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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Пугача Дмитра Вікторовича*

академічної групи *125м-22-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування методів протидії внутрішнім загрозам безпеці інформації підприємства*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Пугачу Дмитру Вікторовичу*** **академічної групи** ***125м-22-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Обґрунтування методів протидії внутрішнім загрозам безпеці інформації підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Стан питания. Постановка задачі	02.11.2023
Розділ 2	Спеціальна частина	16.11.2023
Розділ 3	Економічна частина	30.11.2023

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Пугач Д.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 104 сторінки, 4 рисунки, 9 таблиць, 4 додатки, 12 посилань.

Мета кваліфікаційної роботи – підвищення рівня інформаційної безпеки (ІБ) комерційного підприємства за рахунок застосування методів протидії внутрішнім антропогенним загрозам.

Предмет дослідження – внутрішні загрози інформаційній безпеці комерційного підприємства.

Об’єкт дослідження – методи протидії внутрішнім загрозам безпеці інформації підприємства.

У роботі проаналізовані внутрішні загрози інформаційній безпеці підприємства та розроблені методи протидії їм.

В спеціальній частині був проведений аналіз методів протидії внутрішнім антропогенним загрозам ІБ підприємства та розроблений комплекс таких методів, що дозволять підвищити рівень ІБ.

В економічному розділі виконаний розрахунок витрат на створення комплексу методів протидії та обґрунтовано доцільність його застосування.

Наукова новизна полягає у розробці комплексу методів протидії внутрішнім антропогенним загрозам ІБ на комерційному підприємстві.

ВНУТРІШНІ ЗАГРОЗІ, ІНФОРМАЦІЙНА БЕЗПЕКА, РИЗИК, МЕТОДИ ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ, АНТРОПОГЕННІ ЗАГРОЗИ, ПОРУШНИК, ІНФОРМАЦІЙНИЙ РЕСУРС.

ABSTRACT

The explanatory note of qualification work consists of: 104 pages, 4 figures, 9 tables, 4 appendices, 12 references.

The purpose of the qualification work is to increase the level of information security (IS) of a commercial enterprise by using the methods of countering internal anthropogenic threats.

The subject of the research is internal threats to information security of a commercial enterprise.

The object of the study is the methods of countering internal threats to information security of an enterprise.

The work analyzes the internal threats of information security of an enterprise, and develops the methods of its countering.

The special part contains the analysis of methods of countering internal anthropogenic threats to information security of an enterprise and developed complex of such methods that allow to increase the level of information security.

In the economic section the calculation of costs for creating the complex of methods of countering is performed and the expediency of its application is justified.

The scientific novelty consists in developing the complex of methods of countering internal anthropogenic threats to information security of a commercial enterprise.

INTERNAL THREATS, INFORMATION SECURITY, RISK, METHODS TO COUNTER INTERNAL THREATS, ANTHROPOGENIC THREATS, THE OFFENDER, INFORMATION RESOURCE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека;

АС – автоматизована система;

ЕОМ – електронно-обчислювальна машина;

ІС – інформаційна система;

СЗІ - служба захисту інформації;

НСД – несанкціонований доступ;

ПК – персональний комп’ютер.

ЗМІСТ

ВСТУП 7
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 9
1.1 Стан питання 9
1.2 Класифікація порушників та побудова моделі порушників 28
1.3 Модель загроз 39
1.4 Постановка задачі 46
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 48
2.1 Аналіз поширених методів захисту від антропогенних загроз 48
2.2 Комплекс методів для зниження ризиків антропогенних загроз 58
2.3 Висновок 86
РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА 87
3.1 Вступ 87
3.2 Розрахунок капітальних витрат 87
3.3 Розрахунок поточних (експлуатаційних) витрат 90
3.4 Оцінка можливого збитку від порушення інформаційної безпеки 92
3.5 Визначення збитку від поломок обладнання 92
3.6 Загальний ефект від впровадження моделі 94
3.7 Визначення та аналіз показників економічної ефективності моделі 95
3.8 Висновок 96
ВИСНОВКИ 97
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 98
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи 100
ДОДАТОК Б. Перелік документів на оптичному носії 101
ДОДАТОК В. Відгук керівника економічного розділу 102
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи 103

ВСТУП

Від 70 до 80% втрат від злочинів у сфері IT доводиться на загрози зсередини. При цьому топ-менеджери компаній дуже часто недооцінюють збиток, що може бути нанесений бізнесу їхніми власними співробітниками.

Для того, щоб побудувати ефективну систему інформаційної безпеки, необхідні три речі: чітке розуміння того, що має потребу в захисті, поінформованість про відповідні загрози й здатність їх запобігти.

Якщо раніше зловмисники атакували більшою мірою малі й середні погано захищені компанії, то тепер у полі їхньої уваги великі організації, що володіють величезними інформаційними базами. Дрібних грабіжників змінили професіонали, чия мета - інформація. Вони використовують уразливості іншого роду - не проломи в технологіях, а слабкі місця в бізнес-процесах.

Дотепер системи IT-безпеки були схожі на глухі кріпосні стіни з пильно охоронюваними входами. Але в нинішніх умовах такий захист недостатній - ворог перемінив тактику. Для того, щоб залишатися захищеною, компанія повинна бути прозорою - так, щоб жоден процес не залишався за рамками моніторингу й контролю.

Корпоративні скандали й масові витоки інформації приводять до впровадження нових законодавчих норм і правил, і керівництво компаній змушене стежити за відповідністю численним національним і міжнародним правовим актам. Тенденція простежується дуже чітко - якщо компанія не вживає необхідних дій для забезпечення безпеки інформації своїх замовників, то результатом може стати втрата довіри, підрив репутації, зниження вартості акцій, штрафи, і, можливо, кримінальна відповідальність для відповідальних керівних осіб.

Організації, що виконують всі дії для того, щоб відповідати нормам, мають вагому перевагу перед інвесторами. Інформаційна безпека вийшла за рамки процесу керування ризиками, тепер вона має статус фундаментального елементу ведення бізнесу.

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

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Для українського суспільства питання забезпечення інформаційної безпеки постає особливо гостро, що пояснюється наявністю низки проблем, необхідності створення сприятливих умов для подальшого розвитку підприємництва; існування економічної кризи; порушення прав і свобод громадян; зростання рівня злочинності. Необхідною передумовою належного захисту інтересів громадян і підприємств таким різним загрозам є створення та ефективне функціонування підсистем підприємницьких структур, які в комплексі забезпечують економічну цілісність та захист підприємства, протидіють внутрішнім і зовнішнім загрозам.

Під інформаційною безпекою слід розуміти такий стан системи підприємства, котрий дає змогу уникнути зовнішніх загроз і протистояти внутрішнім чинникам дезорганізації за допомогою наявних ресурсів.

Чинники інформаційної безпеки підприємства різноманітні і в кожній галузі виробництва мають свою специфіку. Однак найважливішим є надійний захист комерційної таємниці. Сьогодні ми живемо і працюємо у світі, де поширилась кіберзлочинність. Вона розвинулась через низку чинників. Зокрема, сектор торгівлі та надання послуг здійснюється через електронні засоби телекомунікації. Значну небезпеку для фірм, різних установ являє собою наш помічник, тобто Інтернет. Інфікація комп'ютерів вірусами здатна призвести до: викрадення конфіденційної інформації; руйнування цінної інформації; виведення з ладу комп'ютерних систем.

Для забезпечення інформаційної безпеки підприємства у складі системи безпеки повинні організовувати підрозділи конкурентної розвідки, контррозвідки та інформаційно-аналітичної служби. Кожна з цих служб виконує певні функції, які в сукупності характеризують процес створення та забезпечення інформаційної безпеки. Це різноманітні збори всіх видів інформації, що стосується діяльності того чи іншого суб'єкта господарювання, аналіз

одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів (систематизації, безперервності надходження, всебічного характеру аналітичних процесів) і методів (локальних із специфічних проблем) організації робіт, прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на підприємстві, в країні та у світі для конкретної сфери бізнесу, а також показників, яких необхідно досягти суб'єкту господарювання. Саме в цьому полягає оперативна реалізація заходів з розроблення та охорони інформаційної. Також недостатні професійні знання працівників правоохоронних органів у сфері боротьби з інформаційними злочинами.

На практиці, люди, які працюють у підрозділах інформаційної безпеки схиляються до використання засобів охоронного типу. Варто зазначити, що результати сприяють кращому одержанню не тільки кількісної інформації, але й якісних значень показників безпеки, що відіграє важливу роль у розвитку фірми чи будь-якої установи, а саме безпеки. Досліджуючи інформаційну безпеку підприємства, пропонується застосовувати системний підхід, який дозволяє будь якому підприємству мати перспективну систему захисту. Згідно цієї системи, взаємодія із зовнішнім середовищем має інформаційний і речовий характер. Існує багато типів інформаційної взаємодії. Найпоширенішою являється взаємодія між системою і зовнішнім середовищем, коли відбувається обмін керуючою інформацією, необхідною для існування і функціонування даної фірми. Можна стверджувати, що всі інші види обміну інформацією – це випадки дестабілізуючих чинників, які загрожують безпеці функціонування підприємства, поступаючи із зовнішнього середовища.

Життєздатність підприємства чи організацій в значній мірі залежить від наявного рівня їх інформаційної безпеки. Тому перед всіма суб'єктами господарювання в нашій державі виникає необхідність внутрішньої самооцінки та прогнозування можливих змін в стані їх інформаційної безпеки. В свою чергу інформаційна безпека суспільства, держави характеризується

ступенем захищеності вітчизняних підприємств, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи.

1.1.1 Класифікація основних загроз інформації й інформаційним ресурсам комерційного підприємства

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.

У найзагальнішому випадку загрози проявляються такими шляхами:

– внаслідок дій зловмисників;

– спостереження за джерелами інформації;

– підслухування конфіденційних розмов людей і сигналів акустичних працюючих механізмів;

– перехоплення електричних, магнітних і електромагнітних полів, сигналів електричних і випромінювання радіоактивного;

– несанкціонованого розповсюдження матеріально-речовинних носіїв за межі контрольованої зони;

– розголошення інформації людьми, що володіють секретною або конфіденційною інформацією;

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

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

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

– збоїв в роботі апаратури збирання, оброблення, зберігання і передавання інформації, викликаних її несправністю, а також ненавмисних помилок користувачів або обслуговуючого персоналу;

– впливу потужних електромагнітних і електричних промислових і природних завад.

Загрози інформаційним ресурсам можна в загальному випадку класифікувати:

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.

При цьому:

Розкрадання і знищення інформації розуміються аналогічно по застосуванню до матеріальних цінних ресурсів.

Копіювання інформації - повторення і стала фіксація інформації на матеріальному носії.

Пошкодження - зміна властивостей носія інформації, при якому істотно погіршується його стан, втрачається значна частина його корисних властивостей і він ставати повністю або частково непридатним для цільового використання.

Модифікація інформації - внесення будь-яких змін, крім пов'язаних з адаптацією програми для ЕОМ або баз даних для комп'ютерної інформації.

Блокування інформації - несанкціоноване ускладнення доступу користувачів до інформації, не пов'язане з її знищенням;

Несанкціоноване знищення, блокування, модифікація, копіювання інформації - будь-які, не дозволені законодавством, власником або компетентним користувачем зазначені дії з інформацією.

Обман (заперечення автентичності, нав'язування неправдивої інформації) - навмисне викривлення або приховування істини з метою ввести в оману особа, у веденні якого знаходиться майно, і таким чином домогтися від неї добровільної передачі майна, а також повідомлень з цією метою завідомо неправдивих відомостей.

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 тощо);

– 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 тощо);

– 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 тощо, які виникають на етапі проєктування 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 тощо, 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 тощо, 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).

Два останніх способи 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:

– АС 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: 1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; 2) можуть призвести 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.

При складанні моделі загроз використовуються в даний час варіанти моделей, розроблені фахівцями в області захисту інформації державних і недержавних наукових установ. 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.

Наведена класифікація (рис. 1.1) показує складність визначення можливих загроз і способів їх реалізації.

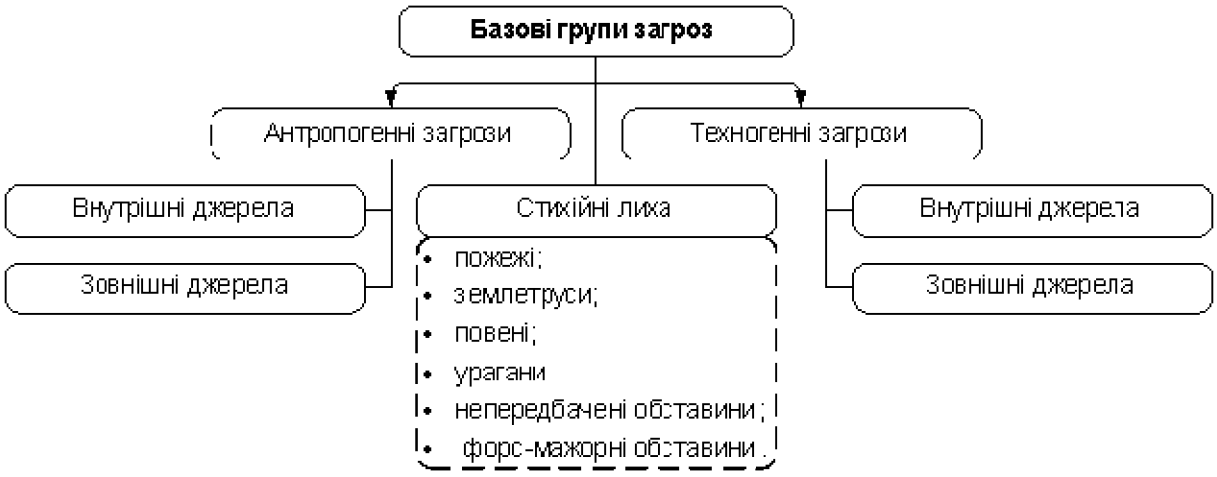

Рисунок 1.1- Класифікація базових загроз інформації

Через їх чисельність відповідно до загальної класифікації загроз національній безпеці, виокремимо загрози інформаційній безпеці, обумовлені діями суб’єкта.

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. 1.2).

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.

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.

Рисунок 1.2- Класифікація антропогенних джерел загроз інформації по відношенню до об’єкта захисту

Внутрішні джерела, як правило, являють собою висококваліфікованих фахівців в галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою вирішуваних завдань, структури та основними функціями та принципами роботи програмно-апаратних засобів

захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

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

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

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

1.1.2 Аналіз внутрішніх загроз та їх джерел

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.

Виходячи із даних антирейдерського союзу підприємців України:

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

2) 17% загроз реалізується ззовні підприємства;

3) 1% загроз реалізується випадково.

Загроза – це потенційні або реальні дії, що призводять до моральної чи матеріальної шкоди.

Найпоширеніші фактори розголошення співробітниками інформації з обмеженим доступом наведені у таблиці 1.1:

Таблиця 1.1 – Фактори розголошення співробітниками інформації

Фактори	%
Надмірна балакучість співробітників підприємств, фірм, банків	32
Прагнення працівників заробляти гроші будь-яким способом і будь-якою ціною	24
Відсутність на підприємстві системи заходів, спрямованих на захист інформації	14
Звичка співробітників ділитись один з одним почутими новинами, чутками, інформацією	12
Безконтрольне використання інформаційних систем	10
Наявність передумов для виникнення серед співробітників конфліктних ситуацій	8

Як видно з таблиці 1.1, 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.

Розглянемо внутрішні загрози більш детально:

а)Необережність персоналу.

Дуже часто співробітники, хоч й не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього. Тож необережність можна поділити на дві категорії: дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації; дії чи бездіяльність співробітників у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки. У першому випадку не можна казати про вину співробітника, скоріше це прорахунки вищого керівництва, яке не потурбувалося роз'яснити персоналу про важливість інформації і про її захист. Якщо мова йде про державну таємницю, то такі ситуації не можуть виникнути, бо є чітко визначений законодавством порядок допуску до державної таємниці. Одним з пунктів є підписання зобов'язання про нерозголошення довірених даних. Багато комерційних фірм використовують законодавство про державну таємницю як приклад для аналогічного захисту своєї, комерційної таємниці. Але цього прикладу додержуються не всі компанії. Інколи керівники, як метод захисту інформації, практикують не казати працівникам про важливість даних. Як приклад можна привести ситуацію: прибиральниця, яка прийшла прибрати кабінет керівника фірми, побачила в нього на столі дуже красиву модель якогось пристрою. Вина керівника полягає вже в тому, що він дозволив прибирати в кабінеті тоді, коли працює там сам, коли документи не сховані в сейфі та працює комп'ютер, де також можуть бути відкриті секретні файли. Але він також не попередив прибиральницю про те, що не потрібно розповідати про будь що, що вона бачила. Прибиральниця, якій сподобалася модель з чисто мистецьких поглядів, може поділитися своїми враженнями з людиною, яка зацікавиться цією інформацією. Тож керівникам потрібно попереджати всіх співробітників, які хоч якось взаємодіють з конфіденційною інформацією і можуть ознайомитися з нею в розмірі, достатньому для відтворення хоча б частини такої інформації. В іншому випадку співробітника повідомили про те, що він

не повинен розголошувати конфіденційні відомості підприємства, але він вважаючи, що його дії не призведуть ні до яких наслідків, призводить до втрати інформації чи ознайомлення з нею третіх осіб. У кримінальному кодексі необережність поділяють саме на злочинну самовпевненість та злочинну недбалість. Під злочинною самовпевненістю розуміють дії чи бездіяльність особи, коли вона знала про можливі негативні наслідки, передбачала їх настання, але зухвало розраховувала на їх відвернення. Злочинною недбалістю є дії чи бездіяльність особи, коли вона не знала, але повинна була знати про можливі негативні наслідки свого діяння. В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії.

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

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

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

- помста;
- матеріальна або інша вигода;
- самореалізація.

Саме з цих причин персонал фірми найчастіше зраджує її інтереси. Багато в чому тут також є прорахунки керівництва. Саме це найчастіше є тим, через що вербують співробітників. Невдоволені працівники краще йдуть на

контакт з промисловими шпигунами, бо не відчувають патріотизму до цієї фірми, мріють поквитатися з кимось із колег чи з керівництвом, або прагнуть покращити своє матеріальне становище. Таким особам пропонують те, чого в них немає і не буде на даній фірмі: або значні матеріальні виплати, або ж пропонування роботи, де їх працю оцінять, де їх будуть поважати, або ж інші речі, що відповідають потребам цих співробітників.

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

Щоб краще побачити серйозність загроз, пов'язаних з персоналом, далі наведені декілька прикладів втрати інформації з обмеженим доступом через внутрішніх порушників.

Три інсайдера з Lockheed Martin вкрали результати проєкту з розробки тренувальної системи для пілотів ВВС США і план дій компаній в боротьбі за контракт Пентагону вартістю $1 млрд. Всі ці відомості були передані конкурентові — підрозділу Link Simulation and Training компанії L-3 Communications. Вся інтелектуальна власність витекла з Lockheed Martin через банальні USB-флешки і CD/DVD-приводи. Інсайдер — керівник відділення Private Banking в Citibank — перейшов на роботу в банк-конкурент UBS, прихопивши конфіденційні дані всіх найбільш спроможних клієнтів. Через деякий час UBS почав переманювати клієнтів Citibank. Проте найцікавіше в тому, що витік відбувся найбанальнішим способом — по електронній пошті.

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. Проаналізувавши загрози конфіденційності даних, які пов'язані з персоналом, можна побачити, що ігнорування цих загроз призводить до серйозних збитків на підприємствах. Мова йде не тільки про

фінансові втрати компанії, але й про різке падіння її іміджу у зв'язку з тим, що вона не може захистити власну конфіденційну інформацію.

1.2 Класифікація порушників та побудова моделі порушників

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, знання, час та місце можливої дії тощо.

Під час розробки моделі порушника ми повинні визначити:

- Припущення щодо осіб, до яких може належати порушник;
- Припущення щодо мотивів дій порушника (цілей які він переслідує);
- Припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушення);
- Обмеження та припущення щодо характеру можливих дій порушника (за часом та за місцем дії, тощо).

Усіх порушників можна класифікувати за рівнем безпеки:

- Знає усі функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;
- має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;
- має високий рівень знань у галузі програмування й обчислювальної техніки, проєктування й експлуатації автоматизованих інформаційних систем;
- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

- застосовує суто агентурні методи отримання відомостей;
- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонент системи);
- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;
- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів
- передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм)

За часом дії:

- у процесі функціонування (під час роботи компонент системи);
- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т. д.);
- як у процесі функціонування, так і в період неактивності компонент системи.

За місцем дії:

- без доступу на контрольовану територію організації;
- з контрольованої території без доступу до будівель та споруд;
- усередині приміщень, але без доступу до технічних засобів;
- з робочих місць кінцевих користувачів (операторів);
- з доступом у зону даних (баз даних, архівів і т. п.);
- з доступом у зону управління засобами забезпечення безпеки.

Враховуються також наступні обмеження і припущення про характер дій можливих порушників:

- робота з підбору кадрів і спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій з подолання системи захисту двох і більше порушників;

- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, системних адміністраторів, а також хиб прийнятої технології обробки інформації і т. д.

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути схарактеризований згідно з класифікаціями, наведеними вище. Всі значені характеристики мають бути оцінені .

Однак при формуванні моделі порушника на її виході обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення і відомості про порушення.

Однак дослідження німецької компанії Result Group говорять про те, що все-таки найбільш часто порушниками стають саме чоловіки. Найбільш типовий інсайдер - це чоловік у віці від 30 до 50 років з вищою освітою, добре розбирається в інформаційних технологіях. Втім, оскільки сьогодні більшість офісних працівників так чи інакше працює з комп'ютером, практично кожному з них при сприятливих обставинах вистачить рівня технічної підготовки для того, щоб сприяти витоку інформації.

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

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

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

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

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

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

Фахівці компанії фокусують увагу винятково на захисті даних від витоку, спотворення і знищення, і тому їх погляди відрізняються більшою глибиною аналізу.

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

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

Скривджені порушники (по-іншому, саботажники) — це співробітники, які прагнуть завдати шкоди компанії за особистими причинами. Найчастіше причиною такої поведінки може бути образа, що виникла із-за недостатньої оцінки їх ролі в компанії, недостатній розмір матеріальної компенсації, неналежне місце в корпоративній ієрархії, відсутність елементів моральної мотивації або відмова у виділенні корпоративних статусних атрибутів (ноутбука, автомобіля, секретаря).

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

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

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

Виходячи з мотивів психологи давно виділили кілька основних типів співробітників, які готові «злити» інформацію, яка їм не належить. Найбільш поширений тип - це «Буратіно». Така людина діє в більшому ступені з цікавості ніж з корисливих спонукань, і нашкодити може скоріше через свою необережність і невміння тримати язик за зубами, ніж через бажання збагатитися або когось підставити. До цього типу може належати співробітник будь-якого рангу і будь компетенції, однак корпоративні політики інформаційної безпеки можуть успішно протидіяти таким особистостям. Як вже говорилося вище, один з найбільш серйозних стимулів для інсайдера - це бажання помститися. Тому наступний за поширеністю психологічний тип інсайдера - «невловимий месник». До цього типу найчастіше відносяться люди, які мстять фірмі поширенням інсайдерської інформації за своє звільнення. Як показали дослідження, проведені компанією Search Inform, 49,5% всіх звільнених працівників готові передати конфіденційну

інформацію, до якої мали доступ на своїй минулій роботі, новому роботодавцю. Це дійсно серйозна проблема, однак її можна вирішити, поступово обмежуючи доступ працівника, якого планується звільнити, до конфіденційних корпоративних даних. Таким чином, можна досягти того, щоб до моменту звільнення та інформація, якою він володіє, була вже неактуальною.

Тип інсайдера, який керується не стільки почуттям помсти, скільки якимись корисливими чи, в дуже рідкісних випадках, ідейними мотивами, називається «Павлик Морозов». Як правило, ця людина використовує для отримання інформації і людей, і комп'ютери, а шляхи видобутку відомостей, в основному, легальні. Інформація, яку він збирає, в багатьох випадках може з боку здатися потрібної йому для роботи - саме тому цей тип інсайдера особливо небезпечний. Фахівці з інформаційної безпеки повинні ретельно контролювати співробітників, які проявляють службове завзяття, прагнучи отримати підвищення, заробити гроші за рахунок бонусів тощо. Багато з цих людей не зможуть встояти перед спокусою легкого заробітку або високої посади в конкуруючій компанії, які стають можливими завдяки вкраденої їм інформації.

Найбільш небезпечний тип інсайдера - це «сірий кардинал». Так психологи називають високопоставлених інсайдерів, які мають доступ до дуже широкого спектру документів. Мотиви, які рухають їм, досить різноманітні, однак найбільш часто такі інсайдери використовують своє становище і доступну їм інформацію для усунення своїх конкурентів і просування по кар'єрних сходах на все більш і більш високі позиції. На жаль, нерідко в компаніях діють політики, що дозволяють керівному складу організації діяти фактично без жодного контролю з боку відділу безпеки, а тому протистояти «сірому кардиналу», навіть якщо його вдасться виявити, дуже і дуже непросто. Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

Відносно АС порушники можуть бути внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами). В таблицях 1.2-1.5 наведені специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо АС, за показником можливостей використання засобів та методів подолання системи захисту, за часом дії, за містом дії. У графі "Рівень загроз" зазначених таблиць наведені у вигляді відносного ранжування оцінки можливих збитків, які може заподіяти порушник за умови наявності відповідних характеристик. Рівень збитків характеризується наступними категоріями:

1 - незначні, 2 – значимі, але, здебільшого, припустимі, 3 – середні, 4 – дуже значні.

Таблиця 1.2 - Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
	Внутрішні по відношенню до АС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти АС	1
ПВ2	Персонал, який обслуговує технічні засоби (інженери, техніки)	2
ПВ3	Користувачі (оператори) АС	2
ПВ4	Співробітники підрозділів (підприємств) розробки та супроводження програмного забезпечення	3
ПВ5	Адміністратори ЛОМ	3
ПВ6	Співробітники служби захисту інформації	4
ПВ7	Керівники різних рівнів посадової ієрархії	4

Так як кожен індивід у демонструванні поведінки керується певними спонуканнями, розуміння таких дає можливість підібрати до нього ключі і в результаті отримати необхідні дані.

Про мотиви такого собі людини дізнаються шляхом його вивчення, причому слід враховувати і ступінь виразності (дуже сильно, досить сильно, слабо) цих спонукань.

Характерні мотиви видачі індивідом специфічною інформації та можливі шляхи їх утилізації такі:

1 Жадібність. (Обіцянка або ж надання грошей і інших матеріальних цінностей).

2 Страх за себе. (Шантажування, а часом і загроза або факт грубого фізичного чи витонченого психологічного впливу).

3 Страх за своїх близьких. (Явна загроза або факт різнотипного насильства - у дусі викрадення, побиття, згвалтування, кастрації, «садіння на голку», повного фізичного усунення).

4 Фактор болю. (Якісна катування або погроза інтенсивного болючого впливу).

5 Сексуальна емоційність. (Спритно підсовування статевого партнера і різної порнографії з перспективою "розслаблення", шантажу або обміну).

6 Байдужість. (Чітка реалізація депресії, що виникає в результаті інспірованих або спонтанних життєвих обставин, а іноді і в результаті психофізичної обробки об'єкта).

7 Внутрішній авантюризм. (Надання шансів індивіду для ведення ним своєї гри).

