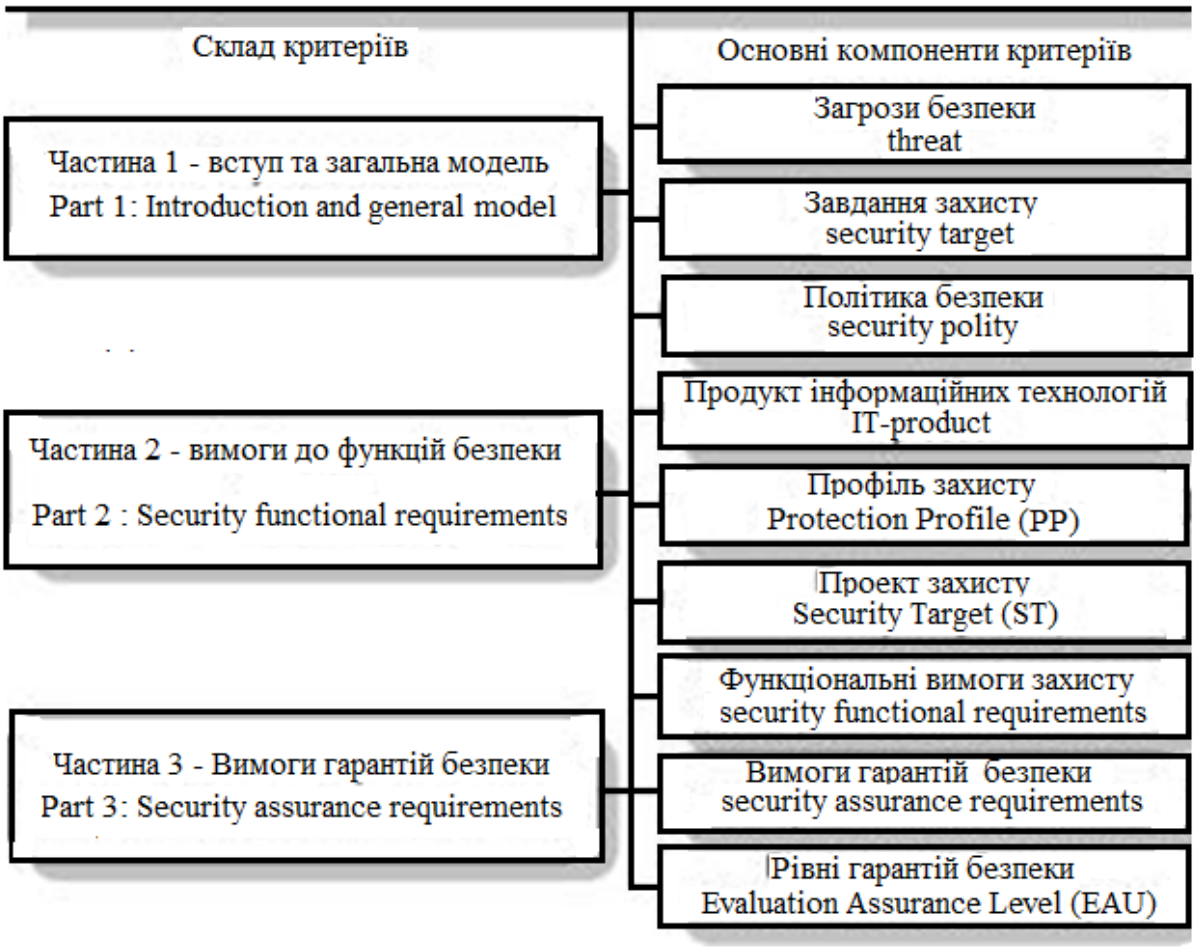


Рис. 4.7. Структура Загальних критеріїв безпеки інформаційних технологій

Стандарт “Загальних критеріїв” описує тільки загальну схему проведення кваліфікаційного аналізу та сертифікації, але не регламентує процедуру їх здійснення. Питаннями методології кваліфікаційного аналізу та сертифікації присвячений окремий документ авторів “Загальних критеріїв” — Загальна методологія оцінки безпеки інформаційних технологій [Common Methodology for Information Technology Security Evaluation (CMITSE)], який є додатком до стандарту.

Кваліфікаційний аналіз [evaluation] — це аналіз обчислювальної системи з метою визначення рівня її захищеності та відповідності вимогам безпеки на основі критеріїв стандарту інформаційної безпеки. Інша назва кваліфікування рівня безпеки (рис. 4.8).

Згідно “Загальних критеріїв” кваліфікаційний аналіз може здійснюватися як паралельно з розробленням IT-продукту, так і після її завершення.

Результатом кваліфікаційного аналізу є висновок про те, що підданий аналізу IT-продукт відповідає представленому проекту захисту.

Потенційні загрози безпеці та типові завдання захисту

Загрози безпеці обчислювальної системи — впливи на обчислювальну систему, які прямо або побічно можуть нанести шкоду її безпеці.

Загрози порушення конфіденційності — загрози безпеці обчислювальної системи, спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення цілісності — загрози безпеці обчислювальної системи, що полягають у спотворенні або зміні неавторизовашім користувачем інформації, що зберігається або передасться. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних виливів із сторони середовища експлуатації системи. Найбільш актуальна ця загроза для систем передавання інформації комп'ютерних мереж і систем телекомунікації.

Загрози порушення працездатності загрози безпеці обчислювальної системи, спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність обчислювальної системи, або її ресурси стають недоступними.

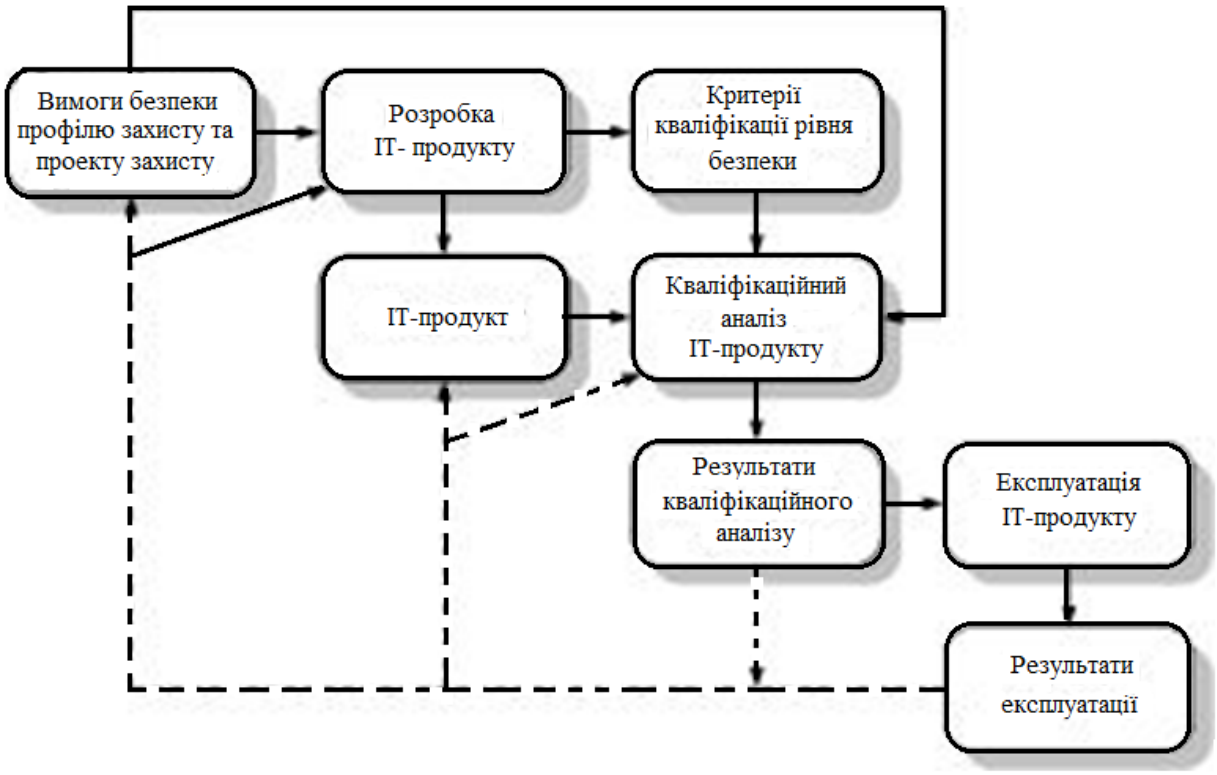


Рис. 4.8. Кваліфікаційний аналіз

Політика безпеки

Політика безпеки [security policy] - сукупність законів, норм і правил, що регламентують порядок оброблення, захисту і розповсюдження інформації комп'ютерної системи.

В системах зв'язку політика безпеки є частиною загальної політики безпеки оператора зв'язку і може включати, зокрема, положення державної політики у галузі захисту інформації.

Для кожної системи (підсистеми) зв'язку політика безпеки може бути індивідуальною і може залежати від технології передавання, оброблення та зберігання інформації, що реалізується, особливостей системи зв'язку, середовища експлуатації і від багатьох інших факторів. Політика повинна визначати ресурси системи зв'язку, які потребують захисту, зокрема, встановлювати категорії інформації, яка передається, оброблюється та зберігається в системі. Мають бути сформульовані основні загрози для системи зв'язку, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Складовими частинами загальної політики безпеки в системі зв'язку мають бути політики забезпечення конфіденційності, цілісності і доступності інформації, що

передається, оброблюється і зберігається. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів системи зв'язку, складає правила розмежування доступу.

Продукт інформаційних технологій

Продукт інформаційних технологій (ІТ-продукт) — сукупність апаратних і (або) програмних засобів, яка поставляється кінцевому споживачеві як готовий до використання засіб оброблення інформації. Сукупність ІТ-продуктів об'єднується в функціонально закінчений комплекс (продукт) для вирішення конкретної прикладної завдання в системі оброблення інформації.

Принциповою відмінністю між ІТ-продуктом і системою оброблення інформації є наступне. ІТ-продукт звичайно розробляється для використання в багатьох системах оброблення інформації, тому його розробник орієнтується тільки на найзагальніші вимоги до середовища його експлуатації (умови його застосування і потенційні загрози інформації).

Навпаки, система оброблення інформації розроблюється вузько спеціалізованою для вирішення конкретних прикладних задач і під конкретні вимоги споживачів, що дозволяє у повній мірі враховувати специфіку впливу зі сторони конкретного середовища експлуатації. Саме тому ІТ-продукт, а не система оброблення інформації, декларується в стандарті як універсальний компонент безпеки.

Профіль захисту

Профіль захисту (Protection Profile (PP)) спеціальний нормативний документ, що регламентує сукупність завдань захисту, функціональних вимог безпеки, вимог гарантій безпеки та їхнє обґрунтування. Профіль захисту визначає вимоги безпеки до певної категорії ІТ-продуктів, не уточнюючи методи і засоби їх реалізації. За допомогою профілю захисту споживачі формують свої вимоги до розробників ІТ-продуктів.

Профіль захисту містить вступ, опис ІТ-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, додаткові відомості, обґрунтування (рис. 4.9).

Вступ складається з ідентифікатора профілю захисту та огляду змісту. Ідентифікатор профілю захисту являє собою унікальне ім'я для його пошуку серед подібних йому профілів і позначення посилань на нього.

Огляд змісту профілю захисту містить коротку анотацію профілю захисту, на основі якої споживач може зробити висновок про придатність даного профілю захисту.

Профіль захисту містить коротку характеристику ІТ-продукту, призначення, принцип роботи, методи використання і т. ін. Ця інформація не підлягає кваліфікаційному аналізу та сертифікації, але подається розробникам і експертам для пояснення вимог безпеки і визначення їхньої відповідності до завдань, що вирішуються за допомогою ІТ-продукту.

Профіль захисту містить опис усіх аспектів функціонування ІТ-продукту, зв'язаних з безпекою. В середовищі експлуатації описуються умови експлуатації, загрози безпеці, політика безпеки.

Опис умов експлуатації ІТ-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, в тому числі обмеження на умови його застосування.

Опис загроз безпеці, що діють у середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози повинно бути вказане її джерело, метод і об'єкт впливу.

