Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Пінчука Костянтина Олександровича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації для зменшення впливу антропогенних загроз на основі оцінки їх ризиків*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Мацюк С.М.			
розділів:				
спеціальний	к.т.н., доц. Мацюк С.М.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Пінчуку Костянтину Олександровичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації для зменшення впливу антропогенних загроз на основі оцінки їх ризиків***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати процес створення політики безпеки на основі нормативно-правового забезпечення України та міжнародних стандартів та визначено	20.10.2022
Розділ 2	Виконати аналіз статистики інцидентів України та світу в сфері інформаційної безпеки, обгрунтувати вибір метода оцінки ризиків антропогенних загроз та розробити рекомендації щодо заходів, направлених на зменшення впливу антропогенних загроз.	16.11.2022
Розділ 3	Розрахувати вартість створення опитувальників та впровадження рекомендацій щодо зменшення ймовірності виникнення антропогенних загроз та зробити висновок щодо доцільності впровадження їх компаніями.	05.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 110 с., 13 рис., 5 табл., 5 додатка, 14 джерел.

Мета роботи: запропонувати процедуру обрання методу оцінки ризиків інформаційної безпеки для загроз пов'язаних з персоналом.

Об`єкт дослідження: процес розробки політики безпеки інформації.

У першому розділі проаналізовано процес створення політики безпеки на основі нормативно-правового забезпечення України та міжнародних стандартів та визначено, що аналіз та оцінка ризиків – процеси, що є основою для створення політики безпеки.

У спеціальній частині проаналізовано статистику інцидентів України та світу в сфері інформаційної безпеки, обгрунтовано вибір метода оцінки ризиків антропогенних загроз та розроблено рекомендації щодо заходів, направлених на зменшення впливу антропогенних загроз.

У економічному розділі розраховано вартість створення опитувальників та впровадження рекомендацій щодо зменшення ймовірності виникнення антропогенних загроз та зроблено висновок щодо доцільності впровадження їх компаніями.

Новизна роботи полягає у визначенні елементів політики безпеки інформації пов'язаних з протидією антропогенним загрозам.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОЦІНКА РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ.

ABSTRACT

Explanatory note: _110_ p., _13_ pic., _5_ tabl., _14_ app., _5_ sources.

Purpose: to propose a procedure for selecting a method of assessing information security risks for personnel-related threats.

Object of study: the process of developing information security policy.

The first section analyzes the process of creating a security policy based on the legal framework of Ukraine and international standards and determined that risk analysis and assessment are the processes that are the basis for creating a security policy.

The special part analyzes the statistics of incidents in Ukraine and the world in the field of information security, substantiates the choice of the method of risk assessment of anthropogenic threats and develops recommendations for measures aimed at reducing the impact of anthropogenic threats.

In the economic section, the cost of creating questionnaires and implementing recommendations to reduce the likelihood of anthropogenic threats is calculated and a conclusion is made about the feasibility of their implementation by companies.

The novelty of the work is to determine the elements of information security policy related to countering anthropogenic threats.

INFORMATION SECURITY, INFORMATION SECURITY POLICY, RISK ASSESSMENT, THREAT MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

Д – доступність;

ІБ – інформаційна безпека;

К – конфіденційність;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОС – операційна система;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

СЗІ – система захисту інформації;

СМБ – сегмент середнього і малого бізнесу;

СУБД – система управління базами даних;

ТОВ – товариство з обмеженою відповідальністю;

Ц – цілісність.

ЗМІСТ

с.

ВСТУП

Сучасний світ створює багато викликів, пов’язаних з інформаційною безпекою. Організація забезпечення безпеки інформації повинна носити комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків. При цьому важливо не випустити істотні аспекти.

Аналіз негативних наслідків припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву і, як наслідок, визначення актуальних загроз безпеки інформації. Одне з найпоширеніших і небезпечних джерел загроз – антропогенні. Природа їх є зрозумілою, проте сталих методів оцінки не застосовується.

Саме отримана оцінка ризиків є основою для створення політики безпеки інформації – документу, котрий регулює вимоги безпеки, систему заходів та механізмів контролю.

І саме тому процес оцінки ризиків інформаційної безпеки для загроз, пов’язаних з персоналом, є важливим етапом як при створенні документу політики безпеки, так і при наявному документі, адже, залежно від результатів оцінки, може суттєво його змінити.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз процесу розробки політики безпеки інформації

Інформація та процеси, що її підтримують, системи і мережі є важливими бізнес-активами. Визначення, досягнення, підтримка та вдосконалення інформаційної безпеки можуть бути суттєвим для підтримки конкурентоспроможності, готівкового обігу, рентабельності, відповідності законодавству та комерційної репутації. Все частіше бізнес-активи зіштовхуються із різними загрозами безпеки. Тому актуальною є задача інформаційного захисту.

Згідно міжнародного стандарту серії ISO/IEC 27002, котрий прийнятий як галузевий стандарт «Звід правил для управління інформаційною безпекою» Національним банком України, інформаційна безпека – процес збереження конфіденційності, цілісності та доступності інформації, крім того можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність (останні три властивості є обов'язковими вимогами інформаційної безпеки, якщо мова йде про банки України).

І саме наявність політики інформаційної безпеки свідчить про зрілість та компетентність підприємства у питаннях забезпечення інформаційної безпеки. Політика безпеки є найдешевшим та одночасно найефективнішим засобом забезпечення інформаційної безпеки.

Політика інформаційної безпеки повинна представляти сукупність вимог, правил, положень та прийнятих рішень, що визначають:

- порядок доступу до інформаційних ресурсів;
- необхідний рівень (клас та категорію) захищеності об'єктів інформатизації;
- організацію захисту інформації в цілому;
- додаткові вимоги щодо захисту окремих компонентів;
- основні напрямки та способи захисту інформації.

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему

заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства.

Щодо структури політики безпеки, рекомендації можна знайти в додатку D міжнародного стандарту серії ISO/IEC27003. Згідно стандарту, в загальному розумінні політика – загальні наміри та вказівки, офіційно викладені керівництвом. Організація може мати декілька політик, по одній для кожної важливої сфери діяльності організації. Щодо політики в сфері інформаційної безпеки, зазвичай такі є ієрархічно структуровані, мають декілька рівнів:

- загальні політики високого рівня (наприклад, політики безпеки, політики секретності, політика розробки продукції);
- політики високого рівня за окремими напрямками;
- детальні політики (наприклад, політика контролю доступу, політика «чистого стола» та «чистого екрана», політика використання мережевих служб).

Зміст політики безпеки має бути скорельований з цілями та задачами організації, структурою і процесами, що наявні в організації, вимогами політик високого рівня (рис.1.1).

Політика безпеки загалом має містити наступні положення:

1) визначення інформаційної безпеки, її загальних цілей і галузі застосування, а також важливості безпеки як механізму уможливлення розповсюдження інформації;

2) положення щодо намірів і підтримки керівництвом мети та принципів інформаційної безпеки згідно з бізнес-стратегією та цілями;

Рисунок 1.1 - Вихідні дані для розробки політик безпеки

3) основ встановлення цілей контролю і контролів, охоплюючи структуру оцінки ризику та управління ризиком;

4) короткого пояснення особливо важливих для організації політики безпеки, принципів, стандартів безпеки і вимог щодо відповідності, охоплюючи:

- відповідність законодавчим, нормативним та контрактним вимогами;
- вимоги до освіти, навчання та поінформованості персоналу щодо безпеки;
- управління безперервністю бізнесу;
- наслідки порушення політики інформаційної безпеки;

5) визначення загальних та спеціальних відповідальностей з управління інформаційною безпекою, включаючи звітування щодо інцидентів інформаційної безпеки;

6) посилань на документацію, яка може підтримувати політику, наприклад, більш детальні політики та процедури для певних інформаційних систем або правила безпеки, які користувачі повинні виконувати.

Орієнтовна структура документу «Політика безпеки інформації» має наступний вигляд:

- загальний опис політики безпеки;
- введення –коротке пояснення предмета політики;

- область дії – зазначає, які частини або дії організації знаходяться під впливом політики;
- цілі, основні призначення політики;
- принципи – опис правил, ключових процесів;
- сфера відповідальності – хто відповідальний за виконання вимог політики безпеки;
- опис ключових результатів, які повинні бути досягнуті;
- пов'язані детальні політики.

Щодо пов'язаних детальних політик, то можливе будь-яке різноманіття таких, що включають принципи та рекомендації по окремим аспектам політики безпеки, наприклад:

1) політика системи менеджмента інформаційної безпеки (СМІБ);

2) політика контролю доступу;

3) політика чистого столута чистого екрану;

4) політика недозволеного програмного забезпечення;

5) політика щодо отримання файлів програмного забезпечення з мережі;

6) політика резервного копіювання;

7) політика щодо обміну інформації поміж організациями;

8) політика щодо використання можливих засобів електронного зв'язку;

9) політика збереження записів;

10) політика використання мережевих служб;

11) політика дистанційної роботи;

12) політика використання криптографічного контроля;

13) політика відповідності;

14) політика ліцензіювання програмного забезпечення;

15) політика видаленняпрограмного забезпечення.

Всі можливі детальні політики безпеки підкріплюють ідентифікацію ризиків та способи обробки ризиків для певних загроз та вразливостей.

Політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її постійної

придатності, адекватності та ефективності. Перегляд повинен охоплювати оцінку можливостей вдосконалення політики інформаційної безпеки організації і підхід до управління інформаційною безпекою в разі змін інфраструктури організації, бізнес обставин, правових умов або технічної інфраструктури.

Перегляд політики інформаційної безпеки повинен враховувати результати переглядів з боку керівництва. Повинні бути визначені процедури перегляду з боку керівництва, охоплюючи графік або періодичність перегляду.

Вхідні дані для перегляду керівництвом повинні містити інформацію щодо:

- зворотного зв'язку від зацікавлених сторін;
- результатів незалежних переглядів;
- статусу запобіжних та коригувальних дій;
- результатів попередніх переглядів з боку керівництва;
- продуктивності процесівта відповідності політиці інформаційної безпеки;
- змін, які можуть вплинути на підхід організації до управління інформаційною безпекою, охоплюючи зміни в інфраструктурі організації, бізнес-обставинах, доступності ресурсів, контрактних, нормативних і правових умовах або в технічній інфраструктурі;
- тенденцій щодо загроз та вразливостей;
- зареєстрованих інцидентів інформаційної безпеки;
- рекомендацій, наданих відповідними повноважними організаціями.

Переглянута політика повинна бути затверджена керівництвом.

Щодо законодавства України, то створення політики безпеки регламентується в наступих нормативних документах:

- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

- НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексноїсистеми захисту інформації в інформаційно-телекомунікаційній системі».

В «Типовому положенні про службу захисту інформації в автоматизованій системі» під політикою безпеки розуміють набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації вАС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації і передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки розробляється на підготовчому етапі (про це детальніше йдеться в НД ТЗІ 3.7-001-99) створення КСЗІ. Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в АС;

- аналіз ризиків;

- визначення вимог до заходів, методів та засобів захисту;

- вибір основних рішень з забезпечення безпеки інформації;

- організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;

- документальне оформлення політики безпеки.

Концепція безпеки інформації в АС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної АС і виконується на підставі аналізу правових або договірних засад, вимог до забезпечення безпеки інформації згідно з завданнями і функціями АС та загроз, котрі впливають на ресурси АС, що підлягають захисту.

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

- правовому;

- організаційному;

- технічному.

Повинні бути вироблені підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування АС в захищеному режимі. План проведення відновлювальних робіт і забезпечення неперервного функціонування АС підлягає перегляду у разі виникнення істотних змін в АС.

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів АС, складають правила розмежування доступу - це певний абстрактним механізм, який виступає посередником при будь-яких взаємодіях об’єктів АС і є найбільш суттєвим елементом політики безпеки.

Результати робіт з розроблення політики безпеки оформлюються у

вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в АС.

В «Загальному положенні щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» політику безпеки інформації в АС вважають частиною загальної політики безпеки організації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Пункт 6.2 нормативного документу «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» містить інформацію щодо порядку розробки політики безпеки:

1 Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт. На цьому етапі проводиться детальне вивчення об'єкта, на якому створюється КСЗІ, уточнюються моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконуються у разі необхідності додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися;

2 Вибір варіанту КСЗІ. У загальному випадку за результатами робіт попереднього етапу готуються альтернативні варіанти концепції створення

КСЗІ і планів їх реалізації, здійснюється оцінка переваг і недоліків кожного варіанту, вибір найбільш оптимального варіанту. Концепція оформлюється у вигляді звіту;

3 Оформлення політики безпеки. На цьому етапі здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій та документальне оформлення політики безпеки інформації.

Також в НД ТЗІ 3.7-003-05 зазначено, що політика безпеки може розроблятись для ІТС в цілому або для окремої компоненти, функціональної задачі, технології обробки інформації. Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001.

Проаналізувавши процес створення політики безпеки стає зрозумілим, що перед тим, як створювати політику безпеки інформації, потрібно виконати аналіз та оцінку ризиків.

Основна ціль оцінки ризиків - ідентифікувати і визначити величини і пріоритети ризиків в залежності від критеріїв прийняття ризику і суттєвих цілей організації. За результатами оцінки ризиків необхідно визначити відповідні дії та пріоритети з управління ризиками інформаційної безпеки та з провадження контролів, обраних для захисту від цих ризиків. Потреба в проведенні процесу оцінки ризиків та вибору контролів може виникнути декілька разів, щоб охопити різні підрозділи організації або окремі інформаційні системи, при тому має здійснюватись системно і містити аналіз ризиків та визначення ризику (процес порівняння кількісно оцінених ризиків з критеріями ризику для встановлення його значимості). Періодичність проведення оцінки ризиків необхідна також для урахування змін у вимогах безпеки і ситуації з ризиками, наприклад, щодо активів, загроз, вразливостей, значних впливів, а також коли відбуваються значні зміни в організації.

Галуззю застосування оцінки ризиків може бути або вся організація, підрозділи організації, окрема інформаційна система, певні компоненти системи або послуги, для яких це є практично здійсненним, прагматичним та корисним.

Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС або організації внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від

втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

Після проведення оцінки ризиків необхідно встановити критерії прийняття ризиків і задокументувати їх. Після проведених дій треба прийняти рішення щодо оброблення ризиків. Можливі варіанти оброблення ризиків включають:

1) застосування належних контролів для зниження ризиків;

2) свідоме й об'єктивне прийняття ризиків із забезпеченням, що вони чітко задовольняють політику організації та критерії прийняття ризику;

3) уникнення ризиків не дозволяючи дії, які можуть спричинити виникнення ризиків;

4) перенесення пов'язаних ризиків на інші сторони, наприклад, страхувальників або постачальників.

Для ризиків, для яких рішенням щодо оброблення ризику є застосування належних контролів, ці контролі повинні бути обрані та впроваджені таким чином, щоб задовольнити вимоги, ідентифіковані оцінкою ризиків. Контролі повинні забезпечити зниження ризиків до прийнятного рівня, беручи до уваги наступні фактори:

- вимоги та обмеження національного і міжнародного законодавства та нормативів;
- цілі організації;
- вартість впровадження та функціонування, пов'язану зі знижуваними ризиками, і збереження її пропорційності вимогам та обмеженням організації;
- функціональні вимоги та обмеження;
- необхідність балансу між інвестиціями у впровадження та функціонування контролів і ймовірною шкодою, до якої можуть призвести відмови політики безпеки.

Тільки на основі проведеної оцінки ризиків та прийняття рішення щодо обробки ризиків наступним етапом є створення документу політики безпеки. За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в АС. Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС.

1.2 Аналіз методів оцінки ризиків

1.2.1 Основні підходи в теорії оцінки ризиків

Існуюча література характеризується неоднозначністю в трактуванні рис, властивостей, елементів ризику, його змісту. Розмаїття думок у розумінні поняття ризику пояснюється багатьма можливими аспектами явища та значним ігноруванням використання в реальній економічній та управлінській діяльності. Корені терміна «ризик» слід шукати в грецьких словах ridsikon, ridsa, що означають «стрімчак, скеля», французькому risdoe– «об'їджати стрімчак, скелю» та італійському risiko – «небезпека, загроза». Можна виділити три основні риси ризику: суперечливість, альтернативність, невизначеність.[3]

Оцінювання ризику – це процедура порівняння існуючого ризику з межею допустимого ризику наступним чином (формула 1.1):

$$\textit{Показник ризику} \leq \textit{Допустимий рівень ризику} \qquad (1.1)$$

Допустимий рівень ризику визначається економічними та соціальними факторами. Економічні фактори пов'язані х економічними можливостями об'єкта ризику, соціальні – з переваг осіб, що приймають рішення.

Показником ризику вважається кількісне значення фактичного рівня ризику.

Оцінка ризиків - основне джерело визначення вимог до інформаційної безпеки організації. Завдяки оцінці ризиків ідентифікуються загрози активам, оцінюється їхня уразливіст,ймовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованих дій порушниками.

Оцінка ризиків є складовою частиною методичного апарату аналізу ризику, котрий, в свою чергу, є важливою частиною теорії та практики управління ризиками. Від ефективної організації аналізу ризику значною мірою залежить подальше рішення щодо прийнятності або неприйнятності ризиків, організації адекватної системи управління ризиками, забезпечення захисту організації за можливої реалізації виявлених загроз.

Тож, оцінка ризиків включає два послідовних етапи: аналіз ризиків та, безпосередньо, оцінка ризиків. В свою чергу аналіз ризиків складається з наступних етапів [4]:

- ідентифікація активів;
- ідентифікація бізнес-вимог і вимог до законодавства, що можуть бути застосовані до ідентифікованих активів;
- оцінка активів з включенням вимог попередніх пунктів;
- ідентифікація можливих загроз та вразливостей ідентифікованих активів;
- оцінка вірогідності реалізації загроз та величини вразливостей.

Оцінювання ж ризиків також включає кілька етапів:

- визначення кількісних та якісних значень ризику;
- формування реєстрів ризику;
- ранжирування ризиків.

Основна проблема аналізу ризиків – виявити показники невизначеності ризику в умовах недостатньої кількості вхідної інформації. Адже обмеженість первинної інформації може призвести до статичної невизначеності, що небезпечно для прийняття рішення.

Джерела інформації умовно можна розділити на внутрішні та зовнішні. Краще користуватися внутрішньою інформацією, якою є дані, отримані

статистичним шляхом за певний період на конкретному об’єкті. Такі дані враховують специфіку функціонування саме досліджуваного об’єкта. Зрозуміло, що інформація зовнішня також має бути врахована, особливо при наявності дефіциту внутрішньої.

Аналізуючи ризики слід використовувати візуалізацію ризиків, що дозволяє більш наочно побачити особливості тих чи інших ризиків, доповнити кількісні та логічні аналізи якісними, що спрощує розуміння ситуації і призводить до прийняття адекватних управлінських рішень. Єдине, при візуалізації не слід зловживати зайвими деталями, що погіршує сприйняття.

1.2.2 Методи аналізу ризиків

Аналіз ризиків може бути виконаний з різним ступенем деталізації, що залежить від критичності ресурсів інформаційного об’єкту, відомих вразливостей, попередніх інцидентів інформаційної безпеки.

Види анализу ризиків розрізняють за повнотою та типом розв’язуванихзадач.

За повнотою задач виділяють кількісний та якісний види аналізу ризиків.

Якісний аналіз ризику призначений для визначення факторів ризику та обставин, що призводять до ризикових ситуацій. Він включає в себе [5]:

- виявлення джерел і причин ризику, тобто встановлення потенційних зон ризику;
- ідентифікацію всіх можливих ризиків;
- виявлення практичних вигод і можливих негативних наслідків, які можуть настати при реалізації;
- ранжування ризиків за експертними даними.

Якісний аналіз дозволяє виділити найбільш значущі ризики, які будуть об'єктом подальшого кількісного аналізу.

Кількісний аналіз ризику передбачає кількісне визначення окремих ризиків і ризику проекту (прийнятого рішення)в цілому та базується на теорії ймовірностей, математичній статистиці, теорії досліджень операцій. Проте,

здійснення кількісної оцінки зустрічає і найбільші труднощі, пов'язані з тим, що для кількісної оцінки ризиків потрібна відповідна кількість вихідної інформація.

За типом розв'язуваних задач аналіз ризику включає його ідентифікацію, оцінювання та прогноз.

Аналіз звичайно починають з ідентифікації ризику – виявлення ризиків, характерних для певного виду діяльності, причин їх виникнення, форм прояву і ризикостворюючих факторів. Ідентифікація заснована на аналізі статистичних даних про небезпечні явища та результати їх взаємодії з антропосферою - стихійних лихах, аваріях і катастрофах, економічних і політичних кризах, а також на аналізі механізмів можливого впливу їх негативних факторів на різні групи населення і суб'єкти діяльності у разі реалізації небезпек.

Для прийняття обгрунтованого рішення важливо виявити всі можливі ризики. Від передбачуваного ризику можна застрахуватися (аж до відмови від проекту), а невиявлений або проігнорований ризик може призвести до краху організації.

В даний час найбільш ефективним є комплексний підхід до аналізу ризиків. З одного боку, такий підхід дозволяє отримувати більш повне уявлення про можливі результати реалізації проекту, тобто відгуки всіх позитивних і негативних несподіванках, а з іншого боку, робить можливим широке застосування математичних методів для аналізу ризиків.

У теорії ризиків виділяють наступні види математичних моделей: прямі, зворотні і завдання дослідження чутливості. У прямих завданнях оцінка ризику, пов'язана з визначенням його рівня, відбувається на підставі апріорі відомої інформації. У зворотних завданнях встановлюються обмеження на один або кілька варійованих вихідних параметрів з метою задоволення заданих обмежень на рівень прийнятного ризику. Основна ідея методу дослідження чутливості, застосовуваного у зв'язку з неминучою неточністю вихідної інформації, полягає в аналізі уразливості, ступеня змінності

результативних показників по відношенню до варіювання параметрів моделей (розподіл ймовірностей, областей зміни тих чи інших величин тощо). Висновки дослідження чутливості інвестиційного проекту відображають ступінь достовірності отриманих при аналізі проектних результатів. У разі їх недостовірності аналітик буде змушений реалізувати одну з наступних можливостей [6]:

- уточнити параметри, неточність яких є найбільш суттєвою в спотворенні результату;

- змінити методи обробки вихідних даних з метою зменшення чутливості відповіді;

- змінити математичну модель аналізу проектних ризиків;

- відмовитися від проведення кількісного аналізу ризиків проекту.

Широко застосовуються для аналізу інвестиційних проектів наступні класи математичних моделей, що враховують невизначеність і різняться за способами її опису:

- стохастичні моделі;

- лінгвістичні моделі;

- нестохастіческіе (ігрові) моделі.

Якщо привести більш загальну класифікацію методів аналізу ризиків у рамках технократичної концепції [7], то отримаємо наступний ряд методів аналізу ризиків:

- феноменологічні;
- детерміністські;
- імовірнісні;
- експертні.

Феноменологічний метод базується на визначенні можливості протікання негативних процесів виходячи з результатів аналізу необхідних і достатніх умов, пов'язаних з реалізацією тих чи інших законів природи. Цей метод найбільш простий у застосуванні, але дає надійні результати, якщо граничний рівень ризику досить високий. Феноменологічний метод кращий

при порівнянні запасів безпеки різних типів потенційно небезпечних об'єктів, тому що реалізується на базі фундаментальних закономірностей, які об'єднують в рамках наукових дисциплін - фізики, хімії та механіки катастроф.

Детерміністський метод передбачає аналіз послідовності етапів розвитку загроз, починаючи від вихідної події через послідовність передбачуваних стадій відмов, деформацій і до усталеного кінцевого стану системи. Метод реалізують за допомогою математичного моделювання, побудови імітаційних моделей і проведення складних розрахунків. Недоліком методу можуть бути:

- випущення з аналізу потенційно важливих, хоч і малоймовірних подій;
- складність побудови адекватних математичних моделей через недостатнє число вихідних даних;
- коштовні розрахункові програм для проведення тестування та експериментальних досліджень.

Імовірнісний метод аналізу ризику передбачає як оцінку ймовірності виникнення негативних подій, так і розрахунок відносних ймовірностей того чи іншого каналу розвитку процесів. При цьому аналізують розгалужені ланцюги подій і відмов обладнання, вибирають відповідний математичний апараті оцінюють повну ймовірність негативних подій. Розрахункові математичні моделі в цьому підході, як правило, можна значно спростити порівняно з детерміністськими схемами розрахунку. Основні обмеження ймовірнісного аналізу безпеки пов'язані з недостатністю відомостей за функціями розподілу параметрів, а також недостатньою статистикою з відмов обладнання. Імовірнісний метод оцінки ризику забезпечує прийняття достовірності результатів аналізу за умови збереження в перспектив і тенденцій розвитку досліджуваної системи та її зовнішнього середовища.

Експертний метод заснований на отриманні кількісних оцінок ризику шляхом обробки думок експертів (висококваліфікованихфахівців у досліджуваній області). На практиці для оцінки тенденцій розвитку широко

використовують методи експертних оцінок. Тому найбільш прийнятним варіантом у практичній діяльності є комбінація імовірнісного та експертного методів.

1.2.3 Методи оцінки ризиків

Конкретні методи ідентифікації, оцінки та прогнозу ризиків залежно від використовуваної вихідної інформації можна звести в такі групи:

- статистичні;
- ймовірносно-статистичні;
- теоретико-імовірнісні;
- експертні (евристичні, засновані на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання або інших нетрадиційних підходів).

Рисунок 1.2 - Область застосування методів оцінки показника ризику ймовірності залежно від об'єму статистичних даних

Всі методи оцінки мають власну область застосування (рис.1.2). Враховуючи, що ймовірність P являє собою відношення числа негативних подій n (формула 1.2) до загального числа спостережень N, то чим вона менша, тим важче її оцінювати (необхідно більше спостережень для того, щоб реалізувалися негативні події).

$$n = P * N \qquad (1.2)$$

Області застосування основних методів оцінки показника ризику типу ймовірності залежно від наявності статистичної інформації і математичних

моделей наведено на рис.2.2.Історично склалося так, що методи оцінки ризику розвивалися від найбільш простого статистичного, застосовного за наявності достатньої статистики, до теоретико-імовірнісного,необхідність у якому виникла тоді, коли на порядок денний встали питання оцінки ризиків рідкісних аварій на потенційно небезпечних об'єктах техносфери з тяжкими наслідками.

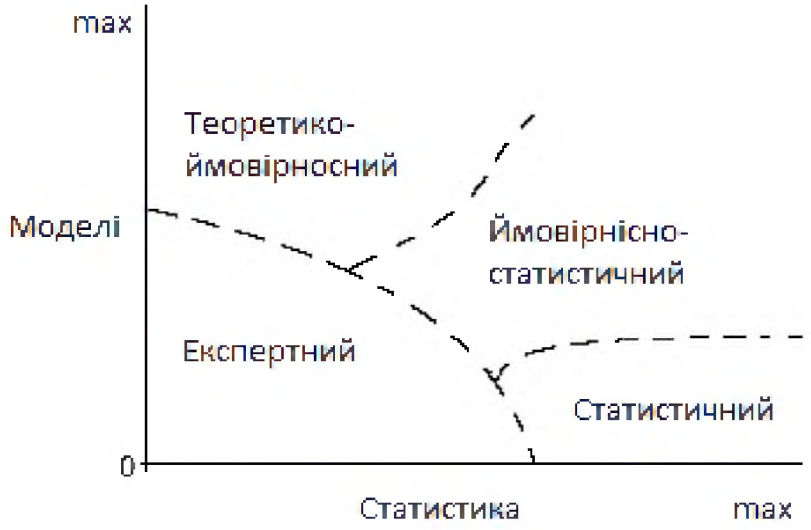


Рисунок 1.3 - Область застосування методів оцінки показника ризику ймовірності залежно від наявності статистичних даних та можливості формалізації даних

Статистичний метод

Найкращим за наявності достатньої статистики є, статистичний метод, так як практика - критерій істини. Статистичний метод широко застосовується в тих випадках, коли при проведенні кількісного аналізу організація має у своєму розпорядженні значний обсяг аналітико-статистичної інформації з необхідних елементів аналізованої системи (обсяг спостережень повинен перевищувати деяку величину N1, залежну від оцінюваної ймовірності, при цьому число реалізувалися негативних подій за один рік має бути більше 100) [8].

Суть цього методу полягає в тому, що для розрахунку ймовірностей виникнення збитків аналізуються всі статистичні дані, що стосуються результативності здійснення фірмою розглянутих операцій.

Статистичний метод оцінки ризику дозволяє проводити порівняння ризикованості напрямів діяльності і конкретних ситуацій за ознаками, вираженими у різних одиницях виміру, шляхом введення коефіцієнта варіації.

Коефіцієнт варіації (V) – це відношення стандартного відхилення до середнього очікуваного значення, виражене у відсотках[10]:

$$V = \frac{\sigma}{x} * 100\% , \qquad (1.3)$$

де σ – середньоквадратичне відхилення доходів;

х – середня величина сподіваних доходів.

Коефіцієнт варіації – величина відносна, тому на її розмір не впливають абсолютні значення досліджуваного показника. За його допомогою можна порівнювати мінливість показників, виражених у різних одиницях виміру. Чим більший коефіцієнт, тим більший розкид значень показників і тим більш ризикованим є проект, що аналізується.

Вченими встановлено таку якісну оцінку різних коефіцієнтів варіації:

– до 10% – слабке коливання;

– від 10% до 25% – помірне коливання;

– понад 25% – високе коливання.

Прикладом використання статистичного методу на практиці служить оцінка галузевого ризику, оцінка ризиків клієнта, розрахунок конкурентних ризиків. Цей метод дає можливість аналізувати та оцінювати сценарії реалізації конкретного виду діяльності. Так, в останні роки набув широкого розповсюдження так званий «метод статистичних випробувань» – метод «Монте-Карло». В інвестиційно-фінансовій сфері як критерій при кількісній оцінці ризику проектів вкладення капіталу широко використовуються показники середнього очікуваного значення і середньоквадратичного відхилення. Статистичний метод з визначення ризику проекту

використовується й у системі ПЕРТ для обчислення очікуваної тривалості кожної роботи та всього проекту загалом.

Головною перевагою статистичної оцінки ризику є можливість визначити ризик не тільки окремого напряму діяльності, але й підприємства у цілому. У той же час цей метод має деякі недоліки. Так, для цього методу необхідний великий масив вихідної інформації, що означає, що тільки створене підприємство статистичний метод використовувати буде не в змозі.

Дисперсія також не може достатньо повно відображати ступінь підприємницького ризику через те, що сигналізуючи про наявність ризику, вона приховує напрям відхилення від очікуваного значення. Підприємцю ж часто потрібно знати, що є найбільш ймовірним: витрати чи прибуток у результаті здійснення проекту. Усунути цю ваду в умові браку інформації неможливо. Значним недоліком є і те, що статистичний метод сприймає ризик як цілісну величину та не аналізує джерела виникнення ризику

Ймовірнісно-статистичний метод

Ймовірнісно-статистичний метод заснований на знаходження інформації функції розподілу збитків для об'єкту аналізів у випадку, якщо загроза реалізується. Для підвищення достовірності отриманих результатів, статистичних даних має бути на декілька вибірок. Проте через те, що з плином часу умови реалізації тієї чи іншої загрози змінюється, не можна об'єднувати статистичні дані кількох вибірок. Такі дані час від часу треба перераховувати з урахуванням тенденції зміни розподілу по збитку.

Теоретико-ймовірносний метод

Теоретико-ймовірностний метод застосовується для оцінки частот або ймовірностей рідкісних подій чи явищ, що мають тяжкі і наслідки і статистика котрих майже відсутня (наприклад, стихійні лиха чи катастрофи на певній території). Ймовірність реалізації такої події – один раз на декілька років, а то і десятків років.

Метод заснований на застосуванні математичних моделей, в основі яких лежать закономірності переходи ініційованих подій в надзвичайній

ситуації,оцінка приватних показників і визначенні частоти (ймовірності) рідкісних негативних подій з урахуванням взаємозв'язку приватних показників. Приватні показники визначають з аналізу джерел потенційної небезпеки на розглянутій території, статистики їх реалізації у формі ініціюючих подій, передбачуваних сценаріїв розвитку та наслідків.

Теоретико-імовірнісний метод досить трудомісткий і має невисоку точність, але за відсутності інших оцінок його використання виправдано.

У рамках цього методу надзвичайна ситуація розглядається як складна подія, що відбувається при спільному настанні наступних випадкових подій:

- виникнення небезпечного явища на розглянутій території;
- вплив негативних факторів небезпечного явища на інфраструктуру розглянутій території;
- руйнування елементів інфраструктури в результаті дії негативних факторів небезпечного явища;
- відмова системи безпеки об'єкта за різних поєднань недостатньою надійності технічних пристроїв і персоналу (антропогенний фактор) та інших причин;
- нанесення збитку інфраструктурі території, що перевищує встановлені критерії для його класифікації як надзвичайна ситуація.

Вплив зазначених факторів (небезпеки, загрози, вразливості, ефективності систем безпеки, збитку) на можливість настання надзвичайних ситуацій оцінюють за допомогою приватних показників, таких як небезпека території, загроза для об’єкту, вразливість об’єкта, ефективність системи безпеки об’єкта, збиток від настання надзвичайної ситуації на об’єкті.

Таким чином, частота настання надзвичайних ситуацій залежить не тільки від характеристик небезпеки території, але і ступеня загрози від джерел небезпеки для об'єктів впливу(просторового, тимчасового і ситуаційного факторів загрози),уразливості (захищеності і стійкості) об'єктів, ефективності систем безпеки небезпечних або важливих об'єктів,оснащених спеціальними системами безпеки, а також розміру збитку.

Метод експертних оцінок

Експертний метод оцінки ризику доцільно застосовувати в тому випадку (див. рис.), коли відсутні не тільки статистичні дані по об'єкту, а й математичні моделі (задача є важко формалізованою), а також, коли проводиться оцінка ризику для такого напряму діяльності, що не має аналогів.

Сутність експертного методу оцінки показників ризику полягає в тому, що експертам пропонують відповісти на питання про стан або майбутню поведінку об'єктів, що характеризуються невизначеними параметрами або невивченими властивостями. Експертні оцінки оформляють, зокрема, у вигляді якісних характеристик або кількісних значень ймовірностей розглянутих подій, віднесених до певного проміжку часу.

Важливе значення при цьому надають формуванню оціночної шкали, використовуваної експертами. Оптимальна оціночна шкала повинна мати порівняно невелике число градацій(від 3 до 8), і кожній градації приписують певний імовірнісний інтервал. Крім того, кожна градація повинна супроводжуватися короткою текстовою якісною характеристикою.

Для інтерпретації та математичної обробки експертних даних можна залучати моделі, засновані на використанні нечітких множин.

До недоліків експертного методу відносяться відсутність гарантій достовірності отриманих оцінок, а також труднощі у проведенні опитування експертів і обробці отриманих даних. Другий недолік може бути подоланий, а перший - має принципове значення. Підвищення достовірності експертних оцінок вимагає відповідних процедур відбору експертів з багатьох критеріїв. При правильній організації процедури експертизи та перевірки узгодженості думок експертів забезпечується достатня достовірність оцінок. Підвищити точність експертних оцінок можна шляхом запрошення експертів вищої кваліфікації і збільшення числа незалежних експертів.

1.3 Аналіз антропогенних загроз інформаційної безпеки

1.3.1 Класифікація загроз інформаційної безпеки

Інформаційні загрози становлять небезпеку для індивіда, суспільства та держави. Реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування системи державного управління інформаційною безпекою. Управління загрозами і небезпеками сприяє їх усуненню.

Під загрозою розуміють можливу небезпеку, яка порушує базові властивості інформації та інформаційних мереж. Базовими властивостями інформації є: конфіденційність, цілісність та доступність. Будь-які несанкціоновані дії та доступ до захищених мереж, стають причиною порушення безпеки інформації і (або) нанесення збитків системі.

Також це дії, спрямовані проти об'єкта захисту чи інформаційної мережі, що проявляється в небезпеці спотворень і втрат інформації.

При побудові моделі загроз потрібно враховувати, що джерела загроз можуть знаходитися як всередині організації - внутрішні джерела, так і поза нею - зовнішні джерела.

Загрози інформаційним ресурсам можно в загальному випадку класифікувати (рисунок 1.4):

Рисунок 1.4 – Класифікація загроз інформаційної безпеки

1 За метою реалізації загроз:

а) загрози конфіденційності:

- розкрадання (копіювання) інформації і засобів її обробки (носіїв);
- втрата (ненавмисна втрата, витік) інформації і засобів її обробки (носіїв);

б) загрози доступності:

- блокування інформації;
- знищення інформації і засобів її обробки (носіїв);

в) загрози цілісності:

- модифікація (спотворення) інформації;
- заперечення дійсності інформації;
- нав'язування неправдивої інформації, обман;

2) за принципом впливу на носії інформації – автоматизовану систему (АС):

– з використанням доступу порушника (зловмисника, користувача АС, процесу) до об'єкта (до кімнати переговорів, до файлу даних, каналу зв'язку і т.д.);

– з використанням прихованих каналів - із застосуванням закладних пристроїв, шляхів передачі інформації, що дозволяють двом взаємопов'язаним процесам (легітимного і запровадженого зловмисником) обмінюватися інформацією таким способом, що призводить до втрати інформації.;

3) за характером впливу на систему обробки і передачі інформації:

– активні загрози, пов'язані з виконанням порушником будь-яких дій, (копіювання, несанкціонована запис, доступ до наборів даних, програмами, розтин пароля і т.д.);

– пасивні загрози, здійснюються шляхом спостереження користувачем будь-яких побічних ефектів процесів руху інформації і їх аналізу;

4) за фактом наявності можливою для використання помилки захисту загроза може бути обумовлена однією з наступних причин:

– неадекватністю - невідповідністю режиму безпеки захисту зони охорони.

– помилками адміністративного управління-режиму безпеки;

– помилками в алгоритмах програм, у зв'язках між ними і т.д., які виникають на етапі проектування програм або комплексу програм і з-за яких ці програми можуть бути використані зовсім не так, як описано в документації.

– помилками реалізації алгоритмів програм (помилки кодування), зв'язків між ними і т.д., які виникають на етапах реалізації, наладки і можуть служити джерелом не документованих властивостей;

5) за способом впливу на об'єкт атаки (при активній дії):

– безпосередній вплив на об'єкт атаки (у тому числі з використанням привілеїв), наприклад: безпосередній доступ до зони чутності і видимості, до набору даних, програму, службі, каналу зв'язку і т.д., скориставшись будь-якої помилкою;

– вплив на систему дозволів (у тому числі захоплення привілеїв). При цьому несанкціоновані дії виконуються щодо прав користувачів на об'єкт атаки, а сам доступ до об'єкта здійснюється потім законним чином;

– опосередкований вплив (через інших користувачів):

а) "Маскарад". У цьому випадку користувач привласнює собі будь-яким чином повноваження іншого користувача, видаючи себе за нього;

б) "Використання всліпу". При такому способі один користувач змушує іншого виконати необхідні дії (для системи захисту вони не виглядають несанкціонованими, бо їх виконує користувач, що має на це право), причому останній про них може і не підозрювати. Для реалізації цієї загрози може використовуватися вірус (він виконує необхідні дії і повідомляє про їх результаті того, хто його запровадив).

Способи впливу типу «маскарад» та «використання всліпу» дуже небезпечні. Для запобігання подібних дій потрібен постійний контроль як з боку адміністраторів і операторів за роботою АС в цілому, так і з боку користувачів за своїми власними наборами даних;

6) за способом впливу на ІС:

– в інтерактивному режимі - в процесі тривалої роботи з програмою;

– в пакетному режимі - після довготривалої підготовки швидким впровадженням пакету програм спрямованої дії.

Працюючи з системою, користувач завжди має справу з будь-якою її програмою. Одні програми складені так, що користувач може оперативно впливати на хід їх виконання, вводячи різні команди або дані, а інші так, що всю інформацію доводиться задавати наперед. До перших належать, наприклад, деякі утиліти, управляючі програми баз даних, в основному - це програми, орієнтовані на роботу з користувачем. До других відносяться в

основному системні та прикладні програми, орієнтовані на виконання будь-яких суворо певних дій без участі користувача.

При використанні програм першого класу вплив виявляється тривалим за часом і, отже, має більш високу ймовірність виявлення, але більш гнучким, що дозволяє оперативно змінювати порядок дій. Вплив за допомогою програм другого класу (наприклад, за допомогою вірусів) є короткочасним, важко діагностуються, набагато більш небезпечним, але вимагає великої попередньої підготовки для того, щоб заздалегідь передбачити всі можливі наслідки втручання.

7) за об'єктом загрози:

– автоматизована система в цілому: зловмисник намагається проникнути в систему для подальшого виконання будь-яких несанкціонованих дій. Використовують зазвичай "маскарад", перехоплення або підробку пароля, злом або доступ до АС через мережу;

– об'єкти АС - дані або програми в оперативній пам'яті або на зовнішніх носіях, самі пристрої системи, як зовнішні (дисководи, мережеві пристрої, термінали), так і внутрішні (оперативна пам'ять, процесор), канали передачі даних. Вплив на об'єкти системи зазвичай має на меті доступ до їх вмісту (порушення конфіденційності або цілісності оброблюваної чи зберігається) або порушення їх функціональності (наприклад, заповнення всієї оперативної пам'яті комп'ютера безглуздою інформацією або завантаження процесора комп'ютера завданням з необмеженим часом виконання);

– суб'єкти АС - процесори користувачів. Метою таких атак є або пряме вплив на роботу процесора - його припинення, зміна характеристик (наприклад, пріоритету), або зворотний вплив - використання зловмисником привілеїв, характеристик іншого процесу у своїх цілях. Вплив може надаватися на процеси користувачів, системи, мережі;

– канали передачі даних - прослуховування каналу і аналіз графіка (потоку повідомлень); підміна або модифікація повідомлень у каналах зв'язку

та на вузлах-ретрансляторах; зміна топології і характеристик мережі, правил комутації та адресації;

8) за засобами, що використовуються для реалізації атаки:

- з використанням стандартного програмного забезпечення;
- з використанням спеціально розроблених програм;

9) за станом об'єкта атаки.

– об'єкт атаки зберігається на диску, магнітній стрічці, в оперативній пам'яті або в будь-якому іншому місці в пасивному стані. При цьому дія на об'єкт зазвичай здійснюється з використанням доступу;

– об'єкт атаки знаходиться в стані передачі по лінії зв'язку між вузлами мережі або усередині вузла. Вплив передбачає або доступ до фрагментів переданої інформації (наприклад, перехоплення пакетів на ретрансляторі мережі), або просто прослуховування з використанням прихованих каналів;

– об'єкт атаки (процес користувача) перебувати в стані обробки;

10) за повторюваністю вчинення:

– повторювані — такі загрози, які мали місце раніше;

– продовжувані — неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету;

11) за сферами походження:

– екзогенні — джерело дестабілізації системи лежить поза її межами;

– ендогенні — алгоритм дестабілізації системи перебуває у самій системі;

12) за ймовірністю реалізації:

– вірогідні — такі загрози, які за виконання певного комплексу умов обов'язково настануть. Прикладом може слугувати оголошення атаки інформаційних ресурсів системи управління НБ, яке передує власне атаці;

– неможливі — такі загрози, які за виконання певного комплексу умов ніколи не настануть. Такі загрози зазвичай мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер;

– випадкові — такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах;

13) за значенням:

– допустимі — такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

– неприпустимі — такі загрози, які можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи та до змін, не сумісних із подальшим існуванням СНБ. Так, наприклад, вірус «I love you», спричинив пошкодження комп'ютерних систем у багатьох містах світу і завдав загального збитку майже 100 мільйонів доларів США;

14) за структурою впливу:

– системні — загрози, що впливають одразу на усі складові елементи інформаційної системи;

– структурні — загрози, що впливають на окремі структури системи;

– елементні — загрози, що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу;

15) за характером реалізації:

– реальні — активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

– потенційні — активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування інформаційної системи;

– здійснені — такі загрози, які втілені у життя;

– уявні — псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

Виходячи з проведеного аналізу, всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

- загрози, обумовлені діями суб'єкта (антропогенні загрози);
- загрози, обумовлені технічними засобами (техногенні загрози);
- загрози, обумовлені стихійними джерелами (стихійні лиха, магнітні бурі, радіоактивне випромінювання тощо).

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

Суб'єкти, дії яких можуть призвести до порушення безпеки інформації в корпоративних мережах можуть бути як зовнішні, так і внутрішні (рис.1.5).

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться дії кримінальних структур; рецидивістів і потенційних злочинців; партнерів; конкурентів; політичних супротивників.

Рисунок 1.5 - Класифікація антропогенних джерел загроз інформації по відношенню до об'єкта захисту

Зовнішні джерела антропогенних загроз можуть бути випадковими або навмисними та мати різний рівень кваліфікації. До них відносять:

1) кримінальні структури;
2) потенційні злочинці та хакери;
3) несумлінні партнери;
4) технічний персонал постачальників телематичних послуг;
5) представники наглядових організацій та аварійних служб;
6) представители силових структур.

Кількість внутрішніх загроз у компаніях різних сфер бізнесу на сьогоднішній день перевищує кількість зовнішніх.

Найпоширеніші із внутрішніх загроз - неавторизований доступ у систему (сервер, персональний комп'ютер або базу даних), неавторизований пошук або перегляд конфіденційних даних і спроби обійти або зламати систему безпеки або аудиту. Крім того, це несанкціоновані маніпуляції з інформацією - зміна або знищення даних, а також збереження або обробка конфіденційної інформації в системі, не призначеної для цього.

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

- основний персонал (користувачі, програмісти, розробники);
- представники служби захисту інформації (СЗІ);
- допоміжний персонал (прибиральники, охорона);
- технічний персонал (життєзабезпечення, експлуатація).

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

Внутрішні атаки на інформаційні системи приносять величезний збиток, і не тільки фінансовий - витік конфіденційних даних це серйозний удар по репутації компанії.

1.3.2 Аналіз внутрішніх загроз та їх джерел

За даними різних джерел (рис. 1.6) від 65 % до 85 % інцидентів інформаційної безпеки відбувається з вини працівників компанії і викликано незнанням правил дотримання політики безпеки, її неприйняттям або недостатньою компетентністю,халатністю і безвідповідальністю. Наприклад, компанія витрачає мільйонний бюджет на придбання сучасного та якісного DLP- комплексу, в той же час співробітники компанії записують свої паролі на стікери і приклеюють до моніторів. І тоді сенс в провадженні суперсучасного DLP, місяці копіткої роботи, не кажучи вже про витрачені гроші, абсолютно втрачається.

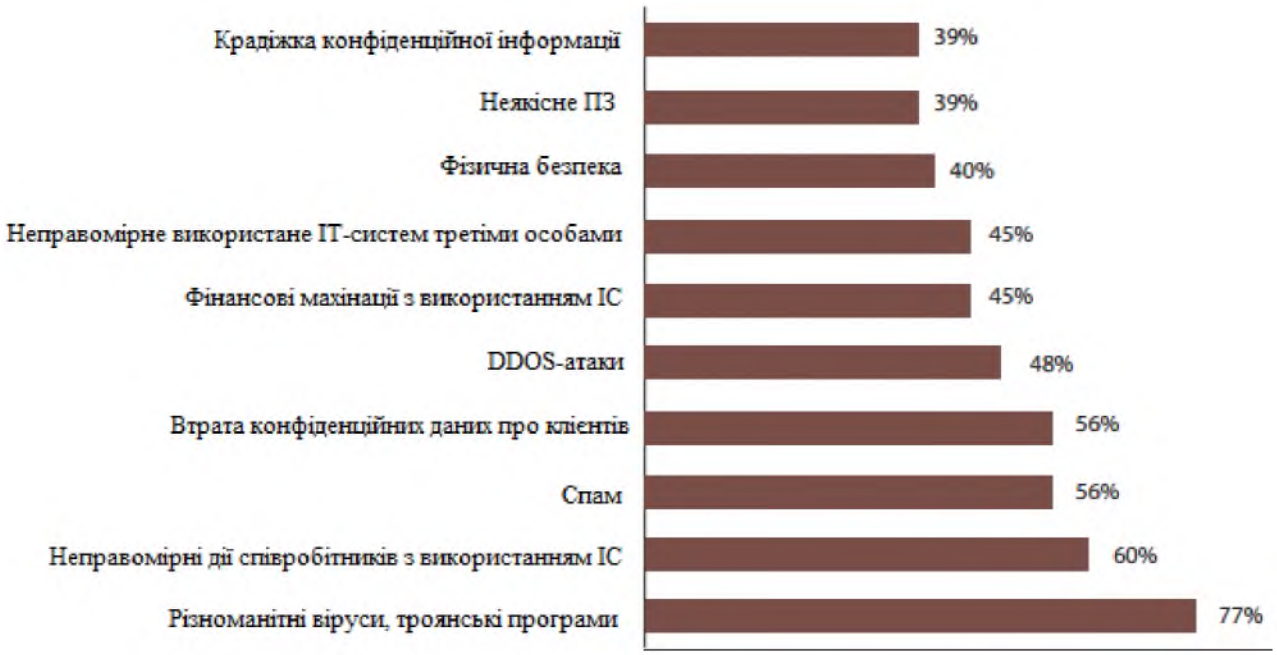


Рисунок 1.6 - Популярність класів загроз ІБ

Антропогенними джерелами загроз у сфері інформаційної безпеки виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові. Ця група представляє великий інтерес з точки зору організації

захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Методи протидії в цьому випадку керовані і залежать від організаторів захисту інформації.

Кваліфікація антропогенних джерел інформації відіграють важливу роль в оцінці їх впливу і враховується при ранжируванні джерел загроз. В якості антропогенного джерела загроз можна розглядати суб'єкт, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні, так і внутрішні.

Внутрішні суб'єкты (джерела), зазвичай, представляють собою висококваліфікованих фахівців у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

1) основний персонал (користувачі, програмісти, розробники);

2) представники служби захисту інформації;

3) допоміжний персонал (прибиральники, охорона);

4) технічний персонал (життєзабезпечення, експлуатація).

Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел становлять особи з порушеною психікою і спеціально впроваджені та завербовані агенти, які можуть бути з основного, допоміжного та технічного персоналу, а також представників служби захисту інформації. Дана група розглядається у складі перерахованих вище джерел загроз, але методи парирування загрозами для цієї групи можуть мати свої відмінності.

Внутрішні загрози – це діяльність чи бездіяльність (у тому числі навмисна та ненавмисна) окремих посадових осіб суб'єктів господарювання, що суперечить їх майновим правам та інтересам, наслідками яких можуть бути нанесення економічної шкоди суб'єкту господарювання, виток або втрата

інформаційних ресурсів (втому числі відомостей, що становлять комерційну таємницю та/або конфіденційну інформацію), підрив їх ділового іміджу, виникнення проблем у взаємостосунках з реальними та потенційними партнерами, конфліктних ситуацій з представниками кримінального середовища, конкурентами, контролюючими та правоохоронними органами, виробничий травматизм або загибель персоналу тощо.

Внутрішні загрози, як правило, обумовлюються наявністю передумов для негативних, протиправних дій персоналу, безконтрольним використанням засобів виробництва, порушенням режимів діяльності банку.

Ураховуючи, що значна частина внутрішніх загроз реалізуються за участю або сприяння персоналу, можна вважати, що основним джерелом таких загроз є самі працівники. Виходячи з цього внутрішні загрози підприємства можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи;
- психологічних та комунікаційних особливостей працівників;
- відсутності нормативної бази, яка б установлювала режими їх діяльності та правила поведінки персоналу;
- низького стану трудової і виробничої дисципліни, слабкої вимогливості керівного складу.

Внутрішні загрози безпеки є постійними і не залежать від ролі, місця, значення підприємства або наявності зовнішніх загроз.

Реалізація загроз має свої особливості відповідно до об'єктів загроз. Для більш повного розуміння можна зазначити, що основними об'єктами загроз можуть бути персонал, фінанси, матеріальні цінності та інформація комерційного підприємства.

Реалізація загроз щодо персоналу може призводити до моральних або фізичних страждань окремих осіб, втрати ними своєї власності, нанесення економічної шкоди.

Матеріальним цінностям підприємства може загрожувати пошкодження будівель, приміщень та іншої нерухомості, виведення із ладу засобів зв'язку і систем комунального обслуговування, пошкодження, крадіжки обладнання, техніки, транспортних засобів.

Інформаційні загрози можуть реалізовуватись через несанкціоноване ознайомлення сторонніх осіб з відомостями, що мають обмежений доступ, модифікацію фінансові чи іншої важливої інформації, її знищення або розголошення.

Головним аспектом у системі захисту інформації є людина. За допомогою технічних, юридичних, організаційних складових люди захищають інформацію від людей. Саме людина, за допомогою технічних чи інших засобів, намагається отримати інформацію. Саме через недбале відношення до довірених людина даних, ці дані можуть бути втрачені.

На сьогоднішній день існує все більше і більше можливостей отримання інформації, в тому числі й інформації з обмеженим доступом (тобто такої інформації, витік якої може завдати шкоди її власнику). З'являється все більше загроз витоку даних. А з розвитком новітніх технологій способи їх отримання постійно вдосконалюються. Отже, існує і багато засобів, що повинні забезпечувати захист інформації з обмеженим доступом. Крім технічних засобів захисту є безліч інструкцій, правил, які регламентують поводження із такою інформацією, а також є ціла низка нормативних актів, з яких ці інструкції випливають.

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

Розголошення співробітниками інформації з обмеженим доступом найчастіше здійснюється через те, що керівництва компаній не приділяють уваги загрозам витоку інформації, пов'язаним з персоналом.

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

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

Свідомість або несвідомість дій порушників можна звести до двох типів наслідків, котрі породжені або необережністю персоналу, або їх умисними діями.

1 Необережність персоналу

Дуже часто співробітники, хоч й не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього. Тож необережність можна поділити на дві категорії: дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації; дії чи бездіяльність співробітників у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки. У першому випадку не можна казати про вину співробітника, скоріше це прорахунки вищого керівництва, яке не потурбувалося роз'яснити персоналу про важливість інформації і про її захист.

У кримінальному кодексі необережність поділяють саме на злочинну самовпевненість та злочинну недбалість. Під злочинною самовпевненістю розуміють дії чи бездіяльність особи, коли вона знала про можливі негативні наслідки, передбачала їх настання, але зухвало розраховувала на їх відвернення. Злочинною недбалістю є дії чи бездіяльність особи, коли вона не

знала, але повинна була знати про можливі негативні наслідки свого діяння. В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії.

2 Умисні дії працівників по розголошенню інформації

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

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

Інсайдерські інциденти відбуваються набагато частіше, ніж зовнішні атаки. Компанії прагнуть не афішувати свої внутрішні проблеми, але авторитетні дослідження все одно віддають пальму першості інсайдерам.

Тож загроза цілісності інформації йде від людини. Можна встановити найсучасніші системи технічного захисту, видати мільйони нормативних актів, які регулюють захист інформації, але поки буде ігноруватися людський фактор (тобто фактор людського впливу на інформацію, загрози, які йдуть від людей та причини цих загроз), доти юридичні, організаційні та технічні засоби будуть мало ефективними.

1 Менеджери. Як особи, які володіють великими організаційними повноваженнями, найбільшу потенційну загрозу для інформаційних ресурсів компанії представляють менеджери. Наприклад, до втрат можуть привести розпорядження надати користувачеві невиправдано високі права, реалізувати в інформаційній системі небезпечний, але зручний функціонал. Іноді інформаційні загрози виникають внаслідок незадовільного виконання керівниками контролюючих функцій. Відомі випадки, коли продавалося обладнання, з дисків якого не видалялася конфіденційна інформація компанії та партнерів.

Для уникнення реалізації загроз доцільно зобов'язати менеджерів погоджувати вирішення питань, пов'язаних з інформаційними ризиками, з керівником служби інформаційної безпеки.

IT-фахівці, адміністратори та особи, які виконують критичні операції.

Хочеться звернути увагу на відбір кандидатів, яким передбачається довірити виконання операцій, що вимагають більших прав в інформаційній системі. Чи не менше значення, ніж професійні навички, мають лояльність кандидата і здатність зберігати відданість інтересам компанії навіть у складних ситуаціях. З цієї причини особи, на вершині системи цінностей яких знаходиться матеріальну винагороду, швидше за все, отримають відмову. З особливою обережністю слід ставитися до кандидатів, котрі занадто часто змінюють роботу, котрі надають недостовірні відомості, притягувались до адміністративної та кримінальної відповідальності, котрі мали психічні або невротичні розлади.

Бажано, щоб окрім співбесіди зі своїм керівником, кандидат зустрівся з професійним психологом. Часто психолог проводить тестування, яке виявляє особливості характеру і потенційні можливості кандидата. Також важливо провести бесіду, в ході якої будуть виявлені система цінностей і особливості поведінки. Це дозволить переконатися втому, що кандидат легко увійде в корпоративну культуру, зрозуміти, яка система мотивації буде для нього найбільш придатною.

Особливу увагу слід приділити тому, щоб робота співробітника в організації відповідала його очікуванням. Зокрема, керівнику слід утриматися від необгрунтованих обіцянок. Психологічний контракт важливий так само, як формальний.

Традиційною проблемою, пов'язаною з IT-співробітниками, є контроль і оцінка результатів діяльності. Небагато керівників здатні сприймати і розбиратись в суті їх роботи, у тому числі в питання захисту даних, володіти глибокими знаннями в IT-технологіях, бути компетентними в питаннях управління.

Наприклад, в IT-підрозділах часто відсутні посадові інструкції і не проводяться атестації. Іноді IT-фахівців розглядають як обслуговуючий персонал, намагаються навантажити додатковою роботою, що не визначена посадовою інструкцією. Це погіршує виконання прямих обов'язків, викликає невдоволення, негативно позначається на лояльності, призводить до високої плинності кадрів. Напевно багатьом відомі випадки, коли адміністратор, що звільняється, блокує паролі сервера.

2 Рядові співробітники. Значною загрозою інформаційної безпеки компанії є низька кваліфікація персоналу, недостатня для коректної роботи з корпоративної інформаційної системою. Особливо небезпечними є некомпетентні співробітники, що видають себе за грамотних користувачів, або які вважають себе такими.

В багатьох компаніях відсутній контроль над встановленням на робочих станціях програмного забезпечення. Не розуміючи можливих наслідків, співробітник може встановити на своєму робочому місці цікаву йому програму або "патч", істотно знизивши ефективність зусиль по забезпеченню корпоративної мережевої безпеки. Подібна загроза виникає і в разі підключення до мережі Інтернет через модем або мобільний телефон, оснащений функцією цифрового зв'язку.

Звичайно, не буде зайвим ще раз згадати про загрози, що виходять від приклеєних до моніторів стікерів з паролями і практики обміну паролями між працівниками, виконують схожі функції.

В ряді випадків проблеми безпеки пов'язані з тим, що легальні користувачі використовують необхідну для роботи інформацію не за призначенням. Причиною може бути злі наміри, недбалість, нерозуміння наслідків поширення доступних їм відомостей. Очевидно, що дана проблема нерозв'язна тільки технологічними заходами.

Найбільшу небезпеку представляють співробітники, ображені на організацію і її керівників. Тому випадки виникнення явних і прихованих конфліктів, невідповідності ситуації, що склалася очікуванням співробітників, можуть розглядатися як потенційні передумови порушень інформаційної безпеки. Особливої уваги вимагають пов'язані з такими ситуаціями випадки звільнення. Як зазначалося вище, працівник, який звільнився з компанії з почуттям образи, легко може стати джерелом інформації для недоброзичливців.

3 Допоміжний персонал. Зазвичай, допоміжному персоналу на підприємстві (охороні, прибиральницям та іншим) приділяється не достатньо уваги з точки зору інформаційної безпеки. Хоча досить імовірною може бути ситуація, коли відповідні функції виконують зовсім не випадкові люди. Тому, приймаючи на роботу прибиральницю чи охоронця, не треба нехтувати детальною перевіркою їх резюме, рекомендацій, доступ їх до приміщень має бути обмеженим та регламентованим, і, за можливістю, супроводжуватись відеофіксацією.

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

1) жадібність - обіцянка або ж надання грошей та інших матеріальних цінностей;

2) страх за власне життя та своїх близьких - шантажування, а часом і загроза або факт грубого фізичного чи витонченого психологічного впливу;

3) внутрішній авантюризм – спекуляція на ідеальних уявленнях людини про себе, прагнення індивіду ведення своєї гри;

4) помста організації або конкретній особі - заздрість і неприязнь з непереборним бажанням завдати «ворогу» певний збиток;

5) явна симпатія до одержувача інформації – спекуляція на почуттях людей;

6) марнославство та легковажність - провокування бажання об'єкта справити певне враження, показати свою значимість і поінформованість.

Внутрішні джерела загроз інформаційної безпеки є надзвичайно небезпечними, можуть бути реалізовані майже кожним співробітником. Основний спосіб уникнути їх - проведення якісної постійної роботи з персоналом і дотримання дициплінарних норм.

Головною умовою ефективної роботи з персоналом є узгоджена робота служби безпеки у різних напрямках, а саме внутрішня безпека, інформаційна безпека, правова безпека, технічна та інше. Та тісна взаємодія служби безпеки з іншими структурними підрозділами організації.

Головною метою організації процесу управління інформаційною безпекою, з одного боку, є виявлення осіб схильних до обману, а з іншого - здатність створення єдиної команди перевірених співробітників. Саме для цього проводяться організаційні та організаційно-технічні заходи, використовуються особисті спостереження та бесіди.

1.4 Висновок. Постановка задачі

В розділі було проаналізовано процес створення політики безпеки на основі нормативно-правового забезпечення України та міжнародних стандартів та визначено, що аналіз та оцінка ризиків – процеси, що є основою

для створення політики безпеки. Тільки на основі проведеної оцінки ризиків та прийняття рішення щодо обробки ризиків можливе створення ефективної політики безпеки інформації.

Також було розглянуто методи оцінки ризиків, можливі загрози інформаційній безпеці, зокрема антропогенні.

В спеціальній частині доцільно виконати наступне:

1 Проаналізувати статистику інцидентів в сфері інформаційної безпеки з метою з'ясування важливості визначення та оцінки антропогенних загроз інфорипційній безпеці;

2 Обрати та обґрунтувати метод оцінки ризиків антропогенних загроз;

3 Розробити рекомендації щодо заходів, направлених на зменшення впливу антропогенних загроз.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз статистичної інформації в сфері інформаційної безпеки

Кількість злочинів в сфері інформаційної безпеки невпинно зростає, причому далеко не про всі стає відомо, оскільки часто «жертви» злочинів або не знають про те, що стали «жертвами», або вони хочуть просто виправити проблему безпеки, якою скористався зловмисник і зберегти в таємниці відомості про інцидент задля уникнення шкоди репутації компанії. Подібна поведінка ускладнює розрахунок реальної статистики комп'ютерних злочинів - скільки їх відбувається щодня, який заподіюється збиток, які методи атак застосовуються зловмисниками.

Проте неможливо замовчати всі інциденти і широкому загалу вони стають відомими як наслідок становлять певний зріз існуючого стану подій. Так, для аналізу статистичної інформації в сфері інформаційної безпеки в якості вихідних даних були взяти статистичні дані наступних компаній:

- Deloitte (статистика України);
- CERT-UA (державна статистика України);
- Searchinform (статистика Українита світу);
- Ernst&Young (статистика України та світу);
- IDC MediaCenter (світова статистика);
- Incidents.su (світова статистика).

Аналізувались дані про витоки конфіденційної інформації невеликихі середніх компаній (далі - сегмент середнього і малого бізнесу, СМБ-компанії). Невеликими компаніями вважатимемо ті, котрі у власній інформаційній системі мають до 50 персональних комп’ютерів, середні ж містять 50-500 персональних комп’ютерів.

До недавнього часу вважалося, що проблема витоків конфіденційної інформації не стосується малого і середнього бізнесу, нібито, вартість інформаційних активів у сегменті СМБ не настільки висока, як у великих компаніях, обсяг конфіденційних даних невеликий і за змістом не впливає на

створення конкурентної переваги, гіпотетичний збиток від витоку даних мінімальний.

Проте результати дослідження показують, що внаслідок недбалого ставлення організацій сегменту СМБ до забезпечення захисту інформації страждають клієнти і співробітники, чиї персональні дані потрапляють в руки шахраїв, що згубно позначається на бізнесі невеликих і середніх компаній, їх репутації.

У рамках дослідження ілюструється ряд характерних для східної Європи особливостей в плані безпеки конфіденційної інформаціїв СМБ. Ключовим фактом є те, що на частку малих і середніх компаній припадає 4 з 10 витоків конфіденційної інформації.

У 2020 році фахівцями аналітичних центрів в середньому зареєстровано 448 випадків витоку конфіденційної інформації в невеликих і середніх компаніях (рис. 2.1). Це трохи менше 40%; від загальної кількості зафіксованих за рік витоків.

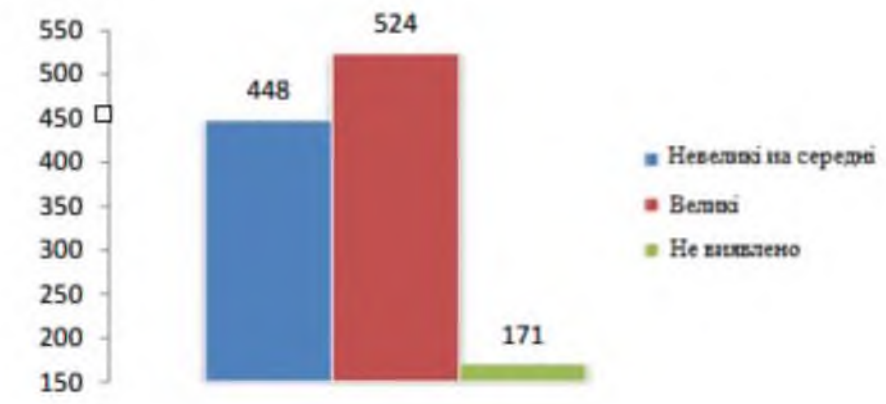


Рисунок 2.1 Розподіл витоків за розміром компанії. Кількість, частки

Три з п'яти найбільш небезпечних загроз тепер припадають на інсайдерів (рис. 2.2): на першому місці як і роком раніше залишається крадіжка інформації (65,8%), але вже на другому місці опинилася недбалість співробітників (55,1%), а на четвертому - саботаж.

Тож, дослідження наочно показують, що витоки інформації зсередини організації мають найбільший негативний вплив на імідж і репутацію організації.

При цьому ризик витоку цінної інформації (70,1%) хвилює респондентів майже в два рази більше будь-якої іншої інсайдерської загрози. Так, рейтинг найбільш небезпечних внутрішніх загроз інформаційній безпеці зображений на рисунку 2.2.

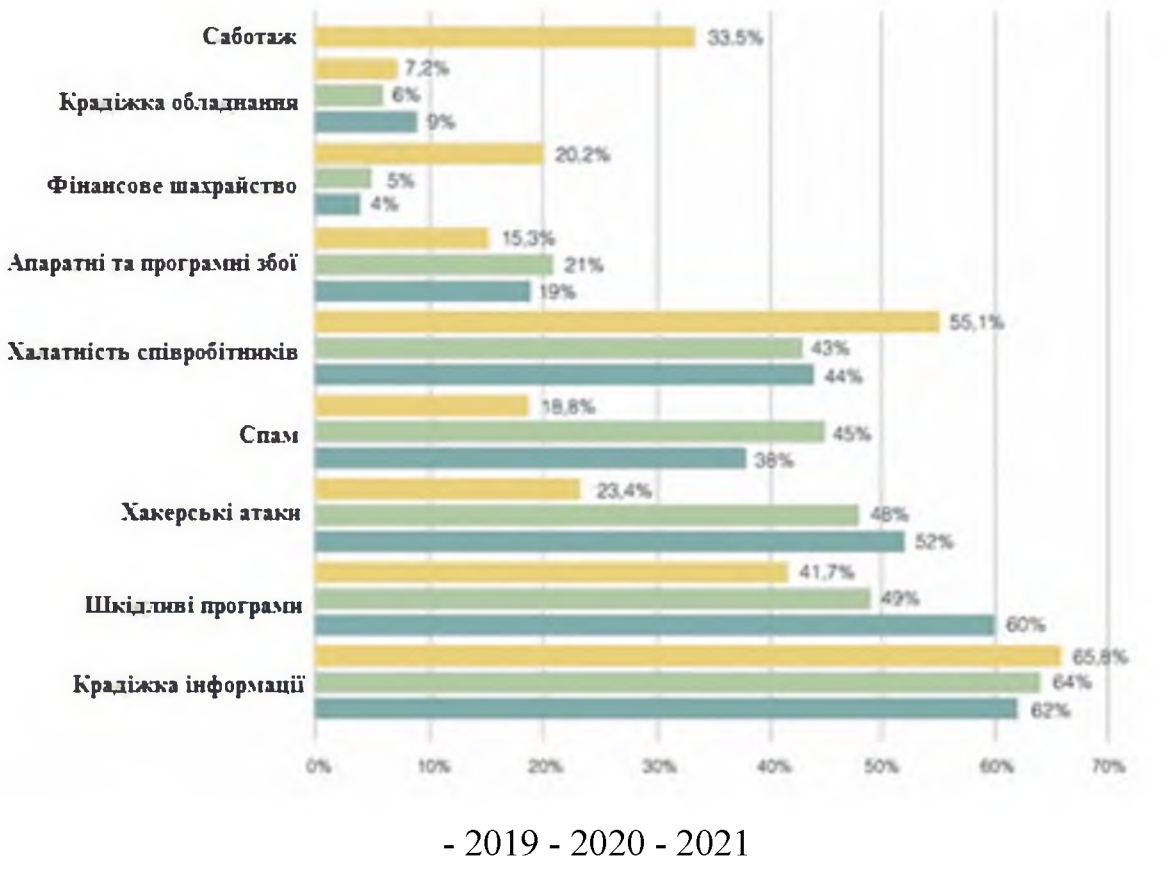
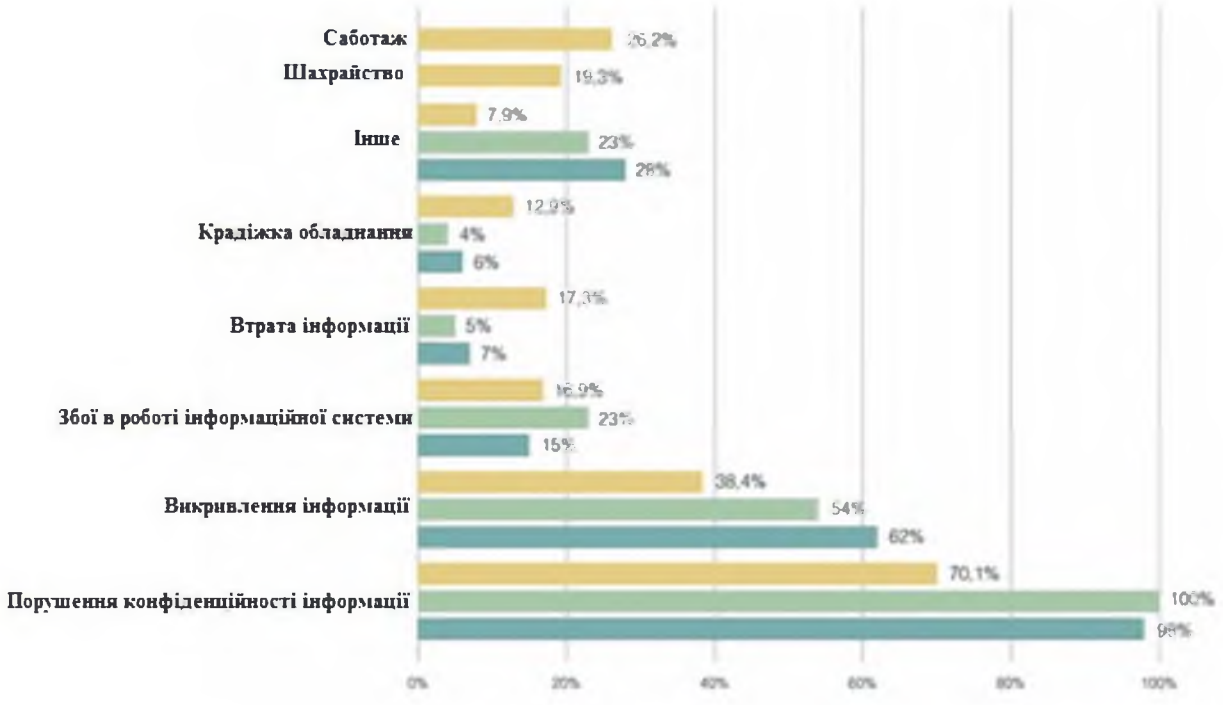


Рисунок 2.2 – Найбільш небезпечні загрози інформаційної безпеки

Як виявилася, найбільше учасники опитування стурбовані прямими фінансовими збитками (46%). На другому місці - погіршення іміджу та громадської думки (42,3%), а на третьому - втрата клієнтів (36,9%).

Серед найбільш небезпечних внутрішніх загроз інформаційній безпеці за статистикою найчастіше трапляються: порушення конфіденційності

інформації, викривлення інформації, саботаж та збої у роботі інформаційної системи (докладніше на рисунку 2.3).



- 2019 - 2020 - 2021

Рисунок 2.3 - Найбільш небезпечні внутрішні загрози інформаційної безпеки

Відсотки витоків інформації за намірами (випадкові та навмисні) різняться не суттєво та в загальному вигляді мають наступний вигляд, представлений на рисунку 2.4.

У всіх випадках витоку інформації є винуватці. Тож, аналізуючи наявну статистику, відсотковий розподіл винуватцев витоку інформації показує, найбільш небезпечними є діючі співробітники організацій та персонали контрагентів (рис. 2.5).

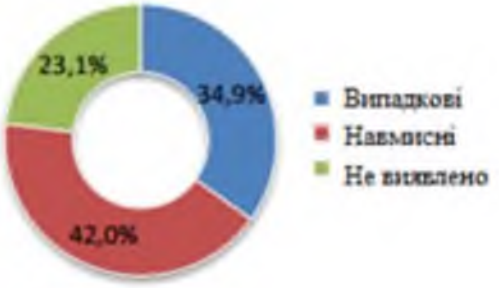


Рисунок 2.4 – Розподіл витоків інформації за намірами

Рисунок 2.5 – Розподіл винуватців у витоках інформації

Розподіл витоків інформації за ймовірними каналами, отримані в результаті аналізу статистичних даних України та світу, є досить різноманітним згідно рисунку 2.6:

Рисунок 2.6 - Розподіл витоків інформації за намірами з врахуванням використаного каналу витоку інформації

Найбільше збитків відбувається від витоків через знімні носії, мережу, електронну пошту - тобто через канали, які можна легко «знешкодити» і контролювати технічними засобами захисту даних.

Успішні реалізації загроз неминуче ведуть до збитків. Діаграма збитків, представлена на рисунку 2.7, наочно порівнює отримані збитки в середньому по Україні та світу. Так, 91% випадків витоку інформації мали збитки розміром до 10000 гривень.

Рисунок 2.7 – Порівняння величини збитку від успішної реалізації загроз

Аналіз статистичної інформації в сфері інформаційної безпеки підтверджує, що інциденті, пов'язані з антропогенними загрозами, є найрозповсюдженим видом порушень. В такому разі тільки чітка ідентифікація та оцінка антропогенних загроз дає можливість вжити необхідних превентивних заходів безпеки.

2.2 Обгрунтування вибору методу оцінки ризиків інформаційної безпеки для антропогенних загроз

Процес оцінки ризиків інформаційної безпеки має включати такі послідовні етапи проведення оцінки:

– визначення контексту оцінки, який визначає вхідні дані: цілі й призначення оцінки, вид оцінки (незалежна оцінка, самооцінка), об'єкт та області оцінки ІБ, обмеження оцінки і ролі;

– визначення критеріїв оцінки;

– визначення моделі оцінки;

– збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів об'єкта оцінки;

– отримання вихідних даних оцінки.

1 Контекст оцінки ризиків включає цілі й призначення оцінки ІБ, вид оцінки, об'єкт та області оцінки ІБ, обмеження оцінки, ролі.

До ролей, які беруть участь у реалізації процесу оцінки, ставляться організатор, аналітик, оцінювач, власник активів, представник об'єкта оцінки.

Організатор (замовник) оцінки ІБ формує ціль оцінки (вдосконалення об'єкта оцінки, визначення відповідності об'єкта оцінки встановленим критеріям і т.д.) і визначає критерій оцінки, об'єкт та область оцінки. Під організатором оцінки розуміється особа або організація, що є внутрішніми або зовнішніми стосовно до оцінюваного об'єкта оцінки, які організовують проведення оцінки та надають фінансові та інші ресурси, необхідні для її проведення. Організатор повинен забезпечити доступ групи оцінки (керівник групи оцінки, оцінювач) до активів об'єкта оцінки для вивчення, до персоналу для проведення опитувань, до інфраструктури, необхідної під час оцінювання. Хоча керівництво об'єкта оцінки безпосередньо не має ніяких конкретних обов'язків з проведення оцінювання, усвідомлення важливості оцінки має дуже велике значення. Це особливо актуально в тому випадку, коли організатор оцінки не є членом керівництва об'єкта оцінки.

По завершенню оцінки організатор передає звітні документи по оцінці зацікавленим сторонам для використання їх у відповідності із заявленою метою оцінки.

Аналітик обирає спосіб оцінки ІБ, модель оцінки і визначає методичне та інформаційне забезпечення оцінки, тобто методики, дані для оцінки. Аналітик оцінки аналізує результати оцінки і формує звіт і рекомендації за результатами оцінки інформаційної безпеки.

Такий розподіл повинен враховувати потребу в незалежності, компетентності фахівців з оцінки та результативному використанні ресурсів. Заходи по вимірюванню та оцінюванню виконуються виключно керівником групи оцінки та оцінювачем, що входять до групи оцінки. Інший персонал (представник об'єкта оцінки, технічний експерт) може брати участь у роботі групи оцінки для забезпечення спеціалізованих знань або консультацій. Вони можуть обговорювати з оцінювачем формулювання суджень, але не нестимуть відповідальність за остаточну оцінку.

Важливим аспектом при визначенні контексту оцінки є вид оцінки: незалежна або самооцінка. Залежно від виду оцінки розрізняється відношення ролей процесу оцінки та об'єкта оцінки.

Незалежна оцінка ризиків досягається шляхом проведення оцінки групою оцінки, члени якої незалежні від об'єкта оцінки. Організатор оцінки може відноситися до тієї ж організації, до якої відноситься об'єкт оцінки, але не обов'язково до оцінюваного об'єкта. Ступінь незалежності може варіюватися відповідно до мети і областю оцінки. У разі зовнішнього організатора оцінки передбачається наявність взаємної угоди між організатором оцінки та організацією, до якої відноситься об'єкт оцінки. Представник об'єкта оцінки бере участь у формуванні свідоцтв оцінки, забезпечує взаємодію групи оцінки з власниками активів. Їх участь у проведенні оцінки дає можливість визначити і врахувати особливості об'єкта оцінки, забезпечити достовірність результатів оцінки.

Самооцінка виконується організацією і організатор самооцінки зазвичай входить до складу об'єкта оцінки, як і члени групи оцінки.

Область оцінки ризиків може включати, наприклад, один або декілька процесів об'єкта оцінки, наприклад, організатор може зосередити увагу на одному або декількох критичних процесах або захисних заходах. Вибір об'єкта оцінки повинен відображати намічене використання організатором вихідних даних оцінки. В контексті оцінки має бути представлено докладний опис об'єкта оцінки, що включає розміри об'єкта оцінки, область застосування продуктів або послуг об'єкта оцінки, основні характеристики (наприклад, обсяг, критичність, складність і якість) продуктів або послуг об'єкта оцінки.

До проблем оцінки можна віднести:

- можливу недоступність основних активів, використовуваних у звичайної ділової діяльності організації;
- недостатній часовий інтервал, виділений для проведення оцінювання;
- необхідність виключення певних частин об'єкта оцінки через стадії життєвого циклу;

- обмеження на кількість і вид даних, які повинні бути зібрані і вивчені.

Зміст контексту оцінки повинне бути погоджене керівником групи оцінки з організатором та уповноваженим представником об'єкта оцінки та задокументовано до початку процесу оцінки. Фіксування контексту оцінки важливо, так як він містить вихідні елементи процесу оцінки.

Під час виконання оцінки можуть відбуватися зміни в контексті оцінки. Зміни повинні бути схвалені організатором оцінки та уповноваженим представником об'єкта оцінки. Якщо ці зміни впливають на часовий графік і ресурси проведення оцінки, то планування оцінки має бути відповідним чином переглянуто.

2 Необхідними умовами забезпечення достовірної оцінки ризиків інформаційної безпеки є:

– використання найбільш достовірних джерел свідоцтв оцінки;

– визначення обсягу вибірки з урахуванням заданої достовірності свідчень оцінки;

– облік факторів, що впливають на ризик, з метою зниження ризику.

Довіра до документальних свідчень оцінки ризиків підвищується при підтвердженні їх достовірності третьою стороною або керівництвом організації. Довіра до фактів, отриманих при опитуванні співробітників об'єкта оцінки, підвищується при підтвердженні даних фактів з різних джерел.

Основними методами одержання свідчень оцінки повинні бути:

– перевірка та аналіз документів, що відносяться до об'єкта оцінки ризику;

– спостереження за процесами об'єкта оцінки;

– опитування співробітників об'єкта оцінки і незалежної (третьої) сторони.

Оцінювачі повинні проявляти достатню ступінь професійного скептицизму у відношенні збираних свідоцтв оцінки, беручи до уваги можливість наявності порушень ІБ.

Перевірка та аналіз документів дозволяють оцінювачу отримати свідоцтва оцінки, що володіють найбільшою повнотою і зручністю сприйняття. Однак ці свідчення мають різну ступінь достовірності залежно від їх характеру і джерела, а також від ефективності контролю за процесом підготовки та обробки поданих документів.

Спостереження являє собою відстеження оцінювачем процедур або процесів забезпечення ІБ, виконуються іншими особами (в т.ч. персоналом організації). Інформація вважається достовірною тільки в тому випадку, якщо вона отримана безпосередньо в момент функціонування процедур або процесів, які перевіряються.

Усне опитування проводять оцінювачі серед співробітників (власників активів), затверджених представником об'єкта оцінки для надання джерел свідоцтв і свідоцтв оцінки. Результати усних опитувань повинні оформлятися у вигляді протоколу чи короткого конспекту, в якому обов'язково має бути зазначено прізвище, ім'я, по батькові оцінювача, який проводив опитування, прізвище, ім'я, по батькові опитуваної особи, а також їх підписи. Для проведення типових опитувань можуть бути підготовлені бланки з переліками питань, що цікавлять. Результати усного опитування слід перевіряти, так як опитуваний може виражати свою суб'єктивну думку.

Поряд з достовірністю джерел свідоцтв слід враховувати часовий період отримання оцінки. Наприклад, довіра до фактів, отриманим при спостереженні за діяльністю, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів; довіру до фактів, отриманим при опитуванні співробітників, підвищується при підтвердженні даних фактів з різних джерел.

3 Інформаційна потреба визначає, що потрібно виміряти для досягнення цілей оцінки ІБ об'єкта оцінки. Вимірювання, пов'язані із забезпеченням ІБ, можуть застосовуватися до різних об'єктів в рамках контексту оцінки. Для ідентифікації об'єктів вимірювання виділяються

критичні атрибути процесів, процедур, захисних заходів, які можуть надати дані, відповідні інформаційній потребі.

Метод кількісного вимірювання вимірює атрибути за допомогою відповідної шкали.

Методи вимірювання можуть бути суб'єктивними або об'єктивними. Суб'єктивні методи покладаються на кількісний вимір, що включає думку людини, тоді як об'єктивні методи використовують кількісне визначення, засноване на числових правилах, які можуть бути реалізовані за допомогою ручних або автоматичних засобів.

Повідомлення результатів оцінки може проходити неформально при внутрішній оцінці або може відбуватися у формі детального звіту за незалежної зовнішньої оцінки. Крім того, для представлення результатів оцінки можуть бути підготовлені і інші висновки і запропоновані плани дій, рекомендації, в залежності від призначення оцінки. Результати можуть бути представлені в абсолютних виразах або у відносних виразах у порівнянні з результатами попередніх оцінок, контрольними даними, в порівнянні з діловими потребами і т.д.

Вихідні дані оцінки включають дату проведення оцінки, вхідні дані оцінки, зібрані свідчення оцінки, опис використовуваного процесу вимірювання та оцінювання. Зареєстровані вихідні дані оцінки можуть зберігатися в різній формі - паперовій або електронній - в залежності від обставин та інструментів, використаних для проведення і підтримки оцінки.

На основі будь-якої угоди про забезпечення конфіденційності або обмежень доступу зареєстровані дані можуть зберігатися організатором оцінки або керівництвом об'єкта оцінки.

Важливими чинниками досягнення мети оцінки ризиків є наступні:

- усвідомлення і мотивація керівництва організації;
- конфіденційність;
- довіра.

Позиція керівництва організації робить істотний вплив на процес оцінки. Тому керівництво організації повинне спонукати учасників оцінки до відкритості і конструктивності. Оцінка об'єкта зосереджується на оцінці процесів, процедур, захисних заходів, а не на функціонуванні персоналу об'єкта оцінки. Сенс оцінки полягає в тому, щоб зробити об'єкт оцінки більш ефективними в досягненні цілей бізнесу, а не в тому, щоб покласти провину на окремих осіб.

Забезпечення зворотного зв'язку та підтримка атмосфери, що заохочує відкрите обговорення попередніх висновків під час оцінювання, сприяють забезпеченню того, щоб вихідні дані оцінки були значущими для об'єкта оцінки. Керівникам організації та персоналу об'єкта оцінки необхідно усвідомлювати, що учасники оцінки є основним джерелом знань і досвіду, пов'язаних з процесом, і що керівники та персонал мають гарну можливість для ідентифікації потенційних слабких місць.

Повага до конфіденційності джерел інформації та документації, зібраної під час оцінювання, необхідно для забезпечення безпеки цієї інформації. У тих випадках, коли використовуються опитування чи обговорення, слід звернути увагу на забезпечення того, щоб їх учасники не відчували загрози або не відчували якогось неспокою щодо конфіденційності. Деяка з наданої інформації може становити власність організації. Тому важливо наявність адекватних засобів контролю для поводження з такою інформацією.

Організатор оцінки, керівництво і персонал об'єкта оцінки повинні вірити в те, що оцінка принесе результат, який є об'єктивним для об'єкта оцінки. Важливо, щоб усі сторони могли бути впевнені в тому, що фахівці з оцінки володіють адекватними знаннями та досвідом для проведення оцінки, неупереджені та володіють адекватним розумінням об'єкта оцінки та його бізнесу для проведення оцінки.

2.2.1 Побудова моделі загроз

Вхідними даними оцінки загроз є модель загроз. Модель загроз безпеки необхідна для визначення вимог до системи захисту. Грамотно складена модель загроз дозволяє адекватно захистити інформацію і зробить мету прийнятих нормативних актів не примарною, а реальною. З іншого боку, погано або поверхнево складена модель загроз зробить всю подальшу роботу марною, не дозволить вірно скласти технічне завдання на розробку системи захисту персональних даних, призведе до необґрунтованих витрат на засоби захисту.

Відповідно до вітчизняних нормативних документів формування моделі загроз є необхідною умовою розробки системи захисту інформації.

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», модель загроз — це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Роботи зі створення моделі загроз безпеки інформації повинна проводитися в відповідності з наступними основними документами:

– ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт.»;

– НД ТЗІ 1.6-003-2004 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації»;

– НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;

– НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

– Постанова КМУ від 16.02.98 №180 «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

Модель загроз формується і затверджується відповідно до даних методичних документів, і може бути переглянута на основі:

– періодично аналізу та оцінки загроз безпеки інформації з урахуванням особливостей і (або) змін конкретної інформаційної системи;

– заходів з контролю за виконанням вимог до забезпечення безпеки інформації при їх обробці в інформаційній системі.

Розробка моделі загроз повинна базуватися на наступних принципах:

1) Безпека інформації при її циркуляції в ІС забезпечується системою захисту інформації.

2) Засоби захисту не можуть забезпечити захист інформації від дій, які виконуються в рамках наданих суб'єкту дій повноважень (наприклад, система захисту не може забезпечити захист інформації від розкриття особами, яким надано право на доступ до цієї інформації). Тому потрібно використовувати організаційні заходи разом з технічними засобами.

3) При формуванні моделі загроз необхідно враховувати як загрози, здійснення яких порушує безпеку інформації (далі - пряма загроза), так і загрози, що створюють умови для появи прямих загроз (далі - непрямі загрози) або непрямих погроз.

4) Інформація обробляються і зберігаються в ІС з використанням певних інформаційних технологій і технічних засобів, що є об'єктами захисту різного рівня, атаки на які створюють прямі або непрямі загрози інформації.

Для розробки моделі загроз необхідно послідовно здійснити наступні кроки:

1) провести категорювання об’єкту інформаційної діяльності;

2) розглянути логічну послідовність процесу порушення інформаційної безпеки;

3) ідентифікувати всі складові моделі загроз та зіставити їх;

4) дослідити зіставлені складові та зробити висновки про їх актуальність;

5) оформити результати висновків відповідно підготовленого шаблону;

Розробка моделі загроз проводиться на основі детального аналізу атрибутів. У випадку побудови моделі загроз, атрибутами є загрози, їх джерела та вразливості.

Після проходження всіх кроків буде сформована модель загроз.

Наступним кроком необхідно визначити фактори, від яких залежить ступінь ризику та оцінити вірогідність виникнення кожного ризику. Ресурс повинен бути проаналізований з точки зору оцінки впливу можливих атак. Крім того необхідно ідентифікувати вразливості, які роблять можливою реалізацію загрози. Тобто необхідно створити модель загроз та на її основі визначити рівень ризику. Для цього послідовно для кожної загрози необхідно визначити:

- найменування загрози;
- об'єкт загрози;
- використані вразливості;
- вплив на властивості інформації (конфіденційність, цілісність, доступність);
- можливі наслідки.

Модель загроз для оцінки антропогенних ризиків для охоронного підприємства «С.Е.Т.» представлена в таблиці 2.1.

Таблиця 2.1 – Модель загроз для охоронного підприємства ТОВ «С.Е.Т.»

Найменування загрози	Об'єкт загрози	Вразливості	Вплив на інформацію (К, Ц, Д)	Можливі наслідки
Крадіжка				
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до носіїв інформації	К, Ц, Д	розкриття інформації, матеріальні втрати
інформації	персонал, відвідувачі, обслуговуючий персонал	збереження ключової інформації на жорстких дисках та в реєстрі	К, Ц, Д	розкриття інформації, матеріальні втрати

засобів доступу	персонал, відвідувачі, обслуговуючий персонал	збереження засобів доступу у загальнодоступному місці	К, Ц, Д	розкриття інформації, матеріальні втрати
технічних засобів	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К, Ц, Д	розкриття інформації, матеріальні втрати
Підміна				
документу при передачі	персонал, відвідувачі, обслуговуючий персонал	не захищеність комп'ютерної мережі	К, Ц, Д	розкриття інформації, матеріальні втрати
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К, Ц, Д	розкриття інформації, матеріальні втрати
ОС та ПЗ	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К, Ц, Д	розкриття інформації, матеріальні втрати
Знищення				
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
ПЗ, ОС, СУБД	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
технічних засобів	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства

каналів зв'язку	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц, Д	втрата інформації, припинення роботи підприємства
інформації при передачі каналами зв'язку	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
Несанкціонований доступ				
при технічному обслуговуванні (ремонті, знищенні) вузлів ПЕОМ	обслуговуючий персонал	відсутність контролю за технічним персоналом	К, Ц, Д	знищення, спотворення, розкриття інформації, матеріальні втрати
при передачі каналами зв'язку	персонал, відвідувачі, обслуговуючий персонал	недостатня захищеність комп'ютерної мережі	К, Ц, Д	знищення, спотворення, розкриття інформації, матеріальні втрати
несанкціоноване вимкнення засобів захисту	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	К, Ц, Д	втрата, розкриття інформації, матеріальні втрати
дія шкідливих програм (вірусів)	персонал, відвідувачі, обслуговуючий персонал	використання комп'ютерів, на яких встановлена СЕД для відвідування сторонніх Інтернет сайтів, встановлення несертифікованого ПЗ, не пов'язаного з виконанням службових обов'язків	К, Ц, Д	розкриття, втрата інформації, матеріальні втрати
Розголошення інформації співробітниками, допущеними до її обробки	персонал	погана інформованість співробітників з боку ІБ, зацікавленість в розкритті інформації	К, Ц, Д	розкриття інформації, матеріальні втрати

2.2.2 Моделі оцінки ризиків для антропогенних загроз

2.2.2.1 Модель якісної оцінки «Ризик атаки – Важливість активу»

Модель якісної оцінки ризики зводиться до побудови таблиці 2.2. Таблиця заповнюється екземплярами інформаційних активів або окремими системами на основі інтуїтивного уявлення заповнюю чого про ту чи іншу інформацію, або на основі заповнення підготовлених анкет для компетентних співробітників організації. Рішення приймається в залежності від конкретної організації для об'єктів, що знаходяться у третій зоні або у третій та другій зонах.

Таблиця 2.2 – «Ризик атаки – Важливість активу»

	Важливий	Критичний	Життєвий
Низький	1	1	2
Середній	1	2	3
Високий	2	3	3

Можливий ще більш спрощений підхід, який називається «основна лінія» і полягає у тому, що організація аналізує стан побудови систем безпеки, який склався в галузі (можливо в організаціях, схожих за профілем), та порівнює з системою безпеки, побудованої в самій компанії. Якщо виявиться відставання, ресурси направляються на приведення ситуації до рівня, близькому до середнього в галузі.

Позитивні сторони оцінки ризику по якісній моделі полягають у наступному:

- розрахунки прискорюються та спрощуються;
- немає необхідності привласнювати грошову вартість активу;
- немає необхідності обчислювати частоту появи загрози та точний розмір збитків;

– не потрібно обчислювати відповідність ефективності запропонованих мір загрозам.

Негативні сторони полягають в основному в суб'єктивності підходу до оцінки та відсутності можливості встановити точну відповідність затрат загрозам.

2.2.2.2 Модель якісної оцінки ризику на основі побудови матриці «Вірогідність - втрати»

Для визначення ступеня впливу та рівня ризику використовують наступні градації: високий, середній, низький. Проте на практиці важливо визначити ступінь впливу кожного ризику відносному вираженні, для чого рекомендують використовувати шкалу від 1 до 5 (Таблиця 2.3).

Таблиця 2.3 – Ступінь впливу ризику

Матриця «Вірогідність - Втрати»		Втрати				
		1	2	3	4	5
Вірогідність	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Ймовірність виникнення відповідають наступним значенням:

1) слабкоймовірні;

2) малоймовірні;

3) ймовірні;

4) досить ймовірні;

5) майже можливі.

Величина втрат приймає наступні значення:

1) мінімальні;

2) низькі;

3) середні;

4) високі;

5) максимальні.

Відповідно рівень ризику набуватиме наступних значень:

1) прийнятні (1-4);
2) виправдані (5-11);
3) неприпустимі (12-25).

2.2.2.3 Кількісна модель оцінки ризиків «Очікуваний річний збиток»

Кількісна модель ризиків оперує такими поняттями, як:

- річна частота події (англ. Annualized Rate of OccurrenceARO);
- очікуваний одиничний збиток (англ. Single Loss Expectancy - SLE);
- очікуваний річний збиток (англ. Annualized Loss Expectancy - ALE), величина, що дорівнює добутку ARO на SLE.

$$ALE = ARO \cdot SLE ,$$

де ARO - частота появи події, що приносить шкоду на рік. Даний показник також можна назвати інтенсивністю події. SLE - показник, який розраховується як добуток вартості інформації (Asset Value - AV) на фактор впливу (англ.Exposure Factor - EF). Фактор впливу - це розмір збитку або впливу на значення активу (від 0 до 1), тобто частина значення, яку актив втратить в результаті події.

$$SLE = AV \cdot EF.$$

Управління ризиками вважається ефективним, якщо витрати на безпеку на рік не перевищують очікуваний річний збиток.

2.2.2.4 Модель узагальненого вартісного результату Міори (GCC)

Модель Міори розроблена як альтернатива кількісної моделі ризиків для поліпшення і полегшення розрахунків і обчислень. Одним з основних недоліків якої є її імовірнісна складова.

Модель Міори не враховує ймовірностей події, вона оперує поняттям збитку від простою як функцією часу після настання події. Для кожного інформаційного активу або групи подібних по ряду ознак активів, званих категорією, визначається розмір можливого збитку, термін початку його впливу на організацію та розподіленість за часом.

Розвиток картини збитку можна представити у вигляді графіка, де категорії - це функції по двох осях: «час у днях»; «збиток в грошах». У результуючому графіку представляються дві криві: сумарний збиток організації за відсутності захисних заходів; сумарний збиток прі наявності захисних заходів.

На такому графіку наочно видно необхідність і ефективність застосовуваних заходів для забезпечення захисту інформації.

2.2.2.5 Модель оцінки ризику за двома факторами

Модель оцінки ризику за двома факторами реалізується в чотири кроки.

На першому кроці оцінюється негативний вплив (показник ресурсу) по заздалегідь визначеній шкалі, наприклад від 1 до 5, для кожного ресурсу, якому загрожує небезпека (колонка b в таблиці).

На другому кроці оцінюється по заздалегідь визначеній шкалі, наприклад від 1 до 5, визначається вірогідність реалізації кожної загрози.

На третьому кроці обчислюється показник ризику. В найпростішому варіанті методики це робиться шляхом множення (b, x, c). Проте для рангових (якісних) шкал вимірювання, якими являються показник негативного впливу та ймовірність реалізації загрози, наприклад, зовсім не обов'язково показник ризику, відповідних ситуації b=3, c=1 буде еквівалентний b=1, c=3.

Відповідно, повинна бути розроблена методика оцінки показників ризику стосовно конкретної організації.

На четвертому кроці загрози ранжуються за значенням їхнього фактора ризику (Таблиця 2.4).

Таблиця 2.4 – Ранжування ризиків

Дескриптор загрози	Показник негативного впливу(ресурса)	Можливість реалізації загрози (суб'єктивна оцінка)	Показник ризику	Ранг ризику
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1

Дана процедура дозволяє порівняти та ранжувати загрози з різним негативним впливом та ймовірністю реалізації. В деяких випадках додатково можуть прийматись до уваги вартісні показники.

2.2.2.6 Модель оцінки ризику за трьома факторами

По кожній групі ресурсів, пов'язаних з даною загрозою, оцінюються рівень загрози (ймовірність реалізації) та рівень вразливості (ступінь легкості, з якою реалізована загроза здатна привести до негативного впливу). Оцінювання проводиться в якісних шкалах. Спочатку визначають рівні загроз, вразливостей, тяжкості наслідків і ризиків.

Рівні загроз ранжуються на:

- низький (Н) – реалізація даної загрози маловірогідна, за останні 2 роки подібних випадків не зафіксовано;
- середній (С) – загроза може бути реалізована протягом 1 року з вірогідністю приблизно 0.3;

– високий (В) – загроза більш за все реалізується протягом року і можливо не один раз.

Рівні вразливостей ранжуються на:

– низький (Н) – захищеність системи дуже висока, реалізація загроз майже ніколи не призводить до негативних наслідків;

– середній (С) – захищеність системи середня, реалізація приблизно 30% загроз призводить до негативних наслідків;

– високий (В) – захищеність системи дуже низька, реалізація загроз майже завжди призводить до негативних наслідків.

Показники негативного впливу (тяжкості наслідків):

1) Negligible (збиток до $100);
2) Minor (збиток до $1000);
3) Moderate (збиток до $10000);
4) Serious (суттєвий негативний вплив на бізнес);
5) Critical (катастрофічний вплив, можлива зупинка).

Показник ризику вимірюється в шкалі від 0 до 8, визначення рівнів ризику представлене в таблиці 2.5.

Таблиця 2.5 – Ступінь серйозності випадків

Ступінь серйозності випадку (ціна втрати)	Рівень загрози								
	Низький			Середній			Високий		
	Рівень вразливості			Рівень вразливості			Рівень вразливості		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

2.2.2.7 Експертні методи оцінки ризику

Експертні методи оцінки ризику досить різноманітні. Найпоширеніші з них описані нижче:

1 Метод номінальних груп. Метод являє собою певний перехід від індивідуального опитування до групового. При реалізації цього методу спочатку здійснюється індивідуальне опитування одних експертів, а потім результати даних інтерв'ю так само автономно і незалежно один від одного обговорюються іншими експертами. Експерти можуть висловити згоду чи незгоду з раніше прозвучали думками, необхідно, щоб критика або вираз солідарності були чітко аргументовані;

2 Мозковий штурм. Метод являє собою спільне очне обговорення проблеми групою експертів. Метод реалізується у два етапи. Перший етап носить назву "конференції ідей", його тривалість становить приблизно 1-1,5 години. У ході цього етапу експерти висувають різні ідеї, що стосуються трактування аналізованої ситуації і чи прогнозу розвитку явища. Ідеї протоколюються, але не обговорюються і не критикуються. Головує принцип: чим більше ідей, тим краще. Після перерви, на другому етапі, ідеї обговорюються, оцінюються, і вибираються ті з них, які визнаються найбільш вірними. Остаточний вердикт з проблеми може бути прийнятий шляхом явного або неявного голосування. Процедури генерації та обговорення ідей можуть бути більшою ними меншій мірі формалізовані;

3 Критична атака. Метод є варіацією методу мозкового штурму, принципова відмінність - у критичній спрямованості обговорення. Реалізація методу включає кілька етапів. На першому етапі кожен учасник експертної групи пропонує своє вирішення поставленого завдання (свою інтерпретацію при аналізі ситуації) або свою версію розвитку подій (при прогнозі). Рішення має пропонуватися з докладною аргументацією. Далі кожен експерт повинен ознайомитися з думками своїх колег і знайти і аргументувати в пропоновані рішення максимально можливе число слабкостей. На наступному етапі експерти збираються разом і по черзі обговорюють усі висунуті рішення.

Завдання кожного учасника - відстояти свою версію рішення, завдання опонентів - "рознести її в пух і прах". За підсумками дискусії експерти вибирають те рішення, яке викликало найменше нарікань і було найбільш обґрунтованим;

4 Експертне фокусування. Метод являє собою одну з форм спільного очного обговорення проблеми. Експерти всебічно розглядають досліджувану ситуацію, "фокусуються" на ній. Основна мета - виявити структуру даної проблеми, визначити по можливості всі фактори, що визначають дану ситуацію, встановити взаємозв'язки між ними. Обговорення носить більш діловий характер, ніж при класичній версії мозкового штурму, тобто проходить без зайвого "марення";

5 Метод інтеграції рішень. Метод полягає у виробленні спільного вирішення проблеми на основі виявлення сильних сторін окремих рішень та їх об'єднання. Метод реалізується в кілька етапів. На першому етапі експертам пропонується завдання, і вони розглядають і вирішують її незалежно один від одного. Потім у заздалегідь підготовлений формуляр експерти заносять свої індивідуальні рішення, тобто трактування аналізованої ситуації або прогноз розвитку подій. На наступному етапі експерти спільно обговорюють завдання і всі запропоновані рішення з метою виявити сильні сторони кожного окремого рішення, які також фіксуються в формулярі. При поданні індивідуальних рішень можливі варіації - або кожне рішення презентується автором і детально аргументується, або дотримується анонімність рішень, щоб уникнути тиску авторитетів. Після того як обговорені всі рішення та визначено сильні сторони кожного з них, виробляється синтезоване рішення на основі комбінування переваг окремих рішень;

6 Ділова гра. Метод може бути реалізований в різних формах. Найбільш поширена форма - моделювання аналізованих процесів і / або майбутнього розвитку прогнозованого явища в різних варіантах і розгляд отриманих даних. Розробка процедури проведення ділової гри - досить

складне завдання, і їй має бути приділено серйозну увагу. Мають бути чітко визначені і формально описані наступні елементи гри: цілі та завдання, ролі учасників, сюжет і регламент. Важливим етапом будь-якої ділової гри є рефлексія - розбір ходу гри і підведення підсумків. У даному випадку рефлексія полягає не тільки в аналізі самого ігрового процесу, а й в аналізі результатів моделювання досліджуваного явища;

7 Метод Дельфі. Метод являє собою заочний і анонімне опитування експертної групи в кілька турів з узгодженням думок експертів. Експертам пропонуються опитувальні листи з досліджуваної проблеми. Ступінь стандартизованість питань може бути різна (вони можуть бути як закритими, так і відкритими, мати на увазі як кількісну, так і якісну відповідь). Можливі варіації і в плані аргументації і обґрунтування експертних оцінок (що може бути обов'язковим чи ні). Як правило, метод Дельфі реалізується в 2-3 туру, причому при повторних опитуваннях експертам пропонується ознайомитися або з думками і аргументами кожного експерта, або з середньою оцінкою. На повторних турах експерти можуть поміняти свою оцінку, взявши до уваги аргументи колег, а можуть залишитися при колишньому думці і висловити обґрунтовану критику інших оцінок. Існують різні методики узгодження експертних оцінок (з урахуванням (або без) кваліфікації експертів (як вагових коефіцієнтів), з відкиданням (або без) крайніх оцінок і інші). Метод Дельфі має вельми істотні переваги, які іноді роблять його незамінним. По-перше, заочність і анонімність дозволяють уникнути конформізму або орієнтації на авторитети, що могло б виникнути, якби експертів зібрали разом і вони повинні були б оприлюднити свою думку. По-друге, експерти мають можливість змінити свою думку без ризику "втратити обличчя".

2.3 Розробка рекомендацій щодо заходів, направлених на зменшення впливу антропогенних загроз

Процес проведення оцінки ризиків інформаційної безпеки пов’язаних з антропогенними загрозами має проводитись згідно концепії документу

«Політика безпеки інформації». Результати оцінки ризиків допоможуть направити і визначити відповідні дії і пріоритети в галузі управління ризиками для захисту інформації, а також в області реалізації засобів управління, обраних для захисту від цих ризиків.

Результати проведеної оцінки ризиків мають корелювати існуючу політику безпеки, а саме в розділах:

- організація захисту інформації (від внутрішніх та зовнішніх загроз);
- захист людських ресурсів (перед прийомом на роботу, під час роботи та після звільнення);
- управління доступом;
- менеджмент інцидентів (обов'язкове ведення статистики інцидентів).

Захист інформації підприємства багато в чому зводиться до реалізації оптимальних методів роботи на основі ефективної корпоративної політики безпеки.

Всі заходи щодо забезпечення інформаційної безпеки можна умовно розділити на правові, організаційні, технічні та психологічні, які мають обов'язково зазначені в документі «Корпоративна політика безпеки інформації».

2.3.1 Правові заходи щодо атак із застосуванням соціальної інженерії

Правові заходи забезпечення збереження комерційної таємниці є першочерговими, тому що вони покликані забезпечити ефективне функціонування інших заходів забезпечення конфіденційності інформації. З цієї точки зору правові заходи є первинними по відношенню до решти заходів.

Даний вид заходів щодо захисту інформації буде ефективний тільки у разі виконання всіх юридичних норм та етапів щодо збереження конфіденціальної інформації, що відповідають чинному законодавству України.

Юридичні заходи являють собою основу всіх наступних заходів протидії, як внутрішніх, так частково і зовнішніх загроз. Так як без правильно вибудуваної правового захисту, подальші заходи з протидії внутрішнім загрозам є не ефективними і безпідставними, з точки зору правомірності тих чи інших рішень з боку керівництва. У такому випадку, накласти на співробітників даного підприємства будь-якої вид відповідальності, за вчинене діяння неможливо.

До таких заходів, в першу чергу, відносяться:

– прийняття положення щодо забезпечення збереження конфіденціальної інформації;

– укладання договорів про матеріальну відповідальність за розголошення конфіденціальної таємниці;

– прийняття розписок про нерозголошення комерційної таємниці, а також попередження про відповідальність за розголошення конфіденційної інформації;

– включення положень про конфіденційну інформацію у договори.

2.3.2 Організаційні заходи щодо запобігання атак із застосуванням соціальної інженерії

Ключові принципи і правила управління персоналом з урахуванням вимог інформаційної безпеки визначені в міжнародному стандарті ISO/IEC 27001 і зводяться до необхідності виконання певних вимог безпеки, підвищення обізнаності співробітників і застосування запобіжних заходів до порушників.

Організаційні заходи, які проводяться в організації, повинні включати в себе:

– регламентацію внутрішньо-корпоративних процедур, в тому числі розробку нормативних документів;

– організацію контролю за діяльністю компанії;

– навчальну та пояснювальну роботу з співробітниками;

– профілактичну роботу з співробітниками (виявлення осіб, схильних до різноманітних правопорушень, роз'яснення наслідків правопорушень та ін.).

Важливу роль для забезпечення інформаційної безпеки відіграє обізнаність користувачів в питаннях безпеки та правила безпечної з точки зору захисту інформації поведінки. Основну роль тут відіграють менеджери організації.

Повинно проводитися навчання та контролювання знань користувачів з наступних питань:

– політика безпеки організації;

– правила вибору, зміни та використання паролів;

– правила отримання доступу до ресурсів інформаційної системи;

– правила поводження з конфіденційною інформацією;

– процедури інформування про інциденти, вразливості, помилки та збої програмного забезпечення та ін.

В організації повинно бути розроблено положення щодо захисту конфіденційної інформації та відповідні інструкції. Ці документи повинні визначати правила та критерії для категорювання інформаційних ресурсів за ступенем конфіденційності (наприклад, відкрита інформація, конфіденційна, суворо конфіденційна), правила маркування конфіденційних документів і правила поводження з конфіденційною інформацією, включаючи режими зберігання, способи звернення, обмеження щодо використання та передачі третій осторонь і між підрозділами організації.

Повинні бути визначені правила надання доступу до інформаційних ресурсів, впроваджені відповідні процедури і механізми контролю, в тому числі авторизація та аудит доступу.

Також в організації повинен бути розроблений дисциплінарний процес, який буде працювати відносно порушників безпеки і який буде передбачати розслідування та ліквідацію наслідків інцидентів.

Основою для ефективності організаційних заходів є контроль виконання даних заходів керівництвом та працівниками підприємства. В іншому

випадку всі прийняті і розроблені заходи з протидії внутрішнім загрозам втрачають свою значимість і ефективність.

Аспекти, пов'язані з безпекою, слід враховувати ще на стадії набору персоналу, включати їх у посадові інструкції та договори, а також контролювати протягом усього часу роботи даного співробітника. Керівник повинен переконатися в тому, що в посадових інструкціях відображена вся відповідна даній посаді відповідальність за безпеку. Слід належним чином перевірити прийнятих на роботу осіб, особливо якщо вони будуть працювати з конфіденційною інформацією. Весь персонал фірми та користувачі інформаційних ресурсів з сторонніх організацій, допущені до конфіденційної інформації повинні підписати зобов'язання про конфіденційність (нерозголошення).

Обов'язки та відповідальність за безпеку, встановлені прийнятої в організації політикою інформаційної безпеки, слід включати до посадових інструкцій, де це необхідно. В інструкціях необхідно відобразити як спільну відповідальність за проведення в життя або підтримку політики безпеки, так і конкретні обов'язки щодо захисту певних ресурсів або відповідальність за виконання певних процедур або дій щодо захисту.

Заяви про прийом на роботу слід ретельно розглянути, якщо робота на даній посаді пов'язана з доступом до конфіденційних інформаційних ресурсів. Усіх кандидатів на зайняття таких вакансій слід перевірки за наступними пунктами:

- як мінімум дві позитивних характеристики, одна ділових і одна особистих якостей;
- перевірка повноти і точності відомостей, повідомлених претендентом на вакансію у своїй автобіографії;
- підтвердження академічних ступенів і професійної кваліфікації;
- перевірка ідентифікації (наприклад паспорта);
- перевірка кредиту для зайнятих в найбільш критичних завданнях, наприклад, перевірка фінансового стану.

Користувачі з сторонніх організацій, не передбачені умовами існуючого договору (зобов'язання про нерозголошення є його частиною), повинні підписати зобов'язання про нерозголошення, перш ніж їм буде надано доступ до інформаційних ресурсів організації.

Не дивлячись на те, що навчання персоналу є прерогатива відділу роботи з персоналом, підвищення обізнаності користувачів у питаннях ІБ – це закриття однієї з вразливостей інформаційної системи. Навчання персоналу не має бути проблемою, тому що керівник підприємства підвищує кваліфікацію своїх співробітників.

В якості основних рішень представлені наступні продукти:

– звичайні курси, які в основному призначені для навчання співробітників при прийомі на роботу або розробляються на замовлення за матеріалами політики безпеки замовника;

– корпоративні системи дистанційного навчання з набором теоретичних і практичних матеріалів, системою планування навчання і системою контролю знань;

– друковані матеріали – постери, календарі тощо відповідної тематики;

– розсилки новин з інформаційної безпеки для користувачів;

– різні рішення для періодичного тестування практичних навичок користувачів.

Усі без винятку перераховані вище продукти можна впровадити в роботу співробітників з метою підвищення обізнаності в галузі інформаційної безпеки.

Крім навчання, всі продукти допомагають вирішити таку важливу задачу, як зміна відношення користувачів до забезпечення інформаційної безпеки, яке зараз різко негативне. Це ставлення результат того, що спочатку вводяться різні технічні обмеження, заборонні інструкції, а вже пізніше користувачам пояснюється, навіщо потрібні ті чи інші правила.

Ці заходи необхідні для того, щоб гарантувати, що процедури захисту виконуються правильно, і для зведення ризику порушення конфіденційності, цілісності та доступності даних через помилки користувача до мінімуму.

Для забезпечення нормального функціонування сервісу Internety користувачі повинні:

– використовувати Internet тільки для службових цілей;

– не заходити на Веб-сайти, що надають платні послуги, без узгодження з системним адміністратором;

– не здійснювати підписку на отримання Internet-інформації та послуг;

– не поширювати в мережі Internet інформацію, що стосується роботи фірми або його співробітників, в тому числі про себе;

– не створювати і не використовувати власних поштових скриньок, Веб-сторінок та інших інформаційних активів в мережі Internet;

– забороняється заходити на Веб-сайти, що містять еротико-порнографічні матеріали та ігрові програми;

– забороняється переносити (копіювати) на свій комп'ютер картинки, художню літературу, музичні та відео, заархівовані файли і будь-яке програмне забезпечення без погодження з керівництвом.

Ці заходи найбільш ефективні для захисту інформації при використанні зловмисниками віртуальних та мережевих методів соціальної інженерії.

2.3.3 Технічні заходи щодо запобігання атак із застосуванням соціальної інженерії

Комплексний підхід до забезпечення безпеки ІС компанії будь-якого розміру і напряму діяльності, звичайно, включає проектування систем безпеки, розробку політики інформаційної безпеки (ІБ) для забезпечення захисту від зловмисників, а також проведення «тесту на проникнення» для перевірки ступеня захищеності інформаційних ресурсів ззовні.

Підхід до тесту здійснюється з позиції потенційного зловмисника і має на увазі активну експлуатацію вразливостей в безпеці, в той же час тест

проводиться висококваліфікованими фахівцями, які дотримуються етики при його проведенні.

Будь-які знайдені відомості, що стосуються безпеки, представляються власникові системи разом з оцінкою потенційного збитку. Також надаються конкретні рекомендації щодо усунення знайдених вразливостей.

Тести на проникнення допомагають на практиці одержати об'єктивну і незалежну оцінку того, наскільки легко здійснити несанкціонований доступ до ресурсів корпоративної мережі компанії. Тест на проникнення - це моделювання дій зловмисників по проникненню в інформаційну систему в умовах, максимально наближених до тих, які виникають при атаці хакерів.

Існує безліч загальновизнаних міжнародних методик «тесту на проникнення», найпоширеніші з них:

- Information Systems Security Assessment Framework (OISSG);
- The Open Source Security Methodology Manual (OSSTMM);
- NIST Guideline on Network Security Testing;
- SACA Switzerland – Testing IT Systems Security With Tiger Teams;
- OWASP Testing Guide.

Для того, щоб зберегти впевненість в захищеності інформаційних активів необхідно завчасно відвертати загрози безпеки, що вимагає безпосередньої уваги.

2.3.4 Психологічні заходи щодо запобігання атак із застосуванням соціальної інженерії

Робота зі співробітниками підприємства, незалежно від ступеня конфіденційності інформації, до якої дані співробітники допущені (допускалися або будуть допускатися), проводиться у кілька етапів:

1) при прийомі кандидата на роботу;

2) в ході виконання співробітником підприємства, допущеним до конфіденційної інформації, посадових обов'язків;

3) безпосередньо перед звільненням і в процесі звільнення працівника з підприємства (переведення на посаду, не пов'язану з доступом до конфіденційної інформації).

Зусилля керівництва підприємства повинні бути зосереджені на наступних основних напрямках роботи зі співробітниками, допущеними до конфіденційної інформації:

- вивчення морально-ділових якостей співробітників підприємства;

- підвищення відповідальності працівників усіх категорій за збереження в таємниці довірених по службі відомостей конфіденційного характеру;

- проведення профілактичної роботи із запобігання (виключення) витоку конфіденційної інформації шляхом її розголошення;

- підвищення рівня теоретичних знань і практичних навичок співробітників в питаннях захисту конфіденційної інформації;

- створення і підтримання сталого морально-психологічного клімату в колективі підприємства;

- створення і застосування системи стимулювання праці співробітників, допущених до конфіденційної інформації.

Одним з методів перевірки відповідності кандидата до роботи є випробування. Порядок встановлення та проведення випробування визначається КЗПП. За результатами випробування роботодавцем може бути прийнято рішення про розірвання трудового договору з даним працівником або про визнання його таким що витримав випробування.

На основі вивчення матеріалів особової справи, анкетних, автобіографічних та інших персональних даних, інших документів кандидата, а також результатів особистої бесіди з кандидатом посадових осіб підприємства (працівників кадрового органу) формується висновок про оцінку відповідності кандидата вимогам. Результати тестування дозволяють визначити рівень підготовленості кандидата до виконання посадових обов'язків, у тому числі знання ним положень нормативно-методичних документів, і наявні в нього практичні навички роботи з даної спеціальності.

При підготовці до співбесіди керівник підрозділу, на посаду в якому претендує кандидат, спільно з кадровим органом повинен:

- сформулювати основні завдання та обов'язки, які належить виконувати співробітнику, що займає зазначену посаду;

- сформувати перелік відомостей конфіденційного характеру, до яких передбачається допустити співробітника;

- підготувати перелік форм і методів стимулювання праці співробітника (у тому числі матеріальної);

- підготувати посадову інструкцію, визначальну вимоги до кандидата для призначення на посаду.

До кандидатів висувають такі основні вимоги, що стосуються їх морально-ділових і особистісних якостей:

- порядність, чесність, принциповість і сумлінність;

- старанність і дисциплінованість;

- емоційна стійкість (самовладання);

- постійне прагнення до підвищення рівня теоретичних знань і практичних навичок;

- здатність виділити головне в роботі, сконцентруватися на вирішенні найбільш важливих питань;

- правильна оцінка власних здібностей і можливостей;

- помірна схильність до можливих ризиків;

- хороша пам'ять.

При відборі кандидатів для призначення на посади перераховані додатково враховується обсяг і важливість відомостей конфіденційного характеру, до яких допускаються співробітники, що займають ці посади.

Також необхідно проводити тестування співробітників, як на етапі прийому на роботу, так і в процесі праці для контролю і аналізу психологічного стану працівника. Тестування необхідно проводити один раз на пів року. Корисними методиками можна відзначити наступні:

- методика діагностики до конфліктної поведінки К. Томаса,

- методика «Ціннісні орієнтації» М. Рокича,
- методика діагностики рівня суб'єктивного контролю Дж. Роттера,
- тест Лірі, тощо.

Сучасні кадрові менеджери для перевірки співробітників застосовують провокацію все частіше і частіше. Роботодавець перевіряє, як кандидат буде поводитися в нестандартних ситуаціях, які мають на увазі сильний стрес. Така перевірка є набагато ефективніше, ніж звичайні тестування, коли працівник встигає підготуватися і відноситься до перевірки більш спокійно.

Керівництво компанії має бути впевненим у тому, що співробітники є повністю лояльними. Також можуть розраховувати на те, що до них підсилають провокатора, ті співробітники, яких компанія планує направити на безкоштовне навчання або перекваліфікацію. Оскільки будь-яке навчання вимагає вкладення коштів, роботодавець повинен бути впевненим в тому, що навчений співробітник не втече в іншу компанію. Для перевірки працівника на вірність, потрібно лише зателефонувати йому, представитися менеджером великої компанії і запропонувати привабливу роботу.

Основними формами контролю якості роботи персоналу підприємства, підвищення професіоналізму співробітників в сфері захисту конфіденційної інформації є:

- перевірки керівництвом підприємства або службою безпеки (режимно-секретних підрозділом) дотримання співробітниками положень нормативно-методичних документів по захисту інформації;
- звіти та доповіді керівників структурних підрозділів про результати роботи підлеглих працівників;
- періодична атестація співробітників, допущених до конфіденційної інформації;
- самоконтроль співробітників.

2.3.5 Методи мотивації персоналу

Особливе місце у діяльності керівництва підприємства і керівників структурних підрозділів по роботі з персоналом займають методи мотивації співробітників, спрямовані на ефективне та якісне виконання покладених на них завдань на тлі суворого дотримання норм і правил захисту конфіденційної інформації.

Мотивація дій співробітників підприємства є основою загальної організаторської та управлінської функції керівника будь-якого рівня. При відсутності мотивації будь-яка організаційна, яка планує, координує та інша управлінська робота втрачає всякий сенс. У найзагальнішому вигляді мотивація - це процес спонукання співробітника підприємства (фірми) до діяльності в ім'я досягнення певних цілей за допомогою внутрішньоособистісних і зовнішніх факторів. В основі спонукання лежить сукупність потреб, інтересів, бажань, цільових установок, ціннісних орієнтацій, очікувань співробітника. Основні фактори, що обумовлюють результативність праці персоналу, - готовність, можливість та умови для результативної діяльності.

Виділяють три основні групи методів мотивації:

- методи безпосередньої мотивації праці;
- методи владної, примусової мотивації;
- методи стимулювання праці (морального, матеріального, трудового);
- методи безпосередньої мотивації праці характеризуються прямим впливом на особистість співробітника. До цієї групи належать методи переконання, навіювання та агітації.

Методи владної, примусової мотивації засновані на реальному примусі або потенційної можливості застосувати примус: виконання вказівок, наказів, розпоряджень та інших директивних рішень.

Методи стимулювання праці спрямовані на створення такої ситуації, яка спонукає співробітника діяти певним чином, і включають:

- моральне стимулювання - направлено на задоволення потреб співробітника в повазі і визнання з боку колективу, до найбільш поширених методів морального стимулювання відносяться заохочення, нагородження медалями, почесними знаками, присвоєння почесних звань;

- матеріальне стимулювання - направлено на підвищення рівня добробуту персоналу, реалізується в грошовій формі (виплата премій, різних надбавок, підвищення заробітної плати, залучення до участі в прибутках) і негрошовій формі (виділення путівок на відпочинок, надання житла, поїздки за місто і кемпінгові намети);

- трудове стимулювання - направлено на задоволення потреб співробітника в самовираженні і полягає в наданні йому можливості службового зростання, а також переведення (призначення) на посади, які більше відповідають його реальним можливостям, здібностям і інтересам.

Для підвищення ефективності праці персоналу, допущеного до конфіденційної інформації, необхідно комплексне використання перерахованих методів і засобів мотивації.

Треба розуміти, що успішна реалізація перелічених підходів можлива тільки при існуванні в організації діючої системи управління інформаційною безпекою, яка характеризується, перш за все, наявністю діючої політики безпеки і організаційної структури, вистроєної у відповідності з цією політикою, а також наявністю процесів, процедур та механізмів контролю. Дані заходи базуються на юридичних заходах боротьби з антропогенними загрозами. Всі організаційні документи повинні бути погоджені з юридичними документами прийнятими на підприємстві, а так само не суперечити чинному законодавству України.

2.4 Висновок

Статистика інцидентів в сфері інформаційної безпеки в світі та України зокрема показує, що інциденті, пов’язані з антропогенними загрозами, є найрозповсюдженим видом порушень. В такому разі тільки чітка

ідентифікація та оцінка антропогенних загроз дає можливість вжити необхідних превентивних заходів безпеки.

Процес оцінки ризиків інформаційної безпеки має включати такі послідовні етапи проведення оцінки:

– визначення контексту оцінки, який визначає вхідні дані: цілі й призначення оцінки, вид оцінки (незалежна оцінка, самооцінка), об'єкт та області оцінки ІБ, обмеження оцінки і ролі;

– визначення критеріїв оцінки;

– визначення моделі оцінки;

– збір свідчень оцінки та перевірка їх достовірності, вимірювання та оцінювання атрибутів об'єкта оцінки;

– отримання вихідних даних оцінки.

Вхідними даними оцінки загроз є модель загроз. Модель загроз безпеки необхідна для визначення вимог до системи захисту. Грамотно складена модель загроз дозволяє адекватно захистити інформацію і зробить мету прийнятих нормативних актів не примарною, а реальною. З іншого боку, погано або поверхнево складена модель загроз зробить всю подальшу роботу марною, не дозволить вірно скласти технічне завдання на розробку системи захисту персональних даних, призведе до необгрунтованих витрат на засоби захисту.

В першу чергу необхідно встановити критерії прийняття ризику та класифікувати ризики в залежності від величини можливих втрат для конкретного підприємства. Для адекватного вибору критеріїв оцінки ризиків необхідно спочатку визначити вартість активів. Це пояснюється тим, що встановивши критерії ризику без урахування їх вартості, всі ризики можуть потрапити в одну категорію, що буде не правильним. Тобто спочатку необхідно визначити вартість активів. Вартість активу визначатиметься на основі опитування співробітників з врахуванням їх коефіцієнту кваліфікації.

Необхідно брати до уваги той факт, що деякі ризики можуть виникати частіше, деякі рідше, тому для адекватної оцінки необхідно аналізувати

ймовірність та частоту виникнення як один показник, значення якого продукується поєднанням даних опитування та статистики.

Підсумовуюча таблиця складатиметься з наступних даних

- вартість активів (очікуваний одиничний збиток);
- ймовірність реалізації;
- фактор впливу (розраховується з даних анкет як формалізована оцінка компетентності респондентів);
- річний збиток;
- ранжування по пріоритетності ризику.

Проаналізувавши основні методи оцінки ризиків інформаційної безпеки обрано в якості прийнятних для оцінки ризиків, пов'язаних з антропогенними загрозами, синтез двох методів: експертної оцінки методом Дельфі та кількісної оцінки «Очікуваний річний збиток».

Використання методу Дельфі дає можливість проведення анонімного опитування з урахуванням кваліфікації експертів, що являється вагомим показником, тому що експертами, зазвичай, виступатимуть працівники підприємства, кваліфікація яких є різною.

Метод «Очікуваний річний збиток» є досить простим у впровадженні, точним та наглядним.

Для окремих груп респондентів необхідно створюватиі окремі опитувальники, відповідно до їх посад.

Процес проведення оцінки ризиків інформаційної безпеки пов'язаних з антропогенними загрозами має проводитись згідно концепії документу «Політика безпеки інформації». Результати оцінки ризиків допоможуть направити і визначити відповідні дії і пріоритети в галузі управління ризиками для захисту інформації, а також в області реалізації засобів управління, обраних для захисту від цих ризиків.

Результати проведеної оцінки ризиків мають корелювати існуючу політику безпеки, а саме в розділах:

- організація захисту інформації (від внутрішніх та зовнішніх загроз);

- захист людських ресурсів (перед прийомом на роботу, під час роботи та після звільнення);
- управління доступом;
- менеджмент інцидентів (обов'язкове ведення статистики інцидентів).

Захист інформації підприємства багато в чому зводиться до реалізації оптимальних методів роботи на основі ефективної корпоративної політики безпеки.

Превентивними заходами від витоку інформації шляхом реалізації антропогенних загроз розділено на правові, організаційні, технічні та психологічні. Набір заходів мають обов'язково бути зазначені в документі «Корпоративна політика безпеки інформації».

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У рамках роботи було обрано та виконано оцінку ризиків інформаційної безпеки, пов'язаних з антропогенними загрозами. При цьому створено анкети-опитувальники співробітників підприємства та розроблено комплекс правових, організаційних, технічних та психологічних методів та рекомендацій для зменшення ризику реалізації атак з застосуванням соціальної інженерії.

Метою економічного розділу є порівняння величини витрат на організацію служби захисту інформації з величиною можливої шкоди, яку може понести підприємство внаслідок втрати інформаційних ресурсів.

3.1 Розрахунок капітальних витрат

До капітальних витрат відносяться:

- витрати на створення опитувальників та комплексу методів;
- витрати на впровадження методики.

3.1.1 Розрахунок трудомісткості створення методики

Трудомісткість створення алгоритму визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації.

Формула для розрахунку трудомісткості має наступний вигляд:

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин}, \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку методики;

$t_{в}$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання методики;

$t_{д}$ – тривалість підготовки технічної документації.

Складові трудомісткості визначаються на підставі умовної кількості операторів Q, яка розраховується за формулою:

$$Q = q \cdot c\,(1 + p), \quad \text{штук}, \qquad (3.2)$$

де q – очікувана кількість операторів;

c – коефіцієнт складності алгоритму;

p – коефіцієнт корекції алгоритму в процесі його опрацювання.

Коефіцієнт складності алгоритму c визначає відносну складність алгоритму щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25…2,0.

Для даної роботи умовна кількість операторів була розрахована за наступним даним: q = 40, c = 1,5, p = 0,07.

Q = 40 · 1,5 (1 + 0,07) = 64 операторів.

Оцінка тривалості складання технічного завдання на розробку алгоритму $t_{тз}$ становить 16 годин.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікацію виконавця оцінюється за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \quad \text{годин}, \qquad (3.3)$$

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію виконавця і визначається стажем роботи за фахом.

Для даної розробки: B = 1,4; k = 1,0. Виходячи з цього тривалість вивчення технічного завдання дорівнює:

$$t_в = \frac{64{,}2 \cdot 1{,}4}{77 \cdot 1{,}0} = 1{,}17 \text{ годин.}$$

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25)\cdot k}, \text{ годин,} \quad (3.4)$$

$$ta = \frac{64,2}{25\cdot 1,0} = 2,57 \text{ годин.}$$

Тривалість складання програми за готовою блок-схемою:

$$tnp = \frac{Q}{(20...25)\cdot k}, \text{ годин,} \quad (3.5)$$

$$tnp = \frac{64,2}{25\cdot 1,0} = 2,57 \text{ годин.}$$

Тривалість опрацювання методики:

$$tonp = \frac{1,5Q}{(4...5)\cdot k}, \text{ годин,} \quad (3.6)$$

$$tonp = \frac{1,5*64,2}{4,5\cdot 1,0} = 21,4, \text{ годин.}$$

Тривалість підготовки технічної документації:

$$t_д = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)}\cdot 0,75 \quad (3.7)$$

$$t_д = \frac{64,2}{18\cdot 1,0} + \frac{64,2}{18}\cdot 0,75 = 6,24.$$

Виходячи з отриманих даних трудомісткість створення алгоритму методики дорівнює:

t = 16 + 1,17 + 2,57 + 2,57 + 21,4 + 6,24 = 49,95 годин.

3.1.2 Розрахунок витрат на створення та впровадження методики

Витрати на створення методики Кпз складаються з витрат на заробітну плату виконавця розробки Ззп і вартості витрат машинного часу, що необхідний для опрацювання алгоритму на ПК Змч:

$$К_{пз} = З_{зп} + З_{мч}. \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{пр}, \text{ грн}, \quad (3.9)$$

де t – загальна тривалість створення методики, годин; t=49,95 годин

Зпр – средньогодинна заробітна плата виконавця з нарахуваннями, грн/годину. Зпр = 40,46 грн.

$$З_{зп}=49,95 \cdot 40,46 = 2020,98 \text{ грн.}$$

Вартість машинного часу для налагодження методики на ПК визначається за формулою:

$$З_{мч}= t_{опр} \cdot С_{мч}+ t_d, \text{ грн}, \quad (3.10)$$

де $t_{опр}$ – трудомісткість налагодження алгоритму на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot Ce + \frac{Фзал \cdot Ha}{Fp} + \frac{Клпз \cdot Hапз}{Fp}, \text{ грн}, \quad (3.11)$$

де P – встановлена потужність ПК, кВт; P = 0,5 кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година; $С_е$=1,44 грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.; $К_{лпз}$ = 12000грн;

$F_р$ – річний фонд робочого часу =1920.

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Річну суму амортизації визначаємо за формулою:

$$A = \frac{C_{поч} \cdot H_a}{100}, \text{ грн,} \quad (3.12)$$

H_a – річна норма амортизації на ПК, частки одиниці. Мінімально допустимий строк корисного використання ПК складає 2 роки, тобто річна норма амортизації не має перевищувати:

$$H_a = 1/T_a * 100\%, \quad (3.13)$$

$$H_a = 1/2 * 100\% = 50\%.$$

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці. Строк дії права користування ліцензійним програмним забезпеченням не може складати менш ніж 2 роки, тобто $H_{апз}$ не має перевищувати:

$$H_{апз} = 1/T_a * 100\%, \quad (3.14)$$

$$H_{апз} = 1/2 * 100\% = 50\%.$$

Початкова вартість ПК складає у середньому 30000 грн.

$$A = \frac{30000 \cdot 50}{100} = 15000 \text{грн.}$$

В даному випадку ПК експлуатувався 1 рік, тобто $Ф_{зал}$ буде складати:

$$Ф_{зал} = С_{поч} - А, \text{ грн,} \quad (3.15)$$

$$Ф_{зал} = 30000 - 15000 = 15000 \text{ грн.}$$

Отже, вартість 1 години машинного часу ПК, становить:

$$С_{мч} = 0,5 \cdot 1,44 + \frac{15000 \cdot 0,5}{1920} + \frac{12000 * 0,5}{1920} = 7,76 \text{ грн,}$$

$$З_{мч} = 21,4 * 7,77 + 6,24 * 7,76 = 214,49 \text{ грн.}$$

Відповідно до отриманих даних, вартість створення алгоритму дорівнює:

$$К_{пз} = 2020,98 + 214,49 = 2235,47 \text{ грн.}$$

Визначена таким чином вартість створення алгоритму Кпз є частиною одноразових капітальних витрат разом з витратами на навчання персоналу.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{навч}, \quad (3.16)$$

$К_{пз}$ – вартість створення основного методики, тис. грн;

$К_{навч}$ – витрати на навчання персоналу, тис. грн; $К_{навч}$= 7000 грн.

Відповідно до заданих даних розраховуємо капітальні витрати:

$$К = 2235,47 + 7000 = 9235,47 \text{ грн.}$$

3.2 Розрахунок вартості інформації

Вартість інформації розрахую за допомогою затратного підходу, при якому інформація оцінюється по собівартості. При затратному підході (за вирахуванням витрат на оренду приміщення, витрат та оплату податків) собівартість інформаційного ресурсу визначається за формулою:

$$S = t \times N \times ЗПм + ЦТЗ \times Ен, \text{ грн.} \quad (3.17)$$

де ЗПм - місячна заробітна плата працівника який розробляє інформацію, грн;

ЦТЗ - вартість технічних засобів (вартість комп'ютерів, програмного забезпечення, засобів друку та копіювання), грн;

t - час на розробку інформації, місяців;

N - кількість працівників, які розробляють інформацію, люд.

Ен - нормативний коефіцієнт ефективності капітальних вкладів в інформаційні технології.

На основі обраної методики розрахую вартість однієї з охоронних систем. Вхідними даними будуть:

ЗПм – заробітна платня спеціаліста з нарахуваннями;

ЗПм = 14600 грн;

ЦТЗ становить близько 54000 грн.;

t - час на розробку системи, t = 2 місяці;

N = 3 людини

Ен = 0,3

$$S = 2 \times 3 \times 14640 + 54000 \times 0,3 = 104040$$

Отже, вартість інформації становить 104040 грн.

3.3 Висновок

У ході виконання роботи було визначено вартість витрат на створення та впровадження методики, яка склала 9235,47 грн., при цьому вартість частини інформації, що знаходиться у володінні підприємства складає 104040 грн.

Таким чином, створення та впровадження анкет-опитувальників співробітників підприємства та методики для зменшення ризику реалізації атак з застосуванням соціальної інженерії є доцільними для підприємств, можливий річний збиток яких складає суму, котра перевищує 113275,47 грн. (суму фіксованих витрат та вартості розробленої інформації).

ВИСНОВКИ

Під час виконання роботи проаналізовано процес створення політики безпеки інформації, виділено та проаналізовано детальніше процес оцінки ризиків, як першочерговий при створенні політики безпеки.

Також проаналізовано загрози інформаційної безпеки, антропогенні зокрема, методи оцінки ризиків інформаційної безпеки та статистичні дані інцидентів в сфері інформаційної безпеки, котрі підтвердили важливість оцінки антропогенних загроз.

В результаті було запропоновано при оцінці ризиків інформаційної безпеки поєднувати два методи оцінки ризиків задля оцінки антропогенних загроз: метод експертних оцінок Дельфі та модель оцінки ризиків «Очікуваний річний збиток». Розроблено типові анкети для опитування співробітників та типову модель загроз.

Підсумком проведеної роботи є визначення елементів ПБ, які пов’язані з протидією антропогенним загрозам та правові, організаційні, технічні та психологічні рекомендації, які мають бути обов’язково зазначеними в документі «Корпоративна політика безпеки інформації».

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

2 НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

3 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

4 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

5 Методология управления IT-рисками (Електрон. ресурс) / Спосіб доступу:http://www.iso27000.org/ - Загол. з екрану.

6 Риск и анализ рисков (Електрон. ресурс) / Спосіб доступу: http://dorlov.blogspot.com/2011/10/fair-2.html - Загол. з екрану.

7 Міжнародний стандарт ISO/IEC 27003. Системи менеджменту інформаційної безпеки.

8 Міжнародний стандарт ISO/IEC 27002. Звід правил для управління інформаційною безпекою

9 Чунарьова А.В. Концепція безпеки інформаційних ресурсів на базі системи оцінки ризиків (Електрон. ресурс) / Спосіб доступу: URL: http://www.info-library.com.ua/books-text-2038.html - Загол. з екрану.

10 НДТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

11 Сайт команди реагування на комп'ютерні надзвичайні події в Україні (Електрон. ресурс) / Спосіб доступу: http://cert.gov.ua - Загол. з екрану.

12 Сайт компанії Searchinform (Електрон. ресурс) / Спосіб доступу: http://searchinform.com/ - Загол. з екрану.

13 Сайт компанії IDC (Електрон. ресурс) / Спосіб доступу: http://www.idc.com/ - Загол. з екрану.

14 Сайт компанії Incidents (Електрон. ресурс) / Спосіб доступу: Incidents.su - Загол. з екрану.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	43	
6	А4	2 Розділ	41	
7	А4	3 Розділ	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	3	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Питання до анкет

1 Чи є КЗ на підприємстві?

2 Як Ви оцінюєте привабливість для хакерів і потенційних злочинців Вашого підприємстві?

3 Охарактеризуйте сумлінність партнерів Вашого підприємства?

4 Як часто відвідують Ваше підприємство представники наглядових організацій та аварійних служб?

5 Який рівень конкуренції в сфері діяльності Вашого підприємства?

6 Як Ви оцінюєте можливість виявлення пошкодження огороджувальних конструкцій?

7 Як би Ви оцінили можливість виявлення порушення режиму охорони об'єкта?

8 Дайте оцінку частоти порушення режиму охорони об'єкта?

9 Як Ви оцінюєте якість технічних засобів На Вашому підприємстві?

10 Чи присутнє у компанії старіння носіїв інформації?

11 Рівень збитку при реалізації загрози?

12 Як Ви оцінюєте якість програмних засобів На Вашому підприємстві?

13 Чи можлива модифікація інформації при передачі по каналах зв'язку і телекомунікації?

14 Рівень збитку при реалізації загрози?

15 Як Ви оцінюєте якість програмних засобів На Вашому підприємстві?

16 Як часто трапляється знищення електронної інформації зовнішніми порушниками?

17 Рівень збитку від таких дій?

18 Як часто трапляється знищення носіїв інформації працівниками?

19 Рівень збитку від таких дій?

20 Як часто трапляється знищення носіїв інформації зовнішніми порушниками?

21 Рівень збитку від таких дій?

22 Як часто трапляється знищення або пошкодження програмного забезпечення працівниками?

23 Рівень збитку від таких дій?

24 Як часто трапляється знищення або пошкодження програмного забезпечення зовнішніми порушниками?

25 Рівень збитку від таких дій?

26 Як часто трапляються збої обробки інформації в наслідок дій працівників?

27 Рівень збитку від таких дій?

28 Як часто трапляються збої обробки інформації в наслідок дій зовнішніх порушників?

29 Рівень збитку від таких дій?

30 Як часто трапляються крадіжки носіїв інформації в наслідок дій працівників?

31 Рівень збитку від таких дій?

32 Як часто трапляються крадіжки носіїв інформації в наслідок дій зовнішніх порушників?

33 Рівень збитку від таких дій?

34 Як часто трапляються крадіжки інформації (читання та несанкціоноване копіювання) внаслідок дій працівників?

35 Рівень збитку від таких дій?

36 Як часто трапляються крадіжки інформації (читання та несанкціоноване копіювання) в наслідок дій зовнішніх порушників?

37 Рівень збитку від таких дій?

38 Як часто трапляються крадіжки і засобів доступу (ключі та паролі) в наслідок дій працівників?

39 Рівень збитку від таких дій?

40 Як часто трапляються крадіжки засобів доступу (ключі та паролі) в наслідок дій зовнішніх порушників?

41 Рівень збитку від таких дій?

42 Як часто трапляються порушення встановленого режиму доступу в наслідок дій працівників?

51 Рівень збитку від таких дій?

52 Як часто трапляються порушення встановленого режиму доступу в наслідок дій зовнішніх порушників?

53 Рівень збитку від таких дій?

54 Як часто трапляються порушення нормальної роботи та пропускної здатності каналів зв'язку в наслідок дій працівників?

55 Рівень збитку від таких дій?

56 Як часто трапляються порушення нормальної роботи та пропускної здатності каналів зв'язку в наслідок дій зовнішніх порушників?

57 Рівень збитку від таких дій?

58 Як часто трапляються помилки при використанні програмного забезпечення в наслідок дій працівників?

59 Рівень збитку від таких дій?

60 Як часто трапляються помилки при використанні програмного забезпечення в наслідок дій зовнішніх порушників?

61 Рівень збитку від таких дій?

62 Як часто трапляються факти використання шкідливого програмного забезпечення в наслідок дій працівників?

63 Рівень збитку від таких дій?

64 Як часто трапляються факти використання шкідливого програмного забезпечення в наслідок дій зовнішніх порушників?

65 Рівень збитку від таких дій?

66 Яка на Вашу думку можливість виявлення порушення режиму використання інформації?

67 Дайте оцінку можливості нейтралізації порушення режиму використання інформації?

68 Визначте частоту виникнення порушень режиму використання інформації?

69 Яку частоту має витік інформації, що підлягає захисту, завдяки несанкціонованому зніманні інформації?

70 Рівень збитку?

71 Яку частоту має витік інформації, що підлягає захисту, завдяки оптичним каналам?

72 Рівень збитку?

73 Дайте оцінку можливості виявити форс-мажорних обставин?

74 Охарактеризуйте можливість нейтралізації форс-мажорних обставин?

75 Визначте частоту форс-мажорних обставин?

76 Як Ви оцінюєте потенційну небезпеку від форс-мажорних обставин?

ДОДАТОК В. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Розробка політики безпеки інформації для зменшення впливу антропогенних загроз на основі оцінки їх ризиків
Пінчука Костянтина Олександровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 110 сторінках та містить 13 рисунків, 5 таблиць, 14 джерел та 5 додатка.

У першому розділі проаналізовано процес створення політики безпеки на основі нормативно-правового забезпечення України та міжнародних стандартів та визначено, що аналіз та оцінка ризиків – процеси, що є основою для створення політики безпеки.

У спеціальній частині проаналізовано статистику інцидентів України та світу в сфері інформаційної безпеки, обґрунтовано вибір метода оцінки ризиків антропогенних загроз та розроблено рекомендації щодо заходів, направлених на зменшення впливу антропогенних загроз.

У економічному розділі розраховано вартість створення опитувальників та впровадження рекомендацій щодо зменшення ймовірності виникнення антропогенних загроз та зроблено висновок щодо доцільності впровадження їх компаніями.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник