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 бакалавра

студентки *Бєлоусової Катерини Антонівни*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к. е. н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студентці ***Бєлоусовій К.А.*** **академічної групи** ***125-20-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

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

на тему ***Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро»***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

Розділ	Зміст	Термін виконання
1	Стан питання, аналіз нормативно-правової бази, постановка задачі.	26.05.2024
2	Розробка політики безпеки інформації, категоріювання, визначення профілю захищеності, аналіз загроз.	19.06.2024
3	Розрахунок річних витрат на розробку політики безпеки, оцінка величини збитку. Розрахунок ефективності запропонованої політики безпеки інформації.	26.06.2024

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Бєлоусова К.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 99 сторінок, 5 рисунків, 5 таблиць, 5 додатків, 18 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи.

Мета кваліфікаційної роботи: підвищення рівня інформаційної безпеки ІКС ТОВ «Фінанс-Дніпро».

У вступі та в першому розділі кваліфікаційної роботи визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в ІКС, огляд основних проблем захисту інформації та шляхів їх вирішення. Виконано аналіз нормативно-правової бази у сфері ЗІ та постановка задачі.

У спеціальній частині кваліфікаційної роботи наведено загальні відомості про підприємство, питання інформаційної безпеки фінансової компанії, категоріювання інформаційних ресурсів та структура інформаційно-комунікаційної системи. Також наведено визначення профілю захищеності ІКС, аналіз загроз та їх джерел, класифікація загроз інформаційним ресурсам, моделі загроз і порушника. Розроблено та наведено політику забезпечення інформаційної безпеки та виконано аналіз ризиків після впровадження політики безпеки.

У економічній частині було розраховані витрати на розробку та впровадження політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків ІБ завдяки впровадженню політики забезпечення інформаційної безпеки.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ.

ABSTRACT

The explanatory note consists of 99 pages, 5 images, 5 tables, 5 appendices, 18 sources.

Object of development: the information security policy of the information and communication system.

The purpose of the qualification work: to increase the level of information security of the ICS of the "Finance-Dnipro" LLC.

In the introduction and in the first section of the qualification work, the relevance of the work is determined, the state of the issue of information security in ICS is analyzed, a review of the main problems of information security and ways of their solution was made. An analysis of the regulatory framework in the sphere of IS and the formulation of the task was performed.

In the special part of the qualification work general information about the enterprise, issues of information security of the financial company, the categorization of information resources and the structure of the information and telecommunication system were presented. In addition, definitions of ICS security profiles, threat analysis and their sources, classification of threats to information resources, threats and the perpetrator are given. The information security policy has been developed and presented and the risk analysis has been performed after the implementation of the security policy.

In the economic part, the costs for the development and implementation of the information security policy of the information and communication system of "Finance-Dnipro" LLC were calculated.

The practical value of the qualification work is to increase the level of information security and reduce the risks of information security due to the implementation of information security policy.

INFORMATION SAFETY, MODEL OF THREATS, INTRUDER MODEL, SECURITY INFORMATION POLICY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

ЗЗІ – засіб захисту інформації;

ЗКЗІ – засіб криптографічного захисту інформації;

ЗОТ – засіб обчислювальної техніки;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІСПД – інформаційна система персональних даних;

ІТ – інформаційні технології;

ІКС – інформаційно-комунікаційна система;

КІ – конфіденційна інформація;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

КСЗвКІ – комплексна система захисту від витоків конфіденційної інформації;

НСД – несанкціонований доступ;

ПБ – політика безпеки;

ПД – персональні дані;

ПЗ – програмне забезпечення;

СЗІ – служба захисту інформації;

СУБД – система управління базами даних.

ЗМІСТ

ВСТУП

Застосування обчислювальних засобів у системі управління державних і комерційних структур вимагає наявності потужних систем обробки і передачі даних. Вирішення цього завдання призвело до створення єдиної інфраструктури. Її використання дозволило людям, що мають комп'ютер і вихід до глобальної мережі Інтернет, отримати доступ до інформації найбільших бібліотек і баз даних світу, оперативно виконувати складні розрахунки, швидко обмінюватися інформацією з іншими респондентами мережі незалежно від відстані та країни проживання. Але такі системи спричинили низку проблем, одна з яких - безпека обробки і передачі інформації. В наш час над проблемою захищеності інформації працює велика кількість фахівців практично в усіх економічно розвинених країнах світу. Можна сказати, що інформаційна безпека сформувалася в окрему дисципліну. Однак, незважаючи на зусилля численних організацій, що займаються захистом інформації, забезпечення інформаційної безпеки продовжує залишатися надзвичайно гострою проблемою.

З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних тощо.

З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи якісно нових загроз, збільшення числа зловмисників, які мають потенційну можливість впливати на систему.

Для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів: використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії тощо. Комплексний характер захисту виникає з комплексних дій зловмисників, які прагнуть будь-якими засобами здобути важливу для них інформацію.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Об’єктами захисту в системі є інформація, що обробляється в ній, та програмно-технічне забезпечення, яке призначене для обробки цієї інформації.

Для забезпечення захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в і інформаційно-комунікаційних системах повинні обов’язково виконуватися наступні процедури:

- автентифікація – процедура встановлення належності користувачеві інформації в системі (далі – користувач) пред’явленого ним ідентифікатора;
- ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред’явленого ідентифікатора повинні блокуватися.

Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних визначається законодавством [1].

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації [2].

Комплексність підходу до захисту інформації є рішення в рамках єдиної концепції двох або більшої кількості різнопланових завдань.

Сучасна система захисту інформації повинна включати структурну, функціональну і часову комплексність. Структурна комплексність припускає забезпечення необхідного рівня захисту у всіх елементах системи обробки інформації.

Функціональна комплексність означає, що методи захисту повинні бути направлені на всі виконувані функції системи обробки інформації.

Часова комплексність припускає безперервність здійснення заходів щодо захисту інформації як в процесі безпосередньої її обробки, так і на всіх етапах життєвого циклу об'єкту обробки інформації [3].

Склад комплексної системи захисту визначається на основі вивчення усіх інформаційних процесів та потоків системи телекомунікацій і, як наслідок, розробці такої моделі загроз, щоб забезпечити мінімізацію втрат. На основі моделі загроз має бути розроблена та запроваджена концепція та політика інформаційної безпеки органів державної влади та створена комплексна система захисту інформації, які мають забезпечувати такі функції:

- конфіденційність інформації – властивість інформації, коли неавторизовані особи, які не мають доступу до інформації, не можуть розкрити зміст цієї інформації;
- цілісність інформації – властивість інформації, яка полягає в тому, що вона не може бути змінена навмисно або випадково користувачем чи процесом. А також властивість, яка полягає в тому, що жодний з її компонентів не може бути усунений, модифікований або доданий з порушенням політики безпеки;
- доступність – властивість ресурсу системи (інформації), яка полягає в тому, що авторизований користувач може отримати доступ до ресурсу тільки із заданим змістом та якістю;
- спостережливість – властивість ресурсу інформаційної технології, що дозволяє реєструвати всі дії користувачів, здійснювати доступ поіменно, відповідно до ідентифікаторів та повноважень, а також реагувати на ці дії з метою мінімізації можливих втрат в системі, що здійснюється також за рахунок застосування криптографічного захисту інформації (КЗІ).

До складу КЗЗІ входять заходи і засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоків технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань, акустоелектричних і інших каналів;

– несанкціонованих дій і несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування помилковій інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів і т.п.;

– спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної інформаційної системи склад, структура і вимоги до КЗЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи (АС) і умовами її експлуатації.

Однією з вимог забезпечення захисту інформації в АС є те, що обробка конфіденційної інформації повинна здійснюватися з використанням захищеної технології, яка містить програмно-технічні засоби захисту і організаційні заходи, які забезпечують виконання загальних вимог з захисту інформації. Загальні вимоги передбачають:

– наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці; у разі потреби можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів і іншими класифікаційними ознаками;

– наявність відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації;

– створення КСЗІ, яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, направлених на забезпечення захисту інформації під час функціонування АС;

– розробку плану захисту інформації в АС;

– наявність атестату відповідності КСЗІ в АС нормативним документам із захисту інформації;

– можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів і декількох класифікаційних рівнів інформації;

– обов'язковість реєстрації в АС всіх користувачів і їх дій щодо конфіденційної інформації;

– можливість надання користувачам тільки за умови службової необхідності санкціонованого і контрольованого доступу до конфіденційної інформації, яка обробляється в АС;

– заборона несанкціонованій і неконтрольованій модифікації конфіденційної інформації в АС;

– здійснення за допомогою СЗІ обліку вихідних даних, отриманих під час рішення функціональної задачі, у формі віддрукованих

– документів, які містять конфіденційну інформацію, відповідно до керівних документів;

– заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації, в електронному вигляді;

– забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації, в електронному вигляді;

– можливість здійснення однозначної ідентифікації і аутентифікації кожного зареєстрованого користувача;

– забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

Приведені вимоги є базовими і застосовуються при захисті інформації від несанкціонованого доступу (НСД) у всіх типах АС [4].

Отже, зважаючи на викладене вище, доступ до інформації у суб'єктивному розумінні – це гарантована державою можливість фізичних, юридичних осіб і державних органів вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законних інтересів інших громадян, прав та інтересів юридичних осіб [5].

Провівши оцінку необхідності захисту інформації від НСД, можна судити про складність КСЗІ, оцінити вірогідність погроз, що проявляються, на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів.

Спираючись на вимоги із захисту інформації від НСД [4], можна привести основні принципи захисних заходів від НСД в АС.

Принцип перший – обґрунтованість доступу. Даний принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню "форму допуску" для отримання інформації потрібного ним рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. У сфері автоматизованої обробки інформації як користувачі

можуть виступати активні програми і процеси, а також носії інформації різного ступеня складності. Тоді система доступу припускає визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій.

Принцип другий – достатня глибина контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип третій – розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

Принцип четвертий – чистота повторно використовуваних ресурсів. Даний принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні бо звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип п’ятий – персональна відповідальність. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, а також за випадкові або умисні дії, які можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її спотворенню або знищенню, або виключенню можливості доступу до такої інформації законних користувачів.

Принцип шостий – цілісності засобів захисту. Даний принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі [6].

При розгляді питань безпеки інформації в АС завжди говорять про наявність “бажаних” станів системи. Ці стани описують “захищеність” системи. Поняття “захищеності” принципово не відрізняється від інших властивостей технічної системи, наприклад “надійної роботи”. Особливістю поняття “захищеність” є його тісний зв’язок з поняттям “загроза” (те, що може бути причиною виведення системи із захищеного стану). Виділяються три компоненти, що пов’язані з порушенням безпеки системи:

- “загроза” – зовнішнє відносно системи джерело порушення властивості «захищеність»;
- “об’єкт атаки” – частина системи, на яку діє загроза;
- “канал дії” – середовище перенесення зловмисної дії.

Інтегральною характеристикою, що об’єднує всі ці компоненти, є політика безпеки – якісний/якісно-кількісний вираз властивостей захищеності в термінах, що представляють систему. Опис політики безпеки повинен включати і враховувати властивості загрози, об'єкта атаки та каналу дії.

За означенням [7, 8], під політикою безпеки інформації розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін “політика безпеки” може бути застосований до організації, автоматизованої системи, операційної системи, послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації. Для кожної автоматизованої системи політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама автоматизована система може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій автоматизованій системі буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

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

Методи мають такий зміст:

- перешкоди – фізичної перешкоди доступу зловмиснику до інформації, що захищається.
- керування доступом – захист інформації шляхом регулювання використання всіх ресурсів комп'ютерної інформаційної системи.
- маскування – захисту інформації шляхом її криптографічного закриття.
- регламентація – захист інформації, що створює такі умови автоматизованої обробки, зберігання й передачі інформації, що захищається, за яких можливості несанкціонованого доступу до неї зводилися б до мінімуму.
- примушення – захист, за якого користувачі й персонал системи змушено дотримувати правил обробки, передачі й використання інформації, що захищається, під загрозою матеріальної, адміністративної або карної відповідальності.
- спонукання – захист, який спонукує користувача й персонал системи не порушувати встановлений порядок за рахунок дотримання моральних і етичних норм, які склалися.

Розглянуті методи забезпечення безпеки реалізуються на практиці шляхом застосування різних засобів захисту, таких, як технічні, програмні, організаційні, законодавчі й морально-етичні. До основних засобів захисту, які використовуються для створення механізму забезпечення безпеки, належать такі:

- Технічні засоби реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Уся сукупність технічних засобів поділяється на апаратні й фізичні.
- Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.
- Організаційні засоби – це організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення та експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їх життєвого циклу.
- Морально-етичні засоби реалізуються у вигляді різних норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи.
- Законодавчі засоби захисту визначаються нормативно-правовими актами, якими регламентуються норми та правила користування, обробки й передачі інформації обмеженого доступу. За порушення цих правил встановлюються відповідальність.

Захист інформації в системі обробки інформації повинен ґрунтуватися на наступних основних принципах:

- системності;
- комплексності;
- безперервності захисту;
- розумної достатності;
- гнучкості керування й застосування;
- відкритості алгоритмів і механізмів захисту;
- простоти застосування захисних заходів і засобів.

Системний підхід до захисту комп'ютерних систем припускає необхідність обліку всіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння й вирішення проблеми забезпечення

безпеки. При створенні системи захисту необхідно враховувати всі слабкі, найбільш уразливі місця системи обробки інформації, а також характер, можливі об'єкти й напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи й несанкціонованого доступу до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення й несанкціонованого доступу до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки [9].

Відповідно до п. 6.1.2.9 НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», за результатами обстеження середовищ функціонування ІКС затверджується перелік об’єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об’єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту[10].

Відповідно до розділу 4 «Загрози для інформації в АС» НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з

метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої і відмови у роботі обладнання та технічних засобів АС;
- наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) АС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);
- наслідки некомпетентного застосування засобів захисту;
- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);
- порушення режимів функціонування АС (обладнання і ПЗ);
- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних

випромінювань і наводів, акустоелектричних перетворень інформаційних сигналів;

- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);
- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);
- можливі способи здійснення загроз.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його

практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-

апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;
- володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

- використовують виключно агентурні методи одержання відомостей;
- використовують пасивні технічні засоби перехоплення інформаційних сигналів;
- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;
- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

- без одержання доступу на контрольовану територію організації (АС);
- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;
- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;
- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Загрози для системи електронного документообігу досить стандартні і можуть бути класифіковані в такий спосіб.

Загроза цілісності - пошкодження і знищення інформації, спотворення інформації - як й не навмисне в разі помилок і збоїв, так і зловмисне.

Загроза конфіденційності - це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміни маршрутів слідування.

Загроза працездатності системи - всілякі загрози, реалізація яких призведе до порушення або припинення роботи системи; сюди входять як умисні атаки, так і помилки користувачів, а також збої в обладнанні та програмному забезпеченні.

Джерел загроз в нашому небезпечному світі не мало: це і низький рівень кваліфікації деяких системних адміністраторів, і техніка, яка має властивість ламатися в самий не підходящий момент, і форс-мажорні обставини, які рідко, але все ж відбуваються. І навіть якщо сервери не постраждають від пожежі, що сталася в будівлі, будьте впевнені - їх неодмінно заллють водою пожежники, що приїдуть гасити пожежу.

В цілому ж, можна виділити кілька основних груп зловмисників: легальні користувачі системи, адміністративний ІТ-персонал, зовнішні зловмисники.

Спектр можливих злодіянь легальних користувачів досить широкий - від скріпок в апаратних частинах системи до умисної крадіжки інформації з корисливою метою. Можлива реалізація погроз в різних класах: загрози конфіденційності, загрози цілісності.

Користувач системи - це потенційний зловмисник, він може свідомо чи несвідомо порушити конфіденційність інформації.

Особлива група - це адміністративний ІТ-персонал або персонал служби ІТ-безпеки. Ця група, як правило, має необмежені повноваження і доступ до сховищ даних, тому до неї треба поставитися з особливою увагою. Вони не тільки мають великі повноваження, але і найбільш кваліфіковані в питаннях безпеки та інформаційних можливостей. Не так важливий мотив цих злочинів, чи був це

корисливий умисел або помилка, від якої ніхто не застрахований, результат один - інформація або загубилася, або набула розголосу. Згідно з численними дослідженнями, від 70 до 80% втрат від злочинів припадають на атаки зсередини.

Набір зовнішніх зловмисників суто індивідуальний. Це можуть бути і конкуренти, і партнери, і навіть клієнти.

Так, за даними цих досліджень, збиток від необережних і неправомірних дій співробітників в кілька разів перевищує обсяг завданої шкоди від дій вірусів і хакерських атак. І це незважаючи на те, що, згідно зі звітом Computer Crime and Security Survey, кількість інцидентів з вини зовнішніх і внутрішніх порушників приблизно однакова.

Цей результат цілком закономірний. Хоча зовнішніх зловмисників дійсно значно більше, але, по-перше, вони менше мотивовані. Відкинувши мале число найманих професіоналів, ми отримаємо величезну масу школярів і студентів, які просто з цікавості пробують викачані утиліти, не переслідуючи якихось певних цілей і часом навіть не знаючи, що робити з отриманою інформацією. По-друге, їм протистоять потужні і зрілі технології периметрового захисту, тобто зовнішньому зловмисникові потрібна велика кваліфікація, щоб подолати всі ці бар'єри.

У внутрішнього порушника, особливо якщо його дії свідомі, а не є помилкою, стимулів може бути більше: від банальної образи до матеріальної вигоди в разі підкупу з боку конкурентів. А можливостей - не в приклад більше. Він вже є легальним користувачем мережі, має доступ в тому числі і до конфіденційних ресурсів організації, може користуватися корпоративними додатками і робочою в них даними на законних підставах.

Будувати систему захисту від зовнішнього ворога набагато простіше. Крім того, займаючись побудовою цього рубежу оборони, ми не впливаємо на працездатність нашої інформаційної системи. Всі бізнес-додатки працюють нормально, ціна помилки адміністрування - за великим рахунком, лише короткочасна відсутність доступу в Інтернет.

Захист від внутрішнього ворога складніше і вимагає великих зусиль. Вона складається з забезпечення безпеки самих додатків і грамотного адміністрування, яке перш за все має на увазі під собою наявність чітких привілеїв співробітників компанії на доступ до ресурсів інформаційної системи (в сформульованому вигляді - це політика безпеки).

Дані привілеї повинні бути достатні для забезпечення нормальної роботи і в той же час мінімальні з точки зору доступу і можливості маніпулювання інформацією.

І часто при появі такого завдання, проблем бачиться більше, ніж рішень.

Перераховувати їх можна довго, проблеми чіпляються один за одного. Наприклад, незахищеність ряду додатків змушує нас використовувати додаткові засоби захисту. Однак ці кошти потрібно не тільки придбати і правильно впровадити, але і супроводжувати. І якщо з процесом впровадження зазвичай проблем не виникає (справляються або штатні фахівці, або найняті консалтингові компанії), проблеми виникають потім, в процесі адміністрування системи. Адже управління засобами захисту здійснюється найчастіше окремо від вже використовуваних в компанії, в тому числі і штатних механізмів. А це означає, що рано чи пізно (в залежності від масштабу інформаційної системи) настає момент, коли налаштування системи захисту і налаштування штатних механізмів починають розходитися.

Розбіжність відбувається ще й тому, що відсутні процедури, які регламентують внесення змін до інформаційної системи і в настройки механізмів безпеки. А внести зміни в реальні настройки системи набагато простіше і швидше, ніж оформити їх. Та й набрати номер адміністратора або забігти до нього по шляху простіше, ніж написати заявку. В результаті - в заданий момент часу практично неможливо відтворити реальну картину того, що відбувається, неможливо відповісти на питання: "Чому до певного ресурсу мають доступ ці користувачі та групи користувачів?". Втрачається історія всіх вироблених змін, і вже не можна визначити - правильно чи неправильно сконфігуровані, нехай навіть найдосконаліші, механізми захисту.

Ціна помилки за неправильне адміністрування вимірюється або наданням користувачеві необґрунтовано великих компетенцій (а так само - створенням величезної уразливості в інформаційній системі), або обмеженням необхідного йому в якийсь момент доступу (при цьому, можливо, зривається виконання завдань організації).

Але вирішити цю проблему тільки організаційними методами не вдається. Виною всьому нестача і недостатня кваліфікація адміністраторів, перевантаженість фахівців і, найголовніше - відсутність механізмів перевірки фактичного стану справ. Все це призводить до того, що навіть при наявності деякої формальної системи управління контроль над інформаційною системою і питаннями безпеки даних в ній все одно втрачається.

До речі, часом просте збільшення штату IT-підрозділу і підрозділу інформаційної безпеки лише поглиблюють проблеми. У цих структурах, в свою чергу, з'являються підрозділи, що спеціалізуються на окремих підсистемах, взаємодія структур порушується ще більше.

Усвідомлюючи всю складність вирішення завдання, а так само відсутність інструментів, фахівці з інформаційної безпеки часто зволікають з вирішенням цієї проблеми.

1.2 Аналіз нормативно-правової бази у сфері ЗІ

Відповідно до мети кваліфікаційної роботи та згідно завдання, в роботі розглядаються питання управління інформаційною безпекою в ІКС організації, забезпечення відповідного рівня інформаційної безпеки в ІКС та питання політики безпеки.

В процесі виконання кваліфікаційної роботи було розглянуто такі основні нормативно-правової документи в сфері захисту інформації:

Закони України:

- Закон України "Про інформацію"
- Закон України "Про телекомунікації"

– Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"

– Закон України «Про захист персональних даних»

Постанови КМУ:

– Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

Нормативні документи в галузі технічного захисту інформації та стосовно створення і функціонування КСЗІ:

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
- НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
- НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Міжнародні стандарти ISO/IEC серії 2700х:

- ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management

1.3 Постановка задачі

Для успішного виконання кваліфікаційної роботи та для досягнення поставленої мети були поставлені наступні задачі:

- Виконати обстеження ОІД.
- Виконати аналіз ризиків.
- Виконати обґрунтування необхідності створення КСЗІ.
- Виконати розробку політики безпеки.
- Виконати аналіз ризиків після впровадження політики безпеки.
- Виконати розрахунок трудомісткості та затрат на створення та впровадження політики безпеки.

1.4 Висновки до Розділу 1

В першому розділі кваліфікаційної роботи визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в ІКС, огляд основних проблем захисту інформації та шляхів їх вирішення. Виконано аналіз нормативно-правової бази в сфері ЗІ та постановка задачі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Повна назва - Товариство з обмеженою відповідальністю «ФІНАНС-ДНІПРО».

Фінансова компанія «Фінанс-Дніпро» зареєстрована 25.06.2015 року.

Компанія «Фінанс-Дніпро» має право надавати наступні фінансові послуги:

– Залучення фінансових активів юридичних осіб із зобов'язанням щодо наступного їх повернення;

– Надання послуг з факторингу;

– Надання поруки;

– Надання гарантій;

– Надання позик;

– Надання послуг з фінансового лізингу;

– Надання фінансових кредитів за рахунок власних коштів;

– Переказ коштів у національній валюті без відкриття рахунків (згідно ліцензії НБУ).

Характеристика об'єкта:

Офісна споруда: офіс ТОВ «Фінанс-Дніпро» знаходиться на другому поверсі триповерхової офісної будівлі за адресою: вул. Мануйлівська, 37, м. Дніпро, 49000, Україна. На цьому ж поверсі та на інших поверхах також знаходяться офіси.

Ситуаційний план наведено на рисунку 2.1.

Фізичні характеристики будівлі і приміщень:

- зовнішні стіни а також стіна, що граничить з коридором – біла цегла, завтовшки 500мм;
- внутрішні стіни – біла цегла, завтовшки 250мм;
- дах будівлі плоский, викладений руберойдом. Вхід на дах здійснюється через пожежні сходи або горище;
- підлога – залізобетонні плити перекриття, завтовшки 220мм, вкриті ламінатом;

– двері головного входу мають розміри 1200 мм * 2000мм, виконані зі звареної листової сталі, оздоблені 2 замками з різними ключами; міжкімнатні двері мають розміри 1200 мм * 2000мм, виконані з ламінованого МДФ;
– на об’єкті металопластикових вікон, різних розмірів з 3-камерним скло-пакетом;

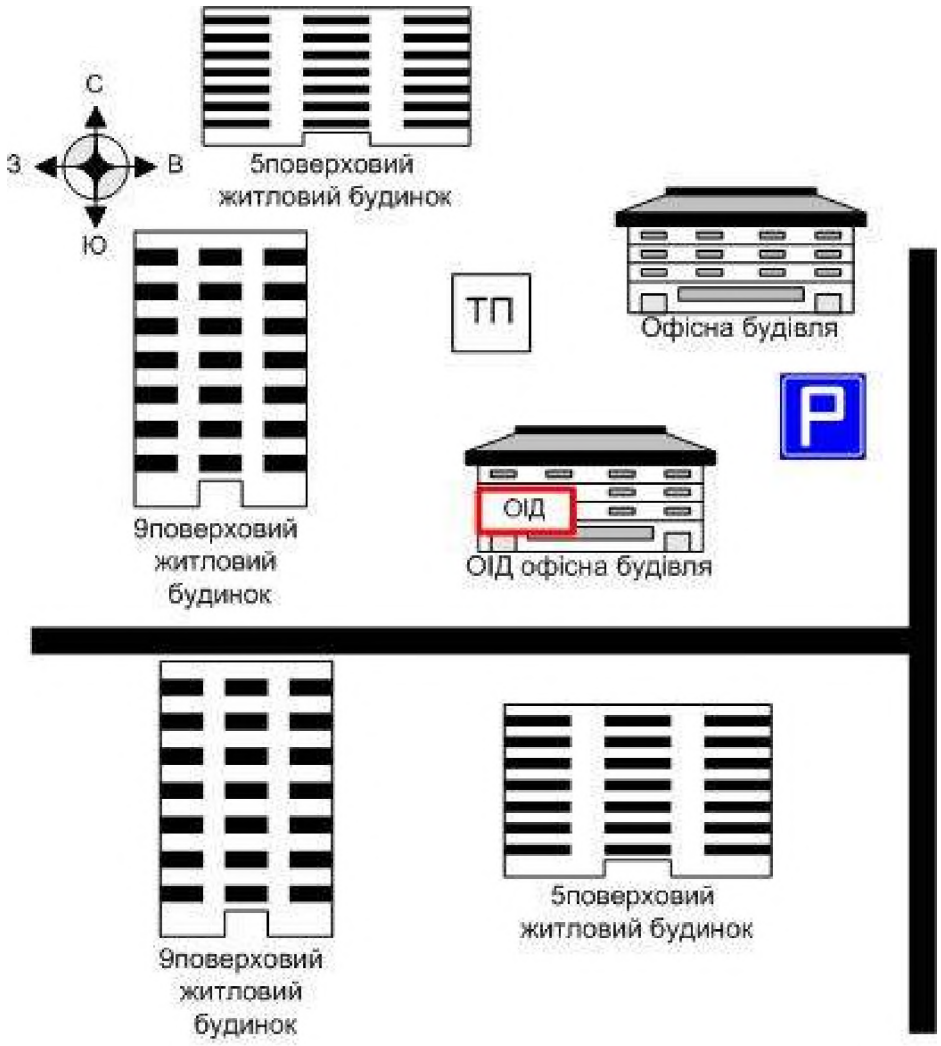

Рисунок 2.1 – Ситуаційний план офісу ТОВ «Фінанс-Дніпро»

Територія, навколо будівлі - відкрита, не обмежена забором, перебування транспорту на цій території не обмежено та не контролюється;

– територію навколо будівлі впорядковано, вона має асфальтове покриття;
– навколо будівлі розташовані багатоповерхові будинки, дитячий майданчик;

Перелік систем, що функціонують в приміщенні:

- приміщення підприємства обладнано системами електропостачання, освітлення, телефонного зв'язку, опалення;
- живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж;
- телефонний зв'язок та Інтернет.

Навколо офісу знаходяться наступні об'єкти:

- з північної сторони розміщена трансформаторна підстанція;
- з північно-західної знаходиться п'ятиповерховий будинок та дитячий майданчик;
- з західної сторони – місце неконтрольованого перебування транспортних засобів та дев'ятиповерховий будинок;
- в південно-західній стороні також знаходиться місце неконтрольованого перебування транспортних засобів та дев'ятиповерховий будинок;
- з південної сторони розташовано місце неконтрольованого перебування транспортних засобів та п'ятиповерховий будинок;
- з південно-східної сторони – дорога проспекту Манулйлівського та п'ятиповерховий будинок;
- на східній стороні - місце неконтрольованого перебування транспортних засобів;
- з північно-східної сторони розташовано місце неконтрольованого перебування транспортних засобів та інша офісна споруда.

Форма власності: приватна власність.

Режим роботи офісу компанії:

Час роботи: 09.00 – 18.00

Перерва: з 13.00 до 14.00

Робочі дні: понеділок – п'ятниця.

Штат співробітників складається з 19 чоловік:

- директор – 1;

– заступник директора – 1;
– секретар – 1;
– менеджери по роботі з юридичними особами – 3;
– менеджери по роботі з фізичними особами – 4;
– юрист – 1;
– маркетологи – 2;
– бухгалтера – 3;
– системний адміністратор – 1;
– охорона – 1;
– прибиральниця – 1.

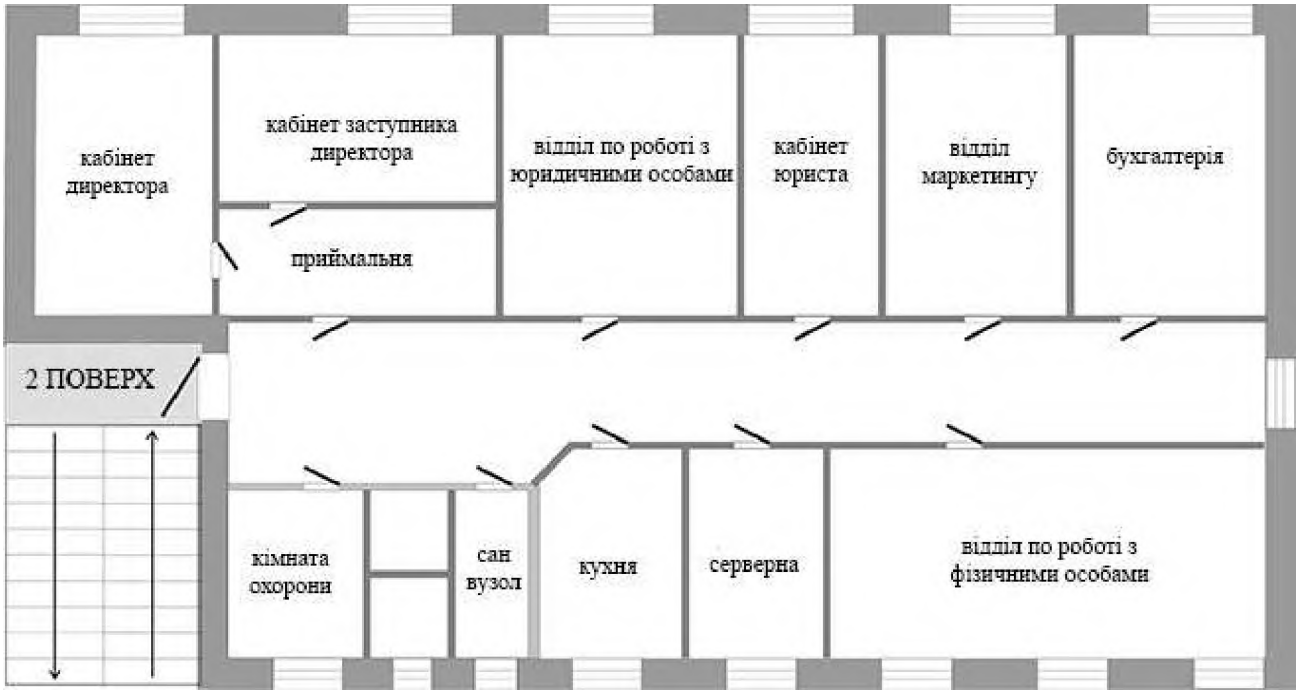

Рисунок 2.2 – План-схема офісу ТОВ «ФІНАНС-ДНІПРО»

2.2 Інформаційна безпека фінансової компанії

Інформаційна безпека фінансової компанії – це організація гарантованого захисту інформаційних ресурсів установи, відповідна професійна підготовка працівників у галузі інформаційних технологій, що забезпечує захист

інформаційних ресурсів та інформаційних потоків від несанкціонованого доступу до них.

Забезпечення інформаційної безпеки є невід'ємною складовою частиною діяльності компаній подібного типу.

Задачами системи інформаційної безпеки є:

– віднесення інформації до категорії обмеженого доступу;

– протидія витоку такої інформації;

– віднесення конфіденційної електронної мережі організації до найбільш небезпечного об'єкту для витоку інформації і з цієї точки зору приділення їй додаткової уваги;

– прогнозування, своєчасне виявлення й усунення загроз інформаційній безпеці; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню нормального функціонування і розвитку організації;

– створення механізму й умов оперативного реагування на загрози інформаційній безпеці компанії;

– ефективне припинення посягань на інформаційні ресурси на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки.

Об'єктами безпеки є:

– інформація про персонал (керівництво, відповідальні виконавці, співробітники);

– інформація щодо технологій, які використовуються компанією;

– інформаційні ресурси (інформація з обмеженим доступом, що складає комерційну таємницю, інша конфіденційна інформація, надана у виді документів і масивів незалежно від форми і виду їхнього представлення), в тому числі:

– інформація щодо діяльності та фінансового стану клієнта, що стала відома організації у процесі обслуговування;

– інформація щодо всіх операцій та фінансова звітність;

– конфіденційні електронні мережі компанії.

Стан інформаційної безпеки банку досягається організацією збору інформації про внутрішнє і зовнішнє середовище компанії, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в організації, аналітичною обробкою інформації; організацією системи інформаційного забезпечення рішень керівництва; визначенням категорій інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідних режимів діяльності; виконанням усіма працівниками компанії норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів втрати інформації та їх перетинанням.

Структурно інформаційну безпеку компаній такого типу складають:

– безпека інформаційних ресурсів;

– безпека інформаційної інфраструктури;

– безпека "інформаційного поля" компанії.

Інформаційні ресурси фінансової компанії – це взаємозв'язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація, яка належить організації. Відповідно безпека інформаційних ресурсів полягає у збереженні такої інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності).

Формування інформаційних ресурсів відбувається компанією самостійно, а також шляхом збирання і надбання документованої інформації про факти, події і обставини, які мають відношення до кредитно-фінансової сфери. З метою створення оптимальних умов для задоволення інформаційних потреб своїх структурних підрозділів, потреб своїх клієнтів і кореспондентів, а також органів державної влади, компанія отримує і використовує інформаційні системи (організаційно упорядковані масиви документів), інформаційні технології і засоби їх забезпечення. Для цього притягуються засоби обчислювальної техніки і зв'язку, які забезпечують обробку, зберігання і передачу інформації.

Безпека інформаційної інфраструктури полягає у такому стані захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних

мереж і мереж електрозв'язку організації, яка забезпечує цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює).

Основними задачами напряму безпеки інформаційних ресурсів є:

– організація і здійснення дозвільної системи допуску виконавців до роботи з документами і відомостями обмеженого доступу;

– організація зберігання і поводження з конфіденційними документами (носіями інформації);

– здійснення закритого листування і шифрованого зв'язку; організація і координація робіт по захисту інформації, що обробляється і передається засобами і системами обчислювальної техніки і зв'язку;

– забезпечення безпеки в процесі проведення конфіденційних нарад, переговорів; здійснення контролю за збереженням конфіденційних документів (носіїв інформації), за забезпеченням захисту інформації, що обробляється і передається засобами і системами обчислювальної техніки і зв'язку.

Найбільш суттєвими загрозами безпеки інформаційних ресурсів є витік або втрата таких ресурсів (зокрема відомостей, що становлять комерційну таємницю).

Основними загрозами інформаційній безпеці є:

– несприятливі події природного, техногенного і соціального характеру;

– терористи і кримінальні елементи;

– залежність від постачальників/провайдерів/партнерів/клієнтів;

– збої, відмови, руйнування / пошкодження програмних і технічних засобів;

– працівники організації, що реалізовують загрози ІБ з використанням легально наданих їм прав і повноважень (внутрішні порушники ІБ);

– працівники організації, що реалізовують загрози ІБ без легально наданих їм прав і повноважень, а також суб'єкти, що не є працівниками організації, та здійснюють спроби НСД і НРД (зовнішні порушники ІБ);

– невідповідність вимогам наглядових і регулюючих органів, чинному законодавству України.

Основними організаційно-технічними заходами щодо забезпечення інформаційної безпеки компанії є:

– постійний і всебічний аналіз інформаційної системи з метою виявлення уразливості інформаційних активів підприємства;

– своєчасне виявлення проблем, потенційно здатних вплинути на інформаційну безпеку підприємства, корегування моделей загроз і порушника;

– розробка і впровадження заходів захисту, адекватних характеру виявлених загроз, з урахуванням витрат на їх реалізацію і сумісності цих заходів з діючим технологічним процесом. При цьому заходи, що приймаються для забезпечення інформаційної безпеки, не повинні ускладнювати досягнення статутних цілей підприємства, а також підвищувати трудомісткість технологічних процесів обробки інформації і створювати додаткові складності для клієнтів;

– контроль ефективності впроваджених заходів захисту;

– персоніфікація та розподіл ролей і відповідальності між користувачами інформаційної системи компанії, виходячи з принципу персональної і одноосібної відповідальності за здійснені операції;

– принцип "чотирьох очей", коли критичні операції та дії здійснюються або підтверджуються мінімум двома уповноваженими особами;

– знання банком чи підприємством своїх клієнтів і персоналу.

Класифікація ресурсів в області діяльності інформаційної безпеки:

– інформаційні ресурси (активи): інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у т.ч. знання співробітників, партнерів, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, заархівована інформація і т.п.;

– програмне забезпечення: прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується в організації

співробітниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами і т.п.;

– фізичні ресурси (активи): співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми і т.п.), носії даних (стрічки, диски і т.п.), меблі, приміщення, виробниче обладнання, інші технічні засоби і т.п.;

– сервісні ресурси (активи): обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку і т.п.), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх співробітники), послугами яких користується банк для отримання, використання, передачі та знищення активів.

2.3 Категоріювання інформаційних ресурсів

Категоріювання інформаційних ресурсів є необхідним елементом організації робіт по забезпеченню інформаційної безпеки ІС, цілями якого є:

– створення нормативно-методичної основи для диференційованого підходу до захисту ресурсів ІС компанії (інформації, завдань, спеціалізованих АРМ, робочих станцій);

– вироблення типових рішень по організаційних заходах захисту, що приймаються, і розподілі апаратно-програмних засобів захисту для різних категорій робочих станцій ІС компанії.

Відповідно до Закону України "Про інформацію" інформація з обмеженим доступом повинна бути надійно захищена. Відповідно до законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист персональних даних" в компанії визначаються наступні категорії інформації з обмеженим доступом:

– комерційна таємниця;

– персональні дані;

– інша конфіденційна інформація.

Згідно статті 2 Закону України "Про захист персональних даних", персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

В процесі своєї діяльності компанія здійснює обробку наступних персональних даних:

– прізвище, ім'я, по батькові (зокрема колишні), стать, дата і місце народження;

– копії паспортів, паспортні дані, дані інших документів, які засвідчують особу (серія, номер, дата видачі, код підрозділу і найменування органу, що видав документ) і громадянство; (Іноземними громадянами і особами без громадянства додатково надаються дані міграційної карти і документа, підтверджуючого право іноземного громадянина на перебування (мешкання) в Україні);

– адреса місця проживання (по паспорту і фактична) і дата реєстрації за місцем проживання або по місцю перебування;

– ідентифікаційний номер платника податків (за наявності);

– номери контактних телефонів, адреса електронної пошти;

– інформація про надані банківські продукти і послуги, зокрема інформація про рахунки і операції по ним;

– інформація про платоспроможність, склад сім'ї і майнові права осіб, що виявили бажання скористатися кредитними продуктами компанії;

– зведення про трудові відносини суб'єктів персональних даних;

– відомості, що збираються в цілях виконання вимог чинного законодавства України при розгляді питань прийому на роботу, забезпечення необхідних умов роботи і професійного зростання, а також отримані в результаті здійснення трудових відносин з працівниками.

Категорії інформаційних ресурсів.

Виходячи з необхідності забезпечити різні рівні захисту різних видів інформації (що не містить відомостей, які складають державну таємницю), що зберігається і оброблюється в організації, вводяться наступні категорії інформаційних ресурсів.

Категорії конфіденційності.

"Цілком конфіденційна" – інформація, що є конфіденційною відповідно до вимог чинного законодавства, а також інформація, обмеження на розповсюдження якої введено рішеннями керівництва компанії (комерційна таємниця), розголошування якої може привести до тяжких фінансово-економічних наслідків для організації, аж до банкрутства (нанесенню тяжкого збитку життєвоважливим інтересам клієнтів, кореспондентів, партнерів або співробітників).

"Конфіденційна" – інформація, не віднесена до категорії «цілком конфіденційна», обмеження на розповсюдження якої вводяться вирішенням керівництва організації відповідно до наданих йому як власникові (уповноваженому власником особі) інформації чинним законодавством правами, розголошування якої може привести до збитків і втрати конкурентоспроможності організації (нанесенню збитку інтересам клієнтів, кореспондентів, партнерів або співробітників).

"Відкрита" – інформація, забезпечення конфіденційності (введення обмежень на розповсюдження) якої не вимагається.

Категорії цілісності.

"Висока" – до даної категорії відноситься інформація, несанкціонована модифікація (спотворення, підміна, знищення) або фальсифікація (підробка) якої може привести до нанесення значного прямого збитку організації, цілісність і автентичність (підтвердження достовірності джерела) якої повинна забезпечуватися гарантованими методами (засобами електронного цифрового підпису), відповідно до обов'язкових вимог чинного законодавства, наказів, директив і інших нормативних актів.

"Низька" – до даної категорії відноситься інформація, несанкціонована модифікація, підміна або видалення якої може привести до нанесення незначного непрямого збитку організації, її клієнтів, партнерів або співробітників, цілісність якої повинна забезпечуватися відповідно до вирішення керівництва відповідно до вимог чинного законодавства, наказів, директив і інших нормативних актів.

"Немає вимог" – до даної категорії відноситься інформація, до забезпечення цілісності (і автентичності) якої вимог не пред'являється.

Залежно від періодичності вирішення функціональних завдань і максимально допустимої затримки отримання результатів вводиться чотири необхідні категорії доступності інформації.

"Безперешкодна доступність" – доступ до інформації такої категорії повинен забезпечуватися у будь-який час (завдання вирішується постійно, затримка отримання результату не повинна перевищувати декількох секунд або хвилин).

"Висока доступність" – доступ повинен здійснюватися без істотних затримок за часом (завдання вирішується щодня, затримка отримання результату не повинна перевищувати декількох годин).

"Середня доступність" – доступ може забезпечуватися з істотними затримками за часом (завдання вирішується раз на декілька днів, затримка отримання результату не повинна перевищувати декількох днів).

"Низька доступність" – затримки за часом при доступі до завдання практично не лімітовані (завдання вирішується з періодом в декілька тижнів або місяців, допустима затримка отримання результату – декілька тижнів).

Окрім того, дуже важливо чітко визначити бізнес-процеси, які працюють з інформацією з обмеженим доступом і повинні бути захищеними.

2.4 Структура інформаційно-комунікаційної системи

Діяльність компанії підтримується інформаційною інфраструктурою, яка забезпечує реалізацію банківських технологій і може бути умовно представлена у вигляді ієрархії наступних основних рівнів:

– фізичного (лінії зв'язку, апаратні засоби та ін.);

– мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

– мережевих додаткових програм і сервісів;

– операційних систем ;

– систем управління базами даних;

– бізнес-процесів організації.

Відповідно до ієрархії рівнів інформаційна система компанії представляється системою, що має в своєму складі структурні і функціональні елементи.

До основних структурних елементів (компонентів) ІС компанії в загальному випадку можуть бути віднесені системи, зокрема, забезпечення технологічних процесів, інженерно-технічного забезпечення і так далі.

Функціональними елементами ІС компанії в загальному випадку є:

– робочі станції (зокрема мобільні, термінальні), за допомогою яких реалізуються автоматизовані робочі місця користувачів;

– сервери (файлів, баз даних, служб друку і т. п.);

– мережеві пристрої (маршрутизатори, комутатори, шлюзи і т. п.);

– термінальні пристрої (POS-термінали і т. п.);

– засоби зв'язку і передачі даних;

– засоби захисту інформації;

– канали і лінії зв'язку

ІС компанії в цілому або її частина майже завжди має статус законодавчо визначеної категорії ІС, такий як інформаційна система персональних даних,

оскільки в різних структурних елементах ІС обробляються персональні дані. Схема ІКС ТОВ «Фінанс-Дніпро» наведено на рисунку 2.3.

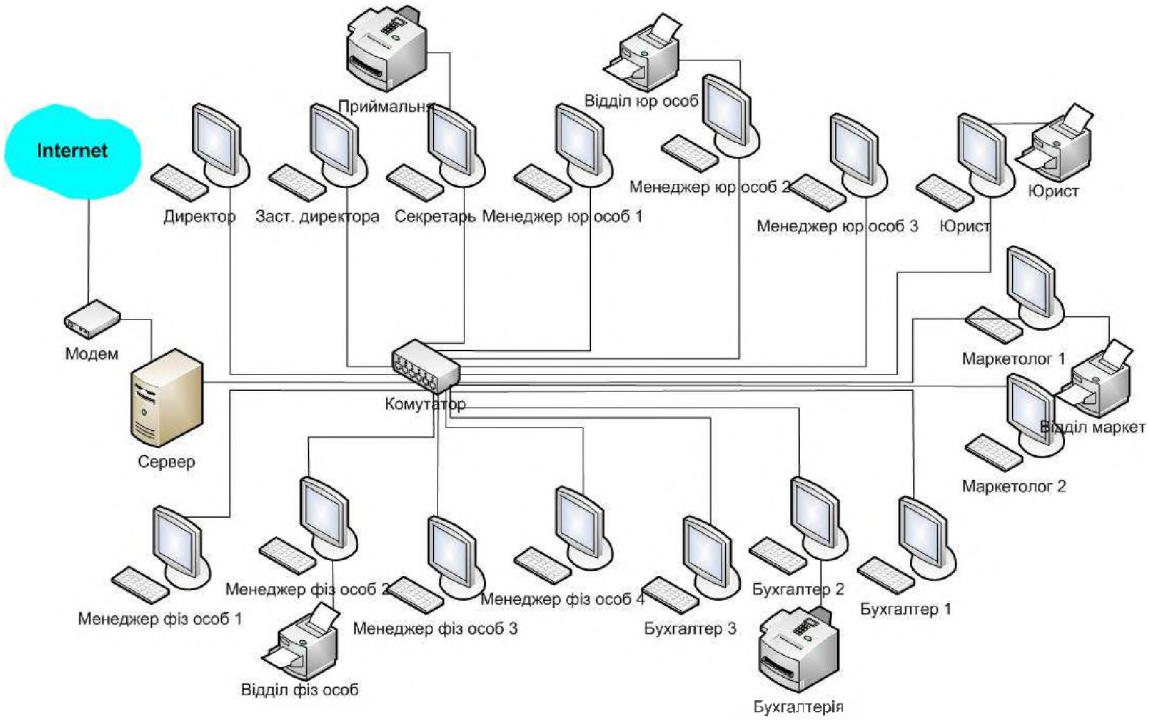

Рисунок 2.3 – Схема ІКС ТОВ «ФІНАНС-ДНІПРО»

Основними технічними засобом у приміщеннях є персональні комп'ютери. Використовується для створення документів та чернеток на електронних носіях, у тому числі, що містять ІзОД.

До складу технічних засобів, що призначені для обробки інформації в тому числі і ІзОД входять: ПК – 16шт.:

- жорсткий диск WD Black 500GB 7200rpm 16MB SATA III;
- клавіатура Logitech Keyboard K120 USB UKR OEM;
- корпус Cooler Master Elite 250 500Вт;
- материнська плата Asus P8B75-V s1155;
- модуль пам'яті Kingston DDR3-1333 2048MB PC3-10600 (2 шт.);
- маніпулятор Logitech B100, USB;
- процесор Intel Core i5-3570K 3.4 ГГц /5GT/s s1155 BOX;
- монітор 23" LG 23MP55A-P.

Сервер – 1шт.:

– жорсткий диск WD RE 1TB 7200rpm 64MB 3.5" SATA III;
– клавіатура Logitech Keyboard K120 USB UKR OEM;
– корпус RIM 2000 X07 Black 460Вт;
– материнська плата Supermicro MBD-X10SLL-F;
– модуль пам'яті Kingston DDR3-1600 4096MB PC3-12800;
– маніпулятор Logitech B100, USB;
– процесор Intel Xeon E3-1280V2 3.6/5GT/s LGA1155 BOX;
– інтегрований графічний процесор Aspeed AST2400;
– монітор 23" LG 23MP55A-P.

Мережевий комутатор – 1шт.:

– TP-LINK TL-SG2424P (4 x SFP (mini-GBIC);24 x Gigabit Ethernet (10/100/1000 Мбіт/с)).

ADSL-модем – 1шт.:

– TP-LINK TD-W8980 (Швидкість LAN портів: 1 Гбіт/с; Швидкість Wi-Fi: 300 Мбіт/с; WAN-порт: Ethernet, ADSL; Інтерфейси: 4 порта RJ45 10/100/1000 Мбит/с;1 порт RJ11; 2 порта USB 2.0).

До складу допоміжних технічних засобів, не призначених для обробки, зберігання та передачі ІзОД, входять:

– БФП HP LaserJet Pro M227sdn (G3Q74A) (2 шт.);
– Принтери HP LaserJet Pro M102a (G3Q34A) (4 шт.)
– джерело безперервного електроживлення APC Smart-UPS RT 1000VA (17 шт.).

2.5 Визначення профілю захищеності ІКС

Основними загрозами безпеці інформаційних ресурсів, в першу чергу, є загрози шахрайства (підробка, відмова від авторства, відмова від одержання) і порушення технології роботи, а в другу – порушення доступності і конфіденційності. У зв'язку з цим, до комплексів засобів захисту обчислювальних систем банківських установ, що входять до складу банківських ІС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. Вимоги

також істотно залежать від того, чи здійснюється обробка в реальному часі або відкладена обробка. Інформаційні (автоматизовані) системи фінансових компаній, як правило, відносяться до класу 3, тобто є розподіленими.

Згідно рекомендаціям, які надаються в НД ТЗІ 2.5-005-99, стандартні функціональні профілі захищеності в КС, що входять до складу АС класу 3 визначаються підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Інформаційна система компанії являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. Встановлення функціонального профілю захищеності для АС дозволяє вирішити задачі співставлення вимог до комплексу засобів захисту обчислювальної системи з характеристиками АС.

В ІС рекомендується використовувати обчислювальні системи, КЗЗ яких реалізують профілі 3. КЦД.х..

У кваліфікаційній роботі наводиться стандартний функціональний профіль захищеності КС, що входить до складу АС, призначеної для автоматизації діяльності компанії.

Профіль захищеності:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1,

ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.1 – Характеристика профілю захищеності 3.КЦД.2

Атрибут	Характеристика
1	2
Критерії конфіденційності	
Довірча конфіденційність	
КД-2	Базова довірча конфіденційність Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на

	підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту НЕОБХІДНІ УМОВИ: НИ-1
Адміністративна конфіденційність	
КА-2	Базова адміністративна конфіденційність Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта користувача і захищеного об'єкта Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту НЕОБХІДНІ УМОВИ: НО-1, НИ-1

Продовження табл. 2.1

1	2
Повторне використання об'єктів	
КО-1	Повторне використання об'єктів Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною НЕОБХІДНІ УМОВИ: НЕМАЄ
Конфіденційність при обміні	
КВ-2	Базова конфіденційність при обміні Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу НЕОБХІДНІ УМОВИ: НО-1
Критерії цілісності	
Довірча цілісність	
ЦД-1	Базова довірча цілісність Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів

	доступу процесу і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт. КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту НЕОБХІДНІ УМОВИ: НИ-1
Адміністративна цілісність	
ЦА-2	Базова адміністративна цілісність Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту НЕОБХІДНІ УМОВИ: НО-1, НИ-1

Продовження табл. 2.1

Відкат	
ЦО-1	Обмежений відкат Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу НЕОБХІДНІ УМОВИ: НИ-1
Цілісність при обміні	
ЦВ-2	Базова цілісність при обміні Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження НЕОБХІДНІ УМОВИ: НО-1
Критерії доступності	
Використання ресурсів	
ДР-1	Квоти Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження НЕОБХІДНІ УМОВИ: НО-1

Продовження табл. 2.1

1	2
Відновлення після збоїв	
ДВ-1	Ручне відновлення Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС
	Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування НЕОБХІДНІ УМОВИ: НО-1
Критерії спостереженості	
Реєстрація	
НР-2	Захищений журнал Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації НЕОБХІДНІ УМОВИ: НИ-1, НО-1

Продовження табл. 2.1

1	2
	Ідентифікація і автентифікація
НИ-2	Одиночна ідентифікація і автентифікація Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування НЕОБХІДНІ УМОВИ: НК-1
	Достовірний канал
НК-1	Однонаправлений достовірний канал Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем НЕОБХІДНІ УМОВИ: НЕМАЄ
	Розподіл обов'язків
НО-2	Розподіл обов'язків адміністраторів Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі НЕОБХІДНІ УМОВИ: НИ-1
	Цілісність комплексу засобів захисту
НЦ-2	КЗЗ з гарантованою цілісністю Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а

	також механізми захисту, що використовуються для реалізації розподілення доменів КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ НЕОБХІДНІ УМОВИ: НЕМАЄ
Самотестування	
НТ-2	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ НЕОБХІДНІ УМОВИ: НО-1
Ідентифікація і автентифікація при обміні	
НВ-1	Автентифікація вузла Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації НЕОБХІДНІ УМОВИ: НЕМАЄ

2.6 Аналіз загроз

Поняття загрози розуміється як потенційно можливі або реальні дії зловмисників чи конкурентів, здатні нанести компанії матеріальної або моральної шкоди.

Загроза інформаційній безпеці ІС – сукупність умов і чинників, що створюють небезпеку несанкціонованого доступу до інформації, циркулюючої в автоматизованій системі, а також можливі наслідки дій порушника на ІС,

незапобігання, невиявлення і неліквідація якого може привести до погіршення заданих якісних характеристик функціонування ІС компанії або порушенню її працездатності, а також спотворенню і витокам інформації.

2.6.1 Джерела загроз

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІС.

На кожному з рівнів інформаційної інфраструктури загрози та їх джерела (в т.ч. зловмисники), методи і засоби захисту і підходи до оцінки ефективності є різними. Тому необхідними умовами для ефективного функціонування компанії є визначення конкретних об'єктів середовища інформаційних активів на кожному з рівнів інформаційної інфраструктури.

Рівні інформаційної інфраструктури:

– фізичний (лінії зв'язку, апаратні засоби та ін.);

– мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

– мережевих додаткових програм і сервісів;

– операційних систем;

– систем управління базами даних;

– технологічних процесів і додаткових програм;

– бізнес-процесів організації.

Джерела загроз на фізичному рівні, рівні мережевого устаткування і рівні мережевих додаткових програм:

– зовнішні джерела загроз: особи, що поширюють віруси і інші шкідливі програми, хакери і інші особи, що здійснюють НСД;

– внутрішні джерела загроз: особи, що реалізовують загрози в рамках своїх повноважень і за їх межами (персонал, що має права доступу до апаратного устаткування, зокрема мережевому, адміністратори мережевих додаткових програм і тому подібне);

– комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють спільно і/або погоджено.

Джерела загроз на рівнях операційних систем, систем управління базами даних, банківських технологічних процесів:

– внутрішні, такі, що реалізовують загрози в рамках своїх повноважень і за їх межами (адміністратори ОС, адміністратори СУБД, користувачі банківських додаткових програм і технологій, адміністратори ІБ і так далі);

– комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють в змові.

Джерела загроз на рівні бізнес-процесів:

– внутрішні джерела, що реалізовують загрози в рамках своїх повноважень і за їх межами (авторизовані користувачі і оператори АБС, представники менеджменту організації і ін.);

– комбіновані джерела загроз: зовнішні (наприклад, конкуренти) і внутрішні, такі, що діють в змові.

Головною метою зловмисника є отримання контролю над активами на рівні бізнес-процесів. Прямий напад на рівні бізнес-процесу є більш ефективним для зловмисника та найбільш небезпечним для компанії, ніж напад, який здійснюється через нижні рівні. Реалізація такого нападу вимагає специфічного досвіду, знань і ресурсів (в т.ч. тимчасових) і тому є менш ефективним по співвідношенню "витрати/отриманий результат". Визначення конкретних об'єктів захисту здійснюється на кожному з рівнів інформаційної інфраструктури.

2.6.2 Класифікація загроз інформаційним ресурсам

Першочерговою задачею для успішного ведення діяльності компанії, як зазначалося вище, є підтримання стабільного функціонування ІКС та забезпечення безпеки циркулюючих інформаційних потоків.

На рисунку 2.4 представлені базові загрози, які мають вплив на конфіденційність, цілісність та доступність інформаційних ресурсів.

Загрози порушення конфіденційності.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. Конфіденційність передбачає забезпечення захисту даних, що передаються, від пасивних атак, тобто захист потоку даних від можливості його аналітичного дослідження.

До загроз порушення конфіденційності інформації відносять розкрадання (копіювання) і витоки інформації.

Основними видами атак направлених на порушення конфіденційності є пасивне підслуховування і перехоплення в каналах зв'язку, незаконне використання прав, викрадання ключової інформації.

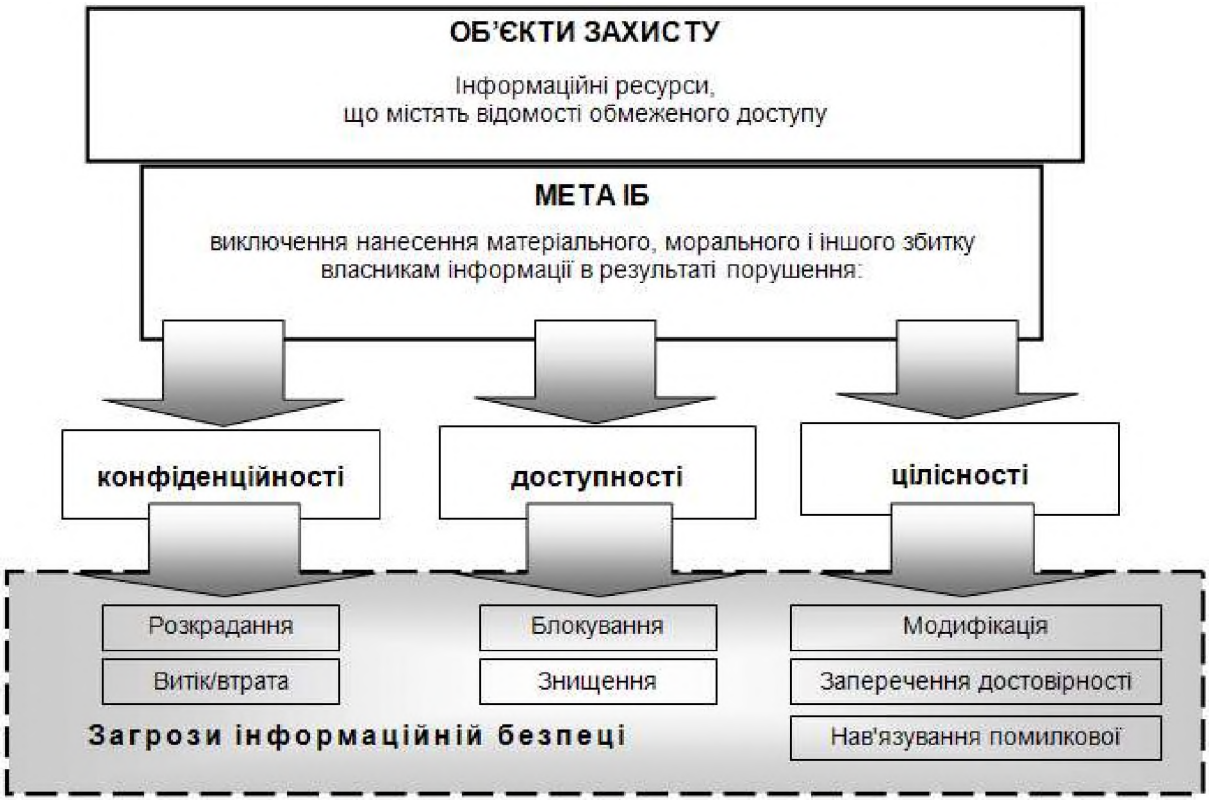

Рисунок 2.4 – Базові загрози безпеці інформаційних ресурсів

Витоки/втрати інформації підривають авторитет компаній і завдають величезні збитки.

Загрози порушення цілісності.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Загрози цілісності даних, програм, апаратури. Цілісність даних і програм порушується при несанкціонованому знищенні, додаванні зайвих елементів і модифікації записів про стан рахунків, зміні порядку розташування даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, при активній ретрансляції повідомлень з їх затримкою. Несанкціонована модифікація інформації про безпеку системи може привести до несанкціонованих дій (невірній маршрутизації або втраті даних, що передаються) або спотворення сенсу повідомлень, що передаються. Цілісність апаратури порушується при її пошкодженні викраданні або незаконній зміні алгоритмів роботи.

Загрози порушення доступності.

Доступність – властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Загрози доступності даних виникають у тому випадку, коли об'єкт (користувач або процес) не дістає доступу до законно виділених йому служб або ресурсів. Ця загроза реалізується захопленням ресурсів, блокуванням ліній зв'язку несанкціонованим об'єктом в результаті передачі по ним своєї інформації або виключенням необхідної системної інформації. Ця загроза може привести до ненадійності