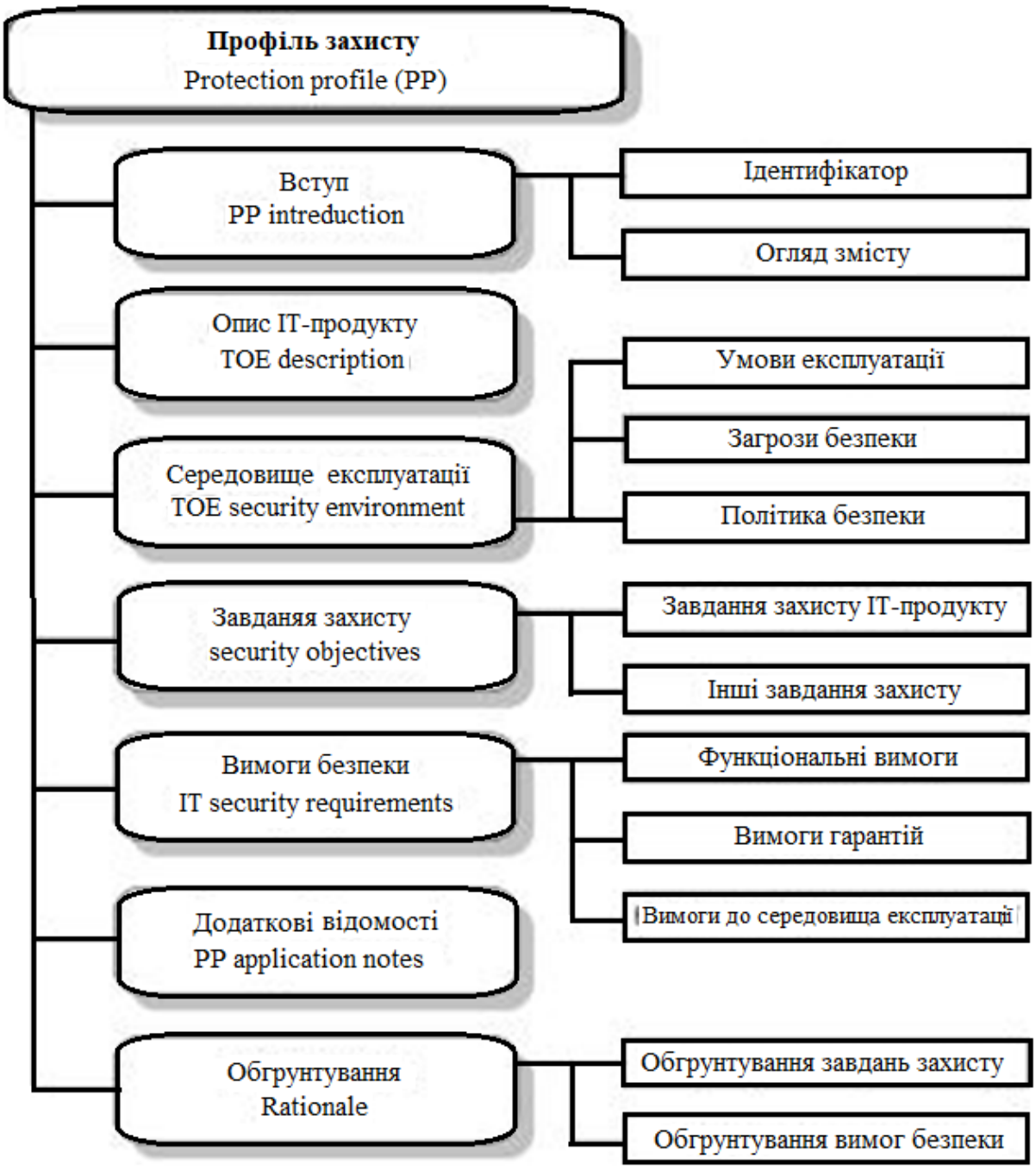


Рис. 4.9. Структура профілю захисту

Опис політики безпеки повинен визначати і, при необхідності, пояснювати правила політики безпеки, яка повинна бути реалізована в IT-продукті.

Профіль захисту: завдання захисту (security objectives) — розділ профілю захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці і (або) реалізації політики безпеки. До складу завдань захисту входять завдання захисту IT-продукту та інші завдання захисту.

Завдання захисту IT-продукту повинні визначати та регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки.

Інші завдання захисту повинні регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки інших компонент комп'ютерної системи, що не відноситися до сфери інформаційних технологій.

Профіль захисту: вимоги безпеки (IT security requirements) - розділ профілю захисту, що містить вимоги, якими повинен задоволвняти ІТ-продукт для вирішення завдань захисту (типових, спеціальних і т. ін.). В розділі виставляються функціональні вимоги безпеки, вимоги гарантій безпеки, вимоги до середовища експлуатації.

Функціональні вимоги повинні містити тільки типові вимоги, передбачені тільки відповідними розділами "Загальних критеріїв". Необхідно забезпечити такий рівень деталізації вимог, який дозволяє продемонструвати їх відповідність до завдань захисту. Функціоналвні вимоги можуть дозволяти або забороняти використання конкретних методів і засобів захисту.

Вимоги гарантій містять посилання на типові вимоги рівнів гарантій "Загалвних критеріїв", проте допускають і визначення додаткових вимог гарантій.

Вимоги до середовища експлуатації є необов'язковими і можуть містити функціональні вимоги та вимоги гарантій, яким повинні задовольняти компоненти інформаційних технологій, що складають середовище експлуатації ІТ-продукту. На відміну від попередніх розділів, використання типових вимог "Загалвних критеріїв" є бажаними, але не обов'язковими.

Профіль захисту: додаткові відомості (PP application notes) - необов'язковий розділ профілю захисту, що містить будь-яку додаткову інформацію, корисну для проектування, розробки, кваліфікаційного аналізу та сертифікації ІТ-продукту.

Профіль захисту: обгруптування (rationale) — розділ профілюзахисту, який невинен демонструвати, що профіль захисту містить повну й зв'язну множину вимог і що ІТ-нродукт, який задовольняє їм, буде протистояти загрозам безпеці середовища експлуатації. Розділ складається з обґрунтування завдань захисту та обґрунтування вимог безпеки.