8 Рахунки з держсистемою або організацією. (Розумне використання ідеологічних розбіжностей та існуючої незадоволеності об'єкта своїм нинішнім становищем або завтрашньою перспективою).

9 Рахунки з конкретними особами. (Розпалювання таких негативних почуттів як помста, заздрість і неприязнь з непереборним бажанням завдати «ворогу» певний збиток).

10 Націоналізм. (Гра на глибинному відчутті певної національної спільноти; ненависті, гордості, винятковості).

11 Релігійні почуття. (Пробудження неприязні до «іновірців» або ж прив'язування певної ситуації до обраних доктрин сповідуваної релігії).

12. Громадянський обов'язок. (Гра на законослухняності).

13 Загальнолюдська мораль. (Гра на порядності).

14 Підсвідома потреба в самоповазі. (Спекуляція на ідеальних уявленнях людини про себе).

15 Корпоративна (кланова) солідарність. (Гра на конкретній елітарності).

16 Явна симпатія до одержувача або його справі. («Резонуюча підстроювання до об'єкта»).

17 Марнославство. (Провокування бажання об'єкта справити певне враження, показати свою значимість і поінформованість).

18 Легковажність. (Приведення людини в безтурботні стан необачності й балакучості. До цього ж можна віднести задіяння «хронотопу» - явно підвищеної довірливості людини в певний час і в певному місці ("випадковий попутник»).

19 Догідливість. (Чітка реалізація підсвідомої (вольовий) і усвідомленої (ділової й фізичної) залежності об'єкта від одержувача).

20 «Божевілля» на чому небудь. (Близька можливість для колекціонера придбати (або втратити) палко бажану річ; гра на фобіях ...)

21 Неприхований розрахунок отримати певну інформацію натомість. (Техніки «баш на баш» або «водіння за ніс»).

Так як мотивів є безліч, але їх можна представити яка основні чотири.

Таблиця 1.3 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самозатвердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок	4

Таблиця 1.4 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо АС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проєктування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки	3
К5	Знає недоліки та "вади" механізмів захисту, які вбудовані у системне програмне забезпечення та його недокументовані можливості	3
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення	4

Таблиця 1.5 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв'язку) упровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації систем обробки інформації.	3
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Таблиця 1.6 - Модель порушника стосовно внутрішніх загроз

Порушник	Використання засобів та методів подолання системи захисту	Рівень кваліфікації	Мотиви здійснення порушень	Рівень загрози
ПВ1	З1	К1	М1	1
ПВ2	З2	К2	М1	1
ПВ3	З3	К3	М2	2
ПВ4	З4	К4	М2	2
ПВ5	З5	К6	М4	4
ПВ6	З5	К5	М4	3
ПВ7	З5	К5	М3	3

1.3 Модель загроз

В умовах реформування української економіки значення банківського сектору в забезпеченні економічної стабілізації та безпеки країни невпинно зростає.

Необхідною умовою побудови та функціонування банківської системи є всебічне забезпечення безпеки у всіх сферах банківської діяльності, важливою складовою якої є безпека економічної інформації.

Сьогодні комерційні підприємства переживають значні зміни, обумовлені глобалізацією фінансових ринків, розвитком інформаційних технологій, розширенням асортименту банківських послуг, впровадженням інноваційних технологій в управлінні. Це, у свою чергу, ще більше загострило ситуацію із забезпеченням надійного захисту інформації.

Такого виду загроз, як наявність каналів витоку інформації. Усе це викликає необхідність перегляду підходів до забезпечення безпеки інформації підприємств та передбачає необхідність створення відповідних систем її захисту.

Проблеми безпечного розвитку держави та підприємств комерційного сектора зокрема є предметом наукових досліджень як вітчизняних, так і зарубіжних вчених та практиків.

Висока значимість проблем захисту економічної інформації від загроз, недостатній рівень її теоретичної розробки, перед усім, з точки зору комплексного підходу обумовили вибір теми.

Дослідження концептуальних положень щодо захисту інформації компаній від внутрішніх загроз та на цій основі розробка напрямів безпечного розвитку комерційних підприємств.

Інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми та внутрішніми. В даний час індустрія інформаційної безпеки розвивається, в основному, на протидії зовнішнім загрозам, пов'язаних з проривом в області високих технологій, Інтернет та електронної комерції.

Водночас, чим більших успіхів досягає людство в боротьбі з зовнішніми загрозами, тим рішучіше на перший план виходять загрози внутрішні, з якими, згідно статистики, пов'язано близько 70% всіх інцидентів безпеки.

Слід зазначити, що серед внутрішніх загроз найбільш небезпечною є загроза наявності каналів витоку інформації. Засоби захисту від несанкціонованого доступу тут є практично безкорисними, оскільки в якості основного джерела загрози виступає «інсайдер» – користувач інформаційної системи, що має цілком легальний доступ до конфіденційної інформації і який застосовує весь арсенал доступних йому засобів для того, щоб використовувати інформацію у своїх цілях .

Отож, останнім часом все більшої актуальності набуває проблема захисту економічної інформації від інсайдерів, оскільки дуже часто доступ до любих інформаційних активів мають чи не всі співробітники підприємства, в тому числі і ті, кому за родом своєї діяльності вони не потрібні.

Для того, щоб організувати ефективну систему захисту, необхідно розглянути загрози, які несуть інсайдери, і засоби, якими вони оперують.

Всіх носіїв внутрішніх загроз можна умовно розділити на декілька груп: несвідомі порушники та свідомі порушники. Дуже часто інсайдери наражають на ризик корпоративні секрети ненавмисно. Так, скажімо, вони можуть випадково викласти секретні документи на веб-сайт, записати дані на ноутбук або кишеньковий комп'ютер, який згодом буде викрадений або втрачений, а також відіслати конфіденційні дані за неправильною адресою.

Для прикладу можна навести випадок, коли фірма Merrill Lunch відправила електронний лист в компанію Standart&Poor's, в якому просила оцінити активи банку Commerzbank. Лист став доступним гласності, що змусило банк виступити із заявою про свою фінансову спроможність.

Іншу категорію несвідомих порушників складають співробітники, які вважають, що здатні на більше, аніж приписано їхніми функціональними обов'язками. Так, скажімо, вони часто беруться за переустановлення

програмного забезпечення, яке, на їх думку, функціонує не зовсім правильно, в результаті чого воно взагалі перестає робити.

Разом з цим, необхідно зазначити, що в решті решт дані особи мають на меті виключно добрі наміри. Значно гірше складається справа з порушниками, які свідомо намагаються нанести шкоду. Як правило, це люди з ураженим самолюбством, завищеною самооцінкою, якості були «недооцінені» керівництвом. До такого типу найнебезпечніших внутрішніх порушників відносяться «ображені» та «саботажники». Головною відміною цих зловмисників є намагання нанести шкоду за особистими, як правило, безкорисливим мотивам. Це накладає свій відбиток на ті загрози, які несуть саботажники, і способи, якими вони можуть скористатися. Справа у тому, що для реалізації своєї мети ображені інсайдери готові піти буквально на все, часто навіть не турбуючись про самозбереження.

Так, скажімо, саботажник може скопіювати вкрай важливу для компанії інформацію на мобільний носій, а потім знищити її на всіх серверах фірми і навіть в резервних копіях на матеріальних носіях. Зрозуміло, що після таких дій в руках зловмисника виявляються важелі тиску на керівництво.

Однак в деяких випадках ображений службовець може видалити всі важливі дані, навіть не залишивши інформацію собі. В цьому випадку порушник хоче просто помститись і перетворюється у диверсанта.

Інша категорія порушників – співробітники, що звільняються із організації в результаті переходу на іншу роботу або конфлікту. На рисунку 1.3 надане класифікації внутрішніх загроз економічній інформації банку, джерелом яких виступає персонал банку.

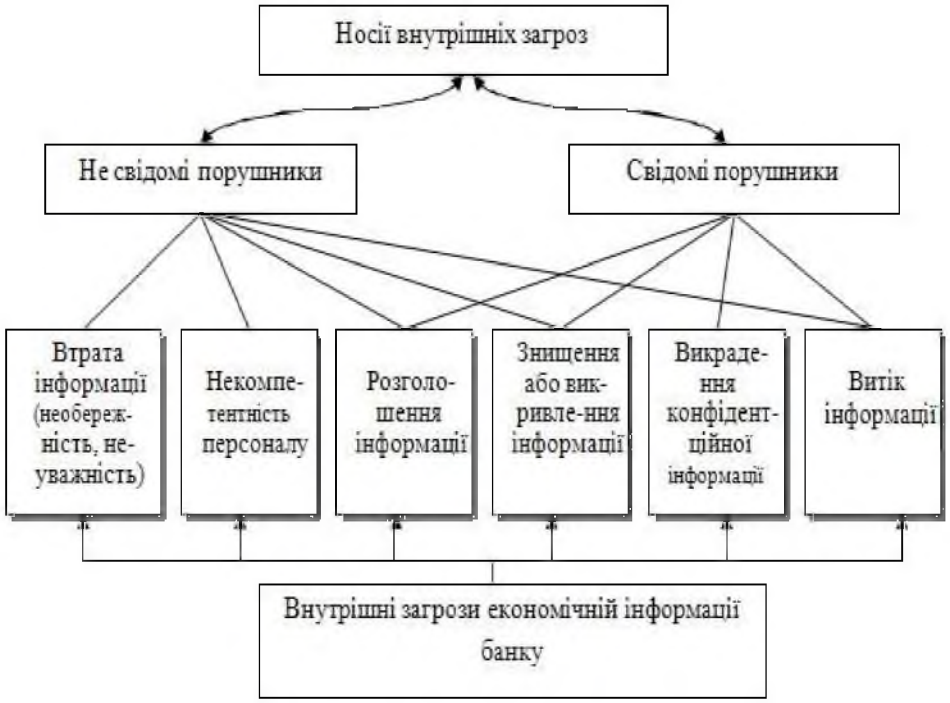

Рисунок 1.3 - Класифікації внутрішніх загроз економічній інформації

Зрозуміло, що дана класифікація є умовною, оскільки на практиці реальні порушники можуть одночасно відноситись до декількох категорій одночасно, або їх мотиви можуть лежати між мотивами описаних категорій носіїв загроз.

Рисунок 1.4 Ризики нелояльності персоналу

Загрози підприємству зі сторони персоналу можуть також проявлятись в недостатній лояльності персоналу, що зображено на рисунку 1.4

Зростаюче занепокоєння ризиком нелояльності персоналу, під якими розуміють свідомі дії персоналу, метою яких є нанесення шкоди (збитку) підприємства із корисливих або інших мотивів, представляють найбільшу загрозу.

Деякі висновки відносно лояльності людини можна зробити на основі регулярного моніторингу опосередкованих факторів: яким чином побудований робочий графік, які документи і в якій кількості копіює, чи чистить свій поштовий ящик або накопичує листи і тому подібне, і тут неоціниме співробітництво з психологами, в тому числі соціальними і фахівцями з управління персоналом.

Однією із основних причин, що стримує розвиток захисту інформації від внутрішніх загроз є небажання керівників підприємств виносити на широке обговорення випадків витоку інформації або збоїв у роботі інформаційної системи з вини власних співробітників, оскільки вони можуть негативно вплинути на імідж з усіма фінансовими наслідками, що випливають.

Згідно даних аналітичних досліджень, в офіційних опитуваннях на питання про те, чи реалізовувались загрози в області інформаційної безпеки із-за дій персоналу, позитивно відповідають не більше 20% установ. В приватних бесідах або в процесі IT-аудиту систем інформаційної безпеки з'ясовується, що постраждалими виявляється близько 80% організацій. З цієї ж причини поки що немає достовірної статистики реалізації загроз, які виходять із кожної групи порушників.

Практика останніх років показала, що найбільший резонанс викликають випадки витоку конфіденційної інформації саме із фінансово-кредитних установ. Більшість інцидентів показали, що прогалини у безпеці, як правило, не є результатами зловмисної діяльності. Навпроти, найчастіше всього загрозу представляють співробітники, які із некомпетентності наражають компанію на ризик. Таке може трапитись, якщо службовець відправляє електронне

повідомлення з додатком, про конфіденційний характер якого йому просто не відомо. У інших випадках співробітник відправляє важливі файли через загально до ступний поштовий веб-сервер або копіює їх на мобільний телефон – таким чином, дані виявляються у незахищеному середовищі.

Підвищена увага до внутрішніх загроз інформаційної безпеки обумовлена тим, що інсайдерські ризики превалюють над зовнішніми загрозами.

Для побудови даної діаграми в категорію внутрішніх загроз було віднесено халатність співробітників, саботаж та фінансове шахрайство, а в категорію зовнішніх загроз – віруси, хакери, спами. Разом з тим, необхідно зазначити, що загрози викрадення інформації, різноманітні збої і викрадення обладнання спеціально не були віднесені ні до однієї із груп, так як вони можуть бути реалізовані як на самому підприємстві, так і за його межами.

Таблиця 1.7 - Модель загроз

Джерело загрози	Загроза	Рівень ризику
Керівники	- Крадіжка - Підміна (модифікація) - Знищення (руйнування) - Порушення нормальної роботи (переривання)	3
Співробітники служби захисту інформації	- Перехоплення інформації - Помилки - Підміна (модифікація) - Крадіжка - Знищення (руйнування)	3
Адміністратори ЛОМ	- Перехоплення інформації - Помилки - Підміна (модифікація) - Порушення нормальної роботи (переривання) - Крадіжка - Знищення (руйнування)	4

Продовження Таблиці 1.7

Співробітники підрозділів	- Помилки - Порушення нормальної роботи (переривання) - Крадіжка - Знищення (руйнування)	2
Користувачі (оператори) АС	- Помилки - Порушення нормальної роботи (переривання) - Крадіжка	1
Персонал, який обслуговує технічні засоби	- Помилки - Порушення нормальної роботи (переривання) - Крадіжка	1
Технічний персонал	- Помилки - Порушення нормальної роботи (переривання) - Крадіжка	1

Розкриття загроз

1 Крадіжка:

- технічних засобів (вінчестерів, ноутбуків, системних блоків);
- носіїв інформації (паперових, магнітних, оптичних і ін.);
- інформації (читання і несанкціоноване копіювання);
- засобів доступу (ключі, паролі, ключова документація і ін.).

2 Підміна (модифікація):

- операційних систем;
- систем управління базами даних;
- прикладних програм;
- інформації (даних), заперечення факту відправки повідомлень;
- паролів і правил доступу.

3 Знищення (руйнування):

- технічних засобів (вінчестерів, ноутбуків, системних блоків);
- носіїв інформації (паперових, магнітних, оптичних і ін.);
- програмного забезпечення (ОС, СУБД, прикладного ПЗ);
- інформації (файлів, даних);

- паролів і ключової інформації.

4 Порушення нормальної роботи (переривання):

- швидкості обробки інформації;
- пропускної спроможності каналів зв'язку;
- об'ємів вільної оперативної пам'яті;
- об'ємів вільного дискового простору;
- електроживлення технічних засобів.

5 Помилки:

- при інсталяції ПЗ, ОС, СУБД;
- при написанні прикладного ПЗ;
- при експлуатації ПЗ;
- при експлуатації технічних засобів.

6 Перехоплення інформації (несанкціоноване):

- за рахунок ПЕМІ від технічних засобів;
- за рахунок наведень по лініях електроживлення;
- за рахунок наведень по сторонніх провідниках;
- по акустичному каналу від засобів висновку;
- по акустичному каналу при обговоренні питань;
- при підключенні до каналів передачі інформації;
- за рахунок порушення встановлених правил доступу (злом).

1.4 Постановка задачі

Загрозам з боку персоналу не можна запобігти повністю, але ними можна управляти й звести до мінімуму. При створенні повномасштабної системи інформаційної безпеки варто враховувати всі можливі способи здійснення внутрішніх атак і шляхи витоку інформації. Необхідні системи захисту, що дозволяють контролювати інформацію, що проходить через кожний вузол мережі, і блокувати всі спроби несанкціонованого доступу до конфіденційних даних.

Для досягнення поставленої мети в кваліфікаційній роботі визначено такі завдання:

- аналіз основних методів захисту від антропогенних загроз;
- розробка технічного завдання;
- розробка комплексу методів протидії внутрішнім загрозам інформаційній безпеці підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз поширених методів захисту від антропогенних загроз

Антропогенними джерелами загроз безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочину. Тільки в цьому випадку можна говорить про заподіяння шкоди. Ця група найбільш обширна і представляє найбільший 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 безпосередньо залежать від волі організаторів захисту інформації.

В якості антропогенного джерела загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами захищається об'єкта. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні, так і внутрішні.

Так як нас цікавлять саме внутрішні загрози, то і розглядатимемо внутрішні суб'єкти (джерела), які, 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:

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 числа 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.

Кваліфікація антропогенних джерел інформації відіграють важливу роль в оцінці їх впливу і враховується при ранжуванні джерел загроз.

Урахуванням множинності категорій і каналів витоку інформації стає очевидно, що в більшості випадків проблему витоку не можна вирішити будь-яким простим способом, тим більше позбавитися від неї остаточно. Крім того, реалізація будь-яких заходів з обмеження доступу до інформації або її поширенню потенційно знижує ефективність основних бізнес-процесів організації. Це означає, що потрібна система організаційно-технічних заходів, що дозволяють перекрити основні канали витоку інформації з певним ступенем надійності і мінімізувати існуючі ризики без значного зниження ефективності бізнес-процесів. Без такої системи права на юридичний захист інтересів організації як власника інформації не реалізовуються.

2.1.1 Робота з персоналом

Основним джерелом витоку інформації з організації є її персонал. Людський фактор здатний «звести нанівець» будь-які найбільш витончені механізми безпеки. Це підтверджується численними статистичними даними, що свідчать про те, що переважна більшість інцидентів безпеки пов'язано з діяльністю співробітників організації. Не дивно, що робота з персоналом - головний механізм захисту.

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.

1. Відповідальність за інформаційну безпеку включена в посадові обов'язки співробітників, включаючи відповідальність за виконання вимог політики безпеки, за ресурси, процеси та заходи щодо забезпечення безпеки.

2. Проводяться відповідні перевірки співробітників при прийомі на роботу, включаючи характеристики і рекомендації, повноту і точність резюме, освіту та кваліфікацію, а також документи, що засвідчують особу.

3. Підписання угоди про нерозголошення конфіденційної інформації кандидатом має бути обов'язковою умовою роботу прийому на.

4. Вимоги інформаційної безпеки, які пред'являються до співробітника, у трудових угодах. Там же має бути прописана відповідальність за порушення безпеки.

2.1.2 Підвищення обізнаності

Важливу роль для забезпечення інформаційної безпеки відіграє обізнаність користувачів в питаннях безпеки та правила безпечної поведінки. Основну роль тут грають менеджери організації.

Проводиться навчання та контролювати знання користувачів з наступних питань:

- правила політики 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.

2.1.3 Політика безпеки та процедури внутрішньофірмової комунікації

Відповідна організація процесу внутрішньофірмової комунікації, дозволяє уникнути витоку інформації та неналежного її використання. Вона включає в себе визначення рівнів доступу до інформації, механізмів контролю та функціональних ролей.

В організації повинно бути розроблено положення щодо захисту конфіденційної інформації та відповідні інструкції. Ці документи повинні визначати правила та критерії для категоріювання 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.

Відповідальність за інформаційну безпеку організації несе її керівник, який делегує цю відповідальність одному з менеджерів. Зазвичай ці функції виконує директор з інформаційної безпеки (CISO) або директор з безпеки (CSO), іноді директор інформаційної служби (CIO).

Рішення про надання доступу до конкретних інформаційних ресурсів повинні приймати власники цих ресурсів, що призначаються з числа керівників підрозділів, що формують і використовують ці ресурси. Крім того, питання надання доступу конкретним співробітникам повинні бути погоджені з їхніми безпосередніми керівниками.

Багато правила політики безпеки зрозумілі співробітникам і виконуються ними в більшості випадків на інтуїтивному рівні. Решта вимагають навчання.

2.1.4 Автентифікація і управління доступом

Традиційні схеми автентифікації і управління доступом в багатьох випадках вже не забезпечують адекватного рівня захисту. На додаток до них доцільно використовувати спеціалізовані сервіси управління правами доступу до електронних документів, які вже починають з'являтися на ринку.

Прикладами відповідних комерційних продуктів є Microsoft RMS (вперше з'явився у Windows Server 2003) та програмно-апаратний комплекс Sentinel RMS, вироблений компанією SafeNet.

RMS (Служби управління правами, сервіси управління правами доступу) - це технологія, використовувана для захисту електронних документів від несанкціонованого використання. Вона дозволяє при поширенні інформації визначати обмеження по використанню останньої. Наприклад, автор документа може обмежити «час життя» документа, а також можливість для певних користувачів відкривати, змінювати, копіювати в буфер обміну, друкувати або пересилати документ. Основна відмінність даної технології від традиційних способів розмежування доступу до інформації полягає в тому, що доступу права і додаткові обмеження по використанню зберігаються в тілі самого документа і діють незалежно від його місцезнаходження. Шифрування документів, реалізований в технології RMS, не дозволяє отримувати доступ до їх вмісту яких-небудь обхідним шляхом.

2.1.5 Фільтрація контенту

Використання RMS, звичайно, не вирішує всіх проблем. Наприклад, ця технологія не захищає від навмисного «зливу» інформації по електронній пошті, що на практиці зустрічається досить часто, і змушує керівництво організації вводити правила по фільтрації виходять з корпоративної мережі повідомлень за їхнім змістом. Аналіз змісту повідомлень за ключовими словами може бути досить ефективним, однак вимагає проведення серйозної роботи по «тюнінгу» системи фільтрації контенту, так як жодна з подібних систем не працює «прямо з коробки». Навіть добре налагоджена система фільтрації вимагає постійної уваги з боку адміністратора безпеки.

2.1.6 Захист документів

Якщо ще до викрадення інформації саботажник або нелояльний співробітник вийде на потенційного «покупця» конкретної інформації, він стає найбільш небезпечним порушником. Захист електронних документів найбільш ефективна в спеціалізованих програмах: системах захищеного документообігу, захищених клієнт-серверних і веб-додатків. Основний принцип таких систем - захист документа з моменту його створення і до моменту його знищення. У тих організаціях, в яких весь документообіг ведеться в системах захищеного документообігу, конфіденційні документи найбільш захищені від внутрішніх загроз. Всі дії авторизованих користувачів з конфіденційними документами, включаючи їх збереження в неавторизованому місці, друк та інші, які становлять загрозу витоку інформації, відслідковуються і документуються. Такі системи зберігають всі чернетки і версії документів, які зміни та спроби несанкціонованих дій фіксуються.

Проте впровадження таких систем з метою захисту від внутрішніх загроз мають і істотні недоліки. Розглянемо їх більш детально:

1. Істотні витрати на впровадження. Такі системи досить дорогі і вимагають одночасного впровадження у всій компанії, як мінімум, а оптимально - в усіх контрагентів. Цей шлях досить дорогий - вартість ПО для однієї робочої станції іноді перевищує сотні доларів, не рахуючи серверних ліцензій.

2. Незвична для роботи середу. Володіння системами документообігу не є обов'язковим при прийомі на роботу, на відміну від знання офісних і поштових програм. Тому всіх користувачів доводиться навчати роботі з новою системою. Останнім часом з'явилися системи, що інтегруються в стандартні офісні пакети, але вони ще не так поширені.

3. Власний формат файлу. Для реалізації стратегії захисту документа всі системи захищеного документообігу використовують закритий формат файлів, які можуть бути відкриті тільки в конкретній системі документообігу.

Слабкість цієї системи захисту полягає в тому, що, оскільки не всі контрагенти мають ці системи документообігу, для передачі їм файлів необхідно конвертувати захищений формат в загальноприйнятий. Після конвертації файли залишаються незахищеними від нецільового використання.

4. Незахищеність на робочих станціях. Як би не було захищено документне сховище, відкритий на робочій станції документ або запит до бази даних вразливий двічі: по-перше, його зміст знаходиться в буфері екрана, тобто можливо копіювання його або його частини в буфер Windows командами Copy або PrintScreen, по-друге, образ екранного буфера знаходиться у тимчасовому файлі, який лежить на диску робочої станції і може бути скопійований з допомогою файлового менеджера. Збереження цієї інформації в незахищеному форматі дозволяє користувачеві надходити з нею на свій розсуд.

2.1.7 Шифрування інформації

Шифрування - один з найбільш надійних способів забезпечення конфіденційності інформації. Криптографічні методи давно і успішно розвиваються у всьому світі, тому в даний час механізми шифрування є найсильнішою ланкою в будь-якій системі забезпечення інформаційної безпеки.

Так, наприклад, доступний і розповсюджений спосіб шифрування інформації при зберіганні для користувачів ОС Microsoft Windows - застосування вбудованого в NTFS сервісу шифровану файлову систему (EFS). У всіх поширених поштових клієнтів підтримуються функції шифрування повідомлень, що дозволяє без додаткових зусиль робити обмін конфіденційною інформацією з зовнішніми респондентами у зашифрованому вигляді.

2.1.8 Моніторинг (аудит) дій користувачів

В організаціях, в яких можливий доступ співробітників до державної таємниці, давно використовуються спеціалізовані робочі місця для роботи з нею. Крім моніторингу рухів миші і клавіатури, на цих станціях здійснюється шифрування інформації на льоту, а також використання спеціальних екранних фільтрів щоб уникнути фотографування інформації з екрану або підглядання за екраном через плече працюючого. Крім того, такі робочі станції позбавлені можливості підключення змінних носіїв, а друк здійснюється з дозволу офіцера-секретчика.

Для доступу до інформації, що становить держтаємницю, це рішення, безумовно, виправдано, оскільки ризик витоку має набагато вищий пріоритет, ніж зручність використання. Однак подібні регламенти роботи з конфіденційною інформацією в динамічних ринкових структурах, які ускладнюють доступ і маніпуляції з інформацією, можуть перешкодити ринкового успіху компанії. Велика кількість співробітників та операцій з документами буде породжувати таку кількість інформації, яка не зможе обробити жодна людина. Тому тотальний контроль дасть лише ілюзію контролю - скористатися його результатами буде складно.

Можна провести аналогію з мовним зв'язком - технічно можливо прослуховувати і записувати всі розмови, що ведуться по телефонах, але в реальності скористатися цією інформацією в оперативному порядку неможливо - тоді на кожного мовця доведеться один слухач. Інша справа - спостереження за конкретним співробітником, що знаходиться в оперативній розробці, тобто підозрюваним у чомусь. Також важливо мати можливість ретроспективного аналізу накопиченої інформації при проведенні розслідувань.

Тому найчастіше застосовується програмне забезпечення, що контролює певні дії користувача в пасивному режимі, - провідне журнал доступу. Досить рідко буває необхідно відстежувати натискання кожної клавіші і кожне переміщення миші, звичайно виділяються небезпечні операції (файлові -

копіювання і перейменування, документні - збереження, друк, копіювання і вставка, системні - копіювання екрану і т. п.). Ці операції контролюються особливо ретельно. Причому якщо ці операції проводилися з документом, не містять конфіденційну інформацію, то програмне забезпечення лише фіксує їх у базі подій, якщо ж ці дії відбувалися з конфіденційним документом - надсилається повідомлення про заборонену операції.

Часто, через брак інформації про спеціальні рішеннях, з метою моніторингу застосовують засоби, призначені для інших цілей. Так, для моніторингу руху файлів використовуються програмні агенти, призначені для аудиту стану програмного забезпечення. Це дає ілюзію захисту, так як ці агенти контролюють лише переміщення файлів за допомогою файлових менеджерів. Якщо ж переміщати файли за допомогою операцій над ними, наприклад при конвертації формату або використовуючи програми для запису на оптичні диски типу Nero, ця операція пройде непоміченою для агента.

2.1.9 Зберігання фізичних носіїв

Зрозуміло, що після абсолютно легального резервного копіювання ніяке програмне забезпечення не в силах зупинити фізичний винос зловмисником носія, його копіювання і занос назад. Тому зараз використовується кілька способів захисту цього каналу витоку. Перший - анонімізації носіїв, тобто працівники, що мають доступ до носіїв, не знають, яка інформація записана на якому носії, вони управляють тільки анонімними номерами носіїв. Ті співробітники, які знають, на якому носії знаходиться яка інформація, у свою чергу, не повинні мати доступ до сховища носіїв. Другий спосіб - шифрування інформації при резервному копіюванні, оскільки розшифрування винесеної інформації потребує деякого часу і дорогої обчислювальної потужності. Безумовно, тут працюють всі технології зберігання цінних речей - замки, що відкриваються тільки двома ключами, що перебувають у різних співробітників, кілька рівнів доступу і т. д. З розвитком технологій радіоідентіфікації (RFID), можливо, з'являться системи автоматичного

оповіщення про спроби винести за межі сховища носії, в які для цієї мети будуть впроваджені радіомітки.

2.1.10 Захист каналів витоку

Під захистом каналів зазвичай розуміють два взаємодоповнюючих процесу - управління доступом до каналу і контроль інформації, що передається через канал. Власне каналів виходу інформації з компанії небагато - електронна пошта, Інтернет, змінні носії (дискети, записувані оптичні диски, USB-пристрої і т. д.), порти вводу-виводу (COM, Wi-Fi, Bluetooth тощо), друк та мобільні пристрої - портативні і кишенькові комп'ютери.

Для контролю доступу до кожного з них є свої програми, як вхідні в засоби управління відповідного додатку, так і продаються окремо. Зазвичай процес відкриття доступу в компаніях регламентований і здійснюється на основі заявок, візуються безпосереднім керівником. Звичайно, факт відмови співробітнику в доступі до каналу гарантує відсутність витоків з цього каналу від цього співробітника. Але не варто забувати, що збереження конфіденційної інформації не є основне завдання бізнесу. Не маючи доступу до корпоративної електронної пошти або принтеру, співробітник не зможе виконувати свої службові обов'язки, а маючи такий доступ - стане потенційним викрадачем інформації.

Останнім часом часто говорять про засоби управління доступом до змінних пристроям як про вирішення проблеми викрадення інформації. Тобто стверджується, що якщо ми обмежимо доступ, наприклад, до портів USB, ми будемо захищені від витоків інформації. Деякі програми дозволяють вирішити використання тільки певного USB-носія і заборонити використання всіх інших. Дійсно, приклад, наведений на самому початку статті, не реалізувався б у випадку, якщо б порт USB не заблокованого користувачем комп'ютера був відкритий тільки для використання певного диска або тільки для читання. Однак нагадаю, що чужі USB-накопичувачі - це інструмент реалізації не внутрішніх загроз, а зовнішніх. Зловмисний порушник завжди імітує

виробничу необхідність чи просто купить КПК і зажадає відкрити порт для синхронізації його з комп'ютером. Змінні карти розширення пам'яті КПК досягають ємності 2 Гбайта, тому при бажанні за допомогою КПК можна винести будь-яку кількість інформації.

Ось чому, крім факту відкриття доступу до каналу, необхідно перевіряти інформацію, що проходить через нього, на предмет вмісту забороненої до виносу за межі компанії. Для цього використовуються різні технології - контентна фільтрація, мітки на конфіденційних файлах та ін. Крім того, є програмні засоби, що зберігають копії скопійованих, посланих і надрукованих файлів для створення доказової бази при розслідуванні інцидентів.

2.2 Комплекс методів для зниження ризиків антропогенних загроз.

2.2.1 Основні напрями і методи роботи з персоналом підприємства, допущеним до конфіденційної інформації.

Постійна робота з персоналом підприємства, які мають доступ до конфіденційної інформації, - одне з найбільш актуальних і важливих напрямів у діяльності керівництва та посадових осіб підприємства. Персонал, що постійно працює з відомостями конфіденційного характеру (їх носіями), - основний суб'єкт правовідносин у сфері захисту конфіденційної інформації. Одночасно він і єдиний її «нематеріальний носій». У вирішенні проблеми комплексного захисту інформації на підприємстві все більш значне місце займає вибір ефективних способів і методів роботи з персоналом. Будучи генератором нових ідей, відкриттів і винаходів, що прискорюють науково-технічний прогрес, персонал направляє максимальні зусилля на підвищення добробуту підприємства в цілому і кожного його співробітника зокрема. Проте персонал часто стає і основним джерелом витоку (розголошення) конфіденційної інформації.

Керівництво підприємства в свою чергу вирішує завдання збереження в таємниці співробітниками підприємства шляхів, методів і способів підвищення добробуту підприємства та досягнення максимального прибутку

в його роботі. Від того наскільки працівник підприємства підготовлений професійно в галузі захисту інформації, якими він володіє морально-діловими і психологічними якостями, цілком залежить його здатність протистояти можливим спробам отримання зловмисниками або представниками організацій-конкурентів важливою для них інформації, віднесеної даним підприємством до категорії конфіденційної. Високий рівень підготовки співробітників підприємства в питаннях захисту конфіденційної інформації дозволить також максимально знизити ймовірність появи ненавмисних помилок у поводженні з цією інформацією (її носіями), наявність яких також потенційно створює передумови до її отримання недоброзичливцями. І навпаки, прояв співробітниками підприємства низьких професійних навичок і негативних морально-ділових якостей значно знизить ефективність системи захисту конфіденційної інформації на підприємстві в цілому, оскільки ніякі заходи організаційного та технічного характеру не компенсують можливу витік інформації з боку співробітників підприємства.

Причинами розголошення конфіденційної інформації допущеним до неї персоналом підприємства найчастіше стають наступні чинники та обставини:

- Недостатній рівень знань положень нормативних актів та внутрішніх організаційно-розпорядчих документів підприємства, що регламентують діяльність по захисту інформації;
- Слабкий контроль з боку керівників всіх рівнів за станом захисту інформації та ефективністю вжитих заходів по недопущенню витоку цієї інформації;
- Недостатня увага до питань організації роботи з персоналом підприємства, вивчення морально-ділових якостей співробітників підприємства, допущених до конфіденційної інформації;
- Несвоєчасне прийняття ефективних та дієвих заходів щодо запобігання розголошення персоналом підприємства конфіденційної інформації, а також заходів за фактами порушень норм і правил захисту інформації співробітниками підприємства.

Поряд з перерахованими факторами і обставинами до витоку інформації, що охороняється, можуть також призвести різні екстремальні ситуації, що виникають у службових приміщеннях підприємства, надзвичайні події та стихійні лиха, локальні несправності в системах комунікації і життєзабезпечення. У таких ситуаціях охороною інформація потенційно може стати надбанням осіб, не допущених до неї, які тимчасово перебувають на території підприємства (прибулих для вирішення різних завдань і питань відкритого характеру). У зв'язку з цим важливо мати необхідну інформацію про осіб, які не є співробітниками підприємства, яким надано право його відвідин (перебування на його території) для вирішення різних питань і завдань. Завчасно визначається коло таких осіб, що включає насамперед:

- Співробітників організацій-партнерів та інших взаємодіючих з підприємством у рамках його основної діяльності організацій і структур;
- Працівників органів державної влади, місцевого самоврядування, територіальних і наглядових органів;
- Представників засобів масової інформації (ЗМІ) регіонального і місцевого рівня;
- Працівників муніципальних (районних) комунальних служб;
- Працівників підприємств харчування та побутового обслуговування, які забезпечують життєдіяльність підприємства;
- Інкасаторів, співробітників банківських структур, підрозділів федеральної поштового та фельд'єгерського зв'язку.
- Саме безпосередню участь в роботі з персоналом підприємства, як правило, приймають кадровий орган, служба безпеки, режимно-секретний підрозділ, підрозділ психологічної та виховної роботи, юридична служба (юрисконсульт), служба охорони та служба власної безпеки.
- Керівництво підприємства, що використовує в своїй роботі конфіденційну інформацію незалежно від її виду та ступеня конфіденційності, а також співробітники перерахованих підрозділів, можуть у своїй діяльності можуть спиратися на положення цивільного кодексу України.

У цивільному кодексі закріплено принцип добровільності доступу до комерційної таємниці працівника підприємства (у випадку, якщо інше не передбачається трудовим договором). Встановлено обов'язки роботодавця по відношенню до співробітника підприємства у зв'язку з охороною конфіденційності інформації, що становить комерційну таємницю.

Роботодавець зобов'язаний:

- ознайомити під розписку працівника, якому для виконання його трудових обов'язків потрібен доступ до інформації, що становить комерційну таємницю, з переліком інформації, що становить комерційну таємницю, власниками якої є роботодавець і його контрагенти;
- ознайомити під розписку працівника із установленим роботодавцем режимом комерційної таємниці й з заходами відповідальності за його порушення;
- створити працівнику необхідні умови для дотримання ним встановленого роботодавцем режиму комерційної таємниці.

2.2.2 Основні етапи роботи з персоналом

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, пов'язану з доступом до конфіденційної інформації (перекладі на цю роботу штатного працівника підприємства, не допущеного до такої інформації);

2 в процесі виконання співробітником підприємства, допущеним до конфіденційної інформації, посадових (функціональних) 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.

Один з найбільш важливих етапів у роботі з персоналом підприємства - процес підбору можливих кандидатів для призначення на посади, пов'язані з конфіденційною інформацією. При підборі кандидатів проводиться оцінка відповідності кожного з них таким основним вимогам:

- За рівнем підготовки та кваліфікації, наявності необхідного досвіду роботи;

- По морально-діловим і особистісним якостям, ступеня відповідальності за прийняті управлінські та виконавські рішення (в залежності від займаної посади).

Оптимальний результат пошуку можливих кандидатів для призначення на посади, пов'язані з конфіденційною інформацією, досягається у випадку, коли розглянуті кандидатури повністю задовольняють зазначеним вимогам.

У число основних методів перевірки і оцінки відповідності кандидата вимогам входять:

- вивчення матеріалів особової справи, анкетних, автобіографічних та інших персональних даних, резюме та інших документів кандидата;

- особиста бесіда з кандидатом посадових осіб підприємства (працівників кадрового органу);

- проведення тестування.

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.

Оптимальний результат роботи з підбору кадрів - відбір необхідного числа кандидатів для призначення на конкретні посади, в повному обсязі задовольняють поставленим вимогам.

При підборі кандидатів для призначення на посади, пов'язані з конфіденційною інформацією, в обов'язковому порядку враховується рівень кожної конкретної посади з точки зору прийняття та реалізації управлінських рішень, виконання організаторських функцій і завдань повсякденної діяльності підприємства. Виходячи з названих критеріїв, такі посади поділяють на такі групи:

- посади керівників підприємства (керівник підприємства, його філії, представництва);

- посади заступників керівника;

- посади керівників структурних підрозділів;

- посади керівників служб безпеки та їх заступників;

- посади співробітників служб безпеки підприємства;

- посади співробітників підприємства, що здійснюють на постійній основі роботу з конфіденційною інформацією у відповідних структурних підрозділах.

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

У ході попередньої бесіди з оформлюваним на роботу громадянином працівник кадрового органу разом з уточненням окремих питань анкети, що заповнюється при оформленні матеріалів на допуск до державної таємниці, виявляє представляють інтерес відомості, не передбачені питаннями анкети:

- чи мав громадянин за останній рік ставлення до секретних робіт, документів та виробів;

- давав він зобов'язання щодо нерозголошення відомостей, що становлять державну таємницю;

- чи працював (служив) на режимних об'єктах. Працівник кадрового органу також запитує необхідні довідки та документи, знайомить громадянина зі змістом договору (контракту) про оформлення допуску до державної таємниці.

Після прийняття рішення про призначення кандидата, що найбільш повно задовольняє пропонованим вимогам, на посаду, пов'язану з допуском до конфіденційної інформації, керівник структурного підрозділу, до якого призначено особу, спільно зі службою безпеки підприємства (режимно-секретним підрозділом) організовує проведення інструктажу. В ході інструктажу до відома новопризначеного особи доводяться його посадові обов'язки, положення нормативно-методичних та внутрішніх організаційно-розпорядчих документів, що регламентують питання захисту конфіденційної інформації на підприємстві. Підготовка співробітника до виконання обов'язків відповідно з новою посадою здійснюється по плану, що затверджується керівником структурного підрозділу, до якого призначений цей працівник.

2.2.3 Методи роботи з персоналом та їх характеристика

У повсякденній діяльності використовуються такі основні методи роботи з персоналом підприємства, що допущений до конфіденційної інформації і працюють з носіями цієї інформації:

- навчання;

- інструктажі;

- індивідуальна і виховна робота;

- перевірка рівня знань;

- контроль.

Метод навчання - першорядний метод роботи з персоналом підприємства, початковий етап у придбанні теоретичних знань і практичних навичок забезпечення захисту конфіденційної інформації в рамках виконання посадових (функціональних) обов'язків за основним фахом. Процес навчання співробітників підприємства повинен бути постійним і планомірним, так як система захисту конфіденційної інформації підприємства вимагає розвитку та вдосконалення.

Завдання навчання персоналу підприємства включають вивчення:

- нормативно-методичних документів по захисту використовуються на підприємстві видів конфіденційної інформації;

- структури, сил і засобів системи захисту конфіденційної інформації підприємства;

- встановлених норм і правил захисту конфіденційної інформації на підприємстві, а також стандартів підприємства, положень про службу безпеки (режимно-секретний підрозділ);

- можливих загроз захисту конфіденційної інформації, їх характеру і можливих способів прояву;

- порядку роботи співробітників підприємства з носіями конфіденційної інформації з урахуванням встановлених вимог щодо режиму секретності (конфіденційності).

Використовуються такі форми навчання:

- лекції, семінари та практичні заняття (тренажі) по діям персоналу в різних ситуаціях;

- тестування співробітників і оцінка рівня їх підготовленості;

- рішення різних ситуаційних завдань, пов'язаних із захистом конфіденційної інформації;

- рішення інтелектуальних завдань, спрямованих на отримання співробітниками підприємства навичок прогнозування різних ситуацій, пов'язаних з виникненням можливих каналів витоку інформації, загроз її безпеки;

- використання спеціалізованих програм навчання для забезпечення лекційних курсів і практичних занять.

Навчання персоналу підприємства з питань захисту конфіденційної інформації проводиться диференційовано, за категоріями посадових осіб - для керівників підрозділів, їх заступників, працівників підприємства. При виборі форм і методів навчання персоналу враховують рівень професійної підготовленості співробітника, стаж роботи за конкретною спеціальністю, специфіку розв'язуваних їм завдань із захисту конфіденційної інформації, результати контролю діяльності співробітника з виконання встановлених вимог щодо захисту інформації на підприємстві.

Метод інструктажів застосовується керівництвом підприємства та керівниками структурних підрозділів для інформування співробітників, що працюють з конфіденційною інформацією, про положення знову прийнятих (затверджених) нормативно-методичних документів, а також вимог вищих органів державної влади (організацій). Під час інструктажів особлива увага повинна приділятися аналізу практичної роботи по вилученню появи каналів витоку відомостей конфіденційного характеру і щодо запобігання виникненню загроз захисту інформації.

Метод індивідуальної та виховної роботи полягає в систематичному і цілеспрямованому впливі на процес формування та розвитку особистості співробітника підприємства в ланцюгах найбільш повного використання його професійних можливостей і здібностей, ділових, високих моральних та інших позитивних якостей для забезпечення схоронності довірених по службі (роботі) відомостей конфіденційного характеру.

Мета перевірки рівня знань - за допомогою оцінки знання співробітниками підприємства положень нормативно-методичних та

внутрішніх організаційно-розпорядчих документів визначити ступінь підготовленості кожного працівника до виконання практичних завдань із захисту інформації. Перевірка рівня знань проводиться як керівництвом підприємства, так і співробітниками режимно-секретного підрозділу, служби безпеки, підрозділи охорони.

Метод контролю у роботі з персоналом підприємства має на меті оцінити ефективність роботи кожного співробітника підприємства щодо забезпечення захисту конфіденційної інформації, використання сукупності сил і засобів підприємства. Контроль може бути періодичним (плановим) і раптовим. Проводиться співробітниками штатних підрозділів підприємства, що вирішують завдання з організації захисту інформації.

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.

2.2.4 Мотивація діяльності 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 внутрішньо особистісних 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.

Готовність до сумлінного виконання посадових обов'язків визначається тим, наскільки працівник схильний їх виконувати. Вона ґрунтується на мотиваційних складових особистості співробітника, а саме: на рівні потреб і інтересів; цільових установках; ціннісних орієнтаціях; бажаннях; задоволеності роботою; очікуванні винагороди залежно від результатів праці і т. п.

Відгуки всього одного співробітника можуть добре позначитися як на мотивації інших співробітників, так і на підвищенні якості роботи в цілому. Можливості співробітника, що дозволяють йому результативно виконувати його посадові обов'язки і поставлені завдання, визначаються як потенціал або сукупність його фізіологічних, інтелектуальних і професійних здібностей. Потенціал співробітника залежить від рівня його знань, освіти, кваліфікації, вікових даних, стану здоров'я, витривалості, енергії і т.п.

Умови являють собою сукупність зовнішніх стимулюючих факторів, що впливають на результативність праці персоналу і знаходяться поза його прямого контролю.

З метою побудови ефективної системи мотивації персоналу керівництво підприємства повинно забезпечити:

- створення реальної «системи влади» на підприємстві;
- задоволення первинних потреб персоналу підприємства - фізіологічних, потреб в безпеці і захищеності;

- умови для задоволення вторинних потреб персоналу - соціальних потреб у повазі і самовираженні.

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 - направлене 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 - направлене 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 - направлене 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.

У роботі зі співробітниками підприємства, допущеними до конфіденційної інформації, особливе місце займає етап їх звільнення (переведення на посади, не пов'язані з конфіденційною інформацією). Після прийняття керівництвом підприємства рішення про звільнення співробітника, допущеного до конфіденційної інформації, або про переведення його на посаду, не пов'язану з доступом до конфіденційної інформації, службою безпеки та кадровим органом підприємства проводиться ряд заходів, спрямованих на запобігання можливого розголошення звільняються співробітником конфіденційної інформації про діяльність підприємства.

Основою проведення даних заходів є прийняття від звільняється співробітника письмових зобов'язань про нерозголошення стали йому відомими в період роботи на підприємстві (в конкретній посаді) відомостей, в установленому порядку віднесених до комерційної таємниці підприємства.

Ці зобов'язання оформляються у вигляді розписки, яка після її оформлення залишається на підприємстві. У розписці вказуються прізвище, ім'я, по батькові працівника і найменування останньої займаної посади; перераховуються відомості конфіденційного характеру, заборонені до розголошення протягом певного терміну, або наводиться посилання на пункти переліку відомостей, віднесених до комерційної таємниці. Згода працівника з умовами нерозголошення перерахованих в розписці відомостей підтверджується підписом співробітника із зазначенням дати. Оформлення розписки здійснюється, як правило, в ході бесіди зі співробітником підприємства представника служби безпеки або режимно-секретного підрозділу. Після оформлення розписки проводиться інструктаж звільняється співробітника про правила його поведінки після звільнення (переведення на іншу роботу) і про недопущення згадки конфіденційних відомостей в ході спілкування з представниками організацій, що є конкурентами даного

підприємства. Особливу увагу в ході інструктажу приділяється необхідності збереження в таємниці конфіденційної інформації при спілкуванні з іноземними громадянами (при взаємодії в процесі майбутньої роботи з іноземними організаціями).

Перед звільненням з підприємства (переведенням на роботу, не пов'язану з конфіденційною інформацією), співробітник зобов'язаний повернути до служби безпеки підприємства (режимно-секретний підрозділ) отримані раніше носії конфіденційної інформації (в тому числі накопичувачі на магнітних дисках), номерні металеві печатки, ключі від сейфів і сховищ. Факт повернення підтверджується відповідними підписами відповідальних посадових осіб в обхідному листі звільняється співробітника. Після заповнення обхідного листа співробітнику видається оформлена трудова книжка та інші документи про звільнення.

Отримавши трудову книжку і провівши повний розрахунок з підприємством, що звільняється співробітник повертає в бюро перепусток (на контрольно-пропускний пункт при вибутті з підприємства) пропуск для проходу на територію та об'єкти підприємства.

2.2.5. Психологічне тестування

Тестування співробітників проводиться на етапі прийому на роботу, а також в процесі праці для контролю і аналізу психологічного стану працівника. Тестування необхідно проводити один раз на пів року.

Нижче наведенні тести які можуть використовуватись у комплексі.

Методика діагностики до конфліктної поведінки К. Томаса. У створенні тесту американський психолог спирався на переконання, що будь-який конфлікт можна вирішити будь-яким з п'яти способів (змагання, пристосування, компроміс, уникнення, співробітництво). У зв'язку з цим Томас сконцентрував увагу на виявлення які форми поведінки в конфліктних

ситуаціях характерні для людей; які з них є більш продуктивними чи деструктивними і яким чином можна стимулювати продуктивну поведінку.

Час на виконання - 10 хвилин.

Час на інтерпретацію результатів - близько 20 хвилин.

Тест є дуже простим і зрозумілим, дає результати з великим ступенем достовірності і є одним з найбільш поширених у відділі персоналу.

Методика «Ціннісні орієнтації» М. Рокича.

Автор методики називає свою «систему ціннісних орієнтацій» філософією життя людини і вважає, що вона може бути описана з двох протилежних сторін: термінальні орієнтації (переконання в тому, що мета може бути гідна, щоб до неї прагнути) та інструментальні орієнтації (переконання у тому , що образ дії або властивості особистості завжди будуть важливішими будь-якої поставленої мети).

Час на виконання - 20 хвилин.

Час на інтерпретацію результатів - близько 20 хвилин.

Результати цього тесту показують менеджеру з персоналу: зрозуміє кандидат фразу «працюємо на результат, можливо, доведеться затриматися на роботі» або ж рівно о шостій його вже не буде на робочому місці.

Методика діагностики рівня суб'єктивного контролю Дж. Роттера.

В основу тесту закладена думка про те, що всі люди різняться між собою по тому, як вони несуть відповідальність за значні в їх житті події. Перший тип вважає, що відбувається з ним є результатом дії зовнішніх сил (воля випадку або дії інших людей). Другий - інтерпретує події як результат свій особистої діяльності.

Час на виконання - 20 хвилин.

Час на інтерпретацію результатів - близько 30 хвилин.

Тест дуже простий у рішенні, і при цьому з великим ступенем достовірності визначає наскільки людина готова взяти відповідальність за свої вчинки на роботі і поза нею

Тест Лірі.

Тест призначений для діагностики уявлення особистості про своє реальне і ідеальне Я. Також тест активно використовується для діагностики взаємин в малих групах, наприклад, у сімейному консультуванні. За допомогою даної методики виявляється переважаючий тип відносин до людей в самооцінці та взаемооцінки.

Для представлення основних соціальних орієнтацій Т. Лірі розробив умовну схему - у вигляді кола, розділеного на сектори. У цьому колі, по горизонтальній і вертикальній осях позначені чотири орієнтації: домінування-підпорядкування і дружелюбність-ворожість. У свою чергу, ці сектори розділені на вісім - відповідно більш приватним відносинам. Для ще тоншого опису, коло ділять на 16 секторів, але частіше використовуються октанти, певним чином орієнтовані відносно двох головних осей.

Схема Т. Лірі заснована на припущенні, що чим ближче виявляються результати випробуваного до центру кола, тим сильніше взаємозв'язок цих двох змінних. Сума балів кожної орієнтації переводиться в індекс, де домінують вертикальна (домінування-підпорядкування) і горизонтальна (дружелюбність-ворожість) осі. Відстань отриманих показників від центру кола вказує на адаптивність або екстремальність інтерперсональної поведінки.

Опитувальник складається з 128 оціночних суджень, які при обробці об'єднуються в 8 октантів (по 16 пунктів у кожному). Випробуваному пропонується оцінити, чи відповідають дані судження оцінюваному об'єкту (реальне Я випробуваного, його ідеальне Я, або особистість іншої людини). При обробці результатів підраховуються індекси дружелюбності й індекси домінування, а також переважаючий тип ставлення до оточуючих.

2.2.6 Морально-матеріальна стимуляція працівників

Найважливішим видом стимулювання є матеріальне, покликаним відігравати провідну роль у підвищенні трудової активності працівників. Цей вид складається з матеріально-грошового і матеріально-негрошового стимулювання, останнє містить частину соціальних стимулів.

Згідно з однією з розширеною трактування моральні стимули ототожнюються з усією сукупністю етичних і моральних мотивів поведінки людини. Проте до області морального стимулювання відноситься тільки частина етичних категорій, а саме ті, які відображають оцінку людини та її поведінки оточуючими і їм самим.

Тарифна система служить основним засобом обліку якості праці і відображення його в заробітній платі. Вона являє собою сукупність нормативів, за допомогою яких здійснюється диференціація і регулювання заробітної плати різних груп працівників залежно від складності, умов праці з метою забезпечення необхідного єдності міри праці та її оплати . Матеріально-грошове стимулювання - це заохочення працівників грошовими виплатами за результатами трудової діяльності.

Застосування матеріально-грошових стимулів дозволяє регулювати поведінку об'єктів управління на основі використання різних грошових виплат і санкцій.

Основною частиною доходу найманого працівника є заробітна плата, яка за своєю структурою неоднорідна. Вона складається з двох частин: постійної і змінної.

Іноді цим частинам присвоюють статус потужного стимулу. Проте за оцінками психологів, ефект збільшення заробітку позитивно діє протягом трьох місяців. Потім людина починає працювати в тому ж, звичному для нього розслабленому режимі.

На неї впливають: вдосконалення нормування праці, впровадження наукової організації, модернізація робочих місць, перегрупування робочої

сили, скорочення зайвого персоналу, посилення зацікавленості в більш складному і кваліфікованому працю.

Необхідно на початок кожного півріччя перегляд усіх ставок зазнали інфляції. Це сприятиме своєчасному подолання відставання тарифної заробітної плати від змін до валового оплаті праці та роздрібних цінах, забезпечити поступовість, поетапність введення нових тарифів у міру досягнення певних результатів виробництва, а разом з тим перешкоджати поглибленню протиріччя між грошовими доходами та їх ринковим товарним покриттям.

Тарифний розряд повинен реально відображати кваліфікацію працівника, що сприятиме зростанню не тільки по вертикалі, а й по горизонталі. Перетворення тарифу на інструмент стимулювання не тільки потенційних, але й реальних результатів праці, є компроміс між потребою в більш гнучкою та енергійної диференціації оплати праці через основну заробітну плату.

Відомо, що індивідуальне розподіл в умовах, коли фактичні відмінності в результаті праці, за оцінками фахівців, становлять в середньому у робітників 23%, а у інженерно технічних працівників досягають 200-300%, є потужним чинником підвищення трудової активності.

Доплатам властиві риси заохочувальних форм матеріального стимулювання, доплата є формою винагороди за додаткові результати праці, за ефект отриманий на конкретній ділянці. Доплати ж одержують лише ті, хто бере участь у досягненні додаткових результатів праці, додаткового економічного ефекту. Доплати на відміну від тарифу не є обов'язковим і постійним елементом заробітної плати. Збільшення розміру доплат залежить головним чином від зростання індивідуальної ефективності праці конкретного працівника і його внеску в колективні результати. При зниженні показників роботи доплати можуть бути не тільки зменшені в розмірі, але і повністю скасовані. Доплати розглядаються як самостійний елемент заробітної плати і

займає проміжне положення між тарифною ставкою і преміальними виплатами.

Необхідно відзначити, що одна група доплат по своїй економічній суті ближча до тарифної частини, інша - до преміальної. Доплати першої групи встановлені в законодавчому порядку, вони поширюються на всіх працівників і їхній розмір не залежить від результатів роботи, вони є мірою оплати основних факторів трудового вкладу. У цьому випадку доплати покликані стимулювати працю в надурочний час, у святкові дні, у нічний час, і за умови праці.

Другій групі доплат більшою мірою властиві риси заохочувальних форм матеріальним грошовим стимулюванням, тому що ці доплати, як і премія, є формою винагороди за додаткові результати праці. До таких доплат ставляться надбавки до тарифних ставок за суміщення професій, збільшення обсягу виконуваних робіт, професійна майстерність і високі досягнення у праці.

Серед цих прогресивних форм стимулювання найбільш поширена - надбавка працівника за суміщення професій і посад.

Надбавка до заробітної плати - грошові виплати понад зарплату, які стимулюють працівника до підвищення кваліфікації, професійної майстерності й тривалому виконанню поєднання трудових обов'язків. В цілому ж слід зазначити, що система доплат до тарифних ставок дозволяє врахувати й заохотити ряд додаткових кількісний і якісних характеристик праці, не охоплених тарифною системою. Ця система створює стимули щодо тривалої дії. Але для її ефективного функціонування необхідно на підприємстві мати чітку систему атестації працівників усіх категорій з виділенням певних ознак або навіть критеріїв для встановлення того чи іншого виду доплат і із широкою участю в цій роботі трудового колективу.

Компенсації - грошові виплати, встановлені з метою відшкодування працівникам витрат, пов'язаних з виконанням ними трудових або інших передбачених федеральним законом обов'язків.

Найважливішим напрямком матеріально грошового стимулювання є преміювання. Премія стимулює особливі підвищені результати праці і її джерелом є фонд матеріального заохочення. Вона представляє одну з найважливіших складових частин заробітної плати.

Мета преміювання - поліпшення насамперед кінцевих результатів діяльності, виражених у певних показниках.

Головна характеристика премії як економічної категорії - це форма розподілу за результатом праці, є особистим трудовим доходом. Премія у своїй частині має нестійкий характер. Її величина може бути більшою або меншою, вона може взагалі не нараховуватися. Ця риса дуже важлива, і якщо вона її втрачає, то премія втрачає свій сенс. По суті вона перетворюється на просту доплату до заробітної плати, і роль її в цьому випадку зводиться до усунення недоліків у тарифній системі.

Застосування премії покликане забезпечити оперативну реакцію на зміну умов і конкретних завдань виробництва.

Керівник повинен враховувати деякі психологічні тенденції, які проявляються при стимулюванні. По-перше, ймовірність ефективної поведінки працівника тим вище. Чим вище цінність і регулярність винагороди, одержуваного в результаті такої поведінки, по-друге, при запізнілому винагороду нижче, ніж при його негайному; по-третє, ефективне трудове поведінку яке заслужено не винагороджується, поступово слабшає, втрачає риси ефективності.

Преміювання як самостійний важіль вирішення завдань має власний механізм впливу на зацікавленість працівників. Цей механізм складається з двох частин: з механізму окремої системи та взаємодії всіх систем преміювання.

Механізм преміювання представляє сукупність взаємопов'язаних елементів. Обов'язковими його складовими є: показники преміювання, умови його застосування, джерело й розмір премії, коло премійованих.

Показник преміювання - центральний, стрижневою елемент системи, що визначає ті трудові досягнення, які підлягають спеціальному заохоченню і повинні бути відображені в особливій частині заробітної плати - премії. Як показники преміювання повинні бути такі показники виробництва, які сприяють досягненню високих кінцевих результатів.

Передбачаються умови преміювання, число логічних умов для діяльності людини не повинно перевищувати чотирьох. При збільшенні цього числа, за проведеними психологічним дослідженням, різко зростає ймовірність виникнення помилки і час, необхідний для прийняття рішення. Необхідно визначитися, хто конкретно включений у коло преміювання. Справа в тому, що преміюванням охоплюються тільки ті працівники, праця яких необхідно додатково заохотити. Ця необхідність обумовлюється завданнями й конкретними умовами праці й виробництва.

Центральне місце в заохочувальної системі займає розмір премії. Він визначає зв'язок результатів праці зі збільшенням розміру заохочення. Ефективність застосовуваної системи преміювання працівник бачить у величині грошової суми, отриманої у вигляді премії. Встановлюватися розмір премії може у відсотках до окладу, до економічного ефекту або ж у твердій ставці. Тобто у відносному й абсолютному вираженні.

Джерелом виплати премії служить фонд матеріального заохочення, який утворюється за рахунок прибутку підприємства в розмірі чотирьох відсотків від фонду заробітної плати.

При визначенні кола премійованих необхідно виходити з адресного та цільового спрямування. Це премії за надпланові, наднормативні досягнення у праці, виконання важливих завдань, проявлену ініціативу дала конкретний результат. В силу своєї цілеспрямованості такі заохочення мають більшу стимулюючої силою і тому ефективніше можуть впливати на підвищення трудової активності.

Другим важливим видом стимулювання є соціальне, мається на увазі заохочення матеріальними, але не грошовими стимулами.

Матеріальні, але не грошові блага мають морально-престижну і стримуючі цінність. Вони привертають увагу всіх і є предметом оцінок і обговорення працівників. При цьому загальна тенденція така, що чим менше предмет (матеріал предмет, послуга, перевага, пільга), що виконує функцію стимулу, тим вище при інших рівних умовах його престижна складова. Причому часто даний не грошовий стимул є більш ефективним, ніж грошовий еквівалент даного подарунка компанії. Ефективне використання спонукального потенціалу матеріальних благ не грошових буквально немислимо без індивідуального підходу.

Розмір грошової винагороди кожний керівник визначає самостійно. Але необхідно обов'язково враховувати цінність працівника та також його стаж праці. Матеріальне заохочення необхідно використовувати також коли працівник у разі загрозі інформаційній безпеці проявляє високий рівень лояльності до інтересів підприємства.

2.2.7 Тест на лояльність

Сучасні кадрові менеджери для перевірки співробітників застосовують провокацію все частіше і частіше. Звичайно, цей метод є не надто коректним з етичної точки зору, але, тим не менш, він досить ефективний. Цікаво, що менеджерів, які добре вміють провокувати, роботодавці цінують все більше і більше. Сьогодні, в умовах жорсткої конкуренції компаній, дуже важливо бути впевненим у тому, що в штаті знаходяться віддані співробітники. Що поробиш, часом для цього доводиться застосовувати і неетичні методи перевірки.

Кадровики теж швидко зрозуміли, які вигоди обіцяє метод провокації. Стресовий інтерв'ю також містить елементи провокації. Вже на співбесіді 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.

Можуть роботодавці поцікавитися й тим, чи мають співробітники схильність до крадіжок.

Перевірку проходять офісні співробітники. Особливі побоювання у роботодавців викликають ті працівники, які мають доступ до конфіденційної інформації.

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.

2.2.8 Взаємоконтроль співробітниками один одного

Джерелами інформації можуть бути люди, які прямо підпорядковані директору, а також співробітники, з якими склалися довірчі відносини, наприклад, секретарі, вахтери, водії й навіть прибиральниці. При обопільного бажання саме вони стають очами й вухами керівника. До того ж збором інформації займаються фахівці з безпеки й кадровики. Крім обслуговуючого персоналу, неофіційна інформація нерідко надходить і від співробітників нижньої ланки.

Інформатори-добровольці можуть керуватися різними мотивами. Наприклад, патріотизмом: інформатор прагне ліквідувати внутрішній конфлікт у колективі, або намагається задовольнити свою потребу в справедливості. Такі донощики думають, що, інформуючи керівництво, вони захищають свої права, сприяють підтримці дисципліни й оптимізують робочий процес.

Страх, заздрість, лінь, бажання просунутися по службових сходах - це друга група мотивів, що спонукають до доносів. Сюди ж можна віднести

прагнення до легких хлібів, бажання позбутися від занадто вимогливого начальника або спрагу помсти. Пристрастю до інформування може заразитися будь-який співробітник, який не зумів проявити себе в професії або досягти результату на займаній посаді. У цьому випадку виказування стає одним з небагатьох способів відчути свою значимість і наблизитися до керівництва.

У доносів є своя специфіка - така інформація має суб'єктивний характер, а її джерело не можна вважати абсолютно достовірним і надійним. Донощик згодом може відмовитися від своїх слів. У цьому випадку менеджер, який вже почав вживати заходів по усуненню неіснуючої проблеми, може опинитися в дурному положенні. Наприклад, в результаті помилкового доносу керівника можуть налаштувати проти цілком лояльного й чесного співробітника, повідомивши про факти злодійства. Підступність в тому, що перевірка дійсно покаже зникнення матеріальних цінностей, але те, що названий співробітник не має до цього відношення, напевно залишиться за кадром. Якщо директор або керівник підрозділу не перевірить інформацію до кінця і спробує звинуватити невинного, цілком імовірна втрата обмовленого співробітника, або, якщо він зуміє виправдатися, постраждає імідж керівника.

Щоб уникнути неприємностей у випадку, коли неофіційна інформація надійшла від однієї з конфліктуючих сторін, найкраще прийняти новину до відома й розібратися в причинах виникнення конфлікту, або проігнорувати донос. На думку психологів, не слід демонструвати донощику свою непоінформованість або ж негайно розголошувати отриману інформацію. Якщо ж зайняти позицію однієї зі сторін конфлікту, цілком імовірно, що незабаром весь колектив стане систематично використовувати доноси для маніпулювання керівництвом.

Неправильна реакція начальства на скарги трудящих чревата погіршенням психологічного клімату в колективі. Начальство ризикує втратити повагу в очах підлеглих, що провокує порушення дисципліни, поява кругової поруки і звільнення з компанії працівників, які не можуть працювати в такій атмосфері.

Фахівці з персоналу помітили, що кожен донос із метою маніпулювання керівником провокує не менше двох нових доповідей від інших маніпуляторів. Ескалація нашіптування швидше протікає на підприємствах, де немає чіткого поділу обов'язків між підрозділами й співробітниками, неясні цілі та завдання компанії, превалюють родинні та інтимні зв'язки між працівниками, а також у колективах, де немає перспектив службового зростання.

У деяких компаніях систематичне одержання «інформації знизу» може бути викликане стилем управління топ-менеджера й навіть регламентується правилами й принципами внутрішніх комунікацій. Наприклад, авторитарний лідер встановлює правила гри, виходячи зі свого життєвого досвіду, нав'язуючи свої рішення й бачення бізнесу згодним і незгодним. Такий керівник нерідко відчуває дефіцит інформації про те, як колектив реагує на його рішення. У нього виникає гостра необхідність в інформаторів з числа підлеглих. У компаніях з демократичним стилем керівництва правила і норми поведінки встановлюються колегіально, а проблеми вирішуються за допомогою конструктивної критики. В атмосфері відкритості й довіри співробітники лояльніші до керівництва, а обмін інформацією, в тому числі й негативною, здійснюється по регламентованих каналах. У цьому випадку колектив цілком може погодитися з ініціативою директора, розуміючи, що у виняткових випадках виказування корисно підприємству.

Прояви побічних ефектів від виказування залежать від того, яку мету переслідує керівник, збираючи інформацію: налагодити ефективну роботу, дисциплінувати співробітників або розпалити штучний конфлікт заради мнимого поліпшення контролю над колективом.

Щоб мінімізувати пагубний вплив доносів, у великих компаніях намагаються впорядкувати канали інформації, по яких співробітники намагаються донести свої повідомлення керівництву.

Деякі організації йдуть далі, створюючи гуртки лояльності для працівників, де у співробітників будь-якого рангу є можливість поспілкуватися з керівництвом у неформальній обстановці. Формування таких

гуртків дозволяє досягти кількох цілей. З одного боку, вони підвищують лояльність персоналу, оскільки люди відчувають свою причетність до управління компанією й вірять у свій вплив на процес прийняття найважливіших рішень. З іншого боку - такі зустрічі дозволяють топ-менеджерам почути "внутрішній голос" компанії. Щоб створити невимушену обстановку, компанії орендують спортзали, де рядові співробітники разом з керівництвом можуть пограти, наприклад, у футбол або волейбол.

Іноді для організації цивілізованого зворотного зв'язку має сенс звернутися до сторонніх фахівців і провести анонімне анкетування співробітників. Це дослідження може допомогти виявити «конфліктні зони» у відносинах між керівництвом і підлеглими, оцінити морально-психологічний клімат у колективі, довідатися ставлення персоналу до політики компанії.

Проте одні тільки опитування й неформальні зустрічі з керівництвом не завжди дозволяють тримати руку на пульсі. Якщо чисельність персоналу перевищує 150-200 осіб, у директора немає можливості особистого спілкування з кожним співробітником. Тому більшість керівників середніх і великих підприємств упевнені, що збирати інформацію повинні професіонали. Щоб полегшити роботу в етичних кодексах багатьох закордонних фірм є пункти, що фактично зобов'язують інформувати керівництво про те, що відбувається в компанії.

Якщо співробітник має інформацію про те, що чиїсь дії загрожують інтересам організації, він зобов'язаний повідомити про це безпосереднього керівника. У випадку, якщо інформація стосується безпосереднього начальника, працівникові варто доповісти про це у відповідний відділ. Передбачається, що співробітник, який знає, що його неправомірні дії обов'язково набудуть розголосу, уважніше ставитися до дотримання трудової дисципліни.

Крім того, західні менеджери ніколи не забувають про те, що будь-який конфлікт на виробництві може стати приводом для судового розгляду. Західні менеджери уважно стежать за що надходить знизу, оскільки конфлікт, що

приводом для позову, негативно позначається на іміджі підприємства й змушує нервувати акціонерів. В Україні поки не прижилася практика звернень до суду через виробничі конфлікти, але до цього має сенс готуватися вже зараз.

2.2.9 Переваги і недоліки запропонованого комплексу методів

Таблиця 2.1 – Порівняння методів

Метод	Переваги	Недоліки
Інформування	Співробітники отримують уявлення про те які методи можуть бути використані проти них	Забирає час роботи співробітника.
Обмеження доступу до інформації	Кожен співробітник має доступ тільки до тієї інформації яка йому потрібна безпосередньо для роботи	Обмеженість пересування співробітника
Психологічне тестування при влаштуванні на роботу, та в процесі праці	- Можливість аналізувати стан співробітника в динаміці - Можливість розкриття прихованих намірів	- Не бажання співробітника проходити тестування - Імовірність помилки
Тестування на лояльність	Можливо виявити на ранній стадії потенційно небезпечного співробітника	Забирає час роботи співробітника
Матеріально – моральне стимулювання	Підвищення мотивації співробітника	Фінансові витрати організації
Взаємоконтроль співробітників	Збільшення контролю за співробітниками	Можливість зловживання співробітниками.

2.3 Висновок

У цьому розділі було виконано аналіз поширених методів захисту від внутрішніх антропогенних загроз та розробка комплексу методів протидії внутрішнім загрозам. Були проаналізовані мотиви порушення ІБ персоналом, були визначені методи роботи з персоналом.

Також було проаналізовано переваги і недоліки комплексу методів протидії внутрішнім загрозам.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

У рамках даної кваліфікаційної роботи був створений комплекс методів для зменшення ризику реалізації внутрішніх загроз на комерційному підприємстві ТОВ «ІнтерАктив». Порівняємо величину витрат на організацію служби захисту інформації з величиною можливої шкоди, яку може понести підприємство внаслідок втрати інформаційних ресурсів.

Для розрахунку вище вказаного необхідно:

– розрахувати капітальних витрат на реалізацію запропонованих рекомендацій;

– розрахувати річні експлуатаційні витрати на виконання рекомендацій;

– сума річних амортизаційних відрахувань на апаратні засоби, необхідні для виконання рекомендацій;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.2 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн;

$К_н$ – витрати на встановлення та налагодження прийняття мір протидії витокам інформації, грн;

$К_{зпз}$ –вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації: резервне копіювання, блок безперервного живлення, кодовий замок, журнал обліку носіїв інформації, контроль стану обладнання, інструктаж з ІБ, Firewall Analyzer Standard Edition, Avast Premium Security.

3.2.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням кодового замка, встановленням фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф , \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 200 грн/год.

Час на налагодження резервного копіювання займе 1 год.

$$З = ТС* Ф = 175*1 = 175 грн.$$

Час на встановлення блоку безперервного живлення займе 1 год, затрати:

$$З = ТС* Ф = 175*1 = 175 грн.$$

Час на встановлення кодового замку займе 1 год, затрати:

$$З = ТС* Ф = 175*1 = 175 грн.$$

Час на встановлення фаєрволу займе 0,5 год, затрати:

$$З = ТС* Ф = 175*0,5 = 87,5 грн.$$

Час на встановлення антивірусу займе 1 год, затрати:

$$З = ТС^* Ф = 175^*1 = 175 \text{ грн.}$$

Час на створення журналу обліку носіїв займе 3 год, затрати:

$$З = ТС^* Ф = 175^*3 = 525 \text{ грн.}$$

3.2.2 Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується в підприємстві.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість
Резервне копіювання	SSD диск Transcend 250S 4TB NVMe M.2 2280 PCIe 4.0 x4 3D NAND TLC (TS4TMTE250S), www.rozetka.com.ua	12329
Блок безперервного живлення	ДБЖ APC Back-UPS 900W/1600VA USB Schuko (BX1600MI-GR), www.rozetka.com.ua	9439
Кодовий замок на серверну	RZ M-1603BK-30, встановлюється своїми силами, www.rozetka.com.ua	820
Облік носіїв інформації	Створення журналу (3 год., переоблік раз на тиждень)	525
Фаєрвол	Firewall Analyzer Standard Edition, hhttps://www.fortsoft.com.ua/	18486
Антивірус	Avast Premium Security www.rozetka.com.ua	569

Фіксовані витрати на проєктування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 175 + 12329 = 12504 \text{ грн.}$$

Блок безперервного живлення:

$$К = 175 + 9439 = 9614 \text{ грн.}$$

Кодовий замок на серверну:

$$К = 175 + 820 = 995 \text{ грн.}$$

Облік носіїв інформації:

$$К = 525 \text{ грн.}$$

Фаєрвол:

$$К = 87,5 + 18486 = 18573,5 \text{ грн.}$$

Антивірус:

$$К = 175 + 569 = 744 \text{ грн.}$$

Загальні затрати складуть 42955,5 грн.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;

- витрати на резервне копіювання;
- витрати на замок на серверну;
- витрати на ліцензію фаєрволу;
- витрати на блок безперебійного живлення;
- витрати на облік носіїв інформації;

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА}$ = 175 грн/год.

Час на резервного копіювання займе 0,5 год/день.

$$С = ТС* Ф = 175*0,5*250 = 21875 \text{ грн.}$$

Час на підтримку фаєрволу займе 0,5 год/тиждень, затрати:

$$С = ТС* Ф = 175*0,5*50 = 4375 \text{ грн.}$$

Час на підтримку антивірусу займе 0,5 год/тиждень, затрати:

$$С = ТС* Ф = 175*0,5*50 = 4375 \text{ грн}$$

Час на створення журналу обліку носіїв займе 1 год/тиждень, затрати:

$$С = ТС* Ф = 175*1*50 = 8750 \text{ грн.}$$

Затрати на продовження ліцензії антивірусу складають 569 грн.

Затрати на продовження ліцензії фаєрволу складають 6500 грн.

Значення загальних річних поточних витрат складає:

$$C = 21875 + 4375 + 4375 + 8750 + 569 + 6500 = 46444 \text{ грн.}$$

3.4 Оцінка можливого збитку від порушення інформаційної безпеки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

3.5 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

–час простою внаслідок поломки, t_n (в годинах), $t_n = 4$ год;

–час відновлення після поломки, $t_в$ (в годинах), $t_в = 2$ год;

–час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 2$ год;

–заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), $Z_0 = 21000$ грн.;

–заробітна плата співробітників, Z_c (грн. в місяць з податками), $Z_c = 20000$ грн.;

–кількість обслуговуючого персоналу, N_0, $N_0 = 2$;

–число співробітників, N_c, N_c = 20;

–прибуток , O (грн. на рік), O = 12000000 грн.;

–вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 4000 грн;

–число зламаного обладнання, I, I = 2;

–число поломок на рік, n, n = 5.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum_{N_c} Z_c}{160} \cdot t_п, \text{ грн.}, \quad (3.4)$$

де місячний фонд робочого часу складає 160 годин.

Підставивши вихідні дані отримаємо:

$$П_П = (20*18000/160)*4 = 9000 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.12),

$П_{пв}$ – вартість відновлення обладнання (формула 3.13).

$$П_{ви} = \frac{\sum_{N_c} Z_c}{160} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum_{N_o} Z_o}{160} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ВИ} = (20*18000/160)*2 = 4500 \text{ грн.}$$

$$П_{ПВ} = (3*21000/160)*2 = 787{,}5 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 4000 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 4500 + 787,5 + 4000 = 9287,5 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.9)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

$$V = (12000000/2080)*(4+2+2) = 46153,85 \text{ грн.}$$

$$U = 9000 + 9287,5 + 46153,85 = 64441,35 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.10)$$

$$ОУ = 5 * 2 * 64441,35 = 644413,5 \text{ грн.}$$

3.6 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \quad (3.11)$$

де $ОУ$– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 644413,5 * 0,4 – 46444 = 211321,4 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.12)$$

де E – загальний ефект від впровадження системи захисту, грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Підставивши відповідні значення, маємо:

$$\text{ROSI} = 211321,4 / 42955,5 = 4,92$$

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.20:

$$ROSI > (N_{деп} – N_{інф})/100) \qquad (3.13)$$

де $N_{деп}$ – річна депозитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Підставивши відповідні значення, маємо:

$$\text{ROSI} > (17 – 21,8)/100),$$

$$4,92 > -0,048$$

Отже, проєкт є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 1 / 4{,}92 = 0{,}2 \text{ року.}$$

3.8 Висновок

Розрахувавши збитки від реалізації можливих несправностей, які склали 644413,5 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 46444 грн., та витратами на розробку моделі 42955,5 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом, термін окупності системи безпеки становить 0,2 року (приблизно 2,5 місяці). Для подальшого функціонування підприємства впровадження даних заходів є обґрунтованим і доцільним.

ВИСНОВКИ

В даній кваліфікаційній роботі було виконано аналіз внутрішніх загроз та їх джерел, розроблено модель загроз та порушника, проведено аналіз основних методів захисту від антропогенних загроз та розроблено комплекс методів зі зниження внутрішніх загроз та підвищення рівня інформаційної безпеки підприємства.

У економічному розділі був виконаний розрахунок капітальних витрат на проєктування та впровадження комплексу методів протидії загрозам ІБ комерційного підприємства. Також був проведений розрахунок річних експлуатаційних витрат на функціонування комплексу методів. Ефективність впроваджених методик доведена розрахунками.

Наукова новизна полягає у розробці комплексу методів протидії внутрішнім загрозам ІБ на комерційному підприємстві.

Практичне значення роботи полягає у підвищенні рівня інформаційної безпеки комерційного підприємства шляхом впровадження комплексу методів протидії внутрішнім загрозам ІБ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс] - Режим доступу: www/ URL: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf.

2 Закон України «Про інформацію» [Електронний ресурс] / Київ, Верховна Рада України - Режим доступу : www/ URL: http://zakon5.rada.gov.ua/laws/show/2657-12 - 21.05.2015 г. - Загл. з екрану.

3 Загрози інформаційній безпеці у банківських установах [Електронний ресурс] - Режим доступу: www/ URL: http://essuir.sumdu.edu.ua/bitstream/123456789/34067/1/Borysova_banking%20establishment.pdf.

4 Методичні вказівки до виконання економічної частини дипломного проєкту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: О.Г. Вагонова, Ю.О. Волотковська, Н.М. Романюк. – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

5 Носенко К.М. Огляд систем виявлення атак в мережевому трафіку / К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління». – 2014. – № 1(24). – С. 67-75.

6 Павлов І.М. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем / І.М. Павлов, С.В. Толюпа, В.І. Ніщенко // Сучасний захист інформації. – №4. – 2014. – С. 44-52.

7 Міжнародний стандарт IEC 31000:2010 «Менеджмент ризику. Принципи та керівництво» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=51073

8 Risk Identification and Analysis – GIAC [Електронний ресурс] - Режим доступу: www/ URL: http://www.nap.edu/read/11183/chapter/6

9 Методика визначення ефективності капітальних вкладень [Електронний ресурс]. – Режим доступу : www/ URL:

http://pidruchniki.com/1541010436255/ekonomika/metodika_viznachennya_efektivnosti_kapitalnih_vkladen

10 Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах / Т.І. Зоріна // Вісник східноукраїнського національного університету ім. В. Даля. – № 15 (204), ч.1. – 2013. – С. 48-54.

11 Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [Електронний ресурс]. – Режим доступу: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

12 Визначення експлуатаційних витрат та результатів проєктування [Електронний ресурс]. – Режим доступу : www/ URL: http://pidruchniki.com/10480304/ekonomika/viznachennya_ekspluatatsiynih_vitrat_rezultativ_proektuvannya

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	2	
5	А4	Розділ 1	39	
6	А4	Розділ 2	39	
7	А4	Розділ 3	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Пугач.ppt

2 Кваліфікаційна робота_Пугач.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-1 Пугача Д.В.

на тему: «Обґрунтування методів протидії внутрішнім загрозам безпеці інформації підприємства»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 104 сторінках.

Тема кваліфікаційної роботи є актуальною, тому що кількість внутрішніх загроз інформаційній безпеці з боку персоналу значно перевищує кількість зовнішніх загроз, і вони наносять не тільки фінансовий збиток, але й серйозний вплив на репутацію підприємства.

У першому розділі кваліфікаційної роботи проаналізовані внутрішні антропогенні загрози ІБ підприємства та їх джерела, виконана класифікація порушників та побудовані моделі загроз та порушника ІБ комерційного підприємства, а також сформульовані основні задачі кваліфікаційної роботи.

У спеціальній частині проаналізовано існуючі методи протидії внутрішнім антропогенним загрозам інформаційної безпеки та розроблено комплекс таких методів для комерційного підприємства.

Практичне значення результатів даної кваліфікаційної роботи полягає у підвищенні рівня ІБ на комерційному підприємстві при впровадженні розробленого комплексу методів протидії внутрішнім антропогенним загрозам інформаційної безпеки на цьому підприємстві.

Перевагами кваліфікаційної роботи є розробка комплексу методів протидії внутрішнім загрозам інформаційної безпеки, який дозволить знизити загальний рівень ризиків ІБ за рахунок зниження ризиків реалізації загроз, пов'язаних з персоналом, які займають значне місце серед всього переліку загроз ІБ на підприємстві.

Серед недоліків роботи слід відзначити: недостатньо глибоке опрацювання теми; незначні відхилення від стандартів при оформленні; недостатньо деталізований аналіз методів протидії внутрішнім антропогенним загрозам інформаційної безпеки.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Пугач Д.В. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
д.т.н., проф. **Корнієнко В.І.**