ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерьскої роботи

на тему:

«ТЕХНОЛОГІЯ СТВОРЕННЯ УНІВЕРСАЛЬНОЇ СИСТЕМИ РОЗРОБКИ ПРАВИЛ ПОЛІТИКИ БЕЗПЕКИ»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
_____ Ярчук А.А._____
(прізвище та ініціали)
Керівник __Кожухівський А.Д.___
(прізвище та ініціали)
Рецензент___
(прізвище та ініціали)
Нормоконтролер _Чумак Н.С___

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібенетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
"___" _____2021 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Ярчуку Андрію Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи «Технологія створення універсальної системи розробки правил політики безпеки»
керівник магістерської роботи Кожухівський А. Д. , к.т.н., _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від « » 2021 р. №

2.Строк подання студентом магістерської роботи 15.12.2021

3. Вихідні дані до магістерської роботи

1. Правила політики безпеки.
2. Законодавство України та міжнародні норми. Стандарти. Рекомендації.
3. Науково-технічна література.
4. Інтернет-ресурси.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Загальні положення про комплексні системи захисту інформації.
2. Склад та зміст основних заходів щодо розробки політики інформаційної безпеки.

3. Порядок здійснення захісту інйормації на об’єктах інформаційної діяльності .
4. Підготовка презентації до захисту.

5. Перелік графічного матеріалу
   1. Об'єкт, предмет і мета роботи та нукові завдання дослідження.
   2. Загальні положення компдексної системи захисту інформації.
   3. Основні підходи до створення системи захисту інформації.
   4. Завдання комплексної системи захисту інформації.
   5. Ризики в системі забезпечення інформаційної безпеки.
   6. Методологія оцінки ризиків інформаційної безпеки.
   7. Розробка політики безпеки.
   8. Результати розробки рекомендацій та атестації щодо розробки політики безпеки.
   9. Висновки.
6. Дата видачі завдання 30.09.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів магістерської роботи	Приміт ка
1.	Уточнення постановки завдання	12.10.2021р.	Вик.
2.	Аналіз технічної літератури	20.10.2021р.	Вик.
3.	Загальні положення комплексної системи захисту інформації	10.11.2021р..	Вик.
4.	Основні заходи для розробки політики інйормаційної безпеки	15.11.2021р.	Вик.
5.	Розробка правил універсальної політики безпеки	25.11.2021р..	Вик.
6.	Реферат, вступ, висновки.	25.11.2021р..	Вик.
7.	Підготовка презентації до захисту.	16.12.2021р..	Вик.

Студент _____ Ярчук А.А.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Кожухівський А.Д .
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА

на магістерську роботу

студента Ярчука Андрія Андрійовича

на тему: «Технологія створення універсальної системи розробки правил політики безпеки»

Актуальність:

У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку. Збереження цілісності, забезпечення безвідмовної доступності, дотримання заздалегідь зазначеного рівня конфіденційності інформаційних ресурсів і зменшення ймовірності несанкціонованого доступу та протиправних дій до цих ресурсів – це і є головною задачею розробки створення універсальної політики безпеки Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. Проведено аналіз нормативно-правової бази в сфері захисту інформації, визначено, основні закони та державні стандарти, які мають бути задіяні в процесі розробки політики безпеки інформації, існуючі технології правил політики безпеки. Визначено предмет, обєкт дослідження, мету роботи.
2. Досліджено основні стратегії захисту інформації, методи оцінки ризиків інформації.
3. Запропоновано варіант варіант атестації та впровадження до експлуатації політики безпеки інформації інформаційно-телекомунікаційної системи.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У роботі бажано було б провести порівняння державних та світових стандартів щодо створення універсальної системи політики безпеки.
2. Запропонований варіант атестації та впровадження до експлуатації політики безпеки інформації інформаційно-телекомунікаційної системи доцільно було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи незначні недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент Ярчук Андрій Андрійович - присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач закладу вищої освіти.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

_____

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Ярчук А.А. до захисту магістерської роботи
Спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
на тему: «**Технологія створення універсальної системи розробки правил політики безпеки»**
Магістерська робота і рецензія додаються.
Директор інституту _____ В.А Савченко.
(підпис)

Довідка про успішність

Ярчук А.А_____за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2016____року до 2021___ року повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Гребенніков А.Б.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент **Ярчук А.А.** обрав тему роботи, метою якої було розробити універсальну систему розробки правил політики безпеки. Перелік використаних джерел свідчить про вміння дипломником розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи **ЯрчукА.А.** показав добру теоретичну та практичну підготовку, вміння вирішувати самостійно питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента **Ярчука Андрія Андрійовича.** на оцінку **«добре»** та присвоїти йому кваліфікацію 3439. Фахівець з організації інформаційної безпеки.

Керівник магістерської роботи _____ Кожухівський А.Д.
(підпис)
“_____” _____ 20 21 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент **Ярчук А.А.**
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри _Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“_____” _____ 2021 рік

РЕФЕРАТ

Текстова частина магістерської роботи: 80 сторінок, 5 рисуноків, 26 джерел.

Об'єкт дослідження – політика безпеки інформаційно-комунікаційних системи та мережі.

Предмет дослідження – технології універсальної системи правил політики безпеки.

Мета роботи – технологія створення розробки правил політики безпеки

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, державних та міжнародних стандартів, їх порівняння, моделювання створення універсальної системи розробки правил політики безпеки.

В роботі проведено аналіз нормативно-правової бази в сфері захисту інформації, визначено, основні закони та державні стандарти, які мають бути задіяні в процесі розробки політики безпеки інформації. Проаналізовано існуючі технології правил політики безпеки.

Наведено загальну характеристику інформаційної діяльності, основні стратегії захисту інформації, методи оцінки ризиків інформації, сформовано загальні положення політики безпеки інформації.

На основі досліджень, проведених в роботі, розроблено варіант атестації та впровадження до експлуатації політики безпеки інформації інформаційно-телекомунікаційної системи.

Галузь використання - кібербезпека інформаційно-телекомунікаційної системи.

ІНФОРМАЦІЙНА БЕЗПЕКА, КСЗІ, ПРИНЦИПИ ПОЛІТИКИ БЕЗПЕКИ, МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, ІНФОРМАЦІЙНА СИСТЕММА, КІБЕРБЕЗПЕКА.

ABSTRACT

Text part of the master's thesis: 80 pages, 5 drawings, 26 sources.

The object of research is the security policy of information and communication systems and networks.

The subject of research is the technologies of the universal system of security policy rules.

The purpose of the work is the technology of creating security policy rules

Research methods - elaboration of literature on this topic, analysis of operational documentation, national and international standards, their comparison, modeling the creation of a universal system for developing security policy rules.

The analysis of the legal framework in the field of information protection is carried out, the basic laws and state standards that should be used in the process of developing information security policy are determined. The existing technologies of security policy rules are analyzed.

The general characteristics of information activity, the main strategies of information protection, methods of information risk assessment are given, the general provisions of the information security policy are formed.

On the basis of the researches carried out in the work, the variant of attestation and introduction to operation of information security policy of information and telecommunication system is developed.

Area of application - cybersecurity of information and telecommunication system.

INFORMATION SECURITY, CCIS, PRINCIPLES OF SECURITY POLICY, INVASION DETECTION METHODS, INFORMATION SYSTEM, CYBER SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЕОМ – електронно-обчислювальна машина;

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КРТ – копіювально-розмножувальна техніка;

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ПЗ – програмне забезпечення;

ТЗІ – технічний захист інформації.

ОІД – об’єкт інформаційної діяльності

ЗМІСТ

ВСТУП

Науково-технічна революція останнім часом прийняла грандіозні масштаби в сфері інформатизації суспільства на базі сучасних засобів обчислювальної техніки, зв'язку, а також сучасних методів автоматизованої обробки інформації. Застосування цих засобів і методів прийняло загальний характер, а створювані при цьому інформаційно-обчислювальні системи і мережі стають глобальними як в сенсі територіального розподілення, так і в сенсі широти охоплення в рамках єдиних технологій процесів збирання, передачі, накопичення, зберігання, пошуку, переробки інформації і видачі її для використання.

У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку. Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху в будь-якій сфері. Монопольне володіння певною інформацією виявляється найчастіше вирішальною перевагою в конкурентній боротьбі і зумовлює, тим самим, високу ціну "інформаційного чинника".

Багато проблем інформаційної безпеки пов'язані з недооціненням важливості такої загрози, як конфіденційність інформації. В результаті для підприємства це може обернутися банкрутством. Навіть одиночний випадок халатності персоналу підприємства може принести йому багатомільйонні збитки, втрату репутації фірми і довіри клієнтів.

Збереження цілісності, забезпечення безвідмовної доступності, дотримання заздалегідь зазначеного рівня конфіденційності інформаційних ресурсів і зменшення ймовірності несанкціонованого доступу та протиправних дій до цих ресурсів – це і є головною задачею розробки створення універсальної політики безпеки.

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Загальні поняття інформаційної безпеки

В даний час інформаційні системи та інформаційно-телекомунікаційні мережі підтримують сервіси та переносять дані в таких кількостях, які важко було собі уявити ще кілька років тому. Їх готовність необхідна для роботи дуже багатьох інфраструктур, наприклад, комунальні або електричні мережі, органи державного, муніципального та регіонального управління, організації, населення і т. д. Тому безпека цих систем стає необхідною умовою їх подальшого розвитку. Для кожного випадку визначення безпеки означає специфікацію політики безпеки, тобто безлічі бажаних цілей. Наприклад, електронна система голосування повинна бути встановлена таким чином, щоб голосувати могли тільки зареєстровані виборці, доступ до вебсервера повинен здійснюватися аутентифікованими користувачами, тільки авторизовані користувачі повинні підключатися до банківської системи і т.д.

Безпека об'єкта проявляється через безпеку його найбільш важливих властивостей або властивостей структурних складових. Якщо об'єктом безпеки є людина, то його безпека полягає в захищеності від загроз йому, як живому організму, і загроз йому, як носію певних психічних і духовних якостей, тобто особистості. Якщо об'єктом безпеки є суспільство (спільність людей на певній території, яка характеризується економічною і духовною єдністю), то його безпека буде полягати в захищеності від загроз його членів, а також історично склавшимися відносинами між людьми. Відповідно, в змісті національної безпеки розрізняють державну, економічну, суспільну, оборонну, інформаційну, екологічну та іншу безпеку. Безпека проявляється як протидія на заданому рівні спробами нанести шкоду функціонуванню або усього об’єкта захисту, або його структурним складовим. Однією з важливих структурних складовиxx багатьох об’єктів безпеки є інформація (або діяльність, предметом котрої є інформація).

1.2 Основні поняття і визначення

Широко поширене в даний час поняття інформаційна безпека підкреслює важливість інформації в сучасному суспільстві і характеризує той факт, що інформаційний ресурс є сьогодні таким же багатством, як корисні копалини, виробничі і людські ресурси, і також як вони підлягає захисту від різного роду посягань, зловживань і злочинів. Під інформаційною безпекою будемо розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або преднавмисних впливів природного або штучного характеру, чреватих нанесенням шкоди власникам або користувачам інформації і підтримувальної інфраструктури. Підхід до проблем інформаційної безпеки необхідно починати з виявлення суб'єктів, зацікавлених у забезпеченні:

- своєчасного доступу (за прийнятний час) до необхідної інформації;
- конфіденційності певної частини інформації;
- достовірності (повноти, точності, адекватності, цілісності) інформації;
- захисту від нав'язування їм неправдивої (недостовірної, перекрученої) інформації (тобто від дезінформації);
- захисту частини інформації від незаконного її тиражування (захисту авторських прав, прав власника інформації тощо);
- розмежування відповідальності за порушення законних прав (інтересів) інших суб'єктів інформаційних відносин і встановлених правил поводження з інформацією;
- можливості здійснення безперервного контролю і управління процесами обробки і передачі інформації.

Очевидно, що забезпечення цих вимог суттєво і для держави в цілому, і для окремих громадських (комерційних) організаций, і для підприємств (юридичних осіб), і для окремих громадян (фізичних осіб), які і є суб'єктами інформаційних відносин. Тому введемо наступні визначення.

Суб'єкт – це активний компонент інформаційної системи, який може стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи.

Об'єкт – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до інформації, яка міститься в ньому. У якості об'єктів, які підлягають захисту в інтересах забезпечення безпеки суб'єктів інформаційних відносин, необхідно розглядати: інформацію і інформаційні ресурси, носії інформації, процеси обробки інформації. Під інформацією розуміють відомості щодо об'єктів та явищах навколишнього середовища, їх параметрах, властивостей і стану, які зменшують ступень невизначеності.

Основними властивостями якості інформації з позиції користувача є: репрезентативность, змістовність, достатність, доступність, актуальність, своєчасність, точність, достовірність і сталість. Інформаційні ресурси – це окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІС). Інформаційні ресурси можна класифікувати: - за видом інформації – правові, науково-технічні, політичні, фінансовоекономічні, статистичні, метрологічні, соціальні, персональні, медичні, про надзвичайні ситуації та т.п.;

- за режимом доступу – відкриті, обмеженого доступу, державна таємниця, конфіденційна інформація, комерційна таємниця, професійна таємниця, службова таємниця, особиста (персональна) таємниця;
- за формою власності – державні, муніципальні, регіональні, приватні, колективні;
- за видом носія – на папері (документи, листи, медичні карти, телефонні довідники організацій, чернетки і т.п.), на екрані, в пам'яті ЕОМ, в каналі зв'язку, на гнучких і жорстких магнітних дисках, на інших носіях.

Носіями інформації можуть бути окремі люди, які володіють важливою інформацією (експерти), а також спеціально завербовані або випадкові інформатори. Поінформованість кінцевого користувача про заходи безпеки повинна проявлятися в умінні розрізняти рівні захисту комп'ютерних та інформаційних ресурсів:

запобігання – доступ до інформації та технологій має тільки авторизований персонал;

виявлення – зловживання стають відомими ще на ранній стадії, навіть у разі обходу механізмів захисту;

обмеження – зменшення розміру втрат, якщо злочин мав місце, незважаючи на вжиті заходи щодо його запобігання;

відновлення – забезпечення ефективного відновлення інформації при наявності документованих і перевірених планів проведення цієї операції.

Далі надані основні поняття щодо інформаційної безпеки комп'ютерних систем (КС). Під безпекою КС розуміють її захищеність від випадкового або навмисного втручання в нормальний процес її функціонування, а також від спроб розкрадання, зміни або руйнування її компонентів. Природа впливів на КС може бути найрізноманітнішою. Це і стихійні лиха (землетруси, урагани, пожежі), і вихід з ладу складових елементів КС, і помилки персоналу, і спроба проникнення зловмисника. Безпека КС досягається вживанням заходів щодо забезпечення конфіденціальності і цілісності оброблюваної нею інформації, а також доступності та цілісності компонентів і ресурсів системи. Під доступом до інформації розуміється ознайомлення з інформацією, її обробка, зокрема копіювання, модифікація або знищення інформації. Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації – це доступ до інформації, що не порушує встановлені правила розмежування доступу. Ці правила служать для регламентації права суб'єктів на доступ до об'єктів. Несанкціонований доступ (НСД) до інформації характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп'ютерних порушень. Конфіденційність даних – це статус, наданий даними і визначає необхідний ступінь їх захисту. За суттю конфіденційність інформації – це властивість інформації бути відомою тільки допущеним особам (авторизованим суб'єктам системи). Для інших суб'єктів системи ця інформація повинна бути невідомою. Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в

семантичному відношенні від даних у вихідних документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування.

Цілісність компонента або ресурсу системи – це властивість компонента чи ресурсу бути незмінними в семантичному сенсі при функціонуванні системи в умовах випадкових або навмисних спотворень або руйнівних впливів.

Доступність компонента або ресурсу системи – це властивість компонента чи ресурсу бути доступним для авторизованих законних суб'єктів системи. Метою захисту систем обробки інформації є протидія загрозам безпеки.

Під загрозою безпеки КС розуміють можливі дії, які прямо або побічно можуть завдати шкоди її безпеки. Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься і обробляється в КС. З поняттям загрози безпеки тісно пов'язане поняття уразливості КС. Комплекс засобів захисту являє собою сукупність програмних і технічних інструментів, що створюються і підтримуються для забезпечення інформаційної безпеки КС. Комплекс створюється і підтримується відповідно до прийнятої в даній організації політики безпеки.

Політика безпеки – це сукупність норм, правил і практичних рекомендацій для надійної роботи засобів захисту КС від безлічі загроз. На практиці найважливішими є наступні аспекти информационої безпеки: доступність, цілісність і конфіденційність.

1.3 Види політики безпеки

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назва політики безпеки.

Для вивчення властивостей способу керування доступом створюється його формальний опис — математична модель. При цьому модель повинна відбивати стану всієї системи, її переходи з одного стану в інше, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього

говорити про яких-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно на виборчому і повноважному способах керування доступом. Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Слід зазначити, що засобу захисту, призначені для реалізації якого-небудь з названих способу керування доступом, тільки надають можливості надійного керування чи доступом інформаційними потоками. Визначення прав доступу суб'єктів до об'єктів і/чи інформаційним потокам (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила.

Для опису властивостей виборчого керування доступом застосовується модель системи на основі матриці доступу (МД), іноді неї називають матрицею контролю доступу. Така модель одержала назву матричної.

Матриця доступу являє собою прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Звичайно виділяють такі типи доступу суб'єкта до об'єкта, як "доступ на читання", "доступ на запис", "доступ на виконання" і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування

доступом реалізує принцип “що не дозволено, те заборонено”, що припускає явний дозвіл доступу суб’єкта до об’єкта. Матриця доступу — найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільше широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

- усі суб’єкти й об’єкти системи повинні бути однозначно ідентифіковані;
- кожному об’єкту системи привласнена влучна критичності, що визначає цінність інформації, що міститься в ньому;
- кожному суб’єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об’єктів, до яких суб’єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Ніж важливіше чи об’єкт суб’єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об’єкти з найбільш високими значеннями мітки критичності.

Кожен суб’єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки — регулювання доступу суб’єктів системи до об’єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

1.4 Принципи політики безпеки

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

- неможливість минати захисні засоби;
- посилення самої слабкої ланки;
- неприпустимість переходу у відкритий стан;
- мінімізація привілеїв;
- поділ обов'язків;
- багаторівневий захист;
- розмаїтість захисних засобів;
- простота і керованість інформаційної системи;
- забезпечення загальної підтримки заходів безпеки.

Пояснимо зміст перерахованих принципів.

Стосовно до межмережевих екранів принцип неможливості минати захисні засоби означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути «таємних» модемних чи входів тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається самою слабкою ланкою. Часто самою слабкою ланкою виявляється не чи комп'ютер програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип багаторівневого захисту наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й аутентификацией — керування доступом і, як останній рубіж, — протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.
Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.

Принцип простоти і керованості інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип загальної підтримки заходів безпеки — носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

1.5 Суб’єкти безпеки підприємства

Забезпеченням безпеки підприємства займаються дві групи суб’єктів. Перша група займається цією діяльністю безпосередньо на підприємстві і підпорядкована його керівництву. Серед цієї групи виділяють спеціалізовані суб’єкти (рада або комітет безпеки підприємства, служба безпеки, пожежна частина, рятувальна служба і т.д.), основним призначенням яких є постійна професійна діяльність щодо забезпечення безпеки підприємства (у рамках своєї компетенції). Іншу частину суб’єктів цієї групи умовно можна назвати напівспеціалізованою, так як частина функцій цих суб’єктів призначена для забезпечення безпеки підприємства (медична частина, юридичний відділ і т.д.). До третьої частини цієї групи суб’єктів

належить увесь інший персонал і підрозділи підприємства, які в рамках своїх посадових інструкцій і положень про підрозділи зобов'язані вживати заходів до забезпечення безпеки.

Слід мати на увазі, що ефективно забезпечувати безпеку підприємства ці суб'єкти можуть тільки в тому випадку, якщо цілі, завдання, функції, права і обов'язки будуть розподілені між ними Т.ч., щоб вони не перетиналися один з одним. До другої групи суб'єктів відносяться зовнішні органи та організації, які функціонують самостійно і не підкоряються керівництву підприємства, але при цьому їх діяльність має суттєвий (позитивний чи негативний) вплив на безпеку підприємства. Суб'єктами цієї групи є:

- законодавчі органи;
- органи виконавчої влади;
- суди;
- правоохоронні органи;
- науково-освітні установи.

Останні (особливо недержавні установи з підготовки приватних охоронців) покликані забезпечити науково-методичне опрацювання проблем безпеки підприємства та підготовку відповідних фахівців у сфері безпеки підприємств. Очевидно, що суб'єкти другої групи за своєю ініціативою підключаються епізодично (або ніколи) до діяльності підприємства із забезпечення своєї безпеки. Організаційною формою такого підключення може стати комплексна програма безпеки підприємства, в якій необхідно передбачити форми і методи цієї роботи. Крім того, можна рекомендувати розробку планів структурних підрозділів і всього підприємства в цілому по організації взаємодії з вищевказаними органами та організаціями.

1.6 Засоби та методи забезпечення безпеки

Серед існуючих засобів забезпечення безпеки виділимо наступні:

Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових пристроїв, бронежилети, загородження і т.д.

Організаційні засоби. Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства.

Інформаційні засоби. Насамперед, це друкована та відеопродукція з питань збереження конфіденційної інформації. Крім цього, найважливіша інформація для прийняття рішень з питань безпеки зберігається в комп'ютерах.

Фінансові кошти. Цілком очевидно, що без достатніх фінансових коштів неможливе функціонування системи безпеки: питання лише в тому, щоб використовувати їх цілеспрямовано і з високою віддачею.

Правові засоби. Тут мається на увазі використання не тільки виданих вищими органами влади законів і підзаконних актів, але й розробка власних, так званих локальних правових актів з питань забезпечення безпеки.

Кадрові кошти. Мається на увазі насамперед достатність кадрів, що займаються питаннями забезпечення безпеки. Одночасно з цим вирішують завдання підвищення їх професійної майстерності в цій сфері діяльності.

Інтелектуальні засоби. Залучення до роботи висококласних фахівців, науковців (іноді доцільно залучати їх з боку) дозволяє впроваджувати нові системи безпеки. Зауважимо, що застосування кожного з вищевказаних засобів окремо не дає необхідного ефекту: він можливий тільки на комплексній основі.

У той же час необхідно відзначити, що одночасне використання всіх вищевказаних коштів в принципі неможливо. Воно проходить зазвичай ряд етапів:

1. виділення фінансових коштів;
2. формування кадрових і організаційних засобів;
3. розробка системи правових засобів.
4. залучення технічних, інформаційних та інтелектуальних засобів.

Перекладені з статичного в динамічний стан вищевказані кошти стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи. Наведемо короткий конкретний перелік цих методів:

технічні – спостереження, контроль, ідентифікація і т.д.;

організаційні – створення зон безпеки, режим, розслідування, пости, патрулі і т.д.;

інформаційні – складання характеристик на співробітників, аналітичні матеріали конфіденційного характеру тощо;

фінансові – матеріальне стимулювання співробітників, що мають досягнення в забезпеченні безпеки, грошове заохочення інформаторів і т.д.;

правові – судовий захист законних прав та інтересів, сприяння правоохоронним органам і т.д.;

кадрові – підбір, розстановка і навчання кадрів, які забезпечують безпеку підприємства, їх виховання і т.д.;

1.7 Концепція безпеки підприємства

Після вивчення всіх вищеописаних елементів системи безпеки підприємства необхідно перейти до складання й концепції. Концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем. В подальшому під поняттям «концепція» розумітимемо концепцію предметної області досліджень, тобто концепцію безпеки підприємства. До будь-якої концепції можна встановити такі вимоги:

1) ***Конструктивність***. Така вимога буде визнана реалізованою, якщо в концепції знаходять відображення:

- початковий стан об’єкта, на перетворення якого спрямована концепція;
- стан об’єкта, досягнутий в результаті реалізації концепції;
- заходи, необхідні для досягнення сформульованих у концепції цілей;

– кошти, необхідні і достатні для досягнення поставлених цілей;
– джерела ресурсного забезпечення, що використовуються в ході реалізації концепції;
– механізм реалізації концепції, тобто способи (методи) використання виділених коштів і ресурсів.

2) ***Сумісність***. Мається на увазі те, що концепція перетворення якогонебудь об'єкту повинна гармонійно вписуватися в систему перетворень взаємопов'язаних в єдину систему об'єктів, одним з компонентів якої він є.

3) ***Відкритість.*** Розроблена концепція повинна давати можливість в її рамках реагувати на зміну умов реалізації концепції і вносити корективи в реалізацію в разі їх необхідності.

Вищевказані вимоги диктують в якості обов'язкової умови включення в логічну структуру концепції наступних позицій:

– виявлення об'єкта і предмета, визначення їх сутності, місця серед множини інших;
– чітке формулювання ролі реалізації концепції і завдань, що стоять при її реалізації;
– виділення умов, необхідних і достатніх для реалізації концепції, і зіставлення їх з реально існуючими;
– визначення кола заходів, що забезпечують перетворення об'єкта реалізації концепції, а також шляхів її реалізації;
– формулювання критеріїв успішності заходів щодо розробки концепції, а також з оцінки результатів її реалізації.

Концепція безпеки підприємства являє собою офіційно затверджений документ, в якому відображена система поглядів, вимог і умов організації заходів безпеки персоналу і власності підприємства.

РОЗДІЛ 2. СКЛАД ТА ЗМІСТ ОСНОВНИХ ЗАХОДІВ ЩОДО РОЗРОБКИ ПОЛІТИКИ БЕЗПЕКИ

2.1 Основні підходи до створення комплексної системи захисту інформації

Існує думка, що проблеми захисту інформації стосуються виключно інформації, що обробляється комп'ютером. Це, мабуть, пов'язано з тим, що комп'ютер і, зокрема, персональний комп'ютер є «ядром», центром зберігання інформації. Об'єкт інформатизації, стосовно до якого спрямовані дії щодо захисту інформації, видається більш широким поняттям порівняно з персональним комп'ютером.

У реальному житті всі ці окремі “об'єкти інформатизації” розташовані в межах одного підприємства і являють собою єдиний комплекс компонентів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д.

Сучасне підприємство – велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх та зовнішніх чинників, які часто не піддаються чіткому кількісному оцінюванню, призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентів.

Характерною особливістю подібних систем є насамперед наявність людини в кожній з складових підсистем і віддаленість людини від об'єкта її діяльності. Якщо звернутися до історії цієї проблеми, то можна умовно виділити три періоди розвитку засобів захисту інформації:

перший ми відносимо до того часу, коли обробка інформації здійснювалася за традиційними (ручними, паперовими) технологіями;

другий – коли для обробки інформації на регулярній основі застосовувалися засоби електронної обчислювальної техніки перших поколінь;

третій – коли використання засобів електронно-обчислювальної техніки набрав масового і повсюдний характер (поява персональних комп'ютерів).

У 60–70 рр. XX ст. проблема захисту інформації вирішувалася досить ефективно застосуванням в основному організаційних заходів. До них належали: режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання цих коштів досягалася за рахунок концентрації інформації в певних місцях (спец. сховища, обчислювальні центри), що сприяло забезпеченню захисту відносно малими силами.

“Розподілення” інформації по місцях зберігання і обробки загострило ситуацію з її захистом. З'явилися дешеві персональні комп'ютери. Це дало можливість побудови мереж ЕОМ, які можуть використовувати різні канали зв'язку. Ці чинники сприяють створенню високоефективних систем розвідки і отримання інформації. Вони знайшли відображення і на сучасних підприємствах.

Сучасне підприємство являє собою складну систему, в рамках якої здійснюється захист інформації.

Розглянемо основні особливості сучасного підприємства:

- складна організаційна структура;
- багатоаспектність функціонування;
- висока технічна оснащеність;
- широкі зв'язки з кооперації;
- необхідність розширення доступу до інформації;
- зростаюча питома вага цифрової технології обробки інформації;
- зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;
- важливість і відповідальність рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації;
- висока концентрація в автоматизованих системах інформаційних ресурсів;
- велике територіальне розподілення компонентів автоматизованих систем;
- накопичення на технічних носіях величезних обсягів інформації;
- інтеграція в єдиних базах даних інформації різного призначення і різної належності;
- довгострокове зберігання великих обсягів інформації на машинних носіях;

- безпосередній і одночасний доступ до ресурсів (також і до інформації) автоматизованих систем великого числа користувачів різних категорій і різних установ;

- інтенсивна циркуляція інформації між компонентами автоматизованих систем, також і віддалених один від одного.

Таким чином, створення індустрії переробки інформації, з одного боку, створює об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, з іншого боку, породжує цілий ряд складних і великомасштабних проблем. Однією з них є забезпечення збереження і встановленого статусу інформації, що циркулює і оброблюється на підприємстві, в організації.

2.1.1 Поняття комплексної системи захисту інформації

Роботи з захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не вважає, що досить провести на підприємстві ряд організаційних заходів, ввести до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі інформації: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів,

адміністрації та обслуговувального персоналу з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ .

На основі теоретичних досліджень і практичних робіт у сфері ЗІ сформульований системно-концептуальний підхід до захисту інформації.

Під системністю як основною частиною системно-концептуального походу розуміється:

системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

системність організаційна, що означає єдність організації всіх робіт по ЗІ і управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх

і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені такі її компоненти:
Вхідні елементи. Це ті елементи, для обробки яких створюється система. Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті;

1. ***Ресурси.*** Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

2. ***Навколишнє середовище***. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі сфер інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій із захисту інформації, переданої сигналами в кабельній лінії, що проходить територіями різних об'єктів. Як би не встановлювались межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними;

3. ***Призначення і функції***. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому

вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

4. *Критерій ефективності*. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декілька варіантів побудови системи, що забезпечують задані цілі функціонування. Для того, щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісне оцінювання на всіх етапах створення системи.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу.

2.1.2 Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації – забезпечення надійності ЗІ. Система ЗІ - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого – самі організовують систему, здійснюючи захисні заходи. Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен

компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами та пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальні СЗІ можуть бути розглянуті, наприклад, види захисту інформації.

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які забезпечують або можуть впливати на якість захисту. Наприклад, система охоплює якісь об'єктів захисту, а всі вони внесені до неї чи ні – це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися все, виходячи з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, в всіх місцях її збирання, зберігання, передачі і використання, весь час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не усуває, а, навпаки, передбачає диференційований підхід до захисту інформації, залежно від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації полягає у:

- інтеграції локальних систем захисту;
- забезпеченні повноти всіх складових системи захисту;
- забезпеченні всеосяжність захисту інформації.

2.1.3 Основні стратегії захисту інформації

Усвідомлення необхідності розробки стратегічних підходів до захисту формувалося в міру усвідомлення важливості, натхнення і проблеми захисту, а також неможливості ефективного її здійснення простим використанням деякого набору засобів захисту.

Під стратегією взагалі розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації.

Відомий канадський фахівець у сфері стратегічного управління Г. Мінцберг запропонував визначення стратегії в рамках системи «5-Р». На його думку, вона містить:

1) план (Plan) - заздалегідь намічені в деталях і контрольовані дії на певний термін, що переслідують конкретні цілі;

2) прийом, або тактичний хід (Ploy), що є короткочасною стратегією, яка має обмежені цілі, спроможна змінюватися та маневруввати з метою використати їх проти противника;

3) модель поведінки (Patten of behaviour) – часто спонтанну, неусвідомлену, що не має конкретних цілей;

4) позицію щодо до інших (Position in respect to others);

5) перспективу (Perspective).

Завдання стратегії полягає в створенні конкурентної переваги, усунення негативного ефекту нестабільності навколишнього середовища, забезпеченні прибутковості, врівноваженні зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими організація стикається в повсякденному житті.

Здатність компанії, організації проводити самостійну стратегію в усіх сферах робить її більш гнучкою, стійкою, дозволяє адаптуватися до вимог часу і обставин.

Стратегія формується під впливом внутрішнього і зовнішнього середовищ, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати.

Фактори, які можуть мати для фірми вирішальне значення в майбутньому, називаються стратегічними. На думку одного з провідних західних фахівців Б. Карлофа, вони, впливаючи на стратегію будь-якої організації, надають і специфічні властивості. До таких факторів належать:

мета, яка відображає філософію фірми, організації її призначення. При перегляді мети, що відбувається в результаті зміни суспільних пріоритетів;

конкурентні переваги, якими організація має в своїй сфері діяльності в порівнянні з суперниками або до яких прагне (вважається, що вони найбільше впливають на стратегію). Конкурентні переваги будь-якого типу забезпечують більш високу ефективність використання ресурсів підприємства;

характер продукції, що випускається, особливості її збуту, післяпродажного обслуговування, ринки та їх межі;

організаційні чинники, серед яких виділяється внутрішня структура компанії та її очікувані зміни, система управління, ступінь інтеграції і диференціації внутрішніх процесів;

наявні ресурси (матеріальні, фінансові, інформаційні, кадрові та ін.). Чим вони більші, тим масштабнішими можуть бути інвестиції в майбутні проекти. Сьогодні для розробки і реалізації стратегії велике значення мають, перш за все, структурні, інформаційні та інтелектуальні ресурси. Порівнюючи значення

параметрів готівки і потрібних ресурсів, можна визначити ступінь їх відповідності стратегії;

потенціал розвитку організації, вдосконалення діяльності, розширення масштабів, зростання ділової активності, інновацій;

культура, філософія, етичні погляди і компетентність управлінців, рівень їх домагань і підприємливості, здатність до лідерства, внутрішній клімат в колективі.

На стратегічний вибір впливають: ризик, на який готова йти фірма; досвід реалізації чинних стратегій, позиції власників, наявність часу.

Розглянемо особливості стратегічних рішень. За ступенем регламентованості вони належать до контурних (надають широку свободу виконавцям стосовно тактики), а за ступенем обов'язковості проходження головним установкам – директивним.

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими способами здійснення в певних ситуаціях тих чи інших дій. З точки зору визначеності, це рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати. З точки зору важливості, стратегічні рішення кардинальні: стосуються основних проблем і напрямків діяльності фірми, визначають основні шляхи розвитку її в цілому, окремих підрозділів або видів діяльності на тривалу перспективу (не менше 5–10 років). Вони випливають насамперед із зовнішніх, а не з внутрішніх умов, повинні враховувати тенденції розвитку ситуації і інтереси безлічі суб'єктів. Практична незворотність стратегічних рішень обумовлює необхідність їх ретельної та всебічної підготовки. Стратегічним рішенням притаманна комплексність. Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами. Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу, ринків, способи реакції на непередбачені події. Практика сформувала нижченаведені вимоги до стратегічних рішень:

Реальність, що передбачає її відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду і навичками працівників і менеджерів, культурі, існуючій системі управління;

Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

Своєчасність (реалізація рішення повинна встигнути призупинити негативне розвиток ситуації або не дозволити упустити вигоду);

Сумісність із середовищем, що забезпечує можливість взаємодії з нею (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

1. виділяти, відстежувати і оцінювати ключові проблеми;
2. адекватно і оперативно реагувати на зміни всередині і в оточенні організації;
3. вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;
4. створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Вихідний момент формування стратегії – постановка глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінювання яких дозволяє вибрати кращу стратегію. Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого

мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено три стратегії захисту:

оборонна – захист від вже відомих загроз здійснюваний автономно, тобто без надання істотного впливу на інформаційно - керувальну систему;

наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно - керувальної системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

упереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для прояву.

2.1.4 Методи захисту інформації

У загальному випадку захист інформації технічними засобами забезпечується в наступних просторово - часових рамках і умовах:

- джерело і носій інформації локалізовані в межах об’єкта захисту, забезпечена механічна перешкода від контакту з ними зловмисника або дистанційного впливу на них полів технічного характеру;
- співвідношення енергії носія і перешкод на виході приймача каналу витоку таке, що зловмиснику не вдається зняти інформацію з носія з необхідною для її використання якістю;
- зловмисник не може виявити джерело або носій інформації;
- замість правдивої інформації зловмисник отримує неправдиву, яку він приймає як справжню.

Цей перелік реалізують такі методи захисту, як перешкоджання безпосередньому проникненню зловмисника до джерела інформації за допомогою інженерних конструкцій, технічних засобів охорони, а також приховування достовірної інформації. Приховування інформації передбачає такі зміни структури і енергії носіїв, при яких зловмисник не може безпосередньо або за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у

власних інтересах. Розрізняють інформаційне та енергетичне приховування. Інформаційне приховування досягається зміною або створенням помилкового інформаційного портрета семантичного повідомлення, фізичного об’єкта або сигналу. Інформаційним портретом можна назвати сукупність елементів і зв'язків між ними, що відображають зміст повідомлення (мовного або даних), ознаки об’єкта або сигналу. Зміна інформаційного портрета об’єкта викликає зміну зображення його зовнішнього вигляду (видових демаскируючих ознак), характерістік випромінюваних їм полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення ознакових структур об’єкта і навколишнього його фону, в результаті чого знижується контрастність зображення об’єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання.

Однак при зміні інформаційного портрета інформація не сприймається не тільки зловмисником, а з її санкціонованим одержувачем. Отже, для нього інформаційний портрет повинен бути відновлений шляхом додаткової передачі йому віддалених елементів і зв’язків або алгоритму (ключа) цих змін. Інформаційне приховування дозволяє: істотно зменшити обсяг інформації, що захищається і тим самим спростити проблему захисту інформації; використовувати в рекламі нової продукції відомості про неї, не побоюючись розголошення. Наприклад, замість захисту інформації, що міститься в сотнях і тисячах аркушів технічної документації, яка розробляється для виробництва нової продукції, захисту підлягають лише кілька десятків листів з інформаційними вузлами. Інший метод інформаційного приховування полягає в трансформації вихідного інформаційного портрета в новий, з помилковою семантичною інформацією або помилковою ознаковою структурою, і “нав'язуванні” нового портрета органу розвідки або зловмиснику. Такий метод захисту називається дезінформуванням. Принципова відмінність інформаційного приховування шляхом змін інформаційного портрета від дезінформування полягає в тому, що перший метод спрямований на утруднення виявлення об’єкта з інформацією серед інших об’єктів (фону), а другий – на створенні на цьому фоні ознак помилкового об’єкта.

Дезінформування відноситься до числа найбільш ефективних способів захисту інформації, однак цей метод захисту практично складно реалізувати. Основна проблема полягає в забезпеченні достовірності помилкового інформаційного портрета. Дезінформування тільки в тому випадку досягне мети, коли у розвідки (зловмисника) не виникне сумніву в істинності неправдивої інформації, яку йому підсовують. В іншому випадку може бути отриманий протилежний ефект, так як при розкритті розвідкою факту дезінформування отримана помилкова інформація звузить область пошуку правдивої інформації.

Тому до організації дезінформування необхідно ставитися дуже серйозно, з урахуванням того, що споживачі інформації чітко уявляють збиток від дезінформації і при найменших сумнівах будуть перевіряти інформацію з використанням інших джерел. Іншим ефективним методом приховування інформації є енертичне приховування. Воно полягає в застосуванні способів і засобів захисту інформації, що виключають або ускладнюють реалізацію енергетичного розвідувального контакту. Енергетичне приховування досягається зменшенням відносини енергії (потужності) сигналів, тобто носіїв з інформацією (електромагнітного або акустичного полів і електричного струму) і перешкод. Зменшення відносини сигнал / перешкода можливо двома методами: зниженням потужності сигналу або збільшенням потужності перешкоди на вході приймача. Вплив перешкод призводить до зміни інформаційних параметрів носіїв: амплітуди, частоти, фази. Якщо носієм інформації є амплітудно-модульована електромагнітна хвиля, а в середовищі поширення каналу присутня перешкода у вигляді електромагнітної хвилі, що має однакову з носієм частоту, але випадкову амплітуду і фазу, то відбувається інтерференція цих хвиль. В результаті цього амплітуда сумарного сигналу випадковим чином змінюються, тобто інформація спотворюється.

2.2 Методика визначення складу захищуваної інформації

Визначення складу захищуваної інформації – це перший крок на шляху побудови системи захисту. Від того, наскільки точно він буде виконаний, залежить

результат функціонування розроблювальної системи. Загальний підхід полягає в тому, що захисту підлягає вся інформація з обмеженим доступом (ІзОД): інформація, яка становить державну таємницю (секретна інформація), інформація, що становить комерційну таємницю і визначається власником, частина відкритої інформації. При цьому ІзОД повинна захищатися від витоку і втрати, а відкрита – тільки від втрати.

Часто можна почути думку, що будь-яка відкрита інформація не може бути предметом захисту. Не всі згодні з внесенням інформації, віднесеної до державної таємниці, до складу ІзОД.

Захист відкритої (публічної) інформації існував завжди і проводився шляхом реєстрації її носіїв, обліку їх руху і місцезнаходження. Створювалися безпечні умови зберігання. Відкритість інформації не применшує її цінності, а цінна інформація потребує захисту від втрати. Цей захист не повинен бути спрямований на обмеження загальнодоступності інформації. Не може бути відмови в доступі до інформації, але доступ повинен здійснюватися з дотриманням вимог щодо її збереження відповідно до вимог обробки та використання (наприклад, бібліотека).

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана, або створена в процесі виконання суб’єктами владних повноважень своїх обов’язків, передбачених чинним законодавством, або яка знаходиться у володінні суб’єктів владних повноважень, інших розпорядників публічної інформації.

Інформація з обмеженим доступом поділяється на:

– конфіденційну;
– таємну;
– службову.

Конфіденційна інформація – це та, доступ до якої обмежений фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватись у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Таємна інформація – це та інформація, доступ до якої обмежується, розголошення якої може завдати шкоду особі, суспільству, державі. Таємною визначається інформація, яка містить державну, професійну, банківську таємницю, таємницю розслідування та іншу передбачену законом таємницю.

До службової може належати нижчеперерахована інформація:

1) Інформація, що міститься в документах суб’єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов’язані з розробкою напряму діяльності установи або здійсненням контрольних наглядових функцій органами державної влади, процесом прийняття рішень, і передують публічному обговоренню та/або прийняттю рішень.
2) Інформація, зібрана в процесі оперативно-розшукової контррозвідувальної діяльності у сфері оборони України, яку не віднесено до державної таємниці.

2.3 Об'єкти захисту КСЗІ

Захист інформації повинен бути системним, що містить в собі різні взаємопов'язані компоненти. Найважливішим із цих компонентів є об'єкти захисту, бо від їх складу належать і методи, і засоби захисту, і склад захисних заходів.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) в певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту.

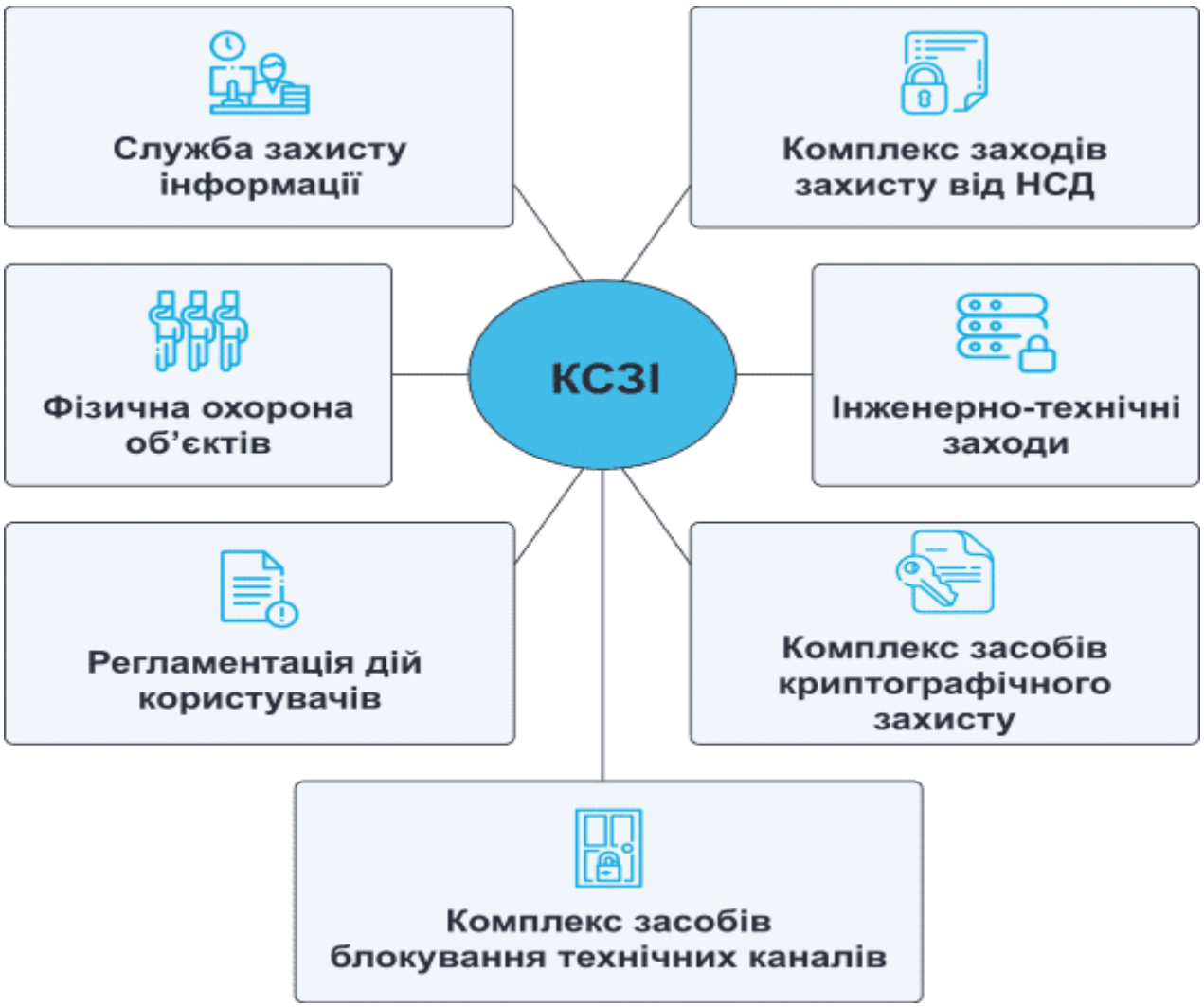

Рис1.Об'єкти захисту КСЗІ

Для запису як секретної, так і несекретної інформації використовуються одні й ті ж носії. Як правило, носії ІзОД охороняються власником цієї інформації.

Носії захищуваної інформації можна класифікувати як документи; вироби (предмети); речовини і матеріали; електромагнітні, теплові, радіаційні та інші випромінювання; акустичні та інші поля і т. п.

Особливим носієм інформації є людина, мозок якої являє виключно складну систему, що зберігає і переробляє інформацію, що надходить із зовнішнього світу. Властивість мозку відображати і пізнавати зовнішній світ, накопичувати в пам'яті колосальні обсяги інформації ставлять людину на особливе місце як носія інформації. Людина має можливість генерувати нову інформацію. І як носій інформації він володіє позитивні та негативні риси.

Позитивні – без згоди суб'єкта-носія захищувана інформація з його пам'яті, як правило, не може бути вилучена. Він може оцінювати важливість наявної у нього інформації і відповідно до цього ставитися до неї. Він може ранжувати і споживачів захищуваної інформації, знати, кому і яку інформацію він може довірити.

Негативні – він може помилятися щодо істинності споживача захищуваної інформації або навмисно не зберігати довірену йому інформацію: зрада чи просто поширення.

Серед найбільш поширених видів носіїв конфіденційної інформації можна виділити нижчевказані.

Паперові носії, в яких інформація фіксується рукописним, машинописним, електронним, типографським і іншими способами в формі тексту, креслення, схеми, формули.

Магнітні носії: аудіокасети (аудіоплівки) для магнітофонів і диктофонів; відеокасети (відеоплівки) для відеомагнітофонів та деяких відеокамер; жорсткі (тверді) диски, дискети, магнітні стрічки для ЕОМ. У цих носіях інформація фіксується (наноситься) за допомогою магнітного накопичення (запису сигналів), що здійснюється магнітним пристроєм, а відображається у вигляді символів. Відтворення (зчитування) інформації здійснюється також магнітним пристроєм за допомогою відновлення сигналів.

Магнітооптичні та оптичні носії (лазерні диски, компакт-диски). Запис даних на них виконується лазерним променем (у магнітооптичних і магнітним полем), інформація відображається у вигляді символів, а її зчитування (відтворення) здійснюється за допомогою лазерного променя.

Продукція, що випускається (вироби). Ці вироби виконують своє пряме призначення і одночасно є носіями захищуваної інформації. У цьому випадку інформація відображається у вигляді технічних рішень.

Технологічні процеси виготовлення продукцій які охоплюють як технологію виробництва продукції, так і застосовувані при її виготовленні компоненти (засоби виробництва): обладнання, прилади, матеріали, речовини, сировину, паливо та ін.

Інформація відображається у вигляді технічних процесів (перша складова) і технічних рішень (друга складова).

Фізичні поля, в яких інформація фіксується шляхом зміни їх інтенсивності, кількісних характеристик, відображається у вигляді сигналів, а в електромагнітних полях і у вигляді образів.

Носії ІзОД як об'єкти захисту повинні захищатися, залежно від їх видів, від несанкціонованого доступу до них, від втрати і від витоку вміщуваної інформації.

Але, щоб забезпечити захист, необхідно захищати і об'єкти, які є підступами до носіїв, і їх захист виступає в ролі певних рубежів захисту носіїв. І чим таких рубежів більше, чим складніше їх подолати, тим надійніше забезпечується захист носіїв.

Як перший рубіж розглянемо прилеглу до підприємства територію. Деякі підприємства на периметрі встановлюють і пропускний пункт. Прилегла територія захищається від несанкціонованого проникнення осіб до будівель підприємства і відходів виробництва (при наявності відходів). Іншим об'єктом захисту є будівлі підприємства. Їх захист здійснюється тими ж способами і має ту ж мету, що і охорона території. Захист будівель є другим рубежем захисту носіїв.

Наступний об'єкт захисту – приміщення, в яких розташовані сховища носіїв, проводиться обробка носіїв і здійснюється управлінсько-виробнича діяльність з використанням носіїв. До таких приміщень належать:

– приміщення підрозділів захисту інформації, в яких розташовані сховища носіїв і здійснюється їх обробка. Ці приміщення повинні бути захищені від несанкціонованого проникнення;

– приміщення, в яких проводиться робота з носіями інформації або протягом робочого дня, або цілодобово: кімнати, в яких з носіями працює персонал; кімнати, в яких проводяться закриті заходи (наради, засідання, семінари та ін.); виробничі ділянки з виготовлення продукції. Ці приміщення повинні захищатися під час перебування в них носіїв від несанкціонованого проникнення, від візуального спостереження за носіями, а також, в разі необхідності, від прослуховування ведуться в них конфіденційних розмов, які можуть вестися в них. Захист

здійснюється в приміщеннях співробітниками, що там працюють, різними технічними засобами, в тому числі в неробочий час засобами охоронної сигналізації.

Ще одним об'єктом захисту є безпосередньо сховища носіїв. Сховища захищаються від несанкціонованого доступу до носіїв. Їх захист здійснюється відповідальними зберігачами за допомогою замків, а у позаробочий час вони можуть, крім замків, захищатися засобами охоронної сигналізації.

Крім того, об'єктами захисту повинні бути:

засоби відображення, ***обробки, відтворення і передачі конфіденційної інформації***, в тому числі ЕОМ, які повинні захищатися від несанкціонованого підключення, побічних електромагнітних випромінювань, зараження вірусом, електронних закладок, візуального спостереження, виведення з ладу, порушення режиму роботи; копіювально-розмножувальна техніка, що захищається від візуального спостереження і побічних електромагнітних випромінювань під час обробки інформації; засоби відео-, звукозаписувальної та відтворювальної техніки, які вимагають захисту від прослуховування, візуального спостереження і побічних електромагнітних випромінювань;

засоби транспортування носіїв конфіденційної інформації, що підлягають захисту від проникнення сторонніх осіб до носіїв або їх знищення під час транспортування;

засоби радіо- і кабельного зв'язку, радіомовлення і телебачення, які використовуються для передачі конфіденційної інформації, що повинні захищатися від прослуховування, виведення з ладу, порушення режиму роботи системи забезпечення функціонування підприємства (електро-, водопостачання, кондиціонування та ін.), які повинні захищатися від використання їх для виведення з ладу засобів обробки і передачі інформації прослуховування конфіденційних розмов, візуального спостереження за носіями.

2.4 Основні вимоги до комплексної системи захисту інформації

Система захисту інформації повинна забезпечувати виконання АС своїх основних функцій без істотного погіршення характеристик останньої. Вона повинна бути економічно доцільною, оскільки вартість системи захисту інформації входить у вартість АС. Захист інформації в АС повинен забезпечуватися на всіх етапах життєвого циклу, при всіх технологічних режимах обробки інформації, в тому числі при проведенні ремонтних і регламентних робіт.

В систему захисту інформації повинні бути закладені можливості її вдосконалення і розвитку відповідно до умов експлуатації та конфігурації АС. Відповідно до встановлених правил КСЗІ повинна забезпечувати розмежування доступу до ІзОД з відволіканням порушника на помилкову інформацію, тобто мати властивості активного і пасивного захисту. При взаємодії захищеної АС з незахищеними АС система захисту повинна забезпечувати дотримання встановлених правил розмежування доступу. Система захисту повинна дозволяти проводити облік і розслідування випадків порушення безпеки інформації в АС.

Застосування системи захисту не повинно погіршувати екологічну обстановку, не бути складною для користувача, не викликати психологічної протидії та бажання обійтися без неї.

2.5 Завдання комплексної системи захисту інформації

Перелік основних завдань, які повинні вирішуватися комплексною системою захисту інформації:

- управління доступом користувачів до ресурсів АС з метою її захисту від неправомірного випадкового або навмисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних і апаратних ресурсів з боку сторонніх осіб, а також осіб з числа персоналу організації та користувачів;
- захист даних, передаваних по каналах зв'язку;
- реєстрація, збір, зберігання, обробка і видача відомостей про всі події, що відбуваються в системі і які стосуються її безпеки;

- контроль роботи користувачів системи з боку адміністрації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримку цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;
- забезпечення замкнутого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм (у яких можуть міститися шкідливі закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і розповсюдження комп'ютерних вірусів;
- управління засобами системи захисту.

2.6 Ризики в системі забезпечення інформаційної безпеки організації

В умовах дедалі більшої складності та інтеграції інформаційних систем питання інформаційної безпеки (ІБ) набуває все більшого значення. З одного боку, потрібна побудова єдиного інформаційного простору підприємства, швидкої інтеграції наявних і впроваджуваних інформаційних систем і комплексів в єдине рішення, що дозволяє здійснювати оперативне і стратегічне управління компанією і виробництвом. З іншого боку, крайня нерівномірність розвитку IT-служб та інфраструктури і різнорідність експлуатованих інформаційних систем перешкоджають забезпеченню необхідного рівня ІБ. Забезпечення ІБ стає одним із пріоритетних завдань підприємств і організацій з метою підтримки її нормальної діяльності, стійкості на ринку і успішного розвитку. В умовах, що склалися необхідна побудова дійсно комплексної корпоративної системи менеджменту інформаційної безпеки (СМІБ), що є однією з найбільш важливих складових в загальній системі менеджменту компанії.

Для сучасного менеджменту ІБ характерний підхід, який передбачає вирішення проблем не «по мірі їх надходження», коли буває вже надто пізно ними займатися, а передбачає завчасний аналіз і попередження можливих проблем, на основі оцінки можливих ризиків ІБ, керуючись при цьому міркуваннями економічної доцільності.

Тому фундаментом для успішного впровадження і функціонування СМІБ є оцінка та аналіз ризиків ІБ.

У роботі визначено ризик порушення ІБ як потенційну можливість використання вразливостей активів організації загрозами ІБ для заподіяння шкоди організації, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ.

Таким чином, в представленому визначенні ризик ІБ є функція як мінімум двох змінних: величини потенційного (негативного) впливу - шкоди для бізнесу організації та ймовірності реалізації загрози ІБ. Друга величина є комплексним показником.

Аналіз ризиків – це процедури виявлення факторів ризиків ІБ і оцінки їх вагомості. Аналіз ризиків ІБ включає оцінку ризиків і методи зниження ризиків або зменшення пов'язаних з ними несприятливих наслідків. При аналізі спочатку проводиться виявлення відповідних факторів і оцінка їх вагомості, повнота виявлених чинників збільшує якість і точність прогнозованих ризиків. До таких факторів належать безліч активів, вразливостей і загроз. Основна мета створення класифікації загроз ІБ - повна, детальна класифікація, що описує всі існуючі загрози ІБ і яка найбільш застосовна для аналізу ризиків реальних інформаційних систем.

Аналіз і управління інформаційними ризиками - один з базових процесів, що визначають ефективність системи забезпечення інформаційної безпеки організації. При організації системи безпеки, що включає різнорідні заходи і способи забезпечення інформаційної безпеки, саме аналіз інформаційних ризиків визначає якість і ефективність функціонування цієї системи.

Користуючись поняттям ризику, можна кількісно і якісно визначити і такі поняття, як ефективність системи захисту інформації, рівень безпеки дій і оптимальність прийнятих рішень.

Незалежно від розмірів організації і специфіки її інформаційної системи, роботи по забезпеченню режиму ІБ зазвичай складаються з наступних етапів:

- визначення політики безпеки;
- визначення сфери (кордонів) системи управління інформаційною безпекою та конкретизація цілей її створення;

– оцінка ризиків;
– вибір контрзаходів, що забезпечують режим ІБ;
– управління ризиками;
– аудит системи управління ІБ.

Як правило, визначення політики безпеки зводиться до наступних практичних кроків:

– Вибір національних і міжнародних керівних документів і стандартів в області ІБ та визначення на їх основі основних вимог і положень політики ІБ компанії, включаючи:
– управління доступом до засобів обчислювальної техніки, програмам і даним; антивірусний захист;
– питання резервного копіювання;
– проведення ремонтних і відновлювальних робіт;
– інформування про інциденти в області ІБ та ін.

Визначення підходів до управління інформаційними ризиками та прийняття рішення про вибір рівня захищеності ІС. Рівень захищеності відповідно до зарубіжних стандартів може бути мінімальним (базовим) або підвищеним. Цим рівням захищеності відповідають мінімальний (базовий) або повний варіант аналізу інформаційних ризиків.

Структуризація контрзаходів щодо захисту інформації за такими основними рівнями: нормативно-правовий, організаційно-управлінський, технологічний, апаратно-програмний.

Визначення порядку сертифікації та акредитації інформаційної системи на відповідність стандартам в області ІБ. Визначення періодичності проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

Визначення меж системи управління інформаційною безпекою і конкретизація цілей її створення. На цьому етапі визначаються межі системи, для якої повинен бути

забезпечений режим ІБ. Відповідно, система управління ІБ буде будуватися саме в цих межах.

Сам опис меж системи рекомендується виконувати за таким планом:

структура організації. Опис існуючої структури і змін, які передбачається внести в зв'язку з розробкою (модернізацією) автоматизованої системи (АС);

ресурси інформаційної системи, що підлягають захисту.

Рекомендується розглянути ресурси АС наступних класів: СВТ, дані, системне і прикладне ПЗ. Всі ресурси представляють цінність з точки зору організації. Для їх оцінки повинна бути обрана система критеріїв і методика отримання оцінок за цими критеріями.

Постановка завдання оцінки ризиків обґрунтовуються вимогами до методики оцінки інформаційних ризиків компанії. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру взятих до уваги загроз (спектра дії загроз) і ефективності потенційних контрзаходів щодо захисту інформації. Розрізняють мінімальні або базові, а також підвищені або повні вимоги до режиму ІБ.

Мінімальним вимогам до режиму ІБ відповідає базовий рівень ІБ. Такі вимоги застосовуються, як правило, до типових проектних рішень. Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як: віруси, збої устаткування, несанкціонований доступ тощо. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їх здійснення і уразливості ресурсів.

Управління ризиками. Розробляється деяка стратегія управління ризиками. Можливі такі підходи до управління інформаційними ризиками компанії:

Зменшення ризиків. Більшість ризиків можуть бути істотно зменшені шляхом використання досить простих і дешевих контрзаходів. Наприклад, грамотне управління паролями знижує ризик несанкціонованого доступу.

Ухилення від ризику. Від деяких класів ризиків можна ухилитися.

Зміна характеру ризику. Якщо не вдається ухилитися від ризику або ефективно його зменшити, можна прийняти деякі заходи страховки.

Прийняття ризику. Більшість ризиків не можуть бути зменшені до незначної величини.

На практиці, після прийняття стандартного набору контрзаходів, ряд ризиків зменшується, але залишається все ще значним. Необхідно знати залишкову величину ризику.

В результаті виконання етапу для інформаційних ризиків компанії, що беруться до уваги, повинна бути запропонована стратегія управління ризиками.

Вибір контрзаходів, що забезпечують режим ІБ. На цьому етапі обґрунтовано вибирається комплекс різних контрзаходів щодо захисту інформації, структурованих по нормативно-правовому, організаційно-управлінському, технологічному і апаратно-програмному рівнях забезпечення інформаційної безпеки. Надалі пропонований комплекс контрзаходів реалізується відповідно до обраної стратегії управління інформаційними ризиками. Якщо проводиться повний варіант аналізу ризиків, для кожного ризику додатково оцінюється ефективність комплексу контрзаходів щодо захисту інформації.

Аудит системи управління ІБ. Перевіряється відповідність обраних контрзаходів щодо захисту інформації цілям і задачам бізнесу, декларованим в політиці безпеки компанії, проводиться оцінка залишкових ризиків і, в разі необхідності, оптимізація ризиків.

2.7 Методологія оцінки та аналізу ризиків інформаційної безпеки

На сьогодні багатьом підприємствам конче необхідно володіти вмінням аналізу й управління інформаційними ризиками не тільки для отримання конкурентних переваг. Проте багатьом організаціям, які функціонують з минулого століття для успішної діяльності процес керування ризиками був не потрібний. На сьогоднішній день питання загострилось. Це пов’язано зі швидкоплинністю часу, значним збільшенням інформаційних загроз, а також обмеженою кількістю технологій та стандартів у минулих десятиліттях порівняно з сьогоденням. Сучасний світ швидко змінюється, для нового інформаційного століття характерні неуявні досі загрози та кризи.

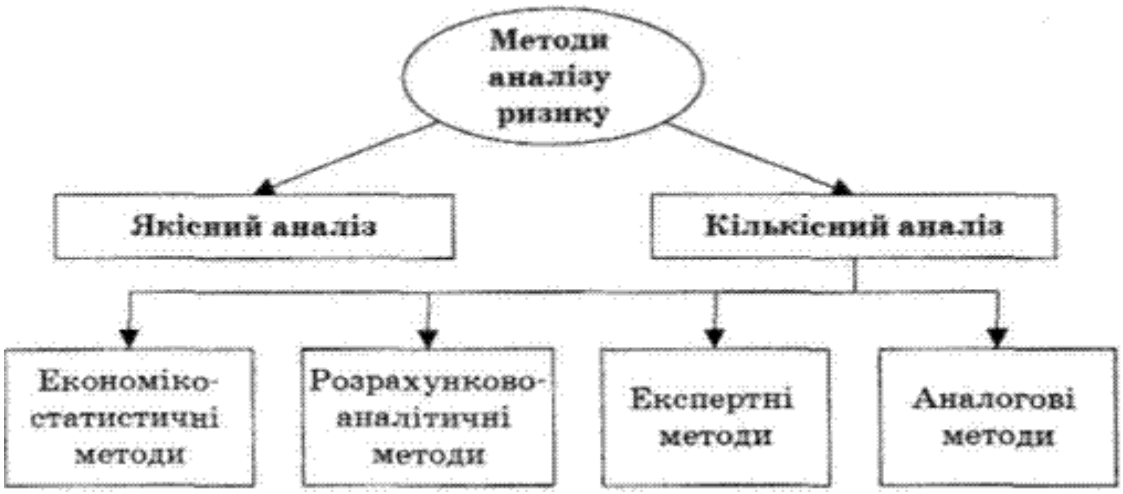

Рис. 2. Схема методів аналізу ризиків

Щоденно реєструється велика кількість мережевих атак і внутрішніх інцидентів інформаційної безпеки. Варто зазначити, що скоординовані атаки на об'єкти інфраструктури (електростанції, телекомунікаційні вузли, системи водо-, тепло-, газопостачання) можуть стати причиною глобальної катастрофи, наслідки якої важко уявити.

Інформаційне забезпечення функціонування ризик-менеджменту складається з різного роду і виду інформації: статистичної, економічної, комерційної, фінансової тощо. Ця інформація включає обізнаність про ймовірність того чи іншого страхового випадку, страхової події, наявність і величину попиту на товари, на капітал, фінансової стійкості та платоспроможності клієнтів, партнерів, конкурентів, ціни, курси й тарифи, в тому числі на послуги, дивіденди і відсотки тощо.

Відповідно до сучасних міжнародних стандартів, ризик — це стан впливу чинників невизначеності на досягання мети. Реалізація ризику призводить до відхилення фактичних результатів діяльності від запланованих. Ризик — це діяльність, пов'язана з подоланням невизначеності в ситуації неминучого вибору, в процесі якої існує можливість кількісно і якісно оцінити ймовірність досягнення передбачуваного результату, невдачі і відхилення від мети.

Сутність сучасної організації пов'язана з використанням існуючих інформаційно-комунікаційних технологій та інших інтелектуальних активів для здійснення господарської діяльності й досягнення цілей. Ця діяльність, як правило, пов'язана з невизначеністю та ризиками. На сьогодні не існує механізмів, що дозволяють повністю

захистити організацію від загроз і ризиків, але ризики можна істотно знизити шляхом впровадження системи управління ризиками інформаційної безпеки.

Інформаційна безпека включає три складові управління: вимоги до управління, політику управління ризиками та механізми ідентифікації, аналіз та оцінку ризику. Вимоги визначаються тими цілями, які ставлять перед собою підприємства для забезпечення безпеки. Політика управління інформаційною безпекою визначається її вагомістю і значенням для ефективної господарської діяльності підприємства. Політика має визначити напрями і заходи досягнення цілей. Організаційно-економічний механізм управління підприємством визначає особливості формування політики. В механізмі управління важливим є визначення інструментів, методів, процедур та інших засобів обґрунтування рішень у процесі забезпечення інформаційної безпеки з визначенням та ідентифікацією всіх видів ризиків.

Методи оцінки ризику поділяються на кількісні і якісні, найбільш ефективним є поєднання цих двох підходів в інтегрованій системі управління ризиками інформаційної безпеки підприємства.

2.8 Методологія оцінки ризиків безпеки IT: кількісні та якісні підходи

Інформаційний ризик – це можливість настання випадкової події в інформаційній системі підприємства, що призводить до порушення її функціонування, зниження якості інформації нижче за допустимий рівень, у результаті чого підприємство зазнає збитків.

Розробка методології оцінки ризиків IT-безпеки є ключовою частиною створення надійної та ефективної програми забезпечення інформаційної безпеки. Всі оцінки ризиків починаються з серії важливих питань. Організації починають оцінювати свої активи. Проаналізувавши інформаційні активи, організація може визначити, які з них представляють найбільший ризик інформаційної безпеки.

Основою будь-якої оцінки ризику інформаційної безпеки є визначення впливу та ймовірності порушення цілісності даних. Незалежно від того, який аналіз використовується (кількісний або якісний), організація повинна ідентифікувати кожну загрозу, що впливає на інформаційну безпеку. Після того, як загрози

визначені, потрібно подивитись інформаційні ресурси, щоб визначити як буде впливати порушення. Одночасно організація має враховувати ймовірність порушення.

Наприклад, анонімне порушення бази даних може мати незначне організаційне пошкодження, при відсутності даних про інтелектуальну власність або даних клієнтів. Дане порушення цілісності даних не несе значного фінансового впливу на компанію.

2.9 Методи кількісної оцінки ризиків інформаційної безпеки

Першою і найбільш простою методологією оцінки ризику безпеки IT є кількісна оцінка ризиків. «Кількісний» означає, що ризик визначається кількісно або вимірюється певними числами, цифрами і відсотками. Ця методологія відповідає на питання «Які фінансові наслідки цього ризику?» та «Скільки даних буде втрачено або скомпрометовано, якби цей ризик був реалізований?». Кількісний аналіз – це визначення конкретного розміру грошового збитку окремих підвидів фінансового ризику та фінансового ризику в цілому.

На даний час найбільш розповсюдженими є:

- статичні методи;
- метод експертних оцінок;
- метод аналогій;
- група аналітичних методів.

Метод експертних оцінок – це евристичний метод, який застосовується у випадках, коли ускладнено знаходження розв’язку математичними методами.

Оцінка ризику виконується на основі суб’єктивних думок експертів-фахівців у конкретній галузі діяльності. Метод експертних оцінок полягає в тому, що команда проекту виділяє певну групу ризиків і розглядає, яким чином вони впливають на діяльність підприємства. Цей розгляд зводиться до подачі бальних оцінок за ймовірність виникнення того чи іншого виду ризику, а також ступеня його впливу на діяльність проекту.

2.9.1 Методика NIST 800-30

Однією з класичних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози. Призначення системи управління ризиками безпосередньо пов'язане з можливістю організацій, установ виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях NIST 800-30, охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, представляється у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий «жорсткий» механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Використання такої методики передбачає наступні етапи:

– опис характеристик системи;

– ідентифікація загроз;

– ідентифікація вразливостей;

– аналіз наявних засобів/заходів захисту;

– визначення значення ймовірності;

– аналіз впливу;

– визначення значення ризику;

– вибір засобів/заходів захисту;

– документування отриманих результатів.

2.9.2 Методика CRAMM

Методика CRAMM (CCTA Risk Analysis and Managment Method), Агентства з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency), що розроблена за поданням Британського уряду і яка прийнята за державний стандарт.

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC.

Грамотне використання методики CRAMM дозволяє отримувати високі результати, серед яких є можливість економічного обґрунтування витрат організації на забезпечення інформаційної безпеки та безперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: «Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?» На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів.

Ця методика, незважаючи на значну універсальність і функціональність, має такі недоліки, як необхідність спеціальної підготовки користувачів і значна вартість ліцензії.

2.9.3 Методика IT-Grundschutz

IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою, яка включає в себе як загальні рекомендації щодо забезпечення безпеки IT, так і допоміжні технічні рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену. У методиці IT-Grundschutz представлені каталоги:

1) модулі;
2) каталоги загроз;
3) каталоги захисту.

Дана методика має більш рекомендаційний, теоретичний характер, ніж практичний.

2.9.4 Методика OCTAVE

В методиках, які були описані раніше існують певні обмеження і суттєві недоліки, складнощі із застосуванням на практиці Методика управління ризиками інформаційної безпеки OCTAVE загальнодоступна й універсальна. Цю методику широко використовують у всьому світі, оцінюючи ризики інформаційної безпеки та впроваджуючи процеси управління ризиками в організаціях загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності.

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена інститутом SoftwareEngineeringInstitute (SEI)при університеті Карнегі-Меллон (США) і передбачає здійснення процесу аналізу ризиків інформаційної безпеки лише працівниками підприємства, тому що вони краще розуміють потреби підприємства і властиві йому ризики.

За цією методикою відбувається розробка профілю загроз, виявлення вразливостей в інформаційній безпеці і розроблення стратегії забезпечення безпеки. Для кожного джерела загроз будується дерево варіантів, яке наочно показує вигляд загрози і шляхи її усунення. При оцінці ризиків інформаційної безпеки формується шкала за трьома позиціями: високий, середній і низький рівень ризику, встановлюється можливий фінансовий збиток. Основною перевагою даної методики є: загальнодоступність і безкоштовність, швидке впровадження, можливість застосування для організацій різного розміру та галузей зайнятості, наявність комерційних програмних продуктів, що реалізують положення методики, високий рівень гнучкості. До недоліків потрібно віднести те, що дана методика не дає кількісної оцінки ризиків.

OCTAVE широко використовують у всьому світі для оцінки ризиків ІБ та впровадження процесів управління ризиками і підприємстві в цілому.

Методика має три модифікації, які розраховані на організації різного розміру:

– методологія оцінки ризиків OCTAVE Method застосовується для достатньо великих підприємств (від 300 робітників та більше);

– спрощена методологія оцінки ризиків OCTAVE-S, орієнтована на підприємства середнього розміру (не більше 100 робітників);

– методологія оцінки ризиків OCTAVE Allegro, яка може застосовуватися консультантами на індивідуальній основі без широкого залучення в процес оцінки ризиків співробітників організації.

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів(рис.1).

Рис.3 Послідовність трьох складових фаз методу OCTAVE

Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять у собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

РОЗДІЛ 3. ПОРЯДОК СТВОРЕННЯ ТА АТЕСТАЦІЯ ПОЛІТИКИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Розробка політики безпеки

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, що виражається через сукупність факторів або критеріїв, які уточнюють мету. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної, безумовно, нетривіальне завдання. Експерт повинен не тільки знати відповідні стандарти і добре розбиратися в комплексних підходах до забезпечення захисту

інформації організації, але й, наприклад, проявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів з організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити такі процеси, пов'язані з розробкою і реалізацією політики безпеки.

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінювання відповідності заходів щодо забезпечення захисту інформації системи деякого еталонного зразка: стандарт, профіль захисту тощо.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданої з безпеки.

4. Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій безпеки для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом, створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно. Відзначимо лише, що для розробки моделей

застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі. Слід відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки дають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що

- всі суб'єкти і об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі, що

1. всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;
2. кожному об'єкту системи привласнена мітка критичності, що визначає цінність, яка міститься в ньому;
3. кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру, і, таким чином, в системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вища його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт, крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала ряду вимог, які будуть розглянуті в наступному розділі.

Створення захищеної роботи

Що означає зробити роботу захищеною? Відповідь заснована на понятті комплексу засобів захисту (КЗЗ) – набору апаратних засобів, програмного забезпечення та інформації з налаштування (setup), від якої залежить захист системи. Взагалі кажучи, не просто з'ясувати, що повинно знаходитися в КЗЗ для даної політики захисту. Щоб захист працював досконалим чином, специфікації для всіх компонент КЗЗ повинні бути досить серйозними, і кожен компонент повинен задовольняти своєї специфікації. Цей рівень сертифікації рідко досягається. По суті, часто погоджуються на щось набагато більш слабке. У будь-якому випадку, має бути ясно, що чим менше розмір КЗЗ – тим краще. Хороший спосіб запобігання шкоди, що можуть заподіяти дефекти в КЗЗ – використовувати захист в глибину (ешелоновану оборону), тобто надлишкові механізми захисту. При цьому порушникові буде складно одночасно використовувати слабкості різних систем на всіх рівнях. Ешелонована оборона не дає строгих гарантій, але насправді, практично допомагає.

Наприклад, система могла б включати: мережевий рівень безпеки; рівень безпеки ОС, використовуючи sandboxing, щоб ізолювати програми. Це може бути зроблено на базовій ОС, такій як Windows (або Unix), або на високорівневій ОС, яку має віртуальна машина Java; рівень безпеки програми, який додатково перевіряє авторизацію. Більшість рішень щодо безпеки було зосереджено на програмних засобах. Але інший важливий компонент КЗЗ є інформація про конфігурацію, кнопки і вимикачі, які говорять програмному забезпеченню, що зробити (setup).

Хоча настроювання набагато простіше ніж програма, воно зазвичай робиться менш кваліфікованими людьми, ніж розробники програм, і в той час, як програма написана одноразово, настроювання різне для кожної інсталяції. Проблема погіршується тим, що настроювання повинно бути засноване на документації для програмного забезпечення, яка є, зазвичай, великою за обсягом, не цілком ясною і неповною. Єдине рішення цієї проблеми полягає в тому, щоб зробити частину настроювання, що відповідає за безпеку, більш простою як для адміністраторів, так

і для користувачів. Не слід робити це, змінюючи базову ОС, так як зміни там важко здійснимі. Замість цього, можна використовувати в своїх інтересах модель безпеки з невеликим числом параметрів настроювання, і потім компілювати ці параметри в численні кнопки і вимикачі базової системи.

Яку форму має прийняти ця модель? Користувачі мають потребу в дуже простій моделі, приблизно з трьома рівнями захисту: я, моя група або підприємство, інші з повноваженнями, які прогресивно зменшуються. Сьогодні браузери класифікують мережу саме таким чином. Персональна інформація, конфіденційні і відкриті відомості повинні бути в трьох частинах файлової системи: мої документи, документи моєї групи і загальні документи. Це комбінує захист даних з тією частиною файлової системи, де вони зберігаються так само, як в реальному світі. Наприклад, так зроблено з дошками оголошень, папками, замкнутими в столах і сейфами. Цей прийом знайомий усім, вимагає меншої роботи, при цьому відразу можна оцінити надійність захисту кожного елемента даних. Адміністратори також потребують досить простої моделі, але вони потребують навіть ще більше в можливості обробити багато користувачів і систем однорідним способом, так як вони не можуть ефективно мати справу з великою кількістю індивідуальних випадків. Одним із способів є визначення, так званих, низькорівневих політик безпеки (НПБ), правил налаштування безпеки, які автоматично застосовуються до груп ПК. Вони включають наступне:

- кожен користувач має право на читання /запис у своїй домашній папці на сервері, і ніхто більше не має цей доступ; - користувач, зазвичай, член однієї з робочих груп, який має доступ до групових домашнім папок на всіх машинах членів групи і на сервері;
- системні папки повинні містити набори файлів, які формують версію ПЗ (реліз), схвалену постачальником;
- всі виконувані програми повинні бути підписані повноважними сторонами.

Щоб робити НПБ керованими, адміністраторам треба визначати групи користувачів і ресурсів, на які вони претендують, і потім коротко сформулювати НПБ в термінах цих груп. В ідеалі, групи ресурсів відображені в структурі файлової

системи, але повинні бути й інші шляхи до їх визначення, щоб прийняти до уваги химерні угоди щодо існуючих мереж, ОС і додатків. Розробники потребують безпечну типизовану мову, яка подібна мові Java. Це усуне безліч дефектів програм. На жаль, більшість дефектів, які ушкоджують захист, знаходяться в системному програмному забезпеченні, яке, наприклад, забезпечує комунікації з мережами. Тому потрібно прагнути до того, щоб системні програми також записувалися подібним чином.

Засоби захисту іеформації

Засоби захисту інформації – це сукупність інженерно-технічних, електричних, електронних, оптичних та інших пристроїв і пристосувань, приладів та технічних систем, які використовуються для вирішення різних завдань із захисту інформації, в тому числі попередження витоку і забезпечення безпеки захищаємої інформації.

В цілому кошти забезпечення захисту інформації в частині запобігання навмисних дій в залежності від способу реалізації можна розділити на групи: технічні (апаратні), програмні, змішані апаратно - програмні, організаційні.

Технічні (апаратні) засоби – це різні за типом пристрої (механічні, електромеханічні, електронні та інші), які апаратними засобами вирішують завдання захисту інформації. Вони перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, перешкоджають доступу до інформації, в тому числі за допомогою її маскування. Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація та ін. Другу – генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, які “перекривають” потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб’єктивних факторів, високу стійкість до модифікації.

До теперішнього часу розроблено значну кількість технічних (апаратних) засобів різного призначення, проте найбільшого поширення набули наступні:

- спеціальні регістри для зберігання реквізитів захисту: паролі, що ідентифікують коди, грифи або рівні секретності;
- пристрої вимірювання індивідуальних характеристик людини (голоси, відбитки пальців і т.д.) з метою її ідентифікації;
- схеми переривання передачі інформації в лінії зв'язку з метою періодичних перевірок адреси видачі даних;
- пристрої для шифрування інформації (криптографічні методи).

Слабкі сторони апаратних засобів захисту – недостатня гнучкість, відносно великі обсяг і маса, висока вартість. Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки – обмежена функціональність мережі, використання частини ресурсів файлсервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів). Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки – висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі. За ступенем поширення і доступності виділяються програмні засоби. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

Загальні принципи інженерно-техничного захисту інформації

Загальновідомо, що відділам безпеки, які займаються захистом інформації, протистоять різні організації і зловмисники, як правило, оснащені апаратними засобами доступу до інформації.

Виходячи з цього, основу захисту інформації повинні складати принципи, аналогічні принципам отримання інформації, а саме:

- безперервність захисту інформації. Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будьякий час;
- активність, яка передбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих захисних заходів;
- скритність, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації;
- цілеспрямованість, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації;
- комплексне використання різних способів і засобів захисту інформації, що дозволяє компенсувати недоліки одних перевагами інших.

Ці принципи хоча і не містять конкретних рекомендацій, проте визначають загальні вимоги до способів і засобів захисту інформації. Наступна група принципів характеризує основні професійні підходи до організації захисту інформації, забезпечує раціональний рівень її захисту і дозволяє: скоротити витрати на відповідність рівня захисту цінності інформації, включаючи гнучкість захисту (можливість модифікації); багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; багаторубіжність захисту інформації на шляху руху зловмисника або поширення носія.

При побудові системи захисту інформації потрібно враховувати також наступні принципи:

- мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;

- надійність в роботі технічних засобів системи, що виключає як нереагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при їх відсутності;
- обмежений і контрольований доступ до елементів системи забезпечення інформаційної безпеки;
- безперервність роботи системи в будь-яких умовах функціонування об’єкта захисту, в тому числі, наприклад, короткочасному відключенні електроенергії;
- адаптованість (пристосовність) системи до змін навколишнього середовища.

Сенс зазначених принципів очевидний, але слід зупинитися докладніше на останньому. Справа в тому, що закрита інформація про способи і засоби захисту інформації в конкретній організації з часом набуває розголосу все більшої кількості людей, в результаті чого збільшується ймовірність попадання цієї інформації до зловмисника. Тому доцільно проводити зміни в структурі системи захисту інформації періодично або при появі досить реальної можливості витоку інформації про систему захисту, наприклад, при раптовому звільнення інформованого співробітника служби безпеки.

3.1.1 Концептуальні підходи до проектування систем захисту

Зараз можна виділити три різних концептуальних підходи до проектування систем захисту.

Підхід перший: "від продукту". Цього підходу дотримуються, як правило, компанії-виробники систем захисту інформації, що мають у своєму складі проектну групу. Фактично, в таких компаніях інтеграція виросла з просто впроваджувального напрямку в той момент, коли замовник попросив не просто продукт, а проект. Таким чином, вся технологія проектування орієнтована на те, щоб продукт, вироблений компанією, був центральним незалежно від розв'язуваної задачі. Даний підхід не завжди реально обґрунтований, особливо в умовах агресивного маркетингу і позиціонування продукту, як "панацеї" від більшості загроз безпеки.

Однак у разі, коли замовник має достатню кваліфікацію, щоб широко дивитися на проблему захисту інформації в цілому і уникати однобоких рішень, реалізуються проекти високої якості, що зрозуміло, адже ніхто, крім виробника не знає продукту краще. Але в цьому випадку потрібна або наявність власних висококласних фахівців, системних архітекторів, або залучення зовнішніх консалтингових компаній.

Позиція друга – компанія виступає постачальником рішень у сфері захисту інформації. Розуміючи відсутність єдиного продукту, що захищає від усіх загроз, компанія пропонує комплексне вирішення проблеми. Воно складається з комбінації декількох технологій захисту, наприклад, міжмережевих екранів для захисту від атак з Інтернету, VPN – для закриття каналів зв'язку і т.п. Ось, здавалося б, оптимальна позиція: кожна технологія, кожен продукт займає свою нішу і усувають певні загрози. Але тут існує одна проблема.

Формально схема виглядає таким чином: зараз існують чотири основні технології захисту – міжмережеве екранування, VPN, криптографічний захист, активний аудит. Кожна технологія має по 3–4 продукти, які дійсно працюють. Тобто, чотири технології по чотири продукти утворюють 16 кубиків, з яких може будуватися система безпеки. Тоді завдання архітектора системи захисту зводиться до того, щоб знайти, куди прилаштувати кожен кубик. Виникає спокуса починати будувати систему, відштовхуючись не від потреб замовника, а від наявних засобів захисту.

Можливо, така технологія роботи була б виправдана в умовах повністю електронного документообігу в організації, але наші реалії такі, що більшість комп'ютерних систем в наших організаціях – це 300–400 друкарських машинок, об'єднаних мережею. В умовах паперового документообігу всі документи готуються на комп'ютері, роздруковуються, а потім у паперовому вигляді рухаються по організації. У мережі існують лише осередки автоматизації, наприклад, у бухгалтерії, в конструкторському відділі іт.п. А всі інші співробітники спілкуються один з одним, в кращому випадку, на e-mail або через спільні папки. Тому буває важко пояснити, навіщо використовувати, наприклад,

VPN, якщо вся інформація надсилається поштою або факсом. Або навіщо встановлювати на комп'ютери електронні замки, якщо всі документи зберігаються в shared папках, не закритих паролями, і їх може отримати практично будь-який співробітник.

Не можна говорити, що підхід від "кубиків" не прийнятний і не життєздатний. В даний час існує великий неосвоєний ринок середніх і дрібних компаній, для яких занадто дорого купувати серйозні консалтингові послуги компаній-інтеграторів. Таким компаніям як раз і потрібен деякий набір продуктів і рішень, які могли б просто об'єднуватися в систему, надаючи їй необхідну функціональність.

Існує ще третя позиція – найскладніша і така, що досить рідко зустрічається на нашому ринку. Яка стандартна схема продажу певного продукту або системи? Постачальник приходить до замовника, вивчає його проблему і пропонує те чи інше рішення, продукт або варіанти рішення, або замовник організує тендер, отримує кілька пропозицій. І в тому, і в іншому випадку замовник самостійно приймає рішення про те, яку систему, технологію впроваджувати. Тобто, відповідальність за прийняття рішень щодо захисту інформації покладається на замовника, який, взагалі кажучи, не є експертом в галузі захисту інформації. Найскладніше завдання, яке може і повинно стояти перед компанією-інтегратором, це прийняти на себе відповідальність за вибір стратегії забезпечення безпеки організації, розвиток системи, її адекватність технологіям, що розвиваються. Системний інтегратор повинен реалізовувати єдину комплексну політику, як технічну, так і організаційну, проводячи її на всіх рівнях організації-замовника.

Перед виробленням рішення з інформаційної безпеки інтегратор повинен провести всебічне глибоке обстеження не просто інформаційної системи замовника, а всього "інформаційного життя" організації. Обстеження має вестися на трьох рівнях: на рівні бізнес-процесів, який виявляє документальні потоки, типи оброблюваної інформації, рівні її конфіденційності; на інфраструктурному рівні – для виявлення вразливих місць серверного парку, мережевого обладнання; на рівні додатків, на якому виявляються уразливості в програмному забезпеченні, помилки в налаштуваннях механізмів розмежування доступу та ін.

На основі отриманих даних необхідно сформувати спочатку концептуальне рішення щодо захисту інформації, що складається з комплексу організаційних, процедурних і програмно-апаратних засобів захисту, а потім, чітко обґрунтовуючи вибір, пропонувати впровадження тих чи інших технологій захисту. При цьому потрібно враховувати, що підсистема інформаційної безпеки є підтримувальною системою стосовно всієї інформаційної системи організації. Вона не повинна відігравати домінуючу роль у розвитку організації та її інформаційної системи. Тобто система інформаційної безпеки повинна захищати інформацію, що забезпечує бізнес-завдання організації.

Таким чином, будь-яка система інформаційної безпеки, що захищає велику організацію з розподіленою інформаційною системою, або система, що являє собою один міжмережевий екран, повинна бути розумно достатньою щодо організації, вона не повинна заважати роботі працівників. Завжди повинен бути адекватний вибір рівня захисту, правильний вибір технологій і засобів захисту.

3.1.2 Визначення й аналіз загроз

Говорити про безпеку об'єкта (системи) можна, лише маючи на увазі, що за допомогою цього об'єкта або над цим об'єктом відбуваються якісь дії. У цьому сенсі, якщо об'єкт не діє, а саме: не функціонує (не використовується, не розвивається і т. д.), або, кажучи іншими словами, не взаємодіє з зовнішнім середовищем, то і розглядати його безпеку безглуздо. Отже, об'єкт необхідно розглядати в динаміці та у взаємодії із зовнішнім середовищем.

Рис. 4 Види загроз інформаційної безпеки

У деяких випадках можна говорити про безпеку системи при її зберіганні. Але навіть при зберігання системи взаємодія з зовнішнім середовищем неминуча.

При функціонуванні об'єкта завжди переслідуються певні цілі. Сукупність дій, що здійснюються об'єктом для досягнення певної мети, реалізується у вигляді результатів, які мають значення для самого об'єкта. Якщо мета операції або сукупності цілеспрямованих дій досягнута, то безпеку операції, а отже, інформації, що циркулює в системі, забезпечено.

Проблема дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації, а також пошуку та обґрунтування комплексу заходів і засобів з їх усунення або зниження характеризується такими особливостями:

– великою кількістю чинників небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;

– необхідністю виявлення і вивчення повного спектра можливих заходів і засобів парирування небезпечних факторів з метою забезпечення безпеки.

Відносно інформаційної системи всю сукупність загроз можна розбити на дві групи: зовнішні і внутрішні, кожна з яких, в свою чергу, ділиться на умисні й випадкові загрози, які можуть бути явними і прихованими.

Виявлення та аналіз загроз захисту є відповідальним етапом при побудові системи захисту інформації на підприємстві. Більшість фахівців вживають термін «загрози безпеки інформації». Але безпека інформації – це стан захищеності інформації від впливів, що порушують її статус. Отже, безпека інформації означає, що інформація знаходиться в такому захищеному вигляді, який здатний протистояти будь-яким дестабілізувальним впливам.

Будь-яка загроза не зводиться до чогось однозначного, вона складається з певних взаємопов'язаних компонентів, кожен з яких сам по собі не створює загрозу, але є її невід'ємною частиною, загроза виникає лише при сукупній їх взаємодії.

Загрози захисту інформації пов'язані з її вразливістю, тобто нездатністю інформації самостійно протистояти таким дестабілізувальним впливам, що порушують її статус. Реалізація загроз призводить, в залежності від їх характеру, до однієї або кількох форм прояву уразливості інформації. При цьому кожній з форм прояву уразливості (або декільком з них) притаманні певні, що стосуються тільки до її загрози з набором відповідних компонентів. Структура конкретної загрози зумовлює конкретну форму. Однак повинна існувати і загальна, так би мовити, типова структура загроз, яка складає основу конкретних загроз. Ця загальна структура повинна базуватися на певних ознаках, характерних для загрози захисту інформації.

Перш за все, загроза повинна мати якісь сутнісні прояви. А будь-який прояв, виявлення чогось прийнято називати явищем. Отже, однією з ознак і разом з тим однією зі складових загрози повинні бути явища.

Але в основі будь-якого явища лежать відповідні причини, які є його рушійною силою і які, в свою чергу, зумовлені певними обставинами або передумовами. Ці причини і обставини (причини) відносяться до чинників, що створюють

можливість дестабілізувального впливу на інформацію. Таким чином, фактори є ще одним приймачем і другою складовою загрози.

Разом з тим чинники можуть стати спонукальною силою для явищ, а останні можуть «спрацювати» лише при наявності певних умов (обставин) для цього. Наявність умов для дестабілізувального впливу на інформацію є третьою ознакою і ще одною складовою загрози.

Визначальною ознакою загрози є її спрямованість, результат, до якого може призвести дестабілізувальний вплив на інформацію. Цим результатом у всіх випадках реалізацій загрози є порушення статусу інформації.

Таким чином, загроза інформації – це сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації.

До явищ сутнісних проявів загрози, відносять:

– джерела дестабілізувального впливу на інформацію (від кого або від чого виходить дестабілізувальний вплив);

– види дестабілізувального впливу на інформацію (яким чином (за якими напрямами) відбувається дестабілізувальний вплив);

– способи дестабілізувального впливу на інформацію (якими прийомами, діями здійснюються (реалізуються) види дестабілізувального впливу).

До факторів, крім причин і обставин, слід віднести наявність каналів і методів несанкціонованого доступу до конфіденційної інформації для впливу на інформацію з боку осіб, які не мають до неї дозволеного доступу.

Що стосується складу структурних частин загрози, то необхідно підкреслити: стрижневими, вихідними є джерела дестабілізувального впливу на інформацію, від їх складу залежать і види, і способи, і кінцевий результат впливу. Хоча склад інших структурних частин загрози також відіграє істотну роль, він на відміну від джерел, не носить визначального характеру і прямо залежить від джерел. Разом з тим ще раз слід зазначити, що джерела самі по собі не є загрозою, якщо від них не виходить той чи інший вплив.

Найпоширенішим, різноманітним і найнебезпечнішим джерелом дестабілізувального впливу на захищувану інформацію є люди, які ділять на такі категорії:

- співробітники даного підприємства;
- особи, які не працюють на підприємстві, але мають доступ до інформації, що захищається підприємством в силу службового становища;
- співробітники державних органів розвідки інших країн і розвідувальних служб конкуруючих вітчизняних та зарубіжних підприємств - конкурентів;
- особи з кримінальних структур, хакери.

У частині співвідношення з видами і способами дестабілізувального впливу на інформацію ці категорії людей поділяються на дві групи: мають доступ до носіїв захищуваної інформації, технічних засобів її відображення, зберігання, обробки, відтворення, передачі і систем забезпечення їх функціонування і не мають такого.

Різниця в конкретно застосовуваних видах і методах дестабілізувального впливу на інформацію між названими групами людей (при однотипності видів і методів) зумовлена переслідуваними цілями. Основною метою другої групи людей є несанкціоноване отримання (розкрадання) інформації, що є ІзОД. Знищення, перекручення, блокування інформації стоять на другому плані, а нерідко і не є метою. Дестабілізувальний вплив з боку цієї групи людей в переважній більшості випадків є навмисним (умисним, свідомим). До того ж, для того щоб здійснити дестабілізувальний вплив на конфіденційну інформацію, людям, що входять в цю групу, потрібно мати канал несанкціонованого доступу до неї.

Для ***першої групи*** людей несанкціоноване отримання ІзОД взагалі не є метою в силу наявності у них доступу до такої інформації. Цілями дестабілізувального впливу з боку цієї групи є розголошення, несанкціоноване знищення, блокування, спотворення інформації (перераховано послідовно, відповідно до ступеня інтенсивності впливу, від більшої інтенсивності до меншої). Розкрадання інформації також притаманне даній групіи, але воно є не метою, а засобом для здійснення знищення або розголошення інформації. Предметом впливу з боку цієї групи є не тільки конфіденційна інформація (хоча вона в першу чергу), але і

захищувана частина відкритої інформації. Вплив з боку людей, що входять до цієї групи, може бути як навмисним, і ненавмисним (помилковим, випадковим). Слід, однак, домовитися про те, що по об'єктах доступу ця група неоднорідна за своїм складом. До неї входять люди, які мають доступ і до носіїв захищуваної інформації, і до засобів відображення, зберігання, обробки, відтворення і передачі інформації (до всіх або частини з них), і до систем забезпечення функціонування цих засобів, люди, які мають доступ тільки до інформації і (іноді або) до засобів її обробки (всіх або окремих); люди, допущені тільки до системи забезпечення функціонування засобів.

Найрізноманітнішим це джерело є тому, що йому, порівняно з іншими джерелами, притаманна значно більша кількість видів і способів дестабілізувального впливу на інформацію.

Найнебезпечнішим це джерело є тому, що, по-перше, воно наймасовіше, по-друге, сторонній вплив носить не епізодичний, а постійний характер, по-третє, як уже зазначалося, його вплив може бути не тільки ненавмисним, як з боку інших джерел, але і навмисним, і, по-четверте, цей вплив може призвести до всіх форм прояву уразливості інформації (з боку інших джерел – до окремих форм).

Друге джерело дестабілізувального впливу на інформацію охоплює системи електропостачання, водопостачання, теплопостачання, кондиціонування.

До ***третього джерела*** відносяться технологічні процеси об'єктів ядерної енергетики, хімічної промисловості, радіоелектроніки, а також об'єктів з виготовлення деяких видів озброєння і військової техніки, які змінюють природну структуру навколишнього середовища.

3.1.3 Методика виявлення способів впливу на інформацію

Залежно від джерела і виду свого впливу він може бути безпосереднім на захищувану інформацію або опосередкованим, через інше джерело впливу.

З боку людей можливі такі види впливу:

1. Безпосередній вплив на носії захищуваної інформації;
2. Несанкціоноване розповсюдження конфіденційної інформації;

3. Вихід з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку;
4. Порушення режиму роботи перерахованих засобів та технології обробки інформації;
5. Вихід з ладу і порушення режиму роботи систем забезпечення функціонування названих засобів.

Способами безпосереднього впливу на носії захищуваної інформації можуть бути: фізичне руйнування носія (поломка, руйнування і ін.), створення аварійних ситуацій для носіїв (підпал, штучне затоплення, вибух і т. д.), видалення інформації з носіїв, створення штучних магнітних полів для розмагнічування носіїв, внесення фальсифікованої інформації у носії.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення і блокування.

До безпосереднього впливу на носії захищуваної інформації можна з застереженням віднести і ненавмисне залишення їх в неохоронній зоні, найчастіше в громадському транспорті, магазині, на ринку, що призводить до втрати носіїв.

Несанкціоноване розповсюдження ІзОД може здійснюватися шляхом:

– словесної передачі (повідомлення) інформації;

– передачі копій (знімків) носіїв інформації;

– показу носіїв інформації;

– введення інформації в обчислювальні мережі;

– опублікування інформації в пресі;

– використання інформації у відкритих публічних виступах, в тому числі по радіо, телебаченню.

До розголошення може призвести і втрата носіїв інформації. Цей вид дестабілізувального впливу призводить до розголошення ІзОД.

До видів дестабілізуючого впливу на захищувану інформацію з боку іншого джерела впливу – технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку – відносять:

1. Виведення засобів з ладу;

2. Збої в роботі засобів;

3. Створення електромагнітних випромінювань.

Вихід засобів з ладу, що призводить до неможливості виконання операцій, може відбуватися шляхом:

– технічної поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);

– виходу з ладу систем забезпечення функціонування засобів;

– впливу природних явищ;

– впливу зміненої структури навколишнього магнітного поля;

– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– руйнування або пошкодження носія інформації, в тому числі розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, перекручення, блокування.

Збої в роботі засобів, що призводять до неправильного виконання операцій (помилок), можуть відбуватися в зв’язку з:

– виникненням технічних несправностей елементів засобів;

– зараженням програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– впливом природних явищ;

– впливом навколишнього магнітного поля;

– частковим розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку;

– порушенням режиму функціонування засобів.

Даний вид дестабілізувального впливу призводить до реалізації чотирьох форм прояву уразливості інформації: знищення, перекручення, блокування, розголошенню (приклад останньої – телефонне з’єднання не з тим абонентом, який набирався, або чутність розмови інших осіб через несправність в ланцюгах комунікації телефонної станції). Електромагнітні випромінювання, в тому числі

побічні, що утворюються в процесі експлуатації засобів, призводять до розкрадання інформації.

Наступне джерело дестабілізувального впливу на інформацію – системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації – має два види впливу:

1. Вихід систем з ладу.

2. Збої в роботі систем.

Вихід систем з ладу може відбуватися шляхом:

– поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);

– виходу з ладу джерел живлення;

– впливу природних явищ.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, блокування, викривлення.

Збої в роботі систем можуть здійснюватися за допомогою:

– появи технічних несправностей елементів систем;

– впливу природних явищ;

– порушення режиму роботи джерел живлення.

Результатом дестабілізувального впливу також є знищення, блокування, спотворення інформації.

Видом дестабілізувального впливу на інформацію з боку технологічних процесів окремих промислових об'єктів є зміна структури навколишнього середовища. Це вплив здійснюється шляхом:

– зміни природного радіаційного фону навколишнього середовища, що відбуваються при функціонуванні об'єктів ядерної енергетики;

– зміни хімічного складу навколишнього середовища, що відбувається при функціонуванні об'єктів хімічної промисловості;

– зміни локальної структури магнітного поля, що відбуваються внаслідок діяльності об'єктів радіоелектроніки і з виготовлення деяких видів озброєння і військової техніки.

Цей вид дестабілізувального впливу в кінцевому підсумку призводить до розкрадання ІзОД.

Останнє джерело дестабілізувального впливу на інформацію – природні явища, що охоплюють стихійні лиха і атмосферні явища (коливання).

До стихійних лих і одночасно видів впливу слід віднести: землетруси, повені, шторми, зсуви, лавини, виверження вулканів; до атмосферних явищ (видів впливу): грозу, дощ, сніг, перепади температури і вологості повітря, магнітні бурі.

Способами впливу з боку і стихійних лих, і атмосферних явищ можуть бути руйнування (поломки), землетруси, загоряння носіїв інформації засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку, систем забезпечення функціонування цих засобів, порушення режиму роботи засобів і систем, а також технології обробки інформації, створення паразитних наведень (грозові розряди).

Ці види впливу призводять до п'яти форм прояву уразливості інформації: втрати, знищення, перекручення, блокування і розкрадання.

При розгляді ознак і складових загрози захищуваній інформації було сказано, що в основі будь-якого дестабілізувального впливу лежать певні причини, спонукальні мотиви, які зумовлюють появу того чи іншого виду і способу впливу. Разом з тим і причини мають під собою підстави – обставини або передумови, які викликають ці чинники, сприяють їхній появі. Однак наявність джерел, видів, способів, причин і обставин (передумов) дестабілізувального впливу на інформацію є потенційно існуючою небезпекою, яка може бути реалізована тільки при наявності певних умов для цього.

3.2 Розроблення плану захисту інформації

На цьому етапі розробляється план ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначаються зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ОІД.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

Заходи захисту інформації повинні:

- бути відповідними загрозам;
- бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;
- забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог ТЗІ.

Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) регламентується нормативними документами системи ТЗІ.

3.3 Реалізація плану захисту інформації

На цьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

Засоби ТЗІ можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право проведення цих робіт, видану Державною службою спеціального зв’язку та захисту інформації України.

3.4 Організація проведення обстеження об’єктів інформаційної діяльності

Метою обстеження об’єктів інформаційної діяльності є вивчення їхньої ІД, визначення об`єктів захисту, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

У ході обстеження необхідно:

1. провести аналіз умов функціонування ОІД підприємства, їх розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

2. дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;
3. вивчити схеми засобів і систем життєзабезпечення ОІД (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;
4. дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі – оброблення) інформації і провести необхідні вимірювання;
5. визначити наявність та технічний стан засобів забезпечення ТЗІ;
6. перевірити наявність на ОІД нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;
7. виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;
8. визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;
9. визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна містити:

- генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;
- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;
- оцінку шкоди, яка передбачається від реалізації загроз.

3.5 Реалізація організаційних заходів захисту

Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

У процесі розроблення і реалізації організаційних заходів потрібно визначити окремі задачі захисту ІзОД. Обґрунтувати структуру і технологію функціонування системи захисту інформації, розробити і впровадити правила реалізації заходів ТЗІ. Також визначити і встановити права та обов`язки підрозділів і осіб, що беруть участь в обробленні ІзОД. Необхідно придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними ОІД підприємства. Установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ, визначити зони безпеки інформації. Розробити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування та забезпечити керування системою захисту інформації.

3.6 Реалізація основних технічних заходів захисту

У процесі реалізації основних технічних заходів захисту потрібно:

– установити засоби виявлення та індикації загроз і перевірити їхню працездатність;

– установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;

– застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє тестування і тестування на відповідність вимогам захищеності;

– застосувати спеціальні інженерно-технічні споруди, засоби (системи).

Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації.

Фрагментарний захист забезпечує протидію певній загрозі.

Комплексний захист забезпечує одночасну протидію безлічі загроз.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

Програмні засоби застосовуються для забезпечення:

– ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

– розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

– цілісності інформації та конфігурації автоматизованих систем;

– реєстрації та обліку дій користувачів;

– маскування оброблюваної інформації;

– реагування (сигналізація, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації.

До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, серед них систем заземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять у відповідній експлуатаційній документації.

3.7 Атестація системи захисту інформації

Атестація комплексу ТЗІ (далі – атестація) здійснюється за відповідними програмою і методиками випробувань.

На підставі результатів випробувань складається висновок щодо відповідності стану ТЗІ, який забезпечується комплексом, вимогам нормативних документів з ТЗІ.

Атестація може бути первинною, черговою та позачерговою. Первинна атестація здійснюється після (або під час) приймання робіт із створення комплексу ТЗІ. Термін проведення чергової атестації визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації.

Позачергову атестацію проводять у разі змін умов функціонування ОІД, що приводять до змін загроз для інформації, та за висновками органів, які контролюють стан ТЗІ.

Етапи атестації:

- визначення організації-виконавця атестації та оформлення відповідних організаційних документів;
- аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ та розроблення і оформлення Програми і методик атестації (ПМА);
- проведення випробувань відповідно до ПМА та оформлення протоколів випробувань і підсумкового документа – акта атестації.

Суб'єкти атестації:

- Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язок);
- організації-замовники атестації;
- організації-виконавці атестації.

Державна служба спеціального зв’язку та захисту інформації України:

- організує розроблення та вдосконалення нормативних документів з атестації;

- контролює виконання вимог щодо атестації та розглядає апеляції;
- узгоджує вибір організації-виконавця атестації, ПМА та результати атестації на особливо важливих ОІД.

Витрати на проведення атестації вносять до кошторису на проектування, будівництво та експлуатацію (утримання) ОІД.

Організацією-виконавцем атестації може бути підприємство, установа чи організація, які мають відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.

Відносини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентуються укладеним між ними договором.

У разі проведення атестації на особливо важливих ОІД визначення організації-виконавця атестації узгоджується з Держспецзв'язку.

Організація-виконавець за результатами аналізу відомостей, наданих організацією-замовником, та, за необхідності, за результатами аналізу умов функціонування ОІД і загроз для інформації безпосередньо на ОІД розробляє проект ПМА та подає його на узгодження організації-замовнику.

Узгоджений організацією-замовником проект ПМА затверджує організація-виконавець.

У разі атестації комплексу ТЗІ на особливо важливих ОІД проект ПМА узгоджується також з Держспецзв'язку.

Організація-замовник створює умови проведення атестації, передбачені договором та ПМА.

До акта атестації додаються протоколи випробувань, передбачених ПМА.

За результатами атестації заповнюється технічний паспорт на комплекс ТЗІ.

У разі проведення атестації на особливо важливих ОІД матеріали з атестації у 5-денний термін організація-виконавець надає Держспецзв'язку. Держспецзв'язку у 2-тижневий термін розглядає результати атестації, приймає рішення щодо можливості їх узгодження, реєструє акт атестації та надсилає його організації-замовнику, одночасно інформуючи про це організацію-виконавця.

3.8 Контроль функціонування та керування системою захисту інформації

Контроль за функціонуванням системи ТЗІ на об’єктах інформаційної діяльності підприємства здійснюється з метою визначення й удосконалення стану ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ, виявлення та запобігання порушенням з ТЗІ в інформаційних системах та об'єктах.

Контроль стану ТЗІ в підрозділах підприємства організується відповідно до планів, затверджених керівниками зазначених органів, шляхом проведення перевірок.

Перевірки стану ТЗІ здійснюються безпосередньо комісіями, на які покладається забезпечення ТЗІ.

Організація проведення перевірок стану ТЗІ, заходи з ТЗІ, які підлягають контролю, висновки та рекомендації визначаються нормативно-правовими актами з питань ТЗІ.

Контрольно-інспекційна робота з питань ТЗІ охоплює планування та проведення перевірок стану ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій щодо вдосконалення заходів з ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

При комплексній перевірці вивчається та оцінюється стан ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ.

При цільовій (тематичній) перевірці вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ТЗІ в підрозділах, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ТЗІ.

При контрольній перевірці перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки.

Зазначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою керівництва підприємства в разі виникнення потреби визначення повноти та достатності заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

Перевірки здійснюються комісіями підприємства, на які покладено виконання завдань щодо здійснення контролю за функціонуванням системи ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ в виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Необхідно провести аналіз функціонування системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати дані для керування системою захисту інформації.

Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

Контроль організаційних заходів з ТЗІ в підрозділах підприємства складається з перевірки:

- переліку відомостей, що підлягають технічному захисту;
- окремої моделі загроз для інформаційної системи або об'єкта;
- плану контрольованої зони органу, щодо якого здійснюється ТЗІ;
- переліку виділених приміщень органу, щодо якого здійснюється ТЗІ, інформаційних систем та об'єктів;
- проведення категоріювання виділених приміщень та об'єктів.

Контроль організаційно-технічних і технічних заходів щодо ТЗІ у виділених приміщеннях, інформаційних системах та об'єктах, повноти та достатності робіт з атестації виділених приміщень містить перевірку відповідності виконання цих заходів нормативно-правовим актам з питань ТЗІ.

Організаційно-технічні й технічні заходи з ТЗІ у виділених приміщеннях, інформаційних системах та об'єктах, роботи з атестації виділених приміщень

виконуються власними силами або суб'єктами підприємницької діяльності в галузі ТЗІ.

За результатами комплексної перевірки комісією складається акт перевірки стану та ефективності заходів з технічного захисту інформації, а цільової та контрольної перевірки – довідка за довільною формою. Ознайомлення керівника суб'єкта системи ТЗІ з актом (довідкою) здійснюється під розпис.

Керівник підрозділу зобов'язаний вжити невідкладних заходів щодо усунення недоліків і реалізації пропозицій комісії відповідно до вимог нормативно-правових актів з питань ТЗІ.

Порушення встановлених норм та вимог з ТЗІ, виявлені під час проведення перевірок, поділяються на три категорії:

Перша – невиконання норм та вимог з ТЗІ, внаслідок чого створюється реальна можливість порушення конфіденційності, цілісності й доступності інформації або її витоку технічними каналами;

Друга – невиконання норм та вимог з ТЗІ, внаслідок чого створюються передумови для порушення конфіденційності, цілісності і доступності інформації або її витоку технічними каналами;

Третя – невиконання інших вимог з ТЗІ.

У разі виявлення порушення першої категорії вживають таких заходів, голова комісії негайно доповідає керівництву підприємства про факт порушення для прийняття рішення про припинення робіт, які проводились з порушенням норм і вимог ТЗІ. Здійснюються заходи з усунення порушень у терміни, погоджені з підрозділом, на який покладено забезпечення ТЗІ.

Організовується в установленому порядку розслідування причин, які призвели до порушень, з метою недопущення їх у подальшому і притягнення осіб, які допустили порушення нормативно-правових актів з питань ТЗІ, до відповідальності згідно з законодавством України.

Дозвіл на відновлення робіт, під час виконання яких були виявлені порушення норм і вимог ТЗІ першої категорії, дає керівник підприємства за погодженням з

підрозділом, на який покладено забезпечення ТЗІ після усунення порушень і перевірки достатності та ефективності вжитих заходів з ТЗІ.

Керівництво підприємства зобов'язано надавати комісії повну інформацію стосовно впроваджених заходів з ТЗІ та сприяти проведенню їх перевірки.

ВИСНОВКИ

В магістерський роботі було визначено поняття інформаційної безпеки, сформовано складові схеми реалізації інформаційної безпеки підприємства, а також було охарактеризовано конкретні цілі, вимоги та задачі, що висуваються до політики безпеки.

Були розгялнуті основні підходи та призначення для створення універсальної політики безпеки, обстеження загроз, середовищь функціонування ІТС та методолігя оцінки ризиків.

Були розглянуті такі методики кількісної оцінки ризиків, як NIST 800-30, CRAMM, OCTAVE та IT-Grundschutz, визначені їх характеристики та основні принципи їх роботи.

Також було наведено принцип розробки політики безпеки, концептуальні підходи до створення універсальної політики безпеки, реалізація плану захісту інформації та основніх організаційних і технічних заходів захисту інйормації її атестація і контроля функціонування та керування системою захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
2. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.
3. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Девянин П. Н. Модели безопасности компьютерных систем : учебное пособие для студ. Высш. Учеб. Заведений – М. : Издательский центр "Академия", 2005. – 144 с.
5. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. / В. В. Домарев. – К. : ТИД "ДС", 2004. – 688 с.
6. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
7. https://www.nist.gov/privacy-framework/nist-sp-800-30.
8. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
9. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
10. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.
11. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".
12. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".
13. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. [Електронний ресурс] / Г. Я. Аніловська. – Режим доступу : http://www.nbuv.eov.ua/.
14. Бердинский А. Концепция безопасности коммерческого банка [Елекшонный ресурс] / А. Бердинский. – Режим доступу : www.bre.ru/.
15. Аволио Ф.М. Защита информации на предприятии / Ф.М. Аволио, Г. Шипли // Сети и системы связи. – 2000. – № 8. – 91-99 с.
16. Диффи У. Защищенность и имитостойкость / У. Диффи, М. Хеллман // Введение в криптографию. – 1979. – № 3. – 79-109 с.

17. Blokdyk G. Cyber-attack Vulnerability Management A Complete Guide - 2019 Edition / Gerardus Blokdyk., 2019. – 328 с.
18. NIST. Creating a Patch and Vulnerability Management Program / NIST., 2013. – 78 с.
19. Palmaers T. Implementing a Vulnerability Management Process / Tom Palmaers. – SANS, 2019. – 24 с.
20. IBM. IBM Security QRadar Vulnerability Manager / IBM., 2014. – 6 с.
21. IBM. IBM X-Force 2012 Trend and Risk Report / IBM., 2014. – 96 с.
22. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
23. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
24. ДСТУ 2941-94. Системи оброблення інформації. Розроблення систем. Терміни та визначення. Чинний від 28.11.1994 р. - К.: Держстандарт України, 1994. - 19 с.
25. Ковальская И.А., Тимофеев Д.С. Методы измерения рисков информационной безопасности.
26. Козлова Е.А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. Молодой учёный. Ежемесячный научный журнал №5 (52)/2013.