Обґрунтування завдань захисту повинно демонструвати, що завдання, які пропонуються у профілі, відповідають параметрам середовища експлуатації, а їх вирішення дозволить ефективно протистояти загрозам безпеці і реалізувати політику безпеки.

Профіль захисту служить керівництвом для виробника та розробника ІТ-продукту, які повинні на його основі і технічних рекомендацій, що запропоновані ним, розробити проект захисту, який служить керівництвом для кваліфікаційного аналізу та сертифікації ІТ-продукту.

Проект захисту

Проект захисту (Security Target (ST)) нормативний документ, який включає вимоги та завдання захисту ІТ-продукту, а також описує рівень функціональних можливостей, реалізованих у ньому засобів захисту, їх обґрунтування і підтвердження ступеню їхніх гарантій. Проект захисту, з однієї сторони є відправною точкою для розробника системи, а з іншої являє собою еталон системи в ході кваліфікаційного аналізу.

Проект захисту містить вступ, опис ІТ-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, загальні специфікації ІТ-продукту, заявку на відповідність профілю захисту, обґрунтування (рис. 4.10). Багато розділів проекту захисту співпадають із однойменними розділами профілю захисту.

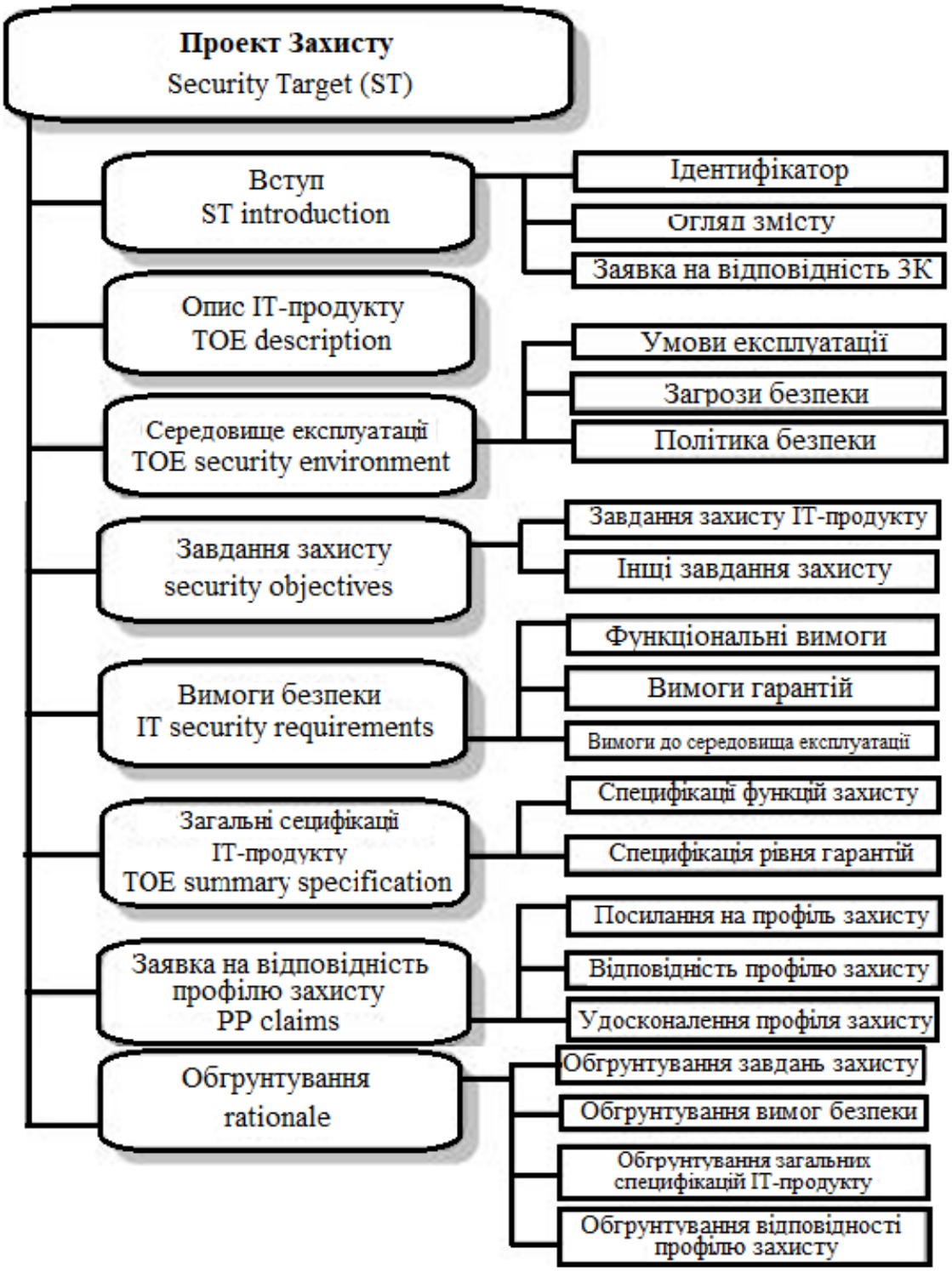


Рис. 4.10. Структура проекту захисту

Проект захисту: вступ (ST introduction) — розділ проекту захисту, який містить інформацію, необхідну для ідентифікації проекту захисту, визначення призначення, а також огляд його змісту та заявку на відповідність вимогам “Загальних критеріїв”.

Ідентифікатор проекту захисту — унікальне ім’я проекту захисту для його пошуку та ідентифікації, а також відповідного IT- продукту.

Огляд змісту проекту захисту — достатньо докладна анотація проекту захисту, що дозволяє споживачам визначати придатність IT-продукту для вирішення завдань.

Заявка на відповідність “Загальним критеріям” — опис усіх властивостей ІТ-продукту, що підлягають кваліфікаційному аналізу на основі “Загальних критеріїв”.

Проект захисту: опис ІТ-продукту (TOE description) — розділ проекту захисту, який містить коротку характеристику ІТ- продукту, призначення, принцип роботи, методи використання і т. ін. Ця інформація не підлягає кваліфікаційному аналізу та сертифікації, але подається розробникам і експертам для пояснення вимог безпеки і визначення їхньої відповідності завданням, що вирішуються за допомогою ІТ-продукту.

Проект захисту: середовище експлуатації, (TOE security environment) - розділ проекту захисту, що містить опис усіх аспектів функціонування ІТ-продукту, зв’язаних з безпекою. В середовищі експлуатації описуються умови експлуатації, загрози безпеці, політика безпеки.

Опис умов експлуатації ІТ-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, в тому числі обмеження на умови його застосування.

Опис загроз безпеці, що діють у середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози повинно бути вказане її джерело, метод і об’єкт впливу.

Опис політики безпеки повинен визначати і, при необхідності, пояснювати правила політики безпеки, яка повинна бути реалізована в ІТ-продукті.

Проект захисту: завдання захисту (security objectives) — розділ проекту захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці і (або) реалізації політики безпеки. До складу задач захисту входять завдання захисту ІТ-продукту та інші завдання захисту.

Завдання захисту ІТ-продукту повинні визначати і регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки.

Інші завдання захисту повинні регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки інших компонент комп’ютерної системи, що не відносяться до сфери інформаційних технологій.

Проект захисту: вимоги безпеки (IT security requirements) — розділ проекту захисту, що містить вимоги безпеки до ІТ-продукту, якими керувався виробник у ході його розроблення. Цей розділ дещо відрізняється від аналогічного розділу профілю захисту.

Розділ функціональних вимог безпеки до ІТ-продукту на відміну від відповідного розділу профілю захисту допускає використання крім типових вимог “Загальних критеріїв” і інших, специфічних для даного продукту та середовища його експлуатації. При описі таких спеціальних вимог необхідно зберігати стиль “Загальних критеріїв” і забезпечувати властиву їм ступінь деталізації.

Розділ вимог гарантій безпеки може включати рівні гарантій, не передбачені в “Загальних критеріях”. В даному випадку опис рівня гарантій повинен бути чітким, несуперечливим і мати ступінь деталізації, що допускає його використання в ході кваліфікаційного аналізу. При цьому бажано використати стиль і деталізації опису рівнів гарантій, прийняті в “Загальних критеріях”.

Проект захисту: загальні специфікації ІТ-продукту (TOE summary specification) — розділ проекту захисту, який описує механізми реалізації завдань захисту за допомогою визначення багаторівневих специфікацій засобів захисту у відповідності до функціональних вимог безпеки та вимог гарантій безпеки, що пред’являються. Складається зі специфікацій функцій захисту та специфікацій рівня гарантій.

Проект захисту: заявка па відповідність профілю захисту (PP claims) — необов’язковий розділ проекту захисту, який містить матеріали, необхідні для підтвердження заявки. Для кожного профілю захисту, на реалізацію якого претендує проект захисту, цей розділ повинен містити посилання на профіль захисту, відповідність профілю захисту, удосконалення профілю захисту.

Посилання на профіль захисту однозначно ідентифікує профіль захисту, на реалізацію якого претендує проект захисту, із зазначенням випадків, в яких рівень захисту, що забезпечується, перевершує вимоги профілю з коректною реалізацією усіх його вимог без виключення. Відповідність профілю захисту визначає можливості ІТ-продукту, які реалізують завдання захисту і вимоги, що містяться в профілі захисту.

Удосконалення профілю захисту відображає можливості ІТ-продукту, які виходять за рамки завдань захисту та вимог, встановлених у профілі захисту.

Проект захисту: обгрунтування (rationale) — розділ проекту захисту, який повинен показувати, що проект захисту містить повну і зв'язну множину вимог, що ІТ-продукт, який реалізує їх, буде ефективно протистояти загрозам безпеці. Крім того, обґрунтування містить підтвердження заявленої відповідності профілю захисту. Розділ деталізується у наступному.

Обґрунтування завдань захисту повинно демонструвати, що завдання захисту, заявлені в проекті захисту, відповідають властивостям середовища експлуатації, тобто їх вирішення дозволить ефективно протидіяти загрозам безпеці і реалізувати вибрану під них політику безпеки.

Функціональні вимоги до засобів захисту

Функціональні вимоги безпеки (ФВБ) (security functional requirements) - вимоги безпеки, які в "Загальних критеріях" регламентують функціонування компонентів ІТ-продукту, що забезпечують безпеку, і визначають можливості засобів захисту. ФВБ декларуються у вигляді добре розробленої формальної структури. Набір ФВБ узагальнює усі існуючі раніше стандарти інформаційної безпеки і відрізняється всеосяжною повнотою і найдокладнішою деталізацією. ФВБ розділені на 11 класів функціональних вимог безпеки і 67 розділів функціональних вимог (рис. 4.11).

Зміст класів ФВБ відрізняється своєю вдосконлюючою повнотою і багаторівневим підходом до забезпечення безпеки. Окремі класи вимог спрямовані на забезпечення безпеки самих засобів захисту, контролю за експлуатацією системи, забезпечення конфіденційності сеансів доступу до системи та організації обміну інформацією (рис. 4.12).

Вимоги конфіденційності, цілісності та керування доступом об'єднані в один клас захисту інформації, що виглядає цілком логічно і повністю відповідає їх призначенню. Слід відзначити наявність, крім політики керування доступом, також політики керування інформаційними потоками, а також відділення вимог до політики безпеки від вимог до засобів реалізації.

Клас вимог до безпеки самих засобів захисту є найбільш об'ємним, що визначається високим ступенем деталізації включених до нього вимог до методів і засобів забезпечення нормального функціонування засобів захисту.

Особлива увага приділяється контролю за доступом до системи і конфіденційності сеансів роботи з нею. Вимоги до організації інформаційного обміну обмежуються неможливістю учасників взаємодії ухилятися від відповідальності.

Розділ ФВБ (assurance family) — складова частина класу ФВБ.

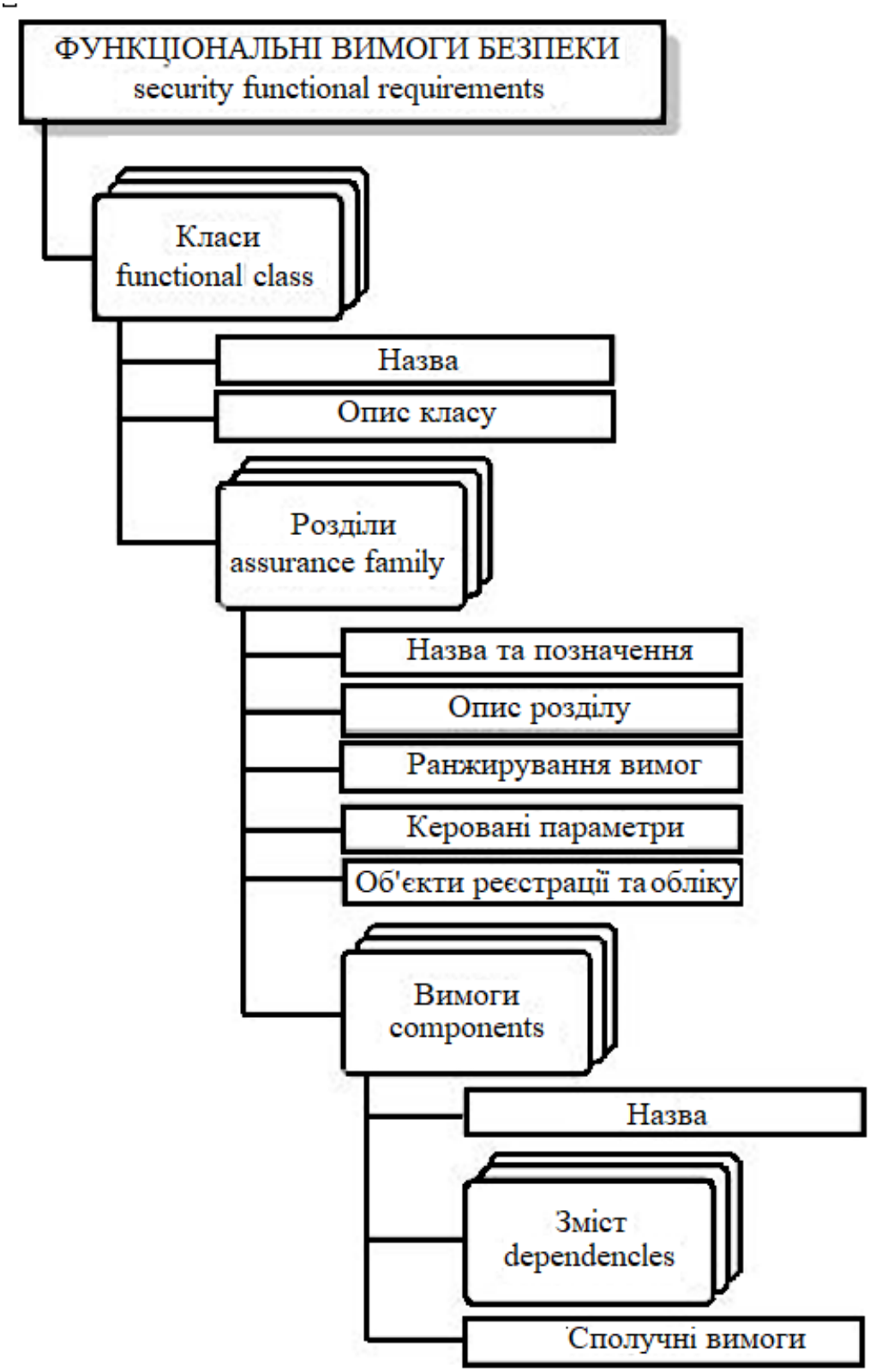


Рис. 4.11. Структура функціональних вимог безпеки

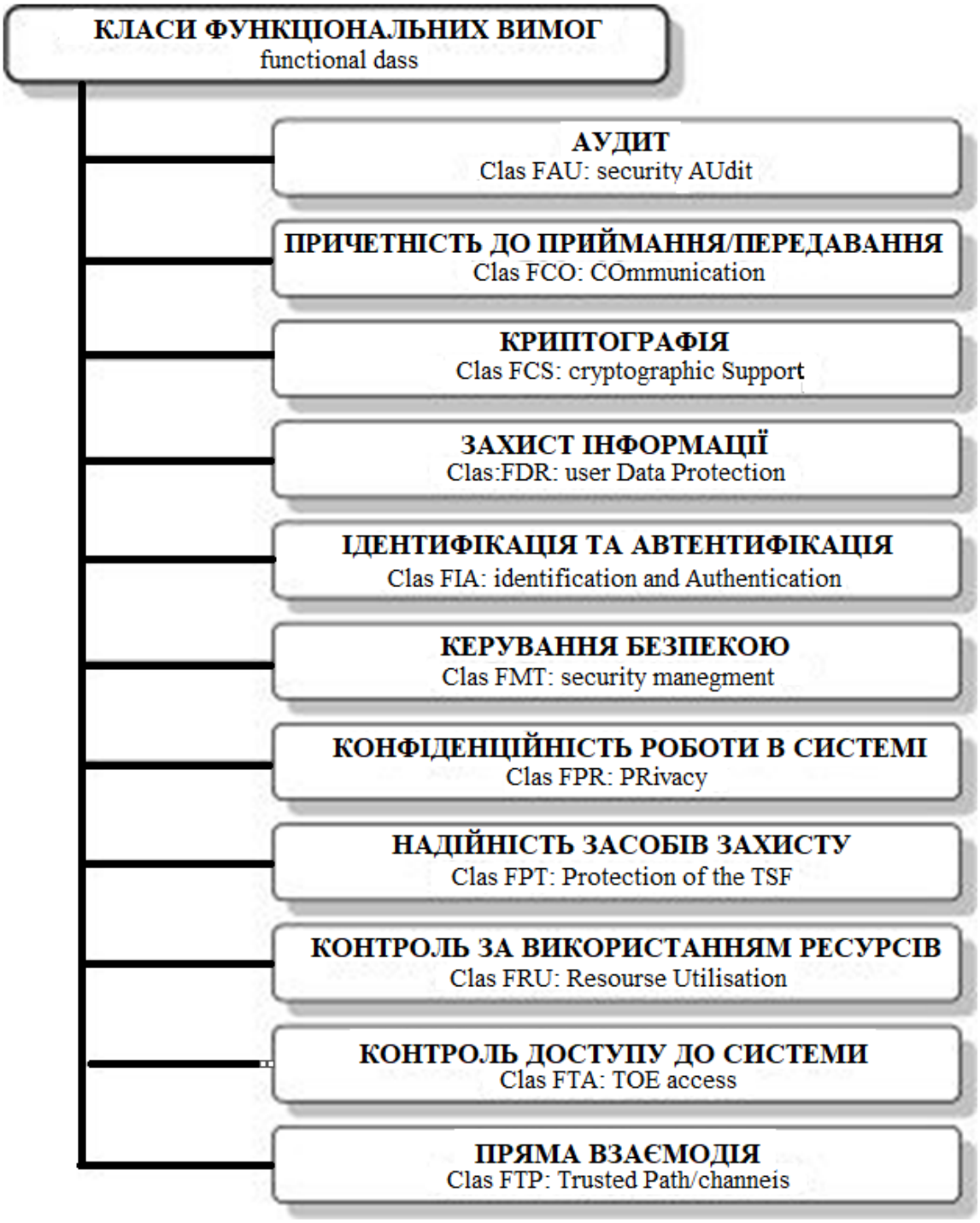


Рис. 4.12. Класи функціональних вимог

Кожний розділ має свою унікальну назву і семисимвольний ідентифікатор, який складається з трибуквенного ідентифікатора класу, знаку підкреслення і трибуквенного позначення розділу (рис. 4.13).

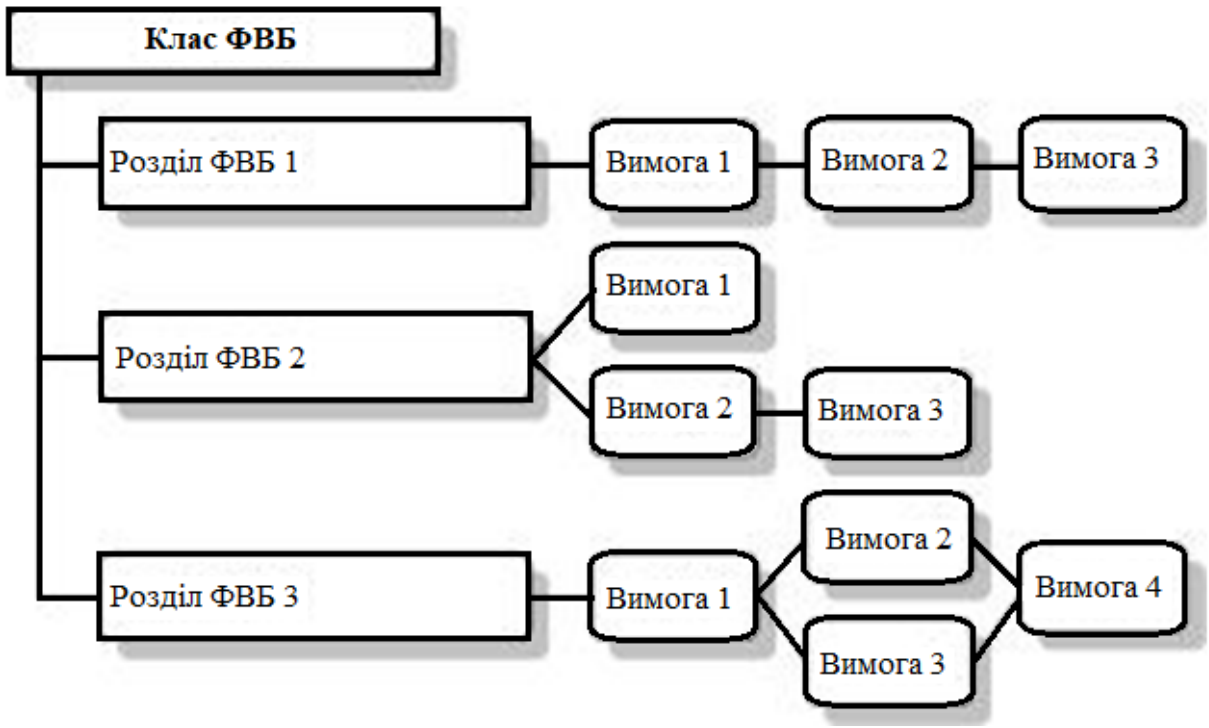


Рис. 4.13. Декомпозиція класу ФВБ

Контрольні запитання для самооцінки рівня знань

1. Сутність забезпечення гарантій виконання політики безпеки на основі методу генерації ізольованих програмних середовищ.
2. Сутність методу генерації ізольованого програмного середовища при проектуванні механізмів гарантованої підтримки політики безпеки.
3. Зміст моделі, що покладена в основу міжнародного стандарту ISO 7498-2.
4. Рівні моделі взаємодії відкритих систем.
5. Які процедури захисту покладені в основу міжнародного стандарту ISO 7498-2.
6. Які сервісні служби захисту інформації покладені в основу міжнародного стандарту ISO 7498-2**?**
7. Зміст моделі, що покладена в основу НД ТЗІ 2.5.
8. Відповідність понять “Критеріїв НД ТЗІ 2.5” та “Жовтогарячої книги”.
9. Загальні відомості про функціональні критерії НД ТЗІ 2.5.
10. Загальні відомості про критерії гарантій безпеки НД ТЗІ 2.5.
11. Функціональні профілі захищеності інформації НД ТЗІ 2.5**.**
12. Семантика функціональних профілів захищеності інформації НД ТЗІ 2.5.
13. Основні положення загальних критеріїв безпеки інформаційних технологій міжнародного стандарту ISO/IEC 15408.
14. Політика безпеки міжнародного стандарту ISO/IEC 15408.
15. Профіль захисту міжнародного стандарту ISO/IEC 15408.
16. Проект захисту міжнародного стандарту ISO/IEC 15408.
17. Функціональні вимоги до засобів захисту міжнародного стандарту ISO/IEC 15408.

Список літератури, рекомендованої для поглибленого вивчення дисципліни

1. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом ‘‘Вильямс’’, 2002. - 208 с.
2. Безопасность информационных технологий. Курс БТ01. М.: Учебный центр ‘‘Информзащита’’, 2003. - 233 с.
3. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2006. - 508 с.
4. Богуш В.М., Довидьков О.А. Проектування захищених комп’ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.
5. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, -К.; ПВП «Задруга», 2014. - 222 с.
6. ГОСТ 34.601- 90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. введен 01.01.92. - М.: Издательство стандартов, 1992. - 7 с.
7. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Изд-во агентства "Яхтсмен", 1996. - 192 с.
8. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
10. ДСТУ 2941-94. Системи оброблення інформації. Розроблення систем. Терміни та визначення. Чинний від 28.11.1994 р. - К.: Держстандарт України, 1994. - 19 с.
11. Защита информации в персональних ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков и др. - М.: Радио и связь, МП ‘‘Веста’’, 1992. - 192.
12. Зегжда Д.П., Ивашко А.П. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.
13. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальних сетевых технологий. - СПб.: Нолидж, 2000. - 288 с.
14. Хохлачова Ю. А. Політика інформаційної безпеки обє’кта. // НАУ України. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. – С. 23-29.
15. Олійник О. В. Державна політика інформаційної безпеки України. // Юридичний вісник, 4 (25) вип. 2012 р. – С. 65-69.
16. Сніцаренко П. М., Саричев Ю. О., Семененко В. М., Ткаченко В. А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського № 2(63), 2018 р. – С. 68-74.
17. Khmelevskoy R., Khmelevskoy Y., Kozachok V., Semko V., Ilin O. Information security and development problems egovernment systems in Ukraine. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2018 р., вип. №3 (35), с. 71-77
18. Козачок В.А., Рой А.А., Бурячок Л.В. Технології протидії шкідливим програмам та завідома фальшивому програмному забезпеченню. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2017р., вип. №2(30), с. 30-34.
19. Козачок В.А., Діхтяр М.В., Семко О.В. Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2017р., вип. №2(30), с. 42-48.
20. Гулак Г.М., Козачок В.А., Складанний П.М., Бондаренко М.О., Вовкотруб Б.В. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних

системах. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2017р., вип. №2(30), с. 65-71.

21. Козачок В.А., Киричок Р.В., Складанний П.М., Бурячок В.Л., Гулак Г.М. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення // Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. №3 (43). С. 48–61.

22. Козачок В.А., Коваленко Ю.Б. Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2015р., вип. 1, с. 41-47

23. Козачок В.А. Концептуальні засади створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. К., ДУТ, Збірник наукових праць «Зв'язок», 2014р., №3 (109), с. 8-13

24. Козачок В.А. Методичні рекомендації щодо проведення обстежень об'єктів інформаційної діяльності військового призначення. К., ВІТІ НТУУ "КПІ", Збірник наукових праць Вип. № 2 . 2008 р., с. 30-36.

25. Липаев В.В. Системное проектирование программных средств, обеспечивающих безопасность функционирования информационных систем // Информационные технологии. - 2000. - № 11. - С. 49-55.

26. Лукацкий А.В. Обнаружение атак. - СПб.: БХВ-Петербург, 2001. - 624.

27. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.

28. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53.

29. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.

30. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.

31. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від від 02.04.2003 р. № 33.

32. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 20.12.2000 р. № 60.

33. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 28.04.1999 р. № 22.

34. НД ТЗІ 3.7-005-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТЗІ СБ України від 08.11.2005 р. № 125.

35. Одинцов И.О. Профессиональное программирование. Системный подход. - СПб.: БХВ-Петербург, 2002. - 512 с.

36. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципи, технологии, протоколы: Учебник для вузов. 3-е изд. - СПб.: Питер, 2006. - 958 с.

37. Орлов С.А. Технологии разработки программного обеспечения. - СПб.: Питер, 2002. - 464 с.

38. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Компания АйТи, 2006. - 400 с.

39. Петренко С.А., Симонов С.А. Управление информационными рисками. Экономически оправданная безопасность. - М.: Компания АйТи, 2004. - 384 с.

40. Программирование алгоритмов защиты информации / А.В. Домашев, В.О. Попов, Д.И. Правиков и др. - М.: Нолидж, 2000. - 288 с.

41. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах: Учеб. пособие для вузов. - М.: Радио и связь, 2000. - 168 с.

42. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты // Защита информации. Конфидент. - 2001. - № 2. - С. 48- 53.

43. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение - М.: СОЛОН-Пресс, 2004. - 192 с.

44. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. - М.: Радио и связь, 2000. - 192 с.

45. Хоффман Л. Современные методы защиты информации: Пер. с анг. / Под ред. В.А. Герасименко. - М.: Сов. радио, 1980, 264 с.

46. Щеглов В.Ю. Защита компьютерной информации от несанкционированного доступа. - СПб.: Наука и техника, 2004. - 384 с.

47. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. - М.: Нолидж, 2001. - 352 с.

48. British Standard. Information security management systems - Specification with guidance for use. British Standard Institution, BS 7799- 2, 2002.

49. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2.1. - CCIMB- 99- 031, August 1999.

50. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. Version 2.1. - CCIMB- 99- 032, August 1999.

51. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. Version 2.1. - CCIMB- 99- 033, August 1999.

52. Common Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology. Version 1.0. - CEM- 99/045, August 1999.

53. DoD 5200.28-STD, Department technology Security techniques Evaluation Criteria. December 1985. NY: U.S. Government printing office, 1999. 122 pp.

54. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.

55. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.

56. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assuracce requirements, 1999. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.

57. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.

58. Neumann P.G. Practical Architectures for survivable Systems and Networks. Technical Report. - SRI International: Computer Science Laboratory, 2001. - 209 pp. - http://www.csl.sri.com/neumann/survivability.dvi.

59. RFC 1244. Site Security Handbook.

60. Tanenbaum A.S. Computer Networks. - NY.: Prentice Hall, 1996.

61. Toward a secure system engineering methodology / C. Salter, O. Saydjari, B. Schneier, J. Wallner.