МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
Доктор економічних наук, доцент	Доктор економічних наук, доцент
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА
на тему:

АНАЛІЗ МЕТОДІВ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Бриль Олексій Васильович _____ (підпис)

КЕРІВНИК: к.т.н. Рабчун Дмитро Ігорович _____ (підпис)

НОРМКОНТРОЛЕР: _____ _____ (підпис)

Київ-2021

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації
Кафедра Управління Інформаційною та Кібернетичною Безпекою

Освітньо-кваліфікаційний рівень – магістр
Галузь знань – «12 Інформаційні технології»
Спеціальність – «125 Кібербезпека»
Спеціалізація – «Управляння інформаційною безпекою»

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
д.е.н., доцент _____ С.В.Легомінова
(підпис)
“___” _____ 20__ року

ЗАВДАННЯ

на магістерську атестаційну роботу студенту

студенту **Брилю Олексію Васильовичу**

1. **Тема роботи – «Аналіз методів та організація захисту інформації від внутрішніх загроз на підприємстві»,** затверджена наказом по університету від «13» жовтня 2020 р. №230
2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020 р.
3. **Вихідні дані до роботи:**

- дослідити вимоги міжнародних та вітчизняних стандартів в галузі ризик-менеджменту;
- проаналізувати методологічні засади оцінки ризиків інформаційної безпеки на підприємстві;
- провести дослідження процесів управління і методик ризиків інформаційної безпеки на підприємстві;
- розробити рекомендації щодо вдосконалення процесів управління і методик оцінки ризиків в організації (для обраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки)

1. Аналіз основ управління ризиками на методологічному рівні;
2. Аналіз процесу управління ризиками у сфері захисту інформації і їх оцінки на підприємстві;
3. Дослідження процесів управління і методик оцінки ризиків на підприємстві.

5. **Перелік демонстраційного матеріалу**:

1. Схема класифікації антропогенних джерел загроз інформації по відношенню до об’єкта захисту;
2. Таблиця характеристик алгоритмів криптозахисту;
3. Схема моделі представлення системи захисту інформації;
4. Схема структури матриці СЗІ;
5. Схема властивостей матриці СЗІ;
6. Презентація доповіді, виконана в Microsoft PowerPoint/

6. **Дата видачі завдання**: 26.10.2020

Календарний графік

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури	29.10.2020р.	
2.	Аналіз та систематизація матеріалу. Вступ.	05.11.2020 р.	
3.	Аналіз основ управління ризиками на методологічному рівні.	13.11.2020 р	
4.	Аналіз процесу управління ризиками у сфері захисту інформації та їх оцінки на підприємстві.	01.12.2020 р.	
5.	Дослідження процесів управління і методик оцінки ризиків на підприємстві.	15.12.2020 р.	
6.	Оформлення та друк пояснювальної записки	25.12.2020 р.	
7.	Отримання відгука та рецензії на роботу	.2020 р.	
8.	Оформлення презентації	.2020 р.	
9.	Попередній захист на кафедрі	.2020 р.	
10.	Захист в ДЕК	20.01.2021 р.	

Керівник _____ Рабчун Дмитро Ігорович

(підпис) (прізвище, ім’я, ініціали)

Завдання приймав

для виконання _____ Бриль Олексій Васильович

(підпис) (прізвище, ім’я, ініціали)

РЕФЕРАТ

Магістерська атестаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел і має 95 сторінок основного тексту, 4 рисунків, 3 таблиць. Загальний обсяг роботи 107 сторінки.

Об'єктом дослідження є управління і оцінка ризиків внутрішніх загроз на підприємстві.

Предметом роботи є дослідження процесу управління і методик оцінки внутрішніх інформаційних ризиків на підприємстві.

Метою роботи є аналіз методів та засобів захисту інформації на підприємстві від внутрішніх загроз та напрямків їх вдосконалення .

У роботі вирішене завдання розробки рекомендацій щодо вдосконалення організації захисту інформації на підприємстві від внутрішніх загроз.

У роботі розроблено методичні рекомендації щодо використання сучасних методів та засобів захисту інформації для вдосконалення захисту інформації на підприємстві від внутрішніх загроз.

Сфера застосування. Запропоновані підходи можуть бути використані при розробці, впровадженні, експлуатації чи модифікації комплексної системи захисту інформації в організаціях різної форми власності.

Можливі напрямки розвитку цієї роботи пов'язані з використанням інших методів та засобів захисту інформації для удосконалення інформаційної безпеки підприємства.

КЛЮЧОВІ СЛОВА: політика інформаційної безпеки, система захисту інформації, загрози інформаційній безпеці, модель порушника, рівень загрози, інформаційна система.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АС – автоматизована система

БД – база даних

ВЧ – висока частота

ЕОМ – електронно-обчислювальна машина

ЗІ – захист інформації

ІБ – інформаційна безпека

ІС – інформаційна система

ІТ – інформаційні технології

КЗЗІ – комплекс засобів захисту

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації

МКНСД – можливі канали несанкціонованого доступу

НСД – несанкціонований доступ

ОС – операційна система

ОТ – обчислювальна техніка

ПБ – політика безпеки

ПЕМВН – побічні електромагнітні випромінювання та наведення

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

СЗІ – система захисту інформації

ТЗЗІ – технічні засоби захисту інформації

ВСТУП

Одне з основних завдань сучасної ділової діяльності полягає в тому, щоб забезпечити безпеку своїх інформаційних активів. Комерційні й технологічні секрети, конфіденційні документи, персональні дані персоналу й клієнтів організації - всю цю класифіковану інформацію необхідно захистити від самих різних загроз.

Найнебезпечнішою загрозою щодо цього є витік конфіденційної інформації. За останні роки актуальність цієї загрози зросла настільки, що сьогодні крадіжка класифікованих відомостей стабільно посідає перші місця у всіх рейтингах загроз IT-безпеки.

Вітчизняні підприємства стурбовані проблемою захисту своїх інформаційних активів. Конфіденційна інформація може покинути внутрішню корпоративну мережу декількома шляхами. У розпорядженні інсайдерів перебувають, як поштові ресурси компанії, так і вихід в Інтернет (веб-пошта, чати, форуми й т.д.). Однак найнебезпечнішим каналом витоку є також комунікаційні можливості робочих станцій, до яких варто віднести цілий ряд портів (USB, LPT, COM, IrDA), різні типи приводів (CD/ DVD-RW, Floppy), бездротові мережі (Bluetooth, Wi-Fi) і т.ін.

Бізнес стурбований проблемою витоку класифікованих даних саме через мобільні накопичувачі. Широко відомий інцидент із японською телекомунікаційною компанією KDDI. інсайдери спокійно скопіювали на CD і USB-флешки персональні дані 4 млн. клієнтів корпорації, а потім зажадали від свого роботодавця викуп у розмірі 90 тис. доларів. У противному випадку інсайдери обіцяли оголосити факт витоку напередодні зборів акціонерів. Крім того, у ході військової кампанії в Афганістані військові сили США допустили витік персональних відомостей солдат, офіцерів і генералів армії США, а також ряду документів під грифом «секретно». Вся ця інформація витекла за допомогою USB-флеш накопичувачів, на які обслуговуючий персонал записав класифіковані відомості.

Однак, слід зазначити, що конфіденційні дані часто витікають не внаслідок навмисних дій нечистих на руку службовців. Дійсно, деякі співробітники воліють брати роботу додому або переписують класифіковані документи на портативний накопичувач, щоб вивчити їх на своєму ноутбуці у відрядженні. Нарешті, службовці можуть просто помилитися й переплутати закриті дані з публічними файлами. Саме такий витік відбувся в американському штаті Огайо, де службовці виборчкому просто переплутали файли й розіслали по політичних об'єднаннях компакт-диски з персональними даними 7 млн. громадян. Інакше кажучи, службовцями можуть рухати й благі спонукання, які на практиці просто приведуть до компрометації конфіденційної інформації організації.

Аналіз методів та засобів захисту інформації дозволяє обрати найбільш оптимальні, для створення, чи модифікації комплексної системи захисту інформації від внутрішніх загроз.

Більшість загроз для інформації підприємства складають внутрішні загрози. Але основною загрозою для інформації – є власний персонал підприємства. Тому організація та вдосконалення захисту інформації на підприємстві від внутрішніх загроз, є, безумовно, актуальною науковою задачею.

Розділ 1
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

1.1 Класифікація загроз та їх характеристики

Загрози оброблюваної інформації в інформаційній системі залежать від характеристик інформаційної системи, фізичного середовища, персоналу і оброблюваної інформації з обмеженим доступом.

Під загрозою розуміють можливу небезпеку, яка порушує базові властивості інформації та інформаційних мереж. Базовими властивостями інформації є: конфіденційність, цілісність та доступність. Будь-які несанкціоновані дії та доступ до захищених мереж, стають причиною порушення політики безпеки інформації і (або) нанесення збитків системі.
Також це дії, спрямовані проти об'єкта захисту чи інформаційної мережі, що проявляється в небезпеці спотворень і втрат інформації.

Уся безліч потенційних загроз по природі їх виникнення розділяються на природні, техногенні та антропогенні.

Природні загрози - це загрози, викликані впливами на інформаційну систему та її елементи, об'єктивних фізичних процесів чи стихійних природних явищ, що не залежать від людини.

Техногенні загрози - це загрози інформаційній системі, викликані діяльністю технічних та програмних засобів і систем.

Антропогенні загрози - це загрози, обумовлені діями суб'єкта.

Техногенні та антропогенні загрози, виходячи з мотивації дій, можливо поділити на передбачені та непередбачені.
Основні передбачувані загрози:

фізичне руйнування системи (шляхом вибуху, підпалу тощо) або вивід з ладу усіх чи окремих найбільш важливих компонентів інформаційної системи (пристроїв, носіїв системної інформації, осіб із числа персоналу тощо);

відключення або вивід із ладу підсистем забезпечення функціонування інформаційної системи (електроживлення, вентиляції, ліній зв'язку тощо);

дії по дезорганізації функціонування системи (зміна режимів робіт пристроїв чи програм, постановка активних радіоперешкод на частоті роботи пристроїв системи тощо);

впровадження агентів у число працівників системи;

вербування (шляхом підкупу, шантажу тощо) працівників або окремих користувачів, що мають визначені повноваження;

застосування підслуховуючих пристроїв, дистанційна фото і відео зйомка тощо;

перехоплення побічних електромагнітних, акустичних та інших випромінювань, а також наводок активних випромінювань на допоміжні технічні засоби, що безпосередньо беруть участь в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

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

розкрадання носіїв інформації (машинних носіїв інформації, мікросхем пам'яті тощо);

несанкціоноване копіювання носіїв інформації;

розкрадання виробничих відходів (роздруківок, записів, списаних матеріальних носіїв інформації тощо);

читання залишеної інформації з оперативної пам'яті та із 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 операційних систем та систем програмування;

незаконне одержання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом

підбору тощо) з наступним маскуванням під зареєстрованого користувача ("маскарад");

несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичний адрес, адресу в системі зв'язку, апаратний блок кодування тощо;

розкриття шифрів криптозахисту інформації;

існує цілий ряд шкідливих заходів, які дозволяють використовувати вразливість програм відносно їх несанкціонованої модифікації;

впровадження апаратних спеціальних внесків, програмних "закладок" та "вірусів";

руйнування файлової структури (зникнення файлів, викривлення каталогів);

незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему та успішної автентифікації із наступним уведенням дезінформації та нав'язування помилкових повідомлень.

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

Основні непередбачені техногенні загрози інформаційній системи (дії, скоєні особою випадково, через незнання, неуважність або недбалість, із цікавості, але без злого наміру):

ненавмисні дії, що приводять до часткового або повного відмовлення системи чи руйнуванню апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування устаткування, видалення, перекручування файлів з важливою інформацією або програм, у тому числі системних тощо);

неправомірне включення устаткування або зміна режимів роботи пристроїв і програм;

ненавмисне псування матеріальних носіїв інформації;

запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання чи зациклення) або здійснюючих необразні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних);

нелегальне впровадження та використання неврахованих програм (ігрових, навчальних тощо, що не є необхідним для виконання своїх посадових і службових обов'язків) з наступною необґрунтованою витратою ресурсів (завантаження процесора, захоплення оперативної пам'яті та пам'яті на зовнішніх носіях);

зараження інформаційної системи вірусами;

необережні дії, що приводять до розголошення інформації з обмеженим доступом, або роблячи її відкритою;

розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, перепусток, ідентифікаційних карток тощо);

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

ігнорування організаційних обмежень (установлених правил);

вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи із змінних магнітних носіїв тощо);

некомпетентне використання, настроювання або неправомірне підключення засобів захисту персоналом;

знищення помилкових даних;

ненавмисне ушкодження каналів зв'язку.

Загрозою є будь-яка обставина або подія, котра потенційно може причинити шкоду системі чи процесу шляхом знищення, розголошення, зміни даних або відмову в обслуговуванні. Із всієї множини способів класифікації загроз, найпридатнішою для аналізу є класифікація загроз, за результатами їх впливу на інформацію та систему її обробки. В цій класифікації загрози

поділяються на чотири класи (конфіденційності, цілісності, доступності і втрати спостережності):

загрози порушення конфіденційності інформації (ознайомлення із інформацією неавторизованими користувачами або процесами);

загрози порушення цілісності інформації (несанкціонована модифікація інформації неавторизованим користувачем);

загроза порушення доступності інформаційних ресурсів (порушення доступу до інформаційних ресурсів для користувачів, що володіють відповідними повноваженнями);

загрози порушення спостережності (обмеження можливостей інформаційної системи контролювати користувачів, процеси і пасивні об'єкти з метою забезпечення установленої політики безпеки).

Також загрози безпеці інформації на підприємстві, за походженням, можна поділити на дві групи:

зовнішні;

внутрішні.

У свою чергу, як перші, так і другі за направленістю і характером впливу на підприємства можуть бути економічними, фізичними та інтелектуальними.

Економічні загрози можуть реалізовуватись у формі корупції, шахрайства, недобросовісної конкуренції, використання підприємствами неефективних технологій виробництва. Реалізація таких загроз завдає збитків підприємствам або веде до втрати ними вигоди.

Основними причинами виникнення економічних загроз можуть бути: недостатня адаптація підприємства до постійно змінних умов ринку; загальна неплатоспроможність суб'єктів господарювання; зростаюча злочинність; споживчий менталітет значної кількості громадян; низький рівень трудової дисципліни та відповідальності працівників підприємства; недостатнє правове регулювання підприємницької діяльності; низький професійний рівень частини керівного складу і працівників на підприємстві.

Фізичні загрози реалізуються у формі крадіжок, пограбувань майна та коштів підприємств, поломок, виведення із ладу обладнання підприємств, неефективної його експлуатації. У результаті реалізації таких загроз завдаються прямі збитки підприємствам, пов'язані з втратою своєї власності та необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів. Основними причинами фізичних загроз є неефективна кадрова політика підприємства, низька професійна підготовка працівників, недостатній рівень охорони підприємства, низький контроль стану роботи працівників на підприємстві.

Інтелектуальні загрози проявляються як розголошення або неправомірне використання конфіденційної інформації підприємства, дискредитація підприємства на ринку послуг, а також можуть бути реалізованими у формі різного роду соціальних конфліктів навколо підприємств або в них самих. Результатом реалізації таких загроз можуть бути збитки підприємств, погіршення їх іміджу, соціальна чи психологічна напруженість навколо підприємств або в їх колективах. Причинами таких загроз, як правило, є загострення конкуренції на регіональних ринках послуг, неефективна кадрова політика, порушення принципу гласності результатів підприємницької діяльності, відсутність або низька ефективність заходів інформаційного режиму на підприємстві.

Розглянемо внутрішні загрози безпеці інформації на підприємстві.

У найзагальнішому випадку внутрішні загрози проявляються такими шляхами:

внаслідок дій зловмисників; спостереження за джерелами інформації;

підслухування конфіденційних розмов людей і сигналів акустичних працюючих механізмів;

несанкціоноване розповсюдження матеріально-речовинних носіїв за межі контрольованої зони;

розголошення інформації людьми, що володіють інформацією секретною або конфіденційною;

втрата носіїв з інформацією (документів, носіїв машинних, зразків матеріалів і т. ін.);

несанкціоноване розповсюдження інформації через поля і електричні сигнали, що випадково виникають в електричних і радіоелектронних приладах в результаті їхнього старіння, неякісного конструювання (виготовлення) та порушень правил експлуатації;

вплив стихійних сил, насамперед, вогню під час пожежі і води в ході гасіння пожежі та витоку води в аварійних трубах водопостачання;

збої в роботі програмних засобів та апаратури збирання, оброблення, зберігання і передавання інформації, викликаних її несправністю, а також ненавмисних помилок користувачів або обслуговуючого персоналу.

1.2 Джерела загроз

Всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

загрози, обумовлені діями суб'єкта (антропогенні загрози);

загрози, обумовлені технічними засобами (техногенні загрози);

загрози, обумовлені стихійними джерелами.

Антропогенні джерела загроз - найбільш широка група і представляє собою найбільший інтерес з точки зору організації протидії цим загрозам, тому що дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватних заходів. Методи протидії цим загрозам керовані і безпосередньо залежать від дій організаторів захисту інформації.

Суб'єкти, дії яких можуть призвести до порушення безпеки інформації в корпоративних мережах можуть бути як зовнішні, так і внутрішні.

Рис. 1.1. Класифікація антропогенних джерел загроз інформації по відношенню до об’єкта захисту

Внутрішні джерела, як правило, являють собою висококваліфікованих фахівців в галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою вирішуваних завдань, структури та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

основний персонал (користувачі, програмісти, розробники);

представники служби захисту інформації (СЗІ);

допоміжний персонал (прибиральники, охорона);

технічний персонал (життєзабезпечення, експлуатація).

Дії зловмисників можуть призвести до ряду небажаних результатів, серед яких стосовно до корпоративних мереж,можна виділити наступні: крадіжка; підміна; руйнування; переривання; помилки; перехоплення інформації.

Техногенні джерела загроз, що визначаються технократичною діяльністю людини та розвитком цивілізації. Однак, наслідки, викликані такою діяльністю вийшли з під контролю людини і існують самі по собі. Ці джерела загроз менш прогнозовані, прямо залежать від властивостей техніки і тому вимагають

особливої уваги. Даний клас джерел загроз безпеки інформації особливо актуальний в сучасних умовах. Внутрішні технічні та програмні засоби, що містять потенційні загрози безпеці інформації:

неякісні технічні засоби обробки інформації;

неякісні програмні засоби обробки інформації;

допоміжні засоби (охорони, сигналізації, телефонії);

інші технічні засоби, що застосовуються в установі;

Стихійні джерела загроз**.** Ця група джерел загроз об'єднує, обставини, що становлять непереборну силу, такі обставини, які мають об'єктивний і абсолютний характер, що поширюється на всіх. До непереборної сили в законодавстві і договірній практиці відносяться стихійні лиха або інші обставини, які неможливо передбачити чи неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню та тому заходи захисту від них повинні застосовуватися завжди. До них відносяться: пожежі; землетруси; повені; урагани; різні непередбачені обставини; інші форсмажорні обставини.

Внутрішніми джерелами загроз безпеці інформації на підприємстві є:

1. Персонал;
2. Технічні засоби;
3. Програмні засоби;
4. Канали зв’язку;
5. Пожежі та наслідки їх ліквідації.

Захоплюючись технічними можливостями витоку та захисту від витоку інформації багато керівників забувають, що загроза витоку інформації може бути пов’язана з їхнім власним персоналом.

Виходячи із даних антирейдерського союзу підприємців України:

1) 82% загроз реалізується власними співробітниками фірми або при їх прямій чи опосередкованій участі;

2) 17% загроз реалізується ззовні підприємства;

3) 1% загроз реалізується випадково.

Найпоширеніші фактори розголошення співробітниками інформації з обмеженим доступом:

1. Надмірна балакучість співробітників (32%);

2. Прагнення співробітників заробляти гроші будь-якими способами та за будь-яку ціну (24%);

3. Відсутність на фірмі служби безпеки(14%);

4. Звичка співробітників фірми ділитися один з одним (традиційний обмін досвідом) (12%);

5. Безконтрольне використання інформаційних систем (10%);

6. Наявність можливостей виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів, відсутність роботи по згуртованості колективу і т.д.(8%);

Як видно, розголошення співробітниками інформації з обмеженим доступом найчастіше здійснюється через те, що керівництво компаній не приділяє уваги загрозам витоку інформації, пов’язаним з персоналом.

Для кращого розуміння можливостей витоку інформації та визначення способів його попередження пропонується розглянути декілька класифікацій самих порушників та класифікацію загроз, пов’язаних з персоналом.

Існує декілька різних класифікацій внутрішніх порушників, яких теоретики звикли називати інсайдерами. Інсайдерами є ті співробітники, що працюючи на підприємстві являються порушниками правил цього підприємства.

Однією з перших кроків в напрямку класифікації зробила міжнародна науково-дослідна компанія IDC, що представила свій погляд на проблему в 2006 році. За версією IDC, система інсайдерів має чотири рівні: «громадяни», «порушники», «відступники», «зрадники».

Верхній рівень складають «громадяни» — лояльні службовці, які дуже рідко (якщо взагалі коли-небудь) порушують корпоративну політику і в основному не є загрозою безпеці.

На другому рівні знаходяться «порушники», що складають велику частину усіх співробітників підприємства. Ці співробітники дозволяють собі невеликі фамільярності, працюють з персональною веб-поштою, грають в комп'ютерні ігри і здійснюють онлайн-покупки. Представники даного рівня порушників створюють загрозу інформаційній безпеці, але ці інциденти є випадковими і ненавмисними.

На наступному рівні знаходяться «відступники» — працівники, які велику частину робочого часу роблять те, що вони робити не повинні. Ці службовці зловживають своїми привілеями по доступу до Інтернету. Більш того, такі співробітники можуть посилати конфіденційну інформацію компанії зовнішнім адресатам, зацікавленим в ній. Таким чином, «відступники» представляють серйозну загрозу безпеці.

На самому нижньому рівні знаходяться «зрадники». Це службовці, які умисно і регулярно піддають конфіденційну інформацію компанії небезпеці (зазвичай за фінансову винагороду від зацікавленої сторони). Такі співробітники представляють реальну загрозу, але їх найскладніше упіймати.

Більш широка класифікація представлена російською компанією Info Watch. Фахівці компанії фокусують увагу винятково на захисті даних від витоку, спотворення і знищення, і тому їх погляди відрізняються більшою глибиною аналізу.

Недбалі порушники (також відомі як «необережні») є найбільш поширеним типом внутрішніх порушників. Їх порушення у відношенні конфіденційної інформації носять немотивований характер, не мають конкретних цілей, наміру, користі.

Порушники, якими маніпулюють – це ті співробітники, яких обманним шляхом штовхають на порушення встановлених норм. Такі співробітники часто і не підозрюють про те, що їхні дії призводять до втрати конфіденційних даних.

Скривджені порушники (по-іншому, саботажники) — це співробітники, які прагнуть завдати шкоди компанії за особистими причинами. Найчастіше причиною такої поведінки може бути образа, що виникла через недостатню

оцінку їх ролі в компанії, недостатній розмір матеріальної компенсації, неналежне місце в корпоративній ієрархії, відсутність елементів моральної мотивації або відмова у виділенні корпоративних статусних атрибутів (ноутбука, автомобіля, секретаря).

Наступний тип внутрішніх порушників — нелояльні порушники. Перш за все, це співробітники, що вирішили змінити місце роботи, або акціонери, що вирішили відкрити власний бізнес.

Співробітники, що підробляють і впроваджені внутрішні порушники — це співробітники, мету яких визначає замовник викрадання інформації. У обох випадках інсайдери прагнуть якомога надійніше замаскувати свої дії (принаймні, до моменту успішного розкрадання).

Останньою класифікацією наведена класифікація, що відображає зовнішні і внутрішні загрози підприємства, які пов'язані з персоналом.

Зовнішньою загрозою є така загроза, що знаходиться за межами підприємства, але саме через існування якої потрібно захищати інформацію і через яку існують загрози внутрішні. Адже, як би не було зацікавлених осіб в отриманні інформації підприємства, її не потрібно було б захищати. До зовнішніх загроз можна віднести протиправну діяльність кримінальних структур, конкурентів, фірм або приватних осіб, що займаються промисловим шпигунством та соціальною інженерією.

До внутрішніх загроз відносяться дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними та потенційними партнерами (аж до втрати цінних контрактів) тощо.

Оскільки для реалізації зовнішніх загроз використовується власний персонал підприємства, недоліки програмного та апаратного забезпечення, то варто розглядати внутрішні та зовнішні загрози, як тісно пов'язані між собою.

Отже розглянемо ці загрози більш детально:

1) Зовнішні:

а) Промислове шпигунство. Вперше термін «промислове шпигунство» було сформульовано на початку 60-х років минулого століття під час семінару з методів збирання інформації для менеджерів вищої ланки, що проводився американською консалтинговою компанією Management Investigation Services. Західні теоретики розуміють під «промисловим шпигунством» добування законним і незаконним шляхом у конкуруючих фірм (монополій, політичних партій, фізичних та юридичних осіб, правоохоронних органів тощо) відомостей або інформації у сфері наукових досліджень, виробництва продукції за найбільш перспективними технологіями тощо, а також персональних даних з метою їх використання у конкурентній боротьбі або у корисливих цілях.

Метою промислового шпигунства частіш всього буває: або перевірка ділового партнера на благонадійність, або ж знищення конкурента чи нанесення йому серйозних збитків. І, якщо в першому варіанті немає загроз підприємству, то в другому, якщо конфіденційна інформація потрапить до рук таких агентів, це може призвести до дуже серйозних наслідків для підприємства, закінчуючи його банкрутством та ліквідацією.

І хоча існує багато технічних засобів для здобуття інформації, промисловим шпигунам інколи просто достатньо поговорити з працівниками які, самі того не підозрюючи, можуть надати досить суттєву інформацію, якою конкуренти не втратять нагоди скористуватися. За оцінками фахівців, на частку людського фактору, тобто на балакучість співробітників, припадає до 60% всього витоку інформації. Інші 40% - це те, що вдається перехопити технічними засобами. Але й використовуючи технічні засоби, промислові шпигуни дуже часто «звертаються» за допомогою до співробітників компанії, про яку хочуть роздобути інформацію. Навіть співробітникам найнижчої ланки під силу встановити відповідну апаратуру для зняття інформації.

Тож промислове шпигунство є тією загрозою, від якої потрібно захищатися. Як би інформація підприємства нікого не цікавила, не було б сенсу

її оберігати. Але, промислові шпигуни не досягали б поставленої мети, якби не загрози внутрішні: необережні чи навмисні дії співробітників.

б) Соціальна інженерія – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним. Зловмисник отримує інформацію, наприклад, шляхом збору персональних даних про службовців об'єкту атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Зловмисник може подзвонити працівникові компанії (під виглядом технічної служби) і вивідати пароль, пославшись на необхідність вирішення невеликої проблеми в комп'ютерній системі. Дуже часто це спрацьовує. Найсильніша зброя в цьому випадку — приємний голос і акторські здібності.

Методи соціальної інженерії:

Претекстінг – це дія, відпрацьована за наперед складеним сценарієм (претексту). В результаті людина повинна видати певну інформацію, або зробити певну дію. Цей вид атак застосовується зазвичай по телефону. Частіше ця техніка включає більше, ніж просто брехню, і вимагає яких-небудь попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку і ін.), з тим, щоб забезпечити довіру людини.

Фішинг – техніка, направлена на шахрайське отримання конфіденційної інформації. Зазвичай зловмисник посилає цілі e-mail, підроблені під офіційний лист, від банку або платіжної системи, що вимагає "перевірки" певної інформації, або здійснення певних дій.

Троянський кінь – ця техніка експлуатує цікавість, або жадібність людини. Зловмисник відправляє e-mail, що містить досить цікаву для людини інформацію, наприклад свіжий компромат на співробітника. Така техніка залишається ефективною, поки користувачі сліпо кликатимуть по будь-яких вкладеннях.

Дорожнє яблуко – цей метод атаки є адаптацією троянського коня, і полягає у використанні фізичних носіїв. Зловмисник може підкинути інфікований CD, або флеш, в місці, де носій може бути легко знайдений. Носій підроблюється під офіційного, і супроводжується підписом, покликаним викликати цікавість.

Кві про кво – зловмисник може подзвонити по випадковому номеру в компанію, і представитися співробітником техпідтримки, що опитує, чи є які-небудь технічні проблеми. У випадку, якщо вони є, в процесі їх "вирішення" людина вводить команди, які дозволяють зловмисникові запустити шкідливе програмне забезпечення.

2) Внутрішні:

а) Необережність персоналу. Дуже часто співробітники, хоч й не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього.

Тож необережність можна поділити на дві категорії:

дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації;

дії чи бездіяльність співробітників, у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки.

У першому випадку не можна казати про вину співробітника, скоріше це прорахунки вищого керівництва, яке не потурбувалося роз’яснити персоналу про важливість інформації і про її захист. Якщо мова йде про державну таємницю, то такі ситуації не можуть виникнути, бо є чітко визначений законодавством порядок допуску до державної таємниці. Одним з пунктів є підписання зобов’язання про нерозголошення довірених даних. Багато комерційних фірм використовують законодавство про державну таємницю як приклад для аналогічного захисту своєї, комерційної таємниці. Але цього прикладу додержуються не всі компанії. Інколи керівники, як метод захисту інформації, практикують не казати працівникам про важливість даних. Як приклад можна привести ситуацію: прибиральниця, яка прийшла прибрати

кабінет керівника фірми, побачила в нього на столі дуже красиву модель якогось пристрою. Вина керівника полягає вже в тому, що він дозволив прибирати в кабінеті тоді, коли працює там сам, коли документи не сховані в сейфі та працює комп'ютер, де також можуть бути відкриті секретні файли. Але він також не попередив прибиральницю про те, що не потрібно розповідати про будь що, що вона бачила. Прибиральниця, якій сподобалася модель з чисто мистецьких поглядів, може поділитися своїми враженнями з людиною, яка зацікавиться цією інформацією. Тож керівникам потрібно попереджати всіх співробітників, які хоч якось взаємодіють з конфіденційною інформацією і можуть ознайомитися з нею в розмірі, достатньому для відтворення хоча б частини такої інформації.

В іншому випадку співробітника повідомили про те, що він не повинен розголошувати конфіденційні відомості підприємства, але він вважаючи, що його дії не призведуть ні до яких наслідків, призводить до втрати інформації чи ознайомлення з нею третіх осіб. У кримінальному кодексі необережність поділяють саме на злочинну самовпевненість та злочинну недбалість.

Під злочинною самовпевненістю розуміють дії чи бездіяльність особи, коли вона знала про можливі негативні наслідки, передбачала їх настання, але зухвало розраховувала на їх відвернення.

Злочинною недбалістю є дії чи бездіяльність особи, коли вона не знала, але повинна була знати про можливі негативні наслідки свого діяння.

В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії.

б) Умисні дії працівників по розголошенню інформації та мотиви цих дій.

На відміну від необережності, умисел передбачає, що метою дій співробітників було саме розголошення інформації, що є конфіденційною. Причому співробітників могли завербувати агенти промислового шпигунства або ж вони самі ініціативно вирішили зрадити організацію, на яку працювали (в цих випадках вони вже самі можуть шукати контактів з представниками конкуруючих фірм чи інших осіб, зацікавлених в отриманні певної інформації).

Для того щоб виявити або попередити такі дії, потрібно визначитися, чому ж саме працівники пішли на них. Кожна людина є індивідуальною, в кожного своє життя та свої проблеми, через які він приймає ті чи інші рішення. Тож кожна ситуація має свої нюанси, але є декілька розповсюджених причин для розголошення інформації співробітниками. До них відносяться:

помста;

матеріальна або інша вигода;

самореалізація.

Саме з цих причин персонал фірми найчастіше зраджує її інтереси. Багато в чому тут також є прорахунки керівництва. Саме це найчастіше є тим, через що вербують співробітників. Невдоволені працівники краще йдуть на контакт з промисловими шпигунами, бо не відчувають патріотизму до цієї фірми, мріють поквитатися з кимось із колег чи з керівництвом, або прагнуть покращити своє матеріальне становище. Таким особам пропонують те, чого в них немає і не буде на даній фірмі: або значні матеріальні виплати, або ж пропонування роботи, де їх працю оцінять, де їх будуть поважати, або ж інші речі, що відповідають потребам цих співробітників.

Інсайдерські інциденти відбуваються набагато частіше, ніж зовнішні атаки. Компанії прагнуть не афішувати свої внутрішні проблеми, але авторитетні дослідження все одно віддають пальму першості інсайдерам. Так, згідно дослідженню 2005 E-Crime Watch Survey, проведеному організацією CERT, в ході якого було опитано більше 800 компаній, кожна друга компанія хоч би раз протягом року постраждала від витоку даних.

Аналітики підрахували, що 33 і 20 % інцидентів викликані нинішніми і колишніми співробітниками відповідно, 11% припадають на частину клієнтів компанії, 8 % відбуваються через партнерів і, нарешті, 7 % викликані тимчасовими службовцями (контрактниками, консультантами і т. д.). Це свідчить про те, що проблема просочування конфіденційної інформації стає на перше місце в списку пріоритетів керівництва компанії.

Щоб краще побачити серйозність загроз, пов’язаних з персоналом, далі наведені декілька прикладів втрати інформації з обмеженим доступом через внутрішніх порушників лише за один рік.

Квітень 2006р. Три інсайдера з Lockheed Martin вкрали результати проекту по розробці тренувальної системи для пілотів ВПС США і план дій компаній в боротьбі за контракт Пентагону вартістю $1 млрд. Всі ці відомості були передані конкурентові, а витік з Lockheed Martin відбувся через USB-флешки і CD/DVD-приводи.

Травень 2006 р. Інсайдер з Міністерства у справах ветеранів США приніс додому ноутбук з персональними даними 26,5 млн. колишніх військових, який був викрадений з будинку в результаті пограбування. Всі ветерани США опинилися під загрозою крадіжки персональних даних особи, оскільки приватні дані не були зашифровані. Потенційні збитки унаслідок витоку оцінюються в $30 млрд.

Червень 2006 р. Інсайдери японського оператора стільникового зв'язку — KDDI — вкрали базу даних клієнтів (записавши на компакт-диски і USB-флешки). Вони шантажували KDDI, загрожуючи розкрити факт витоку перед зборами акціонерів та вимагали $90 тис., але завдяки поліції опинилися за гратами.

Жовтень 2006 р. Керівник місцевого відділення Private Banking в Citibank - перейшов на роботу в банк-конкурент UBS, прихопивши конфіденційні дані всіх найбільш спроможних клієнтів. Через деякий час UBS почав переманювати клієнтів Citibank. Витік відбувся по електронній пошті.

Жовтень 2006 р. Інсайдери з індійського телекому Acme Tele Power вкрали результати інноваційних розробок і передали їх фірмі-конкурентові Lamda Private Limited. За оцінками Ernst & Young, прямі фінансові збитки Acme склали $166 млн. Витік відбувся по електронній пошті.

Тож загроза цілісності інформації йде від людини. Можна встановити найсучасніші системи технічного захисту, видати безліч нормативних актів, які регулюють захист інформації, але поки буде ігноруватися людський фактор

(тобто фактор людського впливу на інформацію, загрози, які йдуть від людей та причини цих загроз), доти юридичні, організаційні та технічні засоби будуть мало ефективними.

Проаналізувавши загрози конфіденційності даних, які пов’язані з персоналом, можна побачити, що ігнорування цих загроз призводить до серйозних збитків на підприємствах. Мова йде не тільки про фінансові втрати компанії, але й про різке падіння її іміджу у зв’язку з тим, що вона не може захистити власну конфіденційну інформацію.

1.3 Модель порушника. Мета та принципи розробки

Якщо на підприємстві існує інформаційна система, у якій циркулює інформація з обмеженим доступом та конфіденційні дані, то знайдеться особа (порушник), метою якої буде ознайомлення з інформацією, її модифікація чи знищення. Для того, щоб розробити комплекс заходів по забезпеченню захищеності інформаційних ресурсів, необхідно побудувати модель можливого порушника. Ця модель може бути побудована з урахування різних критеріїв.
Модель порушника розробляється для того, щоб отримати відповіді на наступні питання:

від кого захищати інформацію?

яка мета порушника?

якими знаннями володіє порушник?

які повноваження в системі має потенційний порушник?

якими методами і засобами користується порушник?

яка обізнаність порушника щодо об’єкта інформаційної діяльності і системи охорони?

Для початку необхідно дати визначення поняттю «модель порушника».

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято

поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники - це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп'ютерної системи. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть працювати в даній системі. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації; порушники пропускного режиму.

При розробці моделі порушника необхідно визначитись, що і у якій мірі має відображати отримана модель. Для цього необхідно визначитись з необхідним ступенем деталізації моделі порушника.

Можна запропонувати наступні ступені деталізації:

змістовна модель порушників - відображає причини й мотивацію дій порушників, переслідувані ними цілі і загальний характер дій у процесі підготовки і здійснення порушення інформаційної безпеки. Побудувавши змістовну модель, адміністратори безпеки можуть визначити мету порушника, його рівень знань, кваліфікацію, розташування та т.п.

сценарії впливу порушників - визначають класифіковані типи порушень з конкретизацією алгоритмів і етапів, а також способи дії на кожному етапі. Розробивши сценарії впливу, адміністратори безпеки отримають можливу послідовність дій зловмисника для нанесення збитків інформаційним ресурсам.

математична модель впливу порушників представляє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що параметрично характеризують результати дій, і функціональних (аналітичних, числових чи алгоритмічних)

залежностей, які описують процеси взаємодії порушників з елементами об’єкту і системи охорони.

Цей вид моделі слід використовувати для кількісних оцінок вразливості об’єкту і ефективності охорони.

Для того, щоб модель порушника найбільш точно і детально характеризувала порушників, алгоритм їх дій і давала кількісні оцінки вразливості об’єкту і ефективності охорони рекомендується розробляти комплексну модель з урахуванням усіх ступенів деталізації.

Під час побудови моделі порушника спочатку необхідно проаналізувати усіх користувачів системи, розподілити їх за категоріями та визначити найбільш критичні. Користувачі таких категорій будуть прийняті як можливі внутрішні порушники системи. Далі необхідно визначитись, які категорії відвідувачів можуть бути зовнішніми порушниками.

Усіх можливих порушників необхідно класифікувати за різними показниками для того, щоб надалі скласти модель порушника. Нижче наведені можливі види класифікацій:

Класифікація порушників інформаційної безпеки за метою порушення. Класифікація за метою порушення проводиться для визначення мотивів порушника. Дії порушника в залежності від мети можуть бути спрямовані як на інформацію,так і на матеріальні носії інформації. Знаючи мету порушника, адміністратори безпеки будуть орієнтуватись, на захист якого ресурсу необхідно приділити більше уваги першочергово.

Класифікація порушників інформаційної безпеки за рівнем знань про автоматизовані системи. Кожен порушник має певний рівень кваліфікації та поінформованості відносно організації функціонування зовнішніх та внутрішніх мереж інформаційного комп’ютерного комплексу. В залежності від рівня знань, якими володіє порушник, може бути нанесений певний рівень збитків інформаційним ресурсам організації. В класифікації враховуються знання можливого порушника та його практичні навички у роботі з комп’ютерними системами та інформаційними технологіями.

Класифікація порушника за місцем дії. Ця класифікація проводиться для визначення розташування порушника відносно організації під час здійснення спроби несанкціонованого доступу до інформаційного ресурсу.

Класифікація порушників за методами і способами, якими вони користуються. Порушник може отримати конфіденційну інформацію та інформацію з обмеженим доступом, користуючись при цьому різними методами та засобами. Порушення може бути скоєне або з використанням певних засобів для отримання інформації, або без них. Методи можуть бути різними, як дозволеними, так і забороненими. Дозволеним вважається отримання інформації без порушення прав власності. Як приклад можна привести використання методів соціальної інженерії.

Класифікація порушників за рівнем можливостей, які надані їм засобами автоматизованої системи та обчислювальної техніки. Внутрішніх порушників можна класифікувати за наданим рівнем повноважень у системі. Адже чим більше повноважень, там більше можливостей доступу до інформації з обмеженим доступом.

Класифікація порушників за мотивом порушень. Зловмисники можуть порушувати інформаційну безпеку з різних причин. Порушення можна розбити на дві групи - навмисні та ненавмисні. Особи, які ненавмисно наносять збитків інформаційним ресурсам, порушуючи конфіденційність, цілісність або доступність інформації, не складають плану дій, не мають мети та спеціальних методів та засобів реалізації запланованого порушення. Ненавмисні порушення частіше всього здійснюються в результаті недостатньої кваліфікації, неуважності персоналу. Порушники, які наносять збитків інформаційним ресурсам навмисно, мають певну мету, готують план реалізації атаки на інформаційний ресурс. Навмисні порушення інформаційної безпеки здійснюються для нанесення збитків організації (матеріальних чи моральних), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів.

Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки на підприємствах, організаціях, які займаються обробкою інформації з обмеженим доступом. Одним з етапів побудови комплексної системи захисту інформації є розробка моделі порушника. Чим точніше буде визначено образ, алгоритм дій ймовірного порушника, тим простіше буде адміністраторам безпеки розробити комплекс заходів для того, щоб запобігти успішним атакам.

Важливу роль в розробці моделі порушника відіграє вибір класифікацій порушників. Отже, для найбільш точного визначення можливих порушників, збитки від яких будуть максимальними, необхідно класифікувати всі типи суб'єктів, які мають потенційну можливість взаємодії з інформаційними ресурсами за всіма можливими для системи показниками, що суттєво спростить процедуру організації ефективної системи інформаційної безпеки.

1.4 Оцінка рівня загрози

Після того як складений перелік загроз, необхідно оцінити ймовірність (можливість) реалізації загроз інформаційній безпеці.

Існує два основних підходи для оцінки ймовірності реалізації загрози:

Експертний (ймовірність реалізації загрози оцінює експерт в області інформаційної безпеки);

Підхід з використанням різних математичних методів, в основі яких лежать статистичні дані про загрози, які відбулися в минулому.

Перший підхід використовується в тому випадку, коли немає статистичних даних про загрози які були в минулому, наприклад бази даних інцидентів інформаційної безпеки. Підприємство запрошує експерта або силами своїх штатних працівників з інформаційної безпеки проводить роботи з оцінки ймовірності реалізації загроз. Якщо експерт зовнішній, по відношенню до

підприємства, то він уже має заготовку шкали оцінки рівня загроз, а якщо експерт внутрішній, то таку шкалу йому доведеться розробити самостійно або скориставшись практикою зарубіжних організацій. Шкала може бути двох видів: якісна та кількісна. Простий приклад якісної шкали: низька ймовірність реалізації загрози, середня ймовірність реалізації загрози, висока ймовірність реалізації загрози. Розшифрувати таку шкалу доволі просто:

Низька ймовірність реалізації загрози – загроза інформаційній безпеці ніколи не реалізується;

Середня ймовірність реалізації загрози – загроза інформаційній безпеці реалізується з ймовірністю 50 %;

Висока ймовірність реалізації загрози – загроза інформаційній безпеці реалізується з ймовірністю більше 50 %.

Цей варіант шкали не найкращий але і не найгірший.

Прикладів з кількісною шкалою не менше ніж з якісною, наприклад: (0;0,25) – низька ймовірність реалізації загрози; (0,25;0,5) – середня ймовірність реалізації загрози; (0,5;1) – висока ймовірність реалізації загрози. Як експерт буде визначати кількісне значення 0,25 чи 0,27 і в чому різниця – відомо лише йому, і цю таємницю він не продасть. Не варто забувати про компетентність експерта (не має значення внутрішній він чи зовнішній), який буде оцінювати значення ймовірності реалізації загрози. Адже оцінку ймовірності реалізації загрози спеціалістом з інформаційної безпеки у котрого з інформаційної безпеки є лише диплом, а він, лише, кілька років працює адміністратором ІТ – не варто вважати об’єктивною. Процедуру оцінки компетентності експерта варто продумати заздалегідь. Одним з ключових моментів в такій процедурі, являються критерії оцінки, які можна представити, наприклад, в такому вигляді:

Наявність вищої освіти за напрямком інформаційна безпека (так-1, ні-0).

Наявність сертифікатів за напрямком інформаційна безпека(так-1, ні-0).

Проходження останнього підвищення кваліфікації (менше трьох років тому – 1, більше трьох років тому - 0).

Досвід роботи і т. д.

Далі необхідно нормувати значення оцінки, щоб величина змінювалась в межах від 0 до 1. На виході отримаємо деяке значення компетентності експерта, котре надалі буде враховуватись при визначенні ймовірності реалізації загрози.

Ймовірність загрози = компетентність експерта * n-у ймовірність реалізації загрози.

Наприклад, експерт поставив ймовірність реалізації загрози 1 = 0,25; ймовірність реалізації загрози 2 =0,5, а значення оцінки компетентності =0,4. Звідси випливає що ймовірність реалізації загрози 1 = 0,1, а ймовірність реалізації загрози 2 =0,2.

Основними недоліками підходу є:

Кінцевим результатом є суб'єктивні оцінки, навіть не зважаючи на введене значення коефіцієнта компетентності експерта, яке звісно наближає значення ймовірності загрози до об'єктивного.

Складність в виборі кількості інтервалів якісної та кількісної шкали. Мала кількість інтервалів може призвести до того що значення ймовірності реалізації загроз для актуальних загроз буде занижене. Велика кількість інтервалів вплине на роботу експерта.

Висновки до першого розділу

Другий підхід оцінки ймовірності реалізації загроз заснований на використовуванні різних математичних апаратів. Якщо подивитися праці різних учених, то з першого погляду можна оцінити всю різноманітність таких підходів.

Хтось пропонує оцінювати вірогідність з використанням теорії випадкових процесів, хтось з використанням нечіткої логіки і нечітких множин, хтось за допомогою теорії надійності і .т. д. Але необхідно помітити, що за безліччю різних формул, термінів, наприклад, "функції приналежності", "фазифікація", "функції і густина розподілу", "інтегральні оцінки", чисельними

методами "монте-карло", "марківські ланцюги і процеси", "кінцеві автомати" - ховаються всі ті ж оцінки експертів, або статистично накопичені дані.

Як і чому вони там використовуються? Для того, що б математична модель почала працювати необхідно щось подати на вхід цієї моделі. Як вхідні дані можуть виступати такі значення: кількість загроз ІБ, що відбулися, інтенсивність загроз ІБ, уразливості програмного забезпечення і засобів захисту, що відбувалися, ступінь виконання вимог ІБ (проста залежність: якщо вимоги виконуються то ймовірність реалізації загрози нижче) і т.д. А на виході виходить значення ймовірності реалізації загрози. Достовірність отриманих результатів залежить від достовірності вхідних даних.

Кількість загроз, що відбулися, може братися з власної БД (якщо вона звичайно ведеться або із загально доступних джерел.

Звідки краще брати інформацію? Краще брати накопичену інформацію по загрозах ІБ і доповнювати її інформацією із загально доступних джерел. При цьому необхідно звертати особливу увагу на вид діяльності організацій для яких представлена статистика. Тут не треба на організацію охорони здоров'я або металургійний комбінат приміряти статистику по загрозах ІБ від банківського сектора.

Переваги підходу:

використання математичних підходів наближає результат оцінки ймовірності реалізації загрози до об'єктивної.

Недоліки:

комерціалізація програмних продуктів з використанням таких підходів дуже низька, практично 0. Всього два російські продукти, з певними поправками, можна віднести до цієї категорії "Авангард" і "Digital Security Office".

Розділ 2
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ

Способи захисту інформації залежать від типу інформації, форми її зберігання, обробки і передачі, типу носія інформації, а також від передбачуваного способу нападу і наслідків його впливу на інформацію (копіювання, спотворення, знищення). В основному, власник інформації не знає де, коли і яким чином буде здійснено напад, тому йому необхідно визначити сам факт нападу.

Визначення потенційної цінності інформації дозволяє подумати, в першу чергу, про безпеку найважливішої інформації, витік якої здатний завдати збитку. При цьому важливо встановити:

1. Яка інформація потребує захисту?
2. Кого вона може зацікавити?
3. Які елементи інформації найцінніші?
4. Який термін дії цієї інформації?
5. В що обійдеться її захист?

2.1 Класифікація методів та засобів захисту

Методи захисту можна розділити на фізичні, технічні, криптографічні, організаційні, програмні, правові (законодавчі), морально-етичні.

Засоби захисту у свою чергу можна розділити на постійно діючі та ті які вмикаються при виявленні спроби нападу. По активності, вони діляться на пасивні, напівактивні і активні. По рівню забезпечення ЗІ засоби захисту підрозділяються на 4 класи: системи слабого захисту (1 клас), системи сильного захисту, системи дуже сильного захисту, системи особливого захисту.

Фізичні засоби захисту — це засоби, необхідні для зовнішнього захисту ЕОМ, території та об’єктів на базі обчислювальної техніки, які спеціально

призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються.

Спектр сучасних фізичних засобів захисту дуже широкий. Це різного роду замки, які можуть встановлюватись на вході в приміщення та на блоках системи, це системи пожежної сигналізації, встановлення охорони на вході в приміщення та по периметру контрольованої зони і т.п. До цієї групи засобів захисту також належать різні засоби екранування робочих приміщень та каналів передачі даних.

Технічними засобами захисту називаються такі засоби захисту інформації, в яких основна захисна функція реалізується технічним пристроєм (комплексом або системою).

Основні функції технічних засобів захисту:

заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;

заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи зумисних дій персоналу;

захист цілісності програмного забезпечення.

Ці функції реалізуються шляхом:

ідентифікації суб’єктів (користувачів, обслуговуючого персоналу) і об’єктів (ресурсів) системи;

аутентифікації суб’єкта по наданому ним ідентифікатору;

перевірки повноважень, яка полягає в перевірці дозволу на певні види робіт;

реєстрації (протоколювання) при звертаннях до заборонених ресурсів;

реєстрації спроб несанкціонованого доступу.

Безперечними перевагами технічних засобів захисту інформації (ТЗЗІ) є:

достатньо висока надійність;

достатньо широкий спектр задач;

можливість створення комплексних систем ЗІ (КСЗІ);

гнучке реагування на спроби несанкціонованої дії;

традиційність методів здійснення захисних функцій, що використовуються.

Основні недоліки ТЗЗІ полягають в наступному:

висока вартість багатьох засобів;

необхідність регулярного проведення регламентних робіт і контролю;

можливість видачі помилкових тривог.

Системну класифікацію ТЗЗІ зручно провести по наступній сукупності критеріїв:

здійснювана функція захисту;

ступінь складності пристрою;

зв'язаність із засобами ОТ.

Приведені значення критеріїв інтерпретуються таким чином.

Зв'язаність із засобами ОТ.

Автономні - засоби, виконуючі свої захисні функції незалежно від функціонування засобів ОТ, тобто повністю автономно.

Зв'язані - засоби, виконані у вигляді самостійних пристроїв, але виконуючі захисні функції в сполученні (спільно) з основними засобами ОТ.

Вбудовані - засоби, які конструктивно включені до складу апаратури ОТ.

Виконувана функція захисту.

Зовнішній захист - захист від дії дестабілізували чинників, що виявляються за межами зони ресурсів.

Розпізнавання - специфічна група засобів, призначених для впізнання людей по різних індивідуальних характеристиках.

Внутрішній захист - захист від дії чинників, що дестабілізували, які виявляються безпосередньо в засобах обробки інформації.

Ступінь складності пристрою.

Прості пристрої - нескладні прилади і пристосування, що виконують окремі процедури захисту.

Складні пристрої - комбіновані агрегати, що складаються з деякої кількості простих пристроїв, здібні до здійснення складних процедур захисту.

Системи - закінчені технічні об'єкти, здатні здійснювати деяку комбіновану процедуру захисту, що має самостійне значення.

Криптографічні методи захисту — це методи, засновані на криптографічних перетвореннях даних, тобто на їх шифруванні.

Основні криптографічні методи захисту:

шифрування з допомогою генератора псевдовипадкових чисел, яке полягає в тому, що генерується гамма шифру за допомогою генератора псевдовипадкових чисел і накладається на відкриті дані з врахуванням зворотності процесу;

шифрування за допомогою криптографічних стандартів шифрування даних (з симетричною схемою шифрування), в основі якого використовуються перевірені і випробувані алгоритми шифрування даних з великою криптостійкістю, наприклад американський стандарт DES;

шифрування за допомогою пари ключів (з асиметричною системою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, другий ключ — закритим і використовується для розшифрування інформації. Прикладом може служити метод RSA.

Криптографічні методи захисту інформації дуже широко використовуються в ІС і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту.

Таблиця 2.1

Характеристики алгоритмів криптозахисту

Характеристика	DES	RSA
Вид алгоритму	Одноключовий	Двоключовий
Швидкість роботи	Швидко	Повільно
Функція, що використовується	Перестановка і підстановка	Піднесення до степеня
Довжина ключа	56 біт	300-600 біт
Найменш затратний крипто аналіз	Перебір по всьому ключовому простору	Розкладання модуля
Стійкість	Теоретична	Практична
Часові витрати на розкриття	Століття	Залежать від довжини ключа
Час генерації ключів	Міллі-секунди	Десятки секунд
Тип ключа	Симетричний	Асиметричний

Порівняльний аналіз алгоритмів криптозахисту дає можливість відмітити такі їх особливості. Алгоритм RSA працює приблизно в тисячу разів повільніше за алгоритм DES і потребує в десять разів довших ключів, його стійкість теоретично не доведена. Але велика перевага RSA полягає у відсутності необхідності організації строго засекреченої процедури обміну ключами. Тому в ІС потрібно застосовувати гібридні системи, засновані на двох алгоритмах, використовувати їх переваги.

Організаційні засоби захисту — це заходи організаційного характеру, регламентуючі процеси функціонування ІС, використання її ресурсів, діяльність персоналу і т. д. Мета цих заходів в найбільшій мірі перешкодити та виключити можливість реалізації загроз безпеки.

Вони включають:

заходи, здійснювані при проектуванні, будівництві та обладнанні обчислювальних центрів та інших об'єктів систем обробки даних;

заходи з розробки правил доступу користувачів до ресурсів системи (розробка політики безпеки);

заходи, здійснювані при підборі та підготовці персоналу системи;

організацію охорони і надійного пропускного режиму;

організацію обліку, зберігання, використання та знищення документів і носіїв із інформацією;

розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.);

організацію явного і прихованого контролю за роботою користувачів;

заходи, здійснювані при проектуванні, розробці, ремонті і модифікаціях обладнання і програмного забезпечення і т.п.

Організаційні заходи відіграють значну роль у забезпеченні інформаційної безпеки підприємства.

Організаційні заходи - це єдине, що залишається, коли інші методи і засоби захисту відсутні або не можуть забезпечити необхідний рівень безпеки. Однак, це не означає, що систему захисту необхідно будувати виключно на їх основі.

Недоліки організаційних заходів:

низька надійність без відповідної підтримки фізичними, технічними та програмними засобами (люди схильні до порушення будь-яких встановлених додаткових обмежень і правил, якщо тільки їх можна порушити);

додаткові незручності, пов'язані з великим обсягом рутинної формальної діяльності.

Організаційні заходи необхідні для забезпечення ефективного застосування інших заходів і засобів захисту в частині, що стосується регламентації дій людей. У той же час організаційні заходи необхідно підтримувати більш надійними фізичними та технічними засобами.

Програмні засоби захисту необхідні для виконання логічних і інтелектуальних функцій захисту, які вбудовані до складу програмного забезпечення системи.

За допомогою програмних засобів захисту реалізуються наступні задачі забезпечення безпеки:

контроль завантаження та входу в систему за допомогою системи паролів;

розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних і т.п.;

захист файлів від вірусів;

автоматичний контроль за роботою користувачів шляхом протоколювання їх дій.

Апаратно-програмні засоби захисту — це засоби, які засновані на синтезі програмних та апаратних засобів. Ці засоби широко використовуються при аутентифікації користувачів ІС. Аутентифікація — це перевірка ідентифікатора користувача перед допуском його до ресурсів системи.

Апаратно-програмні засоби захисту використовуються також при накладанні електронно-цифрових підписів відповідальних користувачів. Найбільш поширеним є використання смарт-карт, які вміщують паролі та ключі користувачів.

До правових заходів захисту відносяться діючі в Україні закони, укази та нормативні акти, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників.

До морально-етичних заходів належать норми поведінки, які традиційно склалися або складаються на підприємстві. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти, однак, їх недотримання веде зазвичай до падіння авторитету, престижу людини, групи осіб чи організації. Морально-етичні норми бувають як неписані (наприклад, загальновизнані норми чесності, патріотизму тощо), так і писані, тобто оформлені як певний перелік правил.

Правові та морально-етичні заходи протидії, є універсальними в тому сенсі, що принципово застосовні для всіх каналів проникнення і НСД до інформаційних систем та інформації. У деяких випадках лише вони можуть бути застосовані, як наприклад, при захисті відкритої інформації від незаконного тиражування.

Існує твердження про те, що створення абсолютної (тобто ідеально надійної) системи захисту принципово неможливо.

Навіть при допущенні можливості створення абсолютно надійних фізичних і технічних засобів захисту, що перекривають всі канали витоку інфрмації, завжди залишається можливість впливу на персонал системи, який забезпечує їх функціонування (адміністратора АС, адміністратора безпеки тощо) . Разом із самими засобами захисту ці люди утворюють так зване "ядро безпеки". У цьому випадку, стійкість системи безпеки буде визначатися стійкістю персоналу з ядра безпеки системи, і підвищувати її можна тільки за рахунок організаційних (кадрових) заходів, законодавчих та морально-етичних заходів. Але навіть маючи досконалі закони і проводячи оптимальну кадрову політику, все одно проблему захисту до кінця вирішити не вдасться. По-перше, тому, що навряд чи вдасться знайти персонал, в якому можна було бути абсолютно впевненим, і щодо якого неможливо було б вчинити дії, що змусили б його порушити політику безпеки. По-друге, навіть абсолютно надійна людина може допустити випадкове, ненавмисне порушення.

Завдання забезпечення інформаційної безпеки повинно вирішуватися системно. Це означає, що різні засоби захисту (апаратні, програмні, фізичні, організаційні і т.д.) повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

На сьогоднішній день існує великий арсенал засобів забезпечення інформаційної безпеки:

засоби ідентифікації і аутентифікації користувачів (так званий комплекс ЗА);

засоби шифрування інформації, що зберігається на комп'ютерах і що передається по мережах;

міжмережеві екрани;

віртуальні приватні мережі;

засоби контентної фільтрації;

інструменти перевірки цілісності вмісту дисків;

засоби антивірусного захисту;

системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожний з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для систем будь-якої складності та конфігурації, незалежно від використовуваних платформ.

«Комплекс ЗА» включає аутентифікацію (або ідентифікацію), авторизацію і адміністрування. Ідентифікація та авторизація - це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ.

Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу з мережних протоколах. Завдання даного засобу захисту ― забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування - високий рівень криптостійкості та легальність використання на території держави.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома чи більш мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів ─ перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних.

Говорячи про криптографію і міжмережеві екрані, слід згадати про захищені віртуальні приватні мережі (Virtual Private Network ─ VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам. Використання VPN можна звести до вирішення трьох основних завдань:

1. Захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);

2. Захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet;

3. Захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму.

Засоби контентної фільтрації дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска (integrity checking). Це

дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують невиробничі затрати праці, пов'язані з розглядом спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не включені до бази антивірусних програм) часто мають ознаки спаму і фільтруються.

Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних - резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій і т.д

2.2 Політика інформаційної безпеки

Під політикою інформаційної безпеки розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Виділяються три компоненти, що пов'язані з порушенням безпеки системи:

загроза ─ зовнішнє, відносно системи, джерело порушення властивості захищеність;

об'єкт атаки ─ частина системи, на яку діє загроза;

канал дії ─ середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує всі ці компоненти, є політика безпеки (ПБ) ─ якісний (або якісно-кількісний) вираз властивостей захищеності в термінах, що представляють систему. Опис ПБ повинен включати або враховувати властивості загрози, об'єкта атаки та каналу дії.

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

ПБ інформації в КС є частиною загальної ПБ організації і може успадковувати, зокрема, положення державної політики у сфері захисту інформації. Для кожної системи ПБ інформації може бути індивідуальною і залежати від конкретної технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища та багатьох інших чинників.

Частина ПБ, яка регламентує правила доступу користувачів і процесів до ресурсів комп'ютерної системи, становить правила розмежування доступу.

Розробка і підтримка ПБ майже завжди означає досягнення компромісу між альтернативами, які обирають власники цінної інформації для її захисту. Отже, будучи результатом компромісу, ПБ ніколи не задовольнить усі сторони, що беруть участь у захисті інформації.

Водночас, вибір ПБ ─ це остаточне рішення: що добре й що погано в поводженні з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Тоді цілком природним критерієм якості системи захисту інформації (СЗІ) стає такий: «побудована СЗІ вдала, якщо вона надійно підтримує виконання правил ПБ, і, навпаки, СЗІ невдала, якщо вона ненадійно підтримує ПБ».

Такий розв'язок проблеми захищеності інформації і проблеми побудови СЗІ дає змогу залучити до теорії захисту точні математичні методи, тобто доводити, що певна СЗІ в заданих умовах підтримує ПБ. Саме в цьому полягає суть доказового підходу щодо захисту інформації, який дозволяє говорити про гарантовано захищену систему.

Сенс гарантованого захисту в тому, що за додержання вихідних умов заздалегідь виконуються всі правила ПБ. Термін гарантований захист уперше зустрічається в стандарті міністерства оборони США на вимоги до захищених систем.

Зважаючи на технічні та програмно-апаратні проблеми, що виникають при організації захисту в захищених АС, у багатьох випадках належний рівень захищеності досягається за рахунок вдало реалізованої ПБ, причому іноді ПБ може залишитися майже єдиним засобом забезпечення захисту. Тому розробка, дослідження та правильні застосування ПБ є надзвичайно актуальною проблемою сучасних СЗІ.

Побудова ПБ ─ це зазвичай такі кроки:

в інформацію вноситься структура цінностей і проводиться аналіз ризику;

визначаються правила для будь-якого процесу користування певним видом доступу до елементів інформації, які мають певну оцінку цінностей.

Однак реалізація цих кроків є дуже складним завданням. Результатом помилкового або бездумного визначення правил ПБ здебільшого є руйнування цінності інформації без порушення ПБ. Тобто при незадовільній ПБ навіть надійна СЗІ може бути прозорою для зловмисника.

ПБ 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 ПБ. Основна мета створення ПБ інформаційної системи й опису її у вигляді формальної моделі ─ це визначення умов, яким має підпорядковуватися поведінка системи, вироблення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при додержанні встановлених правил і обмежень. На практиці це означає, що тільки уповноважені користувачі можуть отримати доступ до інформації і здійснювати з інформацією тільки санкціоновані дії.

Незважаючи на те що створення формальних моделей вимагає суттєвих витрат, вони складні для розуміння і вимагають певної інтерпретації для застосування в реальних системах. Слід констатувати той факт, що формальні моделі потрібні, тому що тільки за їх допомогою можна довести безпеку системи, спираючись на об'єктивні й незаперечні постулати математичної теорії. Загальним підходом щодо всіх моделей є поділ множини сутностей, що становлять систему, на множини суб'єктів і об'єктів, хоча самі визначення понять об'єкт і суб'єкт у різних моделях 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 певним спеціально призначеним для цього суб'єктом і забороняються або дозволяються відповідно до правил ПБ.

ПБ 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.

Види моделей політик інформаційної безпеки

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. Перші дві досить давно відомі й детально досліджені, а рольова політика є недавнім досягненням теорії та практики захисту інформації.

Дискреційна політика безпеки

Основою дискреційної політики безпеки (ДПБ) є дискреційне управління доступом (Discretionary Access Control - DAC), яке визначається двома властивостями:

усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;

права доступу суб'єкта до об'єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Назва пункту є дослівним перекладом з англійської терміну Discretionary policy, ще один варіант перекладу - розмежувальна політика. Ця політика одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі саме ця політика. ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту.

Наведемо приклади варіантів завдання матриці доступу:

1. Листи можливостей: для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких має доступ даний суб'єкт.

2. Листи контролю доступу: для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до цього об'єкта.

До переваг ДПБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлено той факт, що більшість поширених нині захищених автоматизованих систем забезпечують виконання положень саме ДПБ. Однак багатьох проблем захисту ця політика розв'язати не може.

Наведемо найбільш суттєві вади ДПБ:

1. Один з найбільших недоліків цього классу політик ─ вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що система захисту, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Автоматичне визначення прав. Оскільки об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта. Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання певної події, також можливі модифікації, що залежать від інших параметрів.

3. Контроль поширення прав доступу. Найчастіше буває так, що власник файлу передає вміст файлу іншому користувачеві і той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після кількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі певний суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АС. У загальному випадку при використанні ДПБ органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується певним набором правил, стоїть задача, яку алгоритмічно неможливо розв'язати: перевірити, призведуть його дії до порушень безпеки чи ні. Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати ясну і чітку СЗІ в АС. Більш досконалою ПБ виявилася мандатна ПБ.

Мандатна політика

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control - MAC), яке передбачає, що:

всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;

у системі визначено лінійно упорядкований набір міток секретності;

кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, ─ його рівень секретності в АС;

кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС,- максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Основна мета МПБ ─ запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в КС інформаційних каналів згори вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності інформаційних об'єктів. Цінність інформаційних об'єктів (або їх мітки рівня секретності) часто дуже важко визначити. Однак досвід показує, що в будь-якій КС майже завжди для будь-якої пари об'єктів X та *Y* можна сказати, який з них більш цінний.

Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція *c(X),* 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.* Тоді потік інформації від *X* до *Y* дозволяється, якщо *c(X) < c(Y),* і не дозволяється, якщо *c(X) > c(Y).*

Отже, МПБ 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 МПБ описують у термінах, поняттях і визначеннях властивостей моделі

Белла-Лападула. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: «якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний».

Переваги МПБ порівняно з ДПБ:

1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов'язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб'єктів системи до об'єктів, а й стан самої КС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника;

2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи;

3. МПБ стійка до атак типу «Троянський кінь»;

4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона дуже складна для практичної реалізації і вимагає значних ресурсів КС. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Сааме ці вади часто заважають її практичному використанню.

МПБ 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 політика безпеки.

Рольову політику безпеки (РПБ) (Role Base Access Control - RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування 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 є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

У РПБ 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.

РПБ 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 керування 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, користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Наприклад, у реальній системі обробки інформації можуть працювати 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 обмежуються мінімумом, 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. При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження. У моделі РПБ визначаються множини: множина користувачів, множина ролей, множина повноважень на доступ до об'єктів, наприклад, у вигляді матриці прав доступу, множина сеансів роботи користувачів з системою. Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача набір доступних йому ролей.

Правила керування доступом РПБ визначаються певними функціями, які для кожного сеансу визначають користувачів, набір ролей, що можуть бути одночасно доступні користувачеві в цьому сеансі, а також набір доступних у ньому повноважень, що визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі. Як критерій безпеки рольової моделі використовується правило: «система вважається безпечною, якщо будь-який користувач системи, що працює в певному сеансі, може здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження

належать сукупності повноважень усіх ролей, що беруть участь у цьому сеансі».

З формулювання критерію безпеки рольової моделі випливає, що управління доступом здійснюється, головним чином, не за допомогою призначення повноважень ролям, а шляхом встановлення відношення, яке призначає ролі користувачам, і функції, що визначає доступний у сеансі набір ролей. Тому численні інтерпретації рольової моделі відрізняються видом функцій, що визначають правила керування доступом, а також обмеженнями, що накладаються на відношення між множинами. Завдяки гнучкості та широким можливостям РПБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так, вона практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, проте позбавляє систему теоретичної доказової бази (вада). У деяких ситуаціях ця обставина утруднює використання РПБ, однак у кожному разі оперувати ролями набагато зручніше, ніж суб'єктами (знову перевага), оскільки це більше відповідає поширеним технологіям обробки інформації, які передбачають розподіл обов'язків і сфер відповідальності між користувачами. Крім того, РПБ може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам, контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

Наведений огляд сучасних ПБ визначає основні принципи їх функціонування, а також підкреслює їх роль і виключну важливість при побудові та експлуатації захищених АС. Додам, що в багатьох сучасних програмних засобах захисту інформації розглянуті ПБ уже реалізовані. Однак слід зазначити, що це зовсім не означає їх механічного застосування. Зрозуміло, що спочатку в конкретній організації має бути проведений ретельний аналіз

процесів обробки інформації, на основі якого потім створюється і застосовується конкретна ПБ.

Необхідно також зазначити, що, крім загального опису поняття ПБ, в Українському стандарті з технічного захисту інформації більш конкретних нормативних та методичних матеріалів з розробки ПБ для АС поки що немає.
В більшості організацій (як державних, так і недержавних) про поняття ПБ навіть не мають уявлення. Але парадокс якраз полягає в тому, що фактично в будь-якій організації завжди існують конкретні правила, що регламентують процес її функціонування, зокрема і процес захисту інформації, а саме ці правила і є політикою. Отже, фактично в будь-яких АС окремі елементи ПБ завжди наявні.

З практичної точки зору політику безпеки доцільно розділити на три рівні. До верхнього рівня можна віднести рішення, що торкаються організації в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації. Наприклад, список подібних рішень може включати в себе:

формування або перегляд самої комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію цієї програми;

формулювання цілей у сфері інформаційної безпеки та визначення загальних напрямів їх досягнення;

забезпечення технічної бази для дотримання відповідних законів і правил;

формулювання управлінських рішень з тих питань реалізації програмної безпеки, які повинні розглядатися на рівні організації в цілому.

На політику верхнього рівня впливають цілі організації в галузі інформаційної безпеки: вони формулюються, як правило в термінах цілісності, доступності та конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, то на першому плані може стояти зменшення випадків втрат, пошкоджень або спотворень даних. Для організації, що займається наданням послуг, імовірно, важлива актуальність інформації про ці

послуги та їх ціни, а також доступність послуг максимальному числу потенційних покупців. Режимна організація в першу чергу піклується про захист від несанкціонованого доступу ─ конфіденційності.

На верхній рівень виноситься управління ресурсами захисту та координація їх використання, виділення спеціального персоналу для захисту особливо важливих систем, підтримка контактів з іншими організаціями, що забезпечують чи контролюють режим безпеки.

Сфера політики верхнього рівня повинна бути чітко окреслена. Можливо, це будуть комп'ютерні системи самої організації, а, можливо, і деякі аспекти використання домашніх комп'ютерів у співробітників цієї організації. Можна уявити собі, і таку ситуацію, коли в сферу впливу включаються лише окремі найбільш важливі системи політики інформаційної безпеки підприємства. Вироблення програми інформаційної безпеки верхнього рівня і її здійснення - це завдання певних посадових осіб, за виконання якої вони повинні регулярно звітувати.

Нарешті, політика інформаційної безпеки верхнього рівня, очевидно, повинна вписуватися в існуючі закони держави, а щоб бути впевненими в тому, що їй точно й акуратно слідує персонал підприємства, доцільно розробити систему відповідних заохочень і покарань. А взагалі-то кажучи, на верхній рівень слід виносити мінімум питань. До середнього рівня можна віднести окремі аспекти інформаційної безпеки, проте важливі для різних систем, експлуатованих організацією.

Політика середнього рівня по кожному подібному аспекту передбачає вироблення відповідного документованого управлінського рішення, в якому зазвичай є:

Опис аспекту. Наприклад, якщо взяти застосування користувачами неофіційного програмного забезпечення, то про нього обов'язково має бути сказано, що це таке забезпечення, яке не було схвалено і / або закуплено на рівні організації.

Вказівка на область її застосування (розповсюдження тієї чи іншої політики інформаційної безпеки). Іншими словами має бути сертифіковано, де, коли, як, по відношенню до кого і чого застосовується дана політика безпеки.

Чіткий розподіл відповідних ролей та обов'язків. У «політичний» документ необхідно включити інформацію про посадових осіб, відповідальних за проведення політики безпеки в життя. Наприклад, якщо для використання працівником неофіційного програмного забезпечення потрібно офіційний дозвіл, то має бути відомо, у кого і як його слід отримувати. Якщо повинні перевірятися диски, принесені з інших комп'ютерів, необхідно описати процедуру перевірки. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням цього правила.

Механізм забезпечення «законослухняності». Політика має містити загальний опис заборонених дій і покарання за них.

Вказівки на необхідні «точки контакту». Повинно бути точно відомо, куди слід звертатися за роз'ясненнями, допомогою та додатковою інформацією. Зазвичай «точкою контакту» служить посадова особа.

Політика безпеки нижнього рівня відноситься до конкретних сервісів. Вона включає в себе всього два аспекти - мети і правила їх досягнення, тому її часом важко відокремити від питань реалізації (надання послуг з інформаційного забезпечення). На відміну від двох верхніх рівнів, розглянута політика нерідко буває набагато більш детальною. Є багато питань, специфічних для окремих сервісів, які не можна єдиним чином регламентувати в рамках всієї організації. У той же час ці питання настільки важливі для забезпечення режиму безпеки, що рішення, які належать до них, повинні прийматися на управлінському, а не технічному рівні. Ось лише кілька прикладів-запитань, на які слід дати відповідь при розробці політики безпеки нижнього рівня:

Хто має право доступу до об'єктів, що підтримуються сервісом?

За яких умов можна читати і модифікувати дані?

Висновки до другого розділу

При формулюванні цілей, політика нижнього рівня може виходити з міркувань цілісності, доступності та конфіденційності, але вона не повинна на цьому зупинятися. Її цілі мають бути конкретнішими. Наприклад, якщо мова йде про систему розрахунку зарплати, можна поставити мету, щоб тільки працівникам відділу кадрів і бухгалтерії дозволялося вводити і змінювати інформацію. У більш загальному випадку цілі повинні пов'язувати між собою об'єкти сервісу та логічні з точки зору інформаційної безпеки, осмислені, дії з ними. З цілей зазвичай виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим більш формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, і, ймовірно, їх доведеться часто переглядати.

Керівництву необхідно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться надмірно сковані.

Розділ 3
ОСНОВИ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Модель представлення системи захисту інформації

Практична задача забезпечення інформаційної безпеки складається в розробці моделі представлення системи захисту інформації, що на основі науково-методичного апарату, дозволяла б вирішувати задачі створення, використання й оцінки ефективності СЗІ для проектованих і існуючих унікальних ІС.

Що розуміється під моделлю СЗІ? На скільки реально створити таку модель? У спрощеному вигляді модель СЗІ представлена на Рис.3.1.

Рис.3.1. Модель представлення СЗІ

Основною задачею моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанту технічної реалізації системи захисту інформації.

Специфічними особливостями розв'язку задачі створення систем захисту є:

неповнота і невизначеність вихідної інформації про склад ІС і характерних загроз;

багатокритерійність задачі, пов'язана з необхідністю обліку великої кількості частинних показників (вимог) СЗІ;

наявність як кількісних, так і якісних показників, які необхідно враховувати при розв’язанні задач розробки і впровадження СЗІ;

неможливість застосування класичних методів оптимізації.

Така модель повинна задовольняти наступним вимогам:

Використовуватися в якості:

Посібника зі створення СЗІ;

Методики формування показників і вимог до СЗІ;

Інструмента (методики) оцінки СЗІ ;

Моделі СЗІ для проведення досліджень (матриця стану).

Мати властивості:

Універсальність;

Комплексність;

Простота використання;

Наочність;

Практична спрямованість;

Бути самонавчальною (можливість нарощування знань);

Функціонувати в умовах високої невизначеності вихідної інформації;

Дозволяти:

Установити взаємозв'язок між показниками (вимогами);

Задавати різні рівні захисту;

Одержувати кількісні оцінки;

Контролювати стан СЗІ;

Застосовувати різні методики оцінок;

Оперативно реагувати на зміни умов функціонування;

Об'єднати зусилля різних фахівців єдиним задумом;

Як скласти таке представлення про інформаційну безпеку, щоб охопити всі аспекти проблеми? Людина одержує найбільш повне представлення про явище, яке її цікавить, коли їй вдається розглянути це щось невідоме з усіх боків, у тривимірному просторі. Скористаємося цим принципом.

Розглянемо три "координати вимірів" - три групи складових моделі СЗІ.

1. З чого складається (Основи).

2. Для чого призначена (Напрямки).

3. Як працюють (Етапи).

Основами – складовими частинами практично будь-якої складної системи (у тому числі і системи захисту інформації) є:

Законодавча, нормативно-правова і наукова база;

Структура і задачі органів (підрозділів), що забезпечують безпеку ІТ;

Організаційно-технічні і режимні засоби і методи (політика інформаційної безпеки);

Програмно-технічні способи і засоби.

Напрямки формуються виходячи з конкретних особливостей ІС як об'єкта захисту.

У загальному випадку, з огляду на типову структуру ІС і історично сформовані види робіт із захисту інформації, пропонується розглянути наступні напрямки:

Захист об'єктів інформаційних систем;

Захист процесів, процедур і програм обробки інформації;

Захист каналів зв'язку;

Придушення побічних електромагнітних випромінювань;

Керування системою захисту.

Але, оскільки кожен з цих напрямків базується на перерахованих вище основах, то елементи основ і напрямків, розглядаються нерозривно один з одним.

Проведений аналіз існуючих методик (послідовностей) робіт зі створення СЗІ дозволяє виділити наступні етапи:

Визначення інформаційних і технічних ресурсів, а також об'єктів ІС, що підлягають захисту;

Виявлення повної множини потенційно можливих загроз і каналів витоку інформації;

Проведення оцінки вразливості і ризиків інформації (ресурсів ІС) при наявній множині загроз і каналів витоку;

Визначення вимог до системи захисту інформації;

Здійснення вибору засобів захисту інформації і їхніх характеристик;

Впровадження й організація використання обраних методів і засобів захисту.

Здійснення контролю цілісності і керування системою захисту.

У загальному випадку кількість елементів матриці може бути визначено зі співвідношення:

$$K=Oi*Hj*Mk$$

де К - кількість елементів матриці

Oi - кількість складових блоку "Основи"

Hj - кількість складових блоку "Напрямки"

Mk - кількість складових блоку "Етапи"

У нашому випадку загальна кількість елементів "матриці" дорівнює 140 K=4*5*7=140, оскільки Oi=4, Hj=5, Mk=7

Отримано матрицю запитань, відповіді на які дозволять сформувати представлення про стан захищеності інформації у конкретній ІС.

Матриця не існує сама по собі, а формується виходячи з опису конкретної ІС і конкретних задач захисту інформації в цій системі, Рис. 3.2.

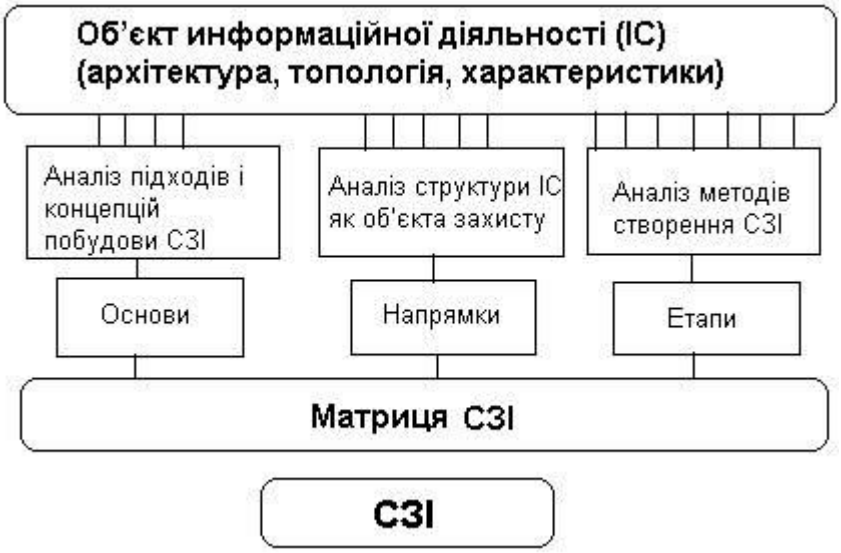

Рис.3.2. Структура матриці СЗІ

Рис.3.3. Властивості матриці СЗІ

Як оцінити ефективність створюваної чи уже функціонуючої СЗІ?

Знову допоможе підхід на основі тривимірної матриці. Тільки тепер по показниках (елементах) матриці треба виставити відповідні оцінки.

Наочно зазначені властивості матриці приведені на Рис. 3.3.

3.2 Вибір засобів захисту від внутрішніх загроз

Багато рішень у сфері захисту інформації часто приймаються на інтуїтивно-понятійному рівні, без будь-яких економічних розрахунків та обґрунтувань. У результаті тільки ті начальники служб ІБ (CISO), які за рахунок своєї "ініціативності" змогли заявити і відстояти потребу в захисті інформації, вплинули на планування бюджету компанії на ІБ.

Однак сучасні вимоги бізнесу, які пред'являються до організації режиму ІБ, диктують нагальну необхідність використовувати у своїй роботі більш обґрунтовані техніко-економічні методи і засоби, що дозволяють кількісно вимірювати рівень захищеності компанії, а також оцінювати економічну ефективність витрат на ІБ.

Для оцінки ефективності корпоративної системи захисту інформації рекомендується використовувати деякі показники ефективності, наприклад показники: сукупної вартості володіння (TCO), економічної ефективності бізнесу і безперервності бізнесу (BCP), коефіцієнти повернення інвестицій на ІБ (ROI) та інші.

Зокрема, відома методика сукупної вартості володіння (TCO) була спочатку запропонована аналітичною компанією Gartner Group в кінці 80-х років (1986-1987) для оцінки витрат на інформаційні технології. Методика Gartner Group дозволяє розрахувати всю видаткову частину інформаційних активів компанії, включаючи прямі і непрямі витрати на апаратно-програмні засоби, організаційні заходи, навчання і підвищення кваліфікації співробітників компанії, реорганізацію, реструктуризацію бізнесу і т. д.

Істотно, що сьогодні методика TCO може бути використана для доказу економічної ефективності існуючих корпоративних систем захисту інформації. Вона дозволяє керівникам служб інформаційної безпеки обґрунтовувати бюджет на ІБ, а також доводити ефективність роботи співробітників служби. Крім того, оскільки оцінка економічної ефективності корпоративної системи захисту інформації стає "вимірною", стає можливим оперативно вирішувати

задачі контролю і корекції показників економічної ефективності і зокрема показника ТСО. Таким чином, показник ТСО можна використовувати як інструмент для оптимізації витрат на забезпечення необхідного рівня захищеності корпоративної інформаційної системи (КІС) та обґрунтування бюджету на ІБ. При цьому в компанії ці роботи можуть виконуватися самостійно, із залученням системних інтеграторів в області захисту інформації, або спільно підприємством і інтегратором.

Слід зазначити, що показник ТСО може застосовуватися практично на всіх основних етапах життєвого циклу корпоративної системи захисту інформації та дозволяє "навести порядок" в існуючих і планувати витрати на ІБ. З цієї точки зору показник ТСО дозволяє об'єктивно і незалежно обґрунтувати економічну доцільність впровадження та використання конкретних організаційних і технічних заходів і засобів захисту інформації.

При цьому для об'єктивності рішення необхідно додатково враховувати стан зовнішнього і внутрішнього середовища підприємства, наприклад показники технологічного, кадрового та фінансового розвитку підприємства, так як не завжди найменший показник ТСО корпоративної системи захисту інформації може бути оптимальний для компанії.

Зрозуміло, що вміле керування ТСО дозволяє раціонально та економно реалізовувати кошти бюджету на ІБ, досягаючи при цьому прийнятного рівня захищеності компанії, адекватного поточним цілям та завданням бізнесу. Істотно, що порівняння певного показника ТСО з аналогічними показниками ТСО по галузі (аналогічними компаніями) і з "кращими в групі" дозволяє об'єктивно і незалежно обґрунтувати витрати компанії на ІБ. Адже часто виявляється досить важко або навіть практично неможливо оцінити прямий економічний ефект від витрат на ІБ. Порівняння ж "родинних" показників ТСО дозволяє переконатися в тому, що проект створення або реорганізації корпоративної системи захисту інформації компанії є оптимальним у порівнянні з деякими середньостатистичними проектами у галузі захисту інформації. Зазначені порівняння можна проводити, використовуючи

усереднені показники ТСО по галузі, розраховані експертами Gartner Group або власні експертами компанії за допомогою методів математичної статистики і обробки спостережень.

Методика ТСО Gartner Group дозволяє відповісти на наступні актуальні питання:

Які ресурси та грошові кошти витрачаються на ІБ?

Оптимальні чи витрати на ІБ для бізнесу компанії?

Наскільки ефективна робота служби ІБ компанії в порівнянні з іншими?

Як ефективно управляти інвестуванням в захист інформації?

Які вибрати напрями розвитку корпоративної системи захисту інформації?

Як обґрунтувати бюджет компанії на ІБ?

Як довести ефективність існуючої корпоративної системи захисту інформації та служби ІБ компанії в цілому?

Яка оптимальна структура служби ІБ компанії?

Як правильно оцінити аутсортінгової послуги з супроводу корпоративної системи захисту інформації?

Як оцінити ефективність проекту в області захисту інформації?

У цілому, визначення витрат компанії на ІБ передбачає вирішення наступних трьох задач:

1. Оцінку поточного рівня ТСО корпоративної системи захисту інформації та КІС в цілому;

2. Аудит ІБ підприємства на основі порівняння рівня захищеності підприємства і рекомендованого рівня ТСО;

3.формування цільової моделі ТСО.

Розглянемо кожну з перерахованих завдань.

Оцінка поточного рівня ТСО. У ході робіт з оцінки ТСО проводиться збір інформації та розрахунок показників ТСО організації за такими напрямами:

Існуючі компоненти КІС (включаючи систему захисту інформації) та інформаційні активи компанії (сервери, комп'ютери клієн-тів, периферійні пристрої, мережеві пристрої);

Існуючі витрати на апаратні і програмні засоби захисту інформації (витратні матеріали, амортизація);

Існуючі витрати на організацію ІБ в компанії (обслуговування СЗІ) та систем корпоративного захисту інформації (СКЗІ), а також штатних засобів захисту периферійних пристроїв, серверів, мережевих пристроїв, планування і управління процесами захисту інформації, розробку концепції та політики безпеки тощо);

Існуючі витрати на організаційні заходи захисту інформації;

Існуючі непрямі витрати на організацію ІБ в компанії і зокрема забезпечення безперервності або стійкості діяльності компанії.

За результатами співбесіди з ТОР-менеджерами компанії і проведення інструментальних перевірок рівня захищеності організації, проводиться аналіз наступних основних аспектів: політики безпеки; організації захисту; класифікації та управління інформаційними ресурсами; управління персоналом; фізичної безпеки; адміністрування комп'ютерних систем і мереж; управління доступом до систем; розробки та супроводу систем; планування безперебійної роботи організації; перевірки системи на відповідність вимогам ІБ.

На основі проведеного аналізу вибирається модель ТСО, порівнянна з середніми і оптимальними значеннями для репрезентативної групи аналогічних організацій, що мають схожі з розглянутою організацією показники за обсягом бізнесу. Така група вибирається з банку даних щодо ефективності витрат на ІБ та ефективності відповідних профілів захисту аналогічних компаній.

Порівняння поточного показника ТСО компанії, що перевіряється з модельним значенням показника ТСО дозволяє провести аналіз ефективності організації ІБ компанії, результатом, якого є визначення "вузьких" місць в організації, причин їх появи та вироблення подальших кроків щодо реорганізації корпоративної системи захисту інформації і забезпечення необхідного рівня захищеності КІС.

Формування цільової моделі ТСО. За результатами проведеного аудиту моделюється цільова (бажана) модель, яка враховує перспективи розвитку

бізнесу та корпоративної системи захисту інформації (активи, складність, методи кращої практики, типи ЗЗІ та СКЗІ, кваліфікація співробітників компанії і т. п.).

Крім того, розглядаються капітальні витрати і трудовитрати, необхідні для проведення перетворень поточного середовища в цільове. У трудовитрати на впровадження включаються витрати на планування, розгортання, навчання і розробку. Сюди ж входять можливі тимчасові збільшення витрат на управління і підтримку.

Для обґрунтування ефекту від впровадження нової корпоративної системи захисту інформації (ROI) можуть бути використані модельні характеристики зниження сукупних витрат (TCO), що відображають можливі зміни в корпоративній системі захисту інформації.

Витрати на операції кінцевих користувачів. Це витрати на самопідтримку кінцевих користувачів, а також на підтримку користувачами один одного на противагу офіційній ІС підтримки. Витрати включають: самостійну підтримку, офіційне навчання кінцевих користувачів, нерегулярне (неофіційне) навчання, самостійні прикладні розробки, підтримку локальної файлової системи.

Витрати на простої. Дана категорія враховує щорічні втрати продуктивності кінцевих користувачів від запланованих і незапланованих відключень мережевих ресурсів, включаючи клієнтські комп'ютери, що спільно використовують сервери, принтери, прикладні програми, комунікаційні ресурси та програмне забезпечення для зв'язку.

Для аналізу фактичної вартості простоїв, які пов'язані з перебоями в роботі мережі і які впливають на продуктивність, вихідні дані отримують з огляду по кінцевим користувачам. Розглядаються тільки ті простої, які ведуть до втрати продуктивності.

Разом з методикою TCO можна використовувати різноманітні методи для розрахунку повернення інвестицій (ROI). Як правило, для оцінки доходної частини спочатку аналізують ті цілі, завдання і напрями бізнесу, які потрібно досягти за допомогою впровадження або реорганізації існуючих проектів в

області системної інтеграції, автоматизації та інформаційної безпеки. Далі використовують деякі вимірні показники ефективності бізнесу, для оцінки ефекту окремо по кожному рішенню. Припустимо, з метою скорочення операційних витрат, забезпечення прийнятної конкурентної спроможності, поліпшення внутрішнього контролю і т. д. Вказані показники не треба вигадувати, вони існують в надмірному вигляді. Далі можна використовувати методики розрахунку коефіцієнтів повернення інвестицій в інфраструктуру підприємства (ROI), на прикладі, також Gartner Group.

Досить результативно використовувати таку комбінацію: TCO як витратну частину і ROI як розрахункову. Крім того, сьогодні існують і інші різноманітні методи і технології розрахунку та вимірювання різних показників економічної ефективності

Для виключення зайвих витрат по захисту вся інформація ділиться на категорії відповідно до необхідного ступеня захисту. Цей ступінь визначається, виходячи з:

можливих збитків для власника при несанкціонованому доступі до інформації, що захищається;

економічної доцільності подолання захисту для противника.

Природно, виробляти таку оцінку для кожного документа було б дуже важко.

Тому склалася практика визначення категорій секретності документів, по яких документи розподіляються за формальними ознаками. Наприклад, в наших державних органах прийнято 4 категорії секретності: «Для службового користування», «Таємно» (кат.3), «Цілком таємно» (кат.2), «Цілком таємно особливої важливості» (кат.1).

Для спрощення вирішення питань захисту слід застосовувати аналогічну схему. Видається інструкція, яка визначає, за якими ознаками документ (інформація) відноситься до тієї чи іншої категорії, і які співробітники до якої категорії мають доступ.

Рішення завдання з розробки автоматизованої системи аналізу фізичної захищеності об'єкта обробки та зберігання інформації передбачає вирішення наступних завдань:

Розгляд типів об'єктів захисту;

Аналіз загроз на об'єктах захисту;

Класифікація можливих елементів захисту.

Під об'єктом захисту розуміють будь-яку структуру приватних, громадських, державних, і комерційних організацій, що містять інформацію, яка має певну цінність для власників.

У загальному випадку, складовими будь-якого об'єкта обробки та зберігання інформації є:

1. Територія організації, будинки та приміщення, в яких зберігається та обробляється інформація і цінності;

2. Засоби обробки інформації (ЕОМ, локальні і глобальні мережі) та оргтехніка, яка використовується для передачі і тиражування інформації (телефони, факси, копіювальні апарати, модеми);

3. Електронні та паперові носії інформації (жорсткі та гнучкі магнітні диски, оптичні накопичувачі, CD / DVD-ROM і ін.);

4. Співробітники і відвідувачі підприємства, які володіють інформацією.

Фізичний захист забезпечується службою охорони, основним завданням якої є попередження несанкціонованого фізичного проникнення на територію, в будівлі та приміщення об'єкта зловмисників та їх стримування протягом розрахункового часу (до прибуття міліції або сил підтримки).

Неодмінною умовою підтримки ІБ є своєчасне припинення можливих акцій порушників. Основними етапами дій потенційного зловмисника при проникненні на об'єкт обробки і зберігання інформації є: виявлення об'єкта; спостереження за об'єктом і розробка варіантів проникнення; реалізація основного або альтернативного варіанту проникнення на об'єкт; відхід з об'єкта захисту з можливою повною або частковою ліквідацією слідів проникнення. Метод проникнення через немережеві периферійні пристрої від інших методів

полягає в тому, що для його виконання необхідно фізична присутність зловмисника на об'єкті обчислювальної техніки. Тому головна мета охорони природним чином може бути розділена на такі підцілі як:

Запобігання несанкціонованого доступу на територію об'єкта і в його життєво важливі зони;

Виявлення проникнення на об'єкт порушника до моменту, коли він може завдати шкоди, та доведення інформації про вторгнення до сил охорони;

Своєчасне припинення дії, яку може зробити порушник, який проник на об'єкт;

Мінімізація збитків.

Усі існуючі механізми захисту працюють тільки на етапі реалізації загрози. Тобто по суті вони є засобами які блокують, а не попереджують атаки. В абсолютній більшості випадків вони захищають від атак, які вже знаходяться в процесі здійснення. І навіть якщо вони змогли запобігти ту чи іншу атаку, то набагато більш ефективним було б попередження атак, тобто усунення самих передумов реалізації вторгнень.

Найбільш важливою і важкою проблемою є проблема своєчасного попередження дій зловмисника на етапі проектування об'єкта обробки та зберігання інформації і в процесі його функціонування. На даних етапах основним завданням є наступне: як і де ввести нові підсистеми захисту на об'єкті захисту або як задіяти старі підсистеми для підвищення рівня захищеності об'єкта в поточний період часу.

Під час впровадження засобів безпеки на об'єкті, людина може зробити помилки, які з легкістю виявить надалі зловмисник. Тому з'являється загальна задача оцінки деяких показників захищеності: час протягом, якого на об'єкт обробки та зберігання інформації не буде зроблено несанкціонованої дії, середній час і ймовірність проникнення на об'єкт, ступінь спостережливості об'єкта захисту та інші.

Проблема витоку інформації з обчислювальної техніки (ОТ) через побічні електромагнітні випромінювання та наведення (ПЕМВН) відома фахівцям вже протягом більш ніж 20 років.

Можливі канали витоку інформації утворюються:

НЧ електромагнітними полями, що виникають при роботі технічних засобів передачі, обробки, зберігання, відображення інформації та допоміжних технічних засобів і систем;

При впливі на технічні засоби передачі, обробки, зберігання, відображення інформації та допоміжні технічні засоби і систем, магнітних і акустичних полів;

При виникненні паразитної ВЧ генерації;

При проходженні інформативних (небезпечних) сигналів у колі електроживлення;

При взаємному впливі ланцюгів;

При проходженні інформативних (небезпечних) сигналів у колі заземлення;

При паразитній модуляції ВЧ сигналу;

Внаслідок помилкових комутацій і несанкціонованих дій.

При передачі інформації з обмеженим доступом в елементах схем, конструкцій, підвідних і з'єднувальних проводах технічних засобів протікають струми інформативних (небезпечних) сигналів. Виникаючі при цьому електромагнітні поля можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації.

Робота персонального комп'ютера, як і будь-якого іншого електронного пристрою, супроводжується електромагнітними випромінюваннями радіодіапазону. Для ПК ці випромінювання реєструються в діапазоні до 1 ГГц з максимумом у смузі 50 МГц - 300 МГц. Такий широкий спектр випромінювання пояснюється тим, що в пристроях ОТ інформацію переносять послідовності прямокутних імпульсів малої тривалості. Тому ненавмисне

випромінювання буде містити складові з частотами, як перших гармонік, так і гармонік більш високих порядків.

До появи додаткових складових в побічному електромагнітному випромінюванні призводить і застосування в ОТ високочастотної комутації. Говорити про будь-які діаграми спрямованості електромагнітних випромінювань ПК не доводиться, оскільки на практиці розташування його складових частин (системний блок, монітор, сполучні кабелі та проводи живлення) відносно один одного має необмежене число комбінацій. Поляризація випромінювань ПК - лінійна. У кінцевому рахунку, вона визначається розташуванням з'єднувальних кабелів, так як саме вони є основними джерелами випромінювань в ПК, у яких системний блок має металевий кожух.

Крім випроміненого електромагнітного поля поблизу працюючого ПК існують квазістатичні магнітні й електричні поля, які швидко зменшуються з відстанню, але викликають наведення на будь-які провідники (металеві труби, телефонні дроти, дроти системи пожежної безпеки і т.д.). Ці поля істотні на частотах від десятків кілогерц до десятків мегагерц. Що стосується рівнів побічних електромагнітних випромінювань ОТ, то вони регламентовані з точки зору електромагнітної сумісності цілим рядом зарубіжних і вітчизняних стандартів, Так, наприклад, відповідно до публікації N22 CISPR (Спеціальний Міжнародний Комітет з радіоперешкод) для діапазону 230-1000 Мгц рівень напруженості електромагнітного поля, випромінюваного обладнанням ВТ, на відстані 10 метрів не повинен перевищувати 37 dB. Очевидно, що цей рівень випромінювання достатній для перехоплення на значних відстанях.

Таким чином, відповідність електромагнітних випромінювань, засобами ОТ, нормам на електромагнітну сумісність не є гарантією збереження конфіденційності оброблюваної в них інформації. Крім того, треба зауважити, що значна частина ПК в Україні не відповідає навіть цим нормам, тому що в гонитві за дешевизною в країну ввозилася техніка в основному «жовтої» збірки, яка не має сертифікатів якості.

Найпотужнішим джерелом випромінювання в ПК є система синхронізації. Однак перехоплення не модульованих гармонік тактової частоти навряд чи зможе когось зацікавити.

При використанні для перехоплення ПЕМВН звичайного побутового радіоприймача можливо розпізнавання на слух моментів зміни режимів роботи ПК, звернення до накопичувачів інформації на жорстких і гнучких магнітних дисках, натиснення клавіш і т.д. Але подібна інформація може бути використана тільки як допоміжна і не більше.

Таким чином, не всі складові побічного випромінювання персональних комп'ютерів є небезпечними з точки зору реального перехоплення оброблюваної в них інформації. Для відновлення інформації аналіз лише рівня електромагнітних випромінювань недостатній, потрібно ще знати їх структуру. Тому в технічному плані простіше всього вирішується завдання перехоплення інформації, яка відображається на екрані дисплея ПК.

Інформація, відображена на екрані дисплея, може бути відновлена у монохромному вигляді за допомогою звичайного телевізійного приймача. При цьому на екрані телевізійного приймача зображення буде складатися з чорних літер на білому тлі, а на екрані дисплея ПК - з білих літер на чорному тлі. Це пояснюється тим, що на відміну від дисплея максимум відеосигналу в телевізійному приймачі визначає рівень чорного, а мінімум - рівень білого.

Виділення з ПЕМВН ПК інформації про сигнал синхронізації зображення являє собою досить складне технічне завдання. Набагато простіше це проблема вирішується використанням зовнішніх переналаштовуючих генераторів синхросигналів. Навіть при використанні звичайних кімнатних телевізійних антен (наприклад, типу «Маяк») перехоплення інформації може бути здійснено на відстанях порядку 10 - 15 метрів . При використанні спрямованих антен з великим коефіцієнтом посилення дальність перехоплення зростає до 50 - 80 метрів. При цьому за кращу якість відновлення інформації відповідає зображення.

Сучасний рівень розвитку електроніки дозволяє виготовити подібні пристрої перехоплення інформації невеликих розмірів, що забезпечить необхідну скритність їх роботи.

В якості технічних способів виключення можливостей перехоплення інформації за рахунок ПЕМВН ПК можна перерахувати такі:

Доопрацювання пристроїв ОТ з метою мінімізації рівня випромінювання;

Електромагнітне екранування приміщень, в яких розташована обчислювальна техніка;

Екрани приміщень виконуються у вигляді суцільнозварної металевої конструкції. На екрані приміщень передбачаються так звані технологічні отвори, які в тій чи іншій мірі знижують ефективність екранування. До таких отворів відносяться: дверні та віконні прорізи, оглядові та вентиляційні отвори, отвори для підведення електроживлення, зв'язку сигналізації та контролю, а також отвори для введення труб водопостачання, опалення та ін.

Для зменшення проникнення випромінювань всі технологічні отвори обладнуються спеціальними фільтрами та екранами.

Дверні прорізи обладнуються ущільнювальними пристроями, що забезпечують хороший контакт обшитих металом дверей з екраном стін. У деяких випадках для підвищення ефективності екранування обладнуються вхідні тамбури з подвійними або потрійними дверима.

Для ослаблення випромінювань на введеннях проводів ланцюгів електроживлення, зв'язку управління, сигналізації і т.д. застосовуються спеціальні фільтри (загороджувальні або поглинаючі). Загороджувальні фільтри являють собою індуктивно-ємнісні ланцюги з зосередженими параметрами. Поглинаючі фільтри засновані на застосуванні твердих і сипучих поглиначів: суміші піску і чавунного дробу, феритових порошків і т.д.

Екранування вентиляційних отворів виконується за допомогою діафрагм і пасток різного перетину, що представляють позамежні хвилеводи. Діафрагми використовуються в основному в діапазоні менше 10000 МГц.

На частотах понад 10000 МГц для екранування вентиляційних каналів доцільно застосовувати пастки. Пастка являє собою зигзагоподібно вигнутий по довжині металевий короб з поперечним перерізом, рівним перетину вентиляційного отвору. На внутрішню поверхню короба наноситься радіопоглинаючий матеріал з рихленою поверхнею. Ефективність пастки визначається якістю радіопоглинаючого матеріалу і числом зигзагів.

Крім сіток для екранування дверей і вікон можливе застосування металізованих штор з струмопровідної тканини. Для виготовлення штор можуть застосовуватися тканини трьох типів. Перший тип являє бавовняну тканину щільного плетіння, на яку методом розпилення нанесений тонкий шар алюмінію або цинку.

Тканини другого типу містить у своїй основі металеві нитки, які при скручуванні утворюють соленоїди. Вихрові струми, що виникають в соленоїді, перешкоджають проходженню радіохвиль через тканину.

Третій тип тканин представляє собою волокнисті матеріали з вмістом вуглецю до 98%.

Підвищення ефективності екранування стін, стелі та підлоги приміщення може бути досягнуто шляхом нанесення на них струмопровідних покриттів, проведення металізації їх поверхонь або обклеювання металевою фольгою.
Проведення часткового екранування може забезпечити, у діапазоні 0.3-10 ГГц, зниження рівня випромінювання від 30 до 80дБ.

Використовуючи різні радіопоглинаючі матеріали та схемотехнічні рішення вдається істотно знизити рівень випромінювань ОТ. Вартість подібної доробки залежить від розміру необхідної зони безпеки і коливається в межах 20-70% від вартості ПК.

Електромагнітне екранування приміщень у широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат і не завжди можливе з естетичних і ергономічних міркувань.

Криптографія, на відміну від заходів фізичного захисту, володіє тією унікальною властивістю, що при правильному виборі методу витрати на

забезпечення захисту інформації на багато менші за витрати на подолання цього захисту.

Мета криптографічної системи полягає в тому, щоб зашифрувати осмислений вихідний текст (також званий відкритим текстом), отримавши в результаті абсолютно безглуздий на погляд шифрований текст (шифртекст, криптограма).

Одержувач, якому він призначений, повинен уміти розшифрувати (кажуть також "дешифрувати") цей шифртекст, відновивши, таким чином, відповідний йому відкритий текст. При цьому противник (криптоаналітик) повинен бути нездатним розкрити вихідний текст. Існує важлива відмінність між розшифруванням (дешифруванням) і розкриттям шифртексту.

Розкриттям криптосистеми називається результат роботи криптоаналітика, що приводить до можливості ефективного розкриття будь-якого, зашифрованого за допомогою даної криптосистеми, відкритого тексту. Ступінь нездатності криптосистеми до розкриття називається її стійкістю.

Питання надійності систем ЗІ - дуже складне. Справа в тому, що не існує надійних тестів, що дозволяють переконатися в тому, що інформація захищена досить надійно. По-перше, криптографія володіє тією особливістю, що на розкриття шифру найчастіше потрібно затратити на кілька порядків більше коштів, ніж на його створення. Отже, тестові випробування системи криптозахисту не завжди можливі. По-друге, багаторазові невдалі спроби подолання захисту зовсім не означають, що наступна спроба не виявиться успішною. Не виключений випадок, коли професіонали довго, але безуспішно билися над шифром, а якийсь новачок застосував нестандартний підхід - і шифр дався йому легко. У результаті такої поганої доказовою надійності засобів ЗІ на ринку дуже багато продуктів, про надійність яких неможливо достовірно судити. Природно, їх розробники розхвалюють на всі лади свій твір, але довести його якість не можуть, а часто це і неможливо в принципі. Як правило, недоказаність надійності супроводжується ще й тим, що алгоритм шифрування тримається в секреті.

На перший погляд, збереження алгоритму служить для додаткового забезпечення надійності шифру. Цей аргумент, розрахований на дилетантів. Насправді, якщо алгоритм відомий розробникам, він вже не може вважатися секретним, якщо тільки користувач і розробник - не одна особа. До того ж, якщо внаслідок некомпетентності або помилок розробника алгоритм виявився нестійким, його секретність не дозволить перевірити його незалежним експертам. Нестійкість алгоритму виявиться тільки тоді, коли він буде вже зламаний, а то і взагалі не виявиться, бо противник не поспішає хвалитися своїми успіхами. Тому криптограф повинен керуватися правилом, вперше сформульованим Керкхоффом: стійкість шифру повинна визначатися тільки секретністю ключа. Іншими словами, правило Керкхоффа полягає в тому, що весь механізм шифрування, крім значення секретного ключа апріорі вважається відомим противнику.

Всі методи шифрування можна розділити на дві групи: шифри з секретним ключем і шифри з відкритим ключем.

Перші характеризуються наявністю деякої інформації (секретного ключа), володіння якою дає можливість як шифрувати, так і розшифровувати повідомлення. Тому вони іменуються також одноключовими. Шифри з відкритим ключем - наявність двох ключів: відкритого та закритого; один використовується для шифрування, інший для розшифровки повідомлень. Ці шифри називають також двоключовими.

Цей тип шифрів має наявність певної інформації (ключа), володіння якою дозволяє як зашифрувати, так і розшифрувати повідомлення. З одного боку, така схема має такі недоліки, як необхідність окрім відкритого каналу для передачі шифрограми наявність також секретного каналу для передачі ключа, а крім того, при витоку інформації про ключ, неможливо довести, від кого з двох кореспондентів стався витік.

З іншого боку, серед шифрів саме цієї групи є єдина в світі схема шифрування, що володіє абсолютною теоретичною стійкістю. Всі інші можна розшифрувати хоча б у принципі. Такою схемою є звичайна шифровка

(наприклад, операцією XOR) з ключем, довжина якого дорівнює довжині повідомлення. При цьому ключ повинен використовуватися тільки раз. Будь-які спроби розшифрувати таке повідомлення марні, навіть якщо є апріорна інформація про текст повідомлення. Здійснюючи підбір ключа, можна отримати в результаті будь-яке повідомлення.

Шифри з відкритим ключем, на увазі наявність двох ключів - відкритого та закритого; один використовується для шифрування, інший для розшифровки повідомлень. Відкритий ключ публікується - доводиться до відома всіх бажаючих, секретний ключ зберігається у його власника і є запорукою секретності повідомлень. Суть методу в тому, що зашифроване повідомлення за допомогою секретного ключа може бути розшифровано лише за допомогою відкритого і навпаки. Ці ключі генеруються парами і мають однозначну відповідність один одному. Причому з одного ключа неможливо обчислити інший.

Характерною особливістю шифрів цього типу, яка значно відрізняє їх від шифрів з секретним ключем, є те, що секретний ключ тут відомий лише одній людині, у той час як у першій схемі він повинен бути відомий принаймні двом. Це дає такі переваги:

Не потрібно захищений канал для пересилання секретного ключа, весь зв'язок здійснюється з відкритого каналу;

Наявність єдиної копії ключа зменшує можливість його втрати і дозволяє встановити чітку персональну відповідальність за збереження таємниці;

Наявність двох ключів дозволяє використовувати дану шифрувальну систему в двох режимах - секретний зв'язок і цифровий підпис.

Криптографічний захист відносно дешевий, а засоби її подолання або дуже дорогі, або взагалі не існують.

Криптосистема не може вважатися надійною, якщо не відомий повністю алгоритм її роботи. Тільки знаючи алгоритм, можна перевірити, чи стійкий захист. Однак перевірити це може лише фахівець, та й то найчастіше така перевірка настільки складна, що буває економічно недоцільна.

Щоб продавати засоби інформаційного захисту, необхідна сертифікація. Такі положення діють в більшості країн.

Для сертифікації необхідною умовою є дотримання стандартів при розробці систем захисту інформації. Стандарти виконують подібну функцію. Вони дозволяють, не проводячи складних, дорогих і навіть не завжди можливих досліджень, отримати впевненість, що даний алгоритм забезпечує надійний захист в достатній мірі.

Активний захист - найефективніший в тих випадках, коли точно відоме джерело загрози для інформації. Якщо це так, то застосовуються активні заходи проти спроб отримати доступ до інформації. Наприклад, такі:

Пошук і виведення з ладу пристроїв для прихованого зняття інформації;

Виявлення і затримання осіб, що встановлюють такі пристрої або здійснюють інші незаконні дії з доступу до інформації;

Виявлення можливих каналів витоку або несанкціонованого доступу до інформації;

Створення помилкових потоків інформації з метою маскування справжніх потоків і відволікання сил супротивника на їх дешифрування;

Демонстрації противнику можливостей захисту (не обов'язково істинних) для створення в нього враження безперспективності спроб подолати захист;

Контррозвідувальні заходи з метою отримати відомості про те, як саме противник отримує доступ до інформації та відповідної протидії.

Активне радіотехнічне маскування передбачає формування і випромінювання в безпосередній близькості від ОТ маскуючого сигналу. Розрізняють енергетичні і неенергетичні методи активного маскування. При енергетичному маскуванні випромінюється широкосмуговий шумовий сигнал з рівнем, який істотно перевищує, у всьому частотному діапазоні, рівень випромінювань ПК. Одночасно відбувається наводка шумових коливань в ланцюги, які відходять. Можливості енергетичного активного маскування можуть бути реалізовані тільки в разі, якщо рівень випромінювань ПК істотно менший норм на допустимі радіоперешкоди від засобів ОТ. В іншому разі

пристрій активного енергетичного маскування буде створювати перешкоди для різних радіопристроїв, які розташовані поблизу від захищуваного засобу ОТ, і необхідно буде узгодження його установки зі службою радіоконтролю.

При установці такого пристрою необхідно переконатися в достатності заходів захисту, так як в його частотній характеристиці можливі провали. Для цього буде потрібно залучення фахівців із відповідною вимірювальною апаратурою.

Пропонується неенергетичний, метод активного маскування, що є для більшості малих і середніх фірм оптимальним способом ЗІ з точки зору ціни, ефективності захисту і простоти реалізації.

Метод активного маскування полягає у зміні ймовірнісної структури сигналу, що приймається приймачем зловмисників, шляхом випромінювання спеціального маскуючого сигналу. Вихідною передумовою в даному методі є випадковий характер електромагнітних випромінювань ПК.

Для опису цих випромінювань використовується теорія марківських випадкових процесів. В якості імовірнісних характеристик застосовуються матриці ймовірностей переходів і вектор абсолютних ймовірностей станів. Сформований за допомогою оригінального алгоритму сигнал випромінюється в простір компактним пристроєм, який може встановлюватися як на корпусі самого ПК, так і в безпосередній близькості від нього. Рівень випромінюваного цим пристроєм маскуючого сигналу не перевершує рівня інформативних електромагнітних випромінювань ПК, тому узгодження установки маскуючого пристрою зі службою радіоконтролю не потрібне. Більш того, подібні пристрої на відміну від пристроїв активного енергетичного маскування не створюють відчутних перешкод для інших електронних приладів, що знаходяться поруч з ними, що також є їх незаперечною перевагою. Установка і включення пристроїв активного маскування, що реалізують цей метод, можуть бути проведені без будь-яких трудомістких монтажних робіт.

Пристрій не вимагає кваліфікованого обслуговування, його надійна робота гарантується вбудованою схемою контролю працездатності. Слід зазначити, що

у випадках: доопрацювання пристроїв ОТ, електромагнітного екранування приміщень та активного енергетичного маскування - показником захищеності є відношення сигнал / шум, що забезпечується на межі мінімально допустимої зони безпеки.

Максимально допустиме відношення сигнал / шум розраховується в кожному конкретному випадку за спеціальними методиками. За активного радіотехнічного маскування з використанням неенергетичного методу як показника, що характеризує захищеність, застосовується матриця ймовірностей переходів. У випадку ідеальної захищеності ця матриця буде відповідати матриці ймовірностей переходів шумового сигналу, всі елементи якої рівні між собою.

3.3 Оцінювання ефективності захисту інформаційної системи

При створенні більшості ІС виникає необхідність розв'язувати задачу розробки ІС з мінімальною вартістю. Вартість створення подібних систем практично найчастіше пропорційна ступеню використання колективних ресурсів. Це означає, що з метою мінімізації вартості ІС доцільно створювати колективний ресурс для всіх її користувачів - юридичних і фізичних осіб, включаючи засоби зберігання інформації, програмні та апаратні засоби її обробки і доступу до інших засобів і систем. Вдало вибрані організація і можливість колективного ресурсу значно знижують вартість створення й експлуатації ІС при реалізації заданих вимог до її функціонування.

Проте зберігання і обробка інформації з використанням можливостей колективного ресурсу не означає, що кожному користувачу ІС доступні ці можливості. Доступність визначається правилами, що формулюються при створенні ІС.

Однак першим все ж є питання: потрібен захист інформації в системі взагалі чи ні. Тільки потім виникає друга задача - визначити величину витрат на захист. Звичайно, для вирішення цих питань розроблено чимало методів,

методик і навіть програмних продуктів. Нижче розглядається один з можливих підходів.

Отже, рішення про необхідність захисту приймається на основі оцінок за двома напрямками:

1) наявність конфіденційної інформації ;

2) небезпека її витоку - економічна необхідність (доцільність) захисту конфіденційної інформації.

Розглянемо метод, призначений для проведення загальної і часткової оцінок, що дозволяють керівникові організації (фірми) прийняти обґрунтоване рішення про необхідність захисту конфіденційної інформації, що циркулює усередині організації (фірми), від конкурентів, з оцінкою майбутніх витрат на захист. Цей підхід допомагає швидко і досить об'єктивно провести експрес-оцінку необхідності захисту конфіденційної інформації і на її основі оперативно прийняти відповідне рішення, тобто він дозволяє керівнику уникнути великих комерційних невдач і втрат прибутку через доступність інформації конкурентам без тривалого шляху навчання на власних помилках і втратах.

Рішення про необхідність захисту конфіденційної інформації, що циркулює усередині фірми, повинно прийматися керівництвом організації (фірми), й у першу чергу її засновником. Ніхто не зацікавлений такою мірою в захисті секретів фірми і ніхто так не знає усієї сукупності циркулюючої на фірмі інформації, її ступеня таємності, внутрішньої і зовнішньої обстановки, як її засновник.

Отже, перша частина методу дає змогу на основі обробки результатів анкетного опитування принципово відповісти на запитання, потрібно чи не потрібно захищати інформацію, що циркулює на фірмі, а друга частина, у випадку позитивного вирішення першого питання, допомагає приблизно оцінити витрати на майбутній ЗІ.

З огляду на зацікавленість і компетентність засновника фірми, запропонований метод максимально враховує знання, досвід і думку самого

засновника фірми. В основу першої частини методу покладено анкетне опитування з наступною обробкою його результатів.

Для реалізації даного методу розроблено перелік анкетних питань для засновника фірми, що охоплює всі сторони діяльності фірми, пов'язані з циркулюючою на ній інформацією.

Питання анкети сформульовано таким чином, що вони не вимагають великих відповідей, а зводяться до односкладових відповідей «так», «ні». Заповнення анкети не вимагає спеціальної підготовки у сфері ЗІ і не викликає труднощів та великих часових витрат. Спеціальні знання щодо ЗІ враховані при розробці анкетних питань і при наступній обробці результатів опитування за участю фахівців із ЗІ.

Кількісна оцінка про стан і необхідність додаткового захисту отримується шляхом математичної обробки відповідей на анкетні питання. З цією метою кожному питанню анкети поставлена у відповідність вагова величина, що чисельно виражає частковий внесок змісту питання в загальну систему захисту конфіденційної інформації. Значення вагових коефіцієнтів отримані експертним методом заздалегідь.

При обробці результатів анкетного опитування можна одержати як загальну оцінку стану захисту на фірмі, так і ряд часткових оцінок за напрямками захисту. Сукупність усіх оцінок допомагає керівнику в кінцевому рахунку прийняти рішення про необхідність організації захисту шляхом проведення режимних, організаційних і технічних заходів.

На основі аналізу оцінок кожної складової захисту виявляються ті її ланки, де ЗІ не забезпечений й імовірність її перехоплення конкурентом (витік) неприпустимо висока. Провівши такий аналіз, керівник фірми може цілеспрямовано проводити роботи з усунення витоку інформації за виявленими напрямками.

Як приклад розглянемо анкету, що використовувалася для вирішення питання необхідності захисту інформації у вищих навчальних закладах.

Порядок проведення оцінок першої частини методики є таким. На першому етапі зацікавлена в ЗІ сторона в особі засновника (керівника) фірми заповнює анкету, відповідаючи на її питання, наведені в табл. 3.1. Відповіді на питання анкети у формі «так» чи «ні» заносяться у графу 5 проти відповідних питань.

Таблиця 3.1

Анкета вирішення питання необхідності захисту інформації у вищих навчальних закладах.

№	Питання анкети	Часткові коефіцієнти		Відповіді ні	Часткові	Загальна
		для загальних оцінок	для часткових оцінок			
1	2	3	4	5	6	7
Рівень конкуренції						
1	1) чи конкурентоспроможне Ваше навчання на внутрішньому ринку?	3,5	35			
	2) чи конкурентоспроможне Ваше навчання на зовнішньому ринку?	5,0	50			
	3) чи є монопольним Ваше навчання на внутрішньому ринку?	1,5	15			
Ступінь конфіденційності інформації, яка циркулює в закладі						
2	1) чи є інформація, призначена тільки особам верхньої ланки управління?	11,0	55			
	2) чи є інформація, призначена обмеженому колу осіб, які виконують конкретні операції та завдання?	5,0	25			
	3) чи є інформація обмеженої доступності тільки працівникам закладу?	4,0	20			

Продовження таблиці 3.1

1	2	3	4	5	6	7
Час "старіння" конфіденційної інформації						
3	1) чи має конфіденційність довготривалий характер (рік та більше)?	5,0	50			
	2) чи має конфіденційність короткотривалий характер (місяць та більше)?	4,0	40			
	3) чи має конфіденційність оперативний характер (до місяця)?	1,0	10			
Режимні та організаційні заходи						
4	1) чи враховуються інтереси збереження таємниці закладу при кадровому відборі верхньої ланки управління?	5,8	15			
	2) те саме при підборі осіб, допущених до конфіденційної інформації?	4,7	20			
	3) те саме при кадровому відборі штатного персоналу закладу в цілому?	3,5	15			
	4) чи налагоджений контроль за зберіганням працівниками закладу комерційної таємниці?	3,8	15			
	5) чи забезпечена охорона закладу і конфіденційної документації, яка містить комерційну таємницю?	4,2	15			
	6) чи є можливим доступ «недопущених» осіб до засобів розмноження та обробки інформації?	4,3	10			

Продовження таблиці 3.1

1	2	3	4	5	6	7
Устаткування службових приміщень технічними засобами						
5	1) телефонними апаратами?	2,5	8,5			
	2) переговорними пристроями?	1,5	5			
	3) датчиками пожежної та охоронної сигналізації?	0,6	3			
	4) електричними та електронними годинниками?	0,8	2,5			
	5) абонентськими гучномовцями?	0,9	3			
	6) телефонними апаратами з авто-набором і концентраторами, які використовуються в системах зв'язку?	1.5	5			
	7) установками прямого телефонного зв'язку?	1,3	4,5			
	8) радіоприймачами?	1,5	5			
	9) телевізорами?	1,5	5			
	10) магнітофонами?	0,5	1,5			
	11) диктофонами?	0,5	1,5			
	12) установкою оперативного зв'язку?	1,5	5			
	13) телефаксами?	2,2	7,5			
	14) персональними ЕОМ?	3,0	10			
	15) відеомагнітофонами?	0,9	3			
	16) автоматичною телефонною станцією?	3,0	10			
	17) радіотелефоном?	1,5	5			
	18) чи організовано технічний захист у закладі?	4,5	15			

На другому етапі із залученням консультанта проводиться аналіз результатів опитування. Якщо відповідь на питання відповідає збільшенню небезпеки витоку інформації, то в графі 6 табл. 3.1. проставляється знак «+», в іншому разі проставляється знак «-».

На третьому етапі проводиться підсумовування часткових коефіцієнтів графи 7, що відповідають знаку «+», із усіх питань анкети. Результат підсумовування є загальною оцінкою (G) для ухвалення рішення про необхідність захисту конфіденційної інформації на фірмі в цілому. При цьому, якщо загальна оцінка G дорівнює чи більша 50 ($G > 50$), то захист необхідно проводити в усіх напрямках.

Якщо загальна оцінка G більша 20, але менша 50 ($50 > G > 20$), то ймовірність витоку інформації досить велика, необхідно провести часткові оцінки, захист необхідний за окремими напрямками. Якщо загальна оцінка менша 20 ($G < 20$), то ймовірність витоку інформації мала і додатковий захист інформації можна не проводити. На четвертому етапі проводиться аналіз за допомогою часткових оцінок по всіх 5 пунктах опитувальної анкети. Для одержання часткових оцінок проводять підсумовування часткових коефіцієнтів графи 6 табл. 3.1., позначених знаком «+», для кожного пункту окремо. При цьому вийде п'ять часткових оцінок:

1) по пункту 1 - оцінка конкурентоспроможності продукції (послуг)- G,;
2) по пункту 2 - оцінка ступеня конфіденційності інформації - G_2;
3) по пункту 3 - оцінка тимчасових характеристик конфіденційності інформації - G_3;
4) по пункту 4 - оцінка ЗІ режимними й організаційними методами - G_4;
5) по пункту 5 - оцінка можливості витоку інформації через технічні засоби- G_s.

Якщо часткова оцінка по кожному з пунктів 1-3 дорівнює чи більша 20 ($G_1,G_2,G_3 > 20$), то це підтверджує необхідність ЗІ.

Якщо часткова оцінка по кожному з пунктів 6, 7 дорівнює чи більша 20 (G_4, $G_5 > 20$), то це вказує на необхідність проведення ЗІ режимними й організаційними методами або за допомогою технічних засобів захисту

відповідно. У тому випадку, якщо часткова оцінка по одному з пунктів 3-5 менша 20 (G_1, G_2, $G_3 < 20$), то ЗІ можна не проводити.

Таким чином, на основі проведених оцінок, керівник фірми приймає рішення про необхідність робіт з організації ЗІ.

Цілком природно, що перед керівником фірми постає інше дуже важливе питання про майбутні витрати на організацію ЗІ. Це питання вирішується за допомогою другої частини методу.

Друга частина методу призначається для визначення орієнтовної оцінки очікуваних витрат, пов'язаних із захистом конфіденційної інформації. У загальному випадку витрати на ЗІ складаються з витрат на проведення організаційно-режимних і технічних заходів. У свою чергу, витрати на технічний захист складаються з витрат на проведення захисту мовної інформації і на захист інших видів інформації, зокрема, дискретної, оброблюваної на ЕОМ, телеграфного, факсимільного й інших видів, використовуваних у діяльності фірми.

Витрати на режимні й організаційні заходи ЗІ визначаються головним чином заробітною платою працівників режимних підрозділів (груп), що забезпечують організацію і контроль режимних заходів, які підвищують безпеку інформації. Розрахунок цих витрат цілком перебуває у віданні керівника фірми й труднощів не викликає. Витрати на ТЗІ складаються з витрат на проведення досліджень, що дають змогу виявити канали витоку інформації, визначити способи її захисту, і з очікуваних витрат на реалізацію технічних рішень захисту.

Розрахунок вартості захисних заходів кожного з видів інформації має деякі особливості, але на етапі орієнтовних розрахунків можна використовувати методику захисту мовної інформації як найбільш просту і загальну. Така методика, що є другою складовою загальної методики оцінки, розроблена і представлена нижче. З огляду на те, що методика призначена для проведення експрес-оцінки вартості ЗІ, що дає змогу керівнику фірми грубо оцінити майбутні витрати, вона максимально спрощена і передбачає проведення

елементарних розрахунків. З цією метою все технічне устаткування, що може бути встановлене на об'єкті (фірмі) і через яке можливий витік інформації, умовно розділено на три групи. Критерієм такого розподілу обрана частка (відсоток) витрат на захист устаткування від вартості самого устаткування (техніки). Часткові коефіцієнти ($К_1$, $К_2$, $К_3$), визначені експертним шляхом, та перелік технічного устаткування по групах із зазначенням значень часткових коефіцієнтів витрат на захисні заходи наведено в табл. 3.2.

У таблиці позначено: $С_1$, $С_2$, $С_3$ - сумарна вартість технічного устаткування відповідної групи, встановленого на об'єкті (фірмі). Значення вартості зразків техніки, які знаходяться в приміщеннях фірми, визначаються за каталогами діючих цін виробника даної техніки.

Таблиця 3.2

Таблиця сумарної вартості

Група	Перелік обладнання	Частка (відсоток) витрат на ЗІ від витоку інформації	Частка (відсоток) витрат на профілактичний контроль ефективності ЗІ
1	Телефонні апарати; переговорні пристрої; датчики пожежної та охоронної сигналізації; електричні та електронні годинники; абонентські гучномовці	$К_1=0,7С_1$	
2	Автонабори і концентратори, які використовуються в системах зв'язку; установки прямого телефонного зв'язку; радіоприймачі; телевізори; магнітофони; диктофони	$К_2=0,3С_2$	$\mathbf{К}_{проф}$ =(0,03-0,1) від ($С_1+С_2+С_3$)
3	Пульти оперативного зв'язку до 100 номерів; персональна комп'ютерна техніка; відеомагнітофони; АТС на 100- 1000 номерів	$К_3=0,13С_3$	

Вартість технічного захисту всього устаткування ($С_{тз}$), що складається з техніки різних груп, визначається за формулою:

$$С_{тз} = С_1К_1 + С_2К_2 + С_3К_3.$$

Зазначимо, що у табл. 3.2. подано вартість захисту устаткування, не призначеного для передачі, обробки і збереження конфіденційної інформації.

Вартість захисту устаткування, призначеного для обробки конфіденційної інформації, визначається індивідуально і може істотно перевищувати зазначену в табл. 3.2.

Вартість щорічного профілактичного контролю визначається за формулою:

$$\mathbf{C}_{\text{проф}} = \mathbf{К}_{\text{проф}}\, \mathbf{C}_{\text{тз}}$$

де $\mathbf{C}_{\text{проф}}$=(0,03-0,1) - коефіцієнт витрат на щорічний профілактичний контроль ефективності ЗІ, визначений дослідним шляхом.

Таким чином, знаючи перелік і кількість встановленого на фірмі технічного устаткування і його вартість, можна легко розрахувати очікувані витрати на ЗІ технічними засобами. Додавши витрати на режимні й організаційні заходи ($C_{роз}$) і на профілактичний контроль у перший рік функціонування, одержимо загальні витрати на ЗІ ($C_{заг}$):

$$C_{заг} = C_{тз} + C_{роз} + C_{проф.}$$

Отже, на основі отриманої величини, а також маючи на увазі прибуткові можливості організації, керівництво приймає рішення щодо певних заходів із захисту інформації в організації.

Не менш важливою є проблема оцінки рівня захищеності уже створеної і навіть функціонуючої СЗІ.

З урахуванням моделей порушника для систем різного призначення і різних вимог повинні існувати різні критерії оцінки достатності захисних заходів. Порушник-професіонал може перебувати поза об'єктом захисту, і йому спочатку необхідно подолати контрольовану межу об'єкта. Порушник-користувач уже має певні повноваження щодо санкціонованого доступу до інформації відповідно до своїх функціональних обов'язків і завдань.

Аналіз об'єктів ІС починається з визначення можливих каналів НСД (МКНСД). Найбільш об'єктивним процесом оцінки доцільно розглянути МКНСД, що очікуються від кваліфікованого порушника-професіонала, який знаходиться на початковій позиції поза об'єктом захисту. У такому разі оцінка буде відрізнятися меншою кількістю МКНСД, ніж у порушника більш низького

класу, а також імовірністю подолання порушником захисних бар'єрів, кількістю шляхів, ймовірностями їх обходу.

Після того як для обраної моделі порушника визначено всі МКНСД і на них встановлено засоби захисту, вважається, що віртуальний контур захисту замкнуто. Тоді для контрольованого МКНСД визначається його вразливість, величина якого буде дорівнювати вразливості найбільш слабкої ланки захисного контуру, для чого використовуємо формулу

$$P_{сзik} = 1 - P_{вбл}(1 - P_{відм}) \cup P_{обх1} \cup P_{обх2} \cup \ldots \cup P_{обхj}, \quad (3.1)$$

де $P_{В}$ бл - імовірність виявлення і блокування несанкціонованих дій порушника, Рвідм - імовірність відмови системи, Робхj- імовірність обходу порушником j-і перешкоди. Ця формула виражає вразливість захисту К-і ланки захисту шляхом порівняння ймовірностей і вибору однієї з них. При цьому для МКНСД, які закриті двома або більше засобами захисту, розрахунок вразливості ланки здійснює за формулою

$$P = \prod_{i=1}^{m} P_i, \quad (3.2)$$

де т - кількість дублюючих перешкод, P_i - вразливість і-ї перешкоди. Для неконтрольованих МКНСД розрахунок здійснюється за формулою

$$P_{сзі} = P_{пр} \cup P_{обх1} \cup P_{обх2} \cup \ldots \cup P_{обхj}, \quad (3.3)$$

де j - кількість шляхів обходу.

Оцінка вразливості системи ідентифікації та автентифікації (СІА) здійснюється за формулою (3.1) з урахуванням таких параметрів:

Ймовірність подолання перешкоди порушником з боку законного введення в систему.

Імовірність виявлення і блокування НСД в СІА. Вона визначається можливістю відповідної програми до відпрацювання даної функції у випадку розбіжності.

Оцінка вразливості системи розмежування і контролю доступу у приміщеннях об'єкта захисту Рпр, визначається виходячи з технічних даних вхідного замка на дверях приміщення, режиму роботи КСА, наявності охоронної сигналізації і значення її параметрів. При цілодобовому режимі роботи, як правило, обмежуються кодовим замком на дверях. При перервах у роботі, коли у приміщенні нікого не повинно бути, апаратура вимикається, приміщення ставиться на дистанційний централізований контроль охоронної сигналізації (про оцінку її вразливості йтиметься нижче).

Імовірність обходу перешкоди порушником Робх слід оцінювати безпосередньо на місці, тобто шляхом огляду приміщення на предмет вразливості стін і відсутності сторонніх люків, пошкоджень стін, стелі, вікон. Особливу увагу необхідно звернути на розміщення вікон і конструкцію їх рам, кватирок, замків, поверховість приміщення, вентиляцію. Якщо приміщення знаходиться на першому поверсі, на вікнах необхідно перевірити установку датчиків охоронної сигналізації.

При оцінці вразливості системи контролю виведення апаратури з робочого контуру обміну інформацією під час ремонту і профілактики технічних засобів вважається, що спроба порушника, який знаходиться в зоні об'єктів ІС, що відрізняється від зони робочого місця функціонального контролю (РМФК), ввести його знову в робочий контур ІС малоймовірна. Значить, можна прийняти $Р_{пр} = 0$. Але можливість обходу цього заходу в порушника існує.

Як показує практика, найбільш вразливим місцем для НСД є носії ПЗ і носії інформації. Цьому сприяє уніфікована конструкція носіїв, відносно невеликі габаритні розміри і маса, великі обсяги інформації, яка зберігається на них, збереження і транспортування на них ОС і прикладних програм.

Особливістю засобів захисту інформації на носіях є необхідність враховувати (залежно від технічного завдання) імовірність потрапляння носія з інформацією за межі об'єкта захисту, в зону, де відсутні засоби виявлення і блокування НСД. Вразливість захисту в таких випадках повинна збільшуватись і досягати такої величини, коли час подолання захисту порушником буде

більшим, ніж час життя інформації, яка розміщена на носіях. Тому оцінка повинна проводитися за окремим показником.

Для захисту інформації і ПЗ на носіях використовуються організаційні, апаратні, програмні і криптографічні засоби.

Засоби реєстрації звертань до інформації, яку необхідно захищати, є достатньо ефективним заходом, який також потребує оцінки якості: виконання програми реєстрації (чи всі звертання реєструються, з якими атрибутами), імовірності її обходу користувачем-порушником, можливості прихованого відключення, часу роботи, безвідмовності.

Однак реєстрація подій з відкладеним виявленням більше служить для профілактичних цілей і подальшого аналізу конкретної ситуації, у зв'язку з чим цей захід слід вважати хоча й обов'язковим, але все ж резервним, тобто тим, що дублює інші заходи захисту.

Засоби управління захистом інформації в ІС виконують функції захисту і є важливою складовою засобів захисту. Управління забезпечує функції контролю, виявлення і блокування НСД, а також безперебійне функціонування апаратних, програмних і організаційних засобів захисту, ведення статистики і прогнозування подій. Усі ці параметри враховуються при оцінці вразливості окремих засобів захисту ІС. У результаті оцінка ефективності засобів управління захистом може проводитися лише з якісного боку на предмет реалізації захисту як єдиного механізму - СЗІ в технічному сенсі розв'язання задачі: технології управління, складу апаратних і програмних засобів управління і організаційних заходів, наявності централізації контролю і управління захистом.

Така оцінка необхідна для визначення ступеня наближення отриманих значень вразливості захисту до дійсних. Чим більше автоматизованих засобів захисту, тим менше експертних оцінок, достовірніші оцінки і вищі гарантії ефективності захисту.

Висновки до третього розділу

Складність і масштаби сучасних систем захисту не дають змоги проводити експерименти з ними, а експерименти з окремими елементами не дозволяють отримати уявлення про цілісні властивості систем. Розв'язання задач оцінки ефективності захисту ускладнюється тим, що в будь-якій системі захисту основною ланкою є людина. Крім того, великі проблеми при створенні точних аналітичних методів розрахунку й оцінки ефективності роботи систем захисту полягають у визначенні складних залежностей між середовищем функціонування ІС, станом джерел інформації та системою захисту.

Залежно від співвідношення ресурсів, що виділяються на захист, та очікуваних результатів від її розв'язання задача синтезу оптимальних СЗІ може формулюватися в таких формах:

1. При фіксованому рівні витрат ресурсів забезпечити максимально можливий рівень захищеності.
2. При фіксованому рівні захищеності мінімізувати витрати на захист.

Однак сьогодні техніко-економічна оптимізація систем захисту дуже складна і далека від вирішення проблема. Незважаючи на це, вона все ж має переваги, а саме:

можливість отримання коректного математичного розв'язку задачі за обраним критерієм якості;

можливість за допомогою сформульованих обмежень зрозуміти суть реальних процесів захисту;

виявити в процесі оптимізації протиріччя у вимогах до системи захисту;

можливість давати прогнозні оцінки у разі зміни умов функціонування;

підвищити ефективність управління системою захисту.

До недоліків оптимізації систем захисту слід віднести:

складність математичної постановки задач проектування оптимальної системи захисту;

суттєву залежність якості оптимальної системи захисту від точності вихідних припущень та характеру змін.

Основна проблема оцінювання інформаційної безпеки полягає у відсутності повноти даних. Але повнота інформації може складатися з тих фактів, які надають, наприклад, антивірусні програми, файли звітів, системи сканування і звіти з безпеки від співробітників. Таким чином, необхідні критерії оцінювання та методи аналізу.

Розділ 4
ОСНОВНІ НАПРЯМКИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ВІД ВНУТРІШНІХ ЗАГРОЗ

Успішне вирішення комплексу завдань із захисту інформації від внутрішніх загроз не може бути досягнуто без створення єдиної основи, так званого «активного кулака» підприємства, здатного концентрувати всі зусилля та наявні ресурси для виключення витоку конфіденційної інформації і недопущення можливості нанесення шкоди підприємству. Таким «кулаком» покликана стати система захисту інформації на підприємстві, створювана на відповідній нормативно-методичній основі і яка відображає всі напрямки та специфіку діяльності даного підприємства.

4.1. Основні підходи та вимоги до вдосконалення захисту інформації

Оскільки внутрішні загрози знаходяться в лідерах інформаційних загроз, відсунувши на другий план традиційних лідерів – хакерські атаки і віруси, то захист інформаційних ресурсів підприємства необхідно зосередити на ліквідацію саме цих загроз.

Джерела внутрішніх загроз безпеки інформації, що циркулює на підприємстві, діляться на три групи:

загрози, обумовлені діями персоналу;

загрози, обумовлені технічними засобами;

загрози, обумовлені стихійними джерелами.

Це означає що основними напрямками вдосконалення захисту інформації на підприємстві від внутрішніх загроз є:

Стосовно персоналу:

Ретельний підбір персоналу (відсутність судимостей, досвід роботи, неприналежність до конкуруючих підприємств і т.д.);

Навчання при використанні нових програмних та технічних продуктів, ознайомлення з технікою безпеки, вивчення своїх службових обов’язків та політики інформаційної безпеки підприємства.

Наділення власного та допоміжного персоналу, відповідними правами доступу до інформації;

Розробка переліку програмних засобів які необхідні для виконання службових обов’язків;

Регулярне проведення роз’яснювальних заходів щодо важливості захисту інформації на підприємстві;

Мінімізація конфліктних ситуацій в колективі;

Забезпечення працівників гідними умовами праці, заробітною платою, відпустками, кар’єрним ростом;

Використання системи розмежування доступу до інформації з використанням паролів, магнітних ключів, біометричних систем;

Використання програмних засобів для контролю трафіку;

Ведення журналів реєстрації НСД до інформації, спроб її модифікації, знищення чи передачі;

Використання систем відео спостереження для контролю за роботою працівників;

Необхідно не допускати передачу по електронній пошті чи копіювання інформації на власні носії працівників чи викрадення носіїв підприємства;

Робота з інформацією повинна проводитися виключно на робочому місці і не повинна видаватися для обробки чи ознайомлення за межами підприємства;

Використання для переговорів, нарад, на яких можлива наявність інформації яка потребує захисту, спеціально обладнаних кімнат, з метою запобігання випадкового ознайомлення персоналу без відповідних прав доступу;

Не допускати встановлення неліцензійного ПЗ, а також ПЗ не призначеного для виконання службових обов’язків;

Необхідно розробити систему штрафів та покарань за порушення ПІБ та службових обов’язків в рамках законодавства України;

При звільненні працівників необхідно дотримуватися принципу “безболісного звільнення”.

Стосовно технічних та програмних засобів, а також паперових носіїв:

Використання оригінальних програмних та технічних засобів приймання, обробки, зберігання та передачі інформації;

Своєчасне оновлення технічних та програмних засобів призначених для роботи з інформацією котра потребує захисту, а також оновлення компонентів СЗІ;

Виконання атестації СЗІ на відповідність вимогам ЗІ;

Використання ліцензійних програмних та технічних засобів захисту;

Використання шифрування інформації, у разі порушення цілісності ІС;

Екранування компонентів ІС та, в разі необхідності, застосування елементів активного захисту;

Використання непрозорих штор чи жалюзі на вікнах кімнат, де наявна інформація з обмеженим доступом;

Використання спеціально захищених кімнат для розміщення серверів;

Використання засобів безперебійного живлення;

Регулярне проведення резервного копіювання даних та створення резервних копій ОС;

Інформацію на дрібних носіях (флеш-накопичувачі, оптичні чи магнітні диски тощо), а також на паперових носіях необхідно зберігати в сейфах;

У разі наявності на підприємстві великої кількості інформації на паперових носіях, необхідне створення підрозділу, відповідального за внесення до архіву, збереження, видачу та знищення документів;

Необхідно забезпечити захист для самої СЗІ;

Після закінчення життєвого циклу компонентів ІС, необхідно провести копіювання наявної на них інформації з подальшим її знищенням з носія;

Документи, термін дії яких минув, необхідно знищити відповідно до способу збереження;

Стосовно стихійних джерел:

Встановлення пожежної сигналізації;

Сейфи для збереження носіїв інформації мають бути герметичними та повинні витримувати високі температури;

Встановлення систем аварійного відключення водо та електропостачання.

Для випадків, коли загроза реалізована, необхідно вчасно відреагувати та, якнайшвидше, забезпечити ліквідацію наслідків реалізації загрози.

Основні принципи вдосконалення захисту інформації:

Принцип комплексного підходу - ефективне використання сил, засобів, способів і методів захисту інформації для вирішення поставлених завдань в залежності від конкретної ситуації, що складається і наявності факторів, що послаблюють або підсилюють загрозу;

Принцип оперативності прийняття управлінських рішень (істотно впливає на ефективність функціонування та гнучкість системи захисту інформації і відображає націленість керівництва і персоналу підприємства на рішення завдань захисту інформації);

Принцип персональної відповідальності - найбільш ефективний розподіл завдань із захисту інформації між керівництвом і персоналом підприємства та визначення відповідальності за повноту і якість їх виконання.

Серед основних умов вдосконалення захисту інформації можна виділити наступні:

Безперервність всебічного аналізу функціонування системи захисту інформації з метою прийняття своєчасних заходів щодо підвищення її ефективності;

Неухильне дотримання керівництвом та персоналом підприємства встановлених норм і правил захисту конфіденційної інформації.

При дотриманні перерахованих умов забезпечується найбільш повне і якісне вирішення завдань щодо захисту конфіденційної інформації на підприємстві.

Для вирішення організаційних завдань зі створення та забезпечення функціонування системи захисту інформації використовуються кілька основних підходів, які виробляються на основі існуючої нормативно-правової бази та з урахуванням методичних розробок з тих чи інших напрямках захисту конфіденційної інформації.

Один з основних підходів до створення системи захисту інформації полягає у всебічному аналізі стану захищеності інформаційних ресурсів підприємства з урахуванням спрямованості конкуруючих організацій до оволодіння конфіденційною інформацією і, тим самим, нанесення шкоди підприємству. Важливим елементом аналізу є робота з визначення переліку захищених інформаційних ресурсів з урахуванням особливостей їх розташування (розміщення) і доступу до них різних категорій співробітників (працівників інших підприємств).

Роботу з проведення такого аналізу безпосередньо очолює керівник підприємства та його заступники за напрямками діяльності. Вивчення захищеності інформаційних ресурсів ґрунтується на позитивному і негативному досвіді роботи підприємства, накопичений протягом останніх кількох років, а також на ділових зв'язках і контактах підприємства з організаціями, які здійснюють аналогічні види діяльності.

При створенні системи захисту інформації, в першу чергу, враховуються найбільш важливі, пріоритетні напрямки діяльності підприємства, які потребують особливої уваги. Перевага також віддається новим, перспективним напрямкам діяльності підприємства, які пов'язані з науковими дослідженнями, новітніми технологіями, що формують інтелектуальну власність, а також розвиток міжнародних зв'язків. Відповідно до названих приорітетів формується перелік можливих загроз інформації, що підлягає захисту, і визначаються конкретні сили, засоби, способи і методи її захисту.

До вдосконалення СЗІ з позиції системного підходу висувається ряд вимог, що визначають цілісність, гнучкість і ефективність СЗІ.

Після вдосконалення СЗІ повинна бути:

централізованою - забезпечує ефективне управління системою з боку керівника та посадових осіб, відповідальних за різні напрямки діяльності підприємства;

плановою - об'єднує зусилля різних посадових осіб та структурних підрозділів для виконання підприємством завдань у сфері захисту інформації;

конкретною і цілеспрямованою - розрахованою на захист абсолютно конкретних інформаційних ресурсів, що представляють інтерес для конкуруючих організацій;

активною - забезпечує захист інформації з достатнім ступенем наполегливості і можливістю концентрації зусиль на найбільш важливих напрямках діяльності підприємства;

надійною і універсальною - охоплює всю діяльність підприємства, пов'язану із створенням та обміном інформацією.

Врахувавши напрямки діяльності підприємства та вимоги до СЗІ, на етапі її проектування чи вдосконалення, можна досягти більш надійного захисту інформації за менші кошти та за менший проміжок часу.

4.2. Основні методи, сили та засоби, що використовуються для вдосконалення організації захисту інформації, на підприємстві, від внутрішніх загроз

Один з найважливіших факторів, що впливають на ефективність системи захисту конфіденційної інформації, - сукупність сил і засобів підприємства, що використовуються для вдосконалення організації захисту інформації.

Сили і засоби різних підприємств відрізняються за структурою, характером і порядком використання. Підприємства, що працюють з конфіденційною інформацією і вирішують завдання щодо її захисту в рамках повсякденної

діяльності на постійній основі, змушені з цією метою створювати самостійні структурні підрозділи і використовувати високоефективні засоби захисту інформації. Якщо підприємства лише епізодично працюють з конфіденційною інформацією в силу її невеликих обсягів, замість створення підрозділів вони можуть включати в свої штати окремі посади фахівців із захисту інформації.

Провідну роль у вдосконаленні організації захисту інформації на підприємстві відіграють керівник підприємства, а також його заступник, який безпосередньо очолює цю роботу.

Керівник підприємства несе персональну відповідальність за організацію і проведення необхідних заходів, спрямованих на вдосконалення захисту інформації, та за витік відомостей, віднесених до конфіденційної інформації, і втрату носіїв інформації. Він зобов'язаний:

знати фактичний стан справ в області захисту інформації, організовувати постійну роботу з виявлення і закриття можливих каналів витоку конфіденційної інформації;

визначати обов'язки і завдання посадовим особам та структурним підрозділам підприємства в цій галузі;

виявляти високу вимогливість до персоналу підприємства в питаннях збереження конфіденційної інформації;

оцінювати діяльність посадових осіб та ефективність заходів із захисту інформації.

Заступник керівника підприємства зобов'язаний постійно вивчати всі сторони і напрями діяльності підприємства для прийняття своєчасних заходів із захисту інформації; керувати роботою служби безпеки (інших структурних підрозділів, що вирішують завдання із захисту інформації); виконувати інші функції із вдосконалення організації захисту інформації в ході проведення підприємством всіх видів робіт.

На підприємствах для вдосконалення організації робіт із захисту інформації можуть створюватися такі основні види структурних підрозділів:

режимно-секретні;

підрозділи з технічного захисту інформації та протидії іноземним технічним розвідкам;

підрозділи криптографічного захисту інформації; мобілізаційні;

підрозділи охорони та пропускного режиму.

Функції, що покладаються на перераховані підрозділи, визначаються рішенням (наказом) керівника підприємства і відображаються у відповідних положеннях.

За рішенням керівника підприємства дані підрозділи організаційно можуть об'єднуватися в службу безпеки, керівник якої в деяких випадках може бути наділений статусом заступника керівника підприємства і повноваженнями посадової особи, яка здійснює керівництво роботою структурних підрозділів підприємства, діяльність яких пов'язана з використанням і захистом інформації.

Режимно-секретний підрозділ, мобілізаційний підрозділ і підрозділ з технічного захисту інформації та протидії іноземним технічним розвідкам створюються на підприємствах, що виконують роботи з використанням відомостей, що становлять державну таємницю (незалежно від наявності на підприємстві іншої інформації з обмеженим доступом).

Режимно-секретний підрозділ є основним структурним підрозділом підприємства і вирішує завдання організації, координації і контролю діяльності інших структурних підрозділів (персоналу підприємства) щодо забезпечення захисту відомостей, що становлять державну таємницю. На підприємствах, які не виконують роботи з відомостями, що становлять державну таємницю, для вирішення аналогічних завдань щодо інших видів інформації з обмеженим доступом створюється і функціонує служба безпеки (служба захисту інформації).

Підрозділ з технічного захисту інформації та протидії іноземним технічним розвідкам вирішує завдання організації і проведення комплексу технічних заходів, спрямованих на виключення або суттєве утруднення добування іноземними розвідками за допомогою технічних засобів відомостей, віднесених до конфіденційної інформації і підлягають захисту.

Підрозділ криптографічного захисту інформації створюється з метою запобігання витоку конфіденційної інформації при її передачі по відкритих каналах (лініях) зв'язку за допомогою технічних засобів, а також при використанні локальних обчислювальних мереж, що мають вихід за межі території підприємства.

Підрозділ охорони та пропускного режиму створюється з метою запобігання несанкціонованого (безконтрольного) перебування на території та об'єктах підприємства сторонніх осіб та транспорту, нанесення збитків підприємству шляхом крадіжок (розкрадань) з території підприємства матеріальних коштів та іншого майна. У деяких випадках для вирішення завдань охорони і пропускного режиму на підприємствах можуть створюватись окремі самостійні підрозділи.

Мобілізаційний підрозділ вирішує завдання всебічної підготовки підприємства до роботи в умовах воєнного часу, заклику і надходження мобілізаційних людських і матеріальних ресурсів.

Крім перерахованих підрозділів підприємства до роботи із вдосконалення організації захисту інформації можуть залучатися й інші структурні підрозділи, для яких виконання заходів з захисту інформації не є основною функцією.

До таких підрозділів відносяться: кадровий орган, орган юридичної служби (юрисконсульт), орган психологічної та виховної роботи, прес-служба підприємства та ін. Особливо необхідно відзначити важливість участі у вдосконаленні організації захисту інформації виробничих, так званих «тематичних» структурних підрозділів (окремих посадових осіб), які створюють продукцію і товари або надають послуги, і в зв'язку з цим самим безпосереднім чином взаємодіють з іншими підприємствами та органами державної влади.

Висновки до четвертого розділу

Для проведення робіт з організації захисту інформації використовуються також можливості різних нештатних підрозділів підприємства, у тому числі колегіальних органів (комісій), що створюються для вирішення специфічних завдань у цій області. У їх числі - постійно діюча технічна комісія, експертна комісія, комісія з розсекречення носіїв конфіденційної інформації, комісія з категоріювання об'єктів інформатизації та ін.

Щоб домогтися максимальної ефективності при вирішенні задач захисту інформації, поряд з можливостями згаданих штатних і позаштатних підрозділів (посадових осіб), необхідно використовувати наявні на підприємстві кошти для вдосконалення захисту інформації.

Ефективне вирішення завдань із вдосконалення організації захисту інформації неможливо без застосування комплексу наявних у розпорядженні керівника підприємства відповідних сил і засобів. Разом з тим визначальну роль у питаннях організації захисту інформації, відіграють методи захисту інформації, що визначають порядок, алгоритм і особливості використання цих сил і засобів у конкретній ситуації.

ВИСНОВКИ

Результатом виконаної роботи є вирішення задачі організації та шляхів удосконалення захисту інформації на підприємстві від внутрішніх загроз, за допомогою різних методів та засобів захисту інформації.

У процесі виконання роботи отримані наступні результати:

1. Дослідження загроз інформаційній безпеці підприємства, вказали на основні джерела та канали витоку інформації. У процесі дослідження було виявлено, що основна частина загроз, інформаційній безпеці підприємства, припадає на внутрішні загрози. Дослідження моделі порушника дало змогу описати потенційних порушників інформаційної безпеки підприємства, визначити послідовність дій під час реалізації загроз, їх мету та мотиви.

2. Дослідження методів та засобів захисту інформації вказало їх переваги та недоліки, а також дало змогу визначити їх ефективність в тих чи інших умовах. Визначено необхідність політики інформаційної безпеки та її види.

3. Сформовані підходи до вибору засобів захисту інформації на підприємстві від внутрішніх загроз, а також підходи до кількісної та якісної оцінки ефективності комплексної системи захисту інформації, що в свою чергу дало змогу виявити слабкі місця в системі захисту інформації та визначити напрямки вдосконалення системи захисту інформації.

4. Запропоновано загальні методи та засоби вдосконалення організації захисту інформації на підприємстві від внутрішніх загроз. Зроблено висновок : забезпечити кращий захист інформації та інформаційних систем, на підприємстві від внутрішніх загроз, може лише застосування комплексу заходів з організації інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Автоматизированные информационные технологии в экономике: Учебник Под ред. Г. А. Титоренко. Москва: Компьютер, ЮНИТИ, 1998. 400 с.
2. Снігерьов О.П., Кухарьонок М.А. Визначення можливих каналів витоку інформації в автоматизованих системах. *Інформаційні технології та захист інформації*. 1998. №1. С.59.
3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Москва: Энергоатомиздат, 1994. 400 с.
4. Головань С.М. Базові вимоги до побудови моделі загроз інформаційних систем. *Інформаційна безпека*. 2009. №1. С.17-25.
5. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів. Запоріжжя, 1998. 144 с.
6. Домарев В.В. Безопасность информационных технологий. Системный подход: Киев: ООО " ТИД ДС", 2004. 992 с.
7. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Част. 3. Методи керування захистом інформаційних технологій. Чинний від 2004-01-01.
8. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. Москва: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с.
9. Ленков С.В., Перегудов А.Д., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. Том I. Несанкционированное получение информации. 464 с.
10. Ленков С.В., Перегудов А.Д., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. Том II. Информационная безопасность. 344 с.
11. Міжнародний стандарт ISO/IEC 17799:2005 Information technology Securitytechniques – Code of practice for information security management.

12. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. Ткачук Т. Шляхи запобігання та протидії промисловому шпигунству. *Бизнес и безопасность*. 2007. №3. С.7.
14. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: підручник. Київ: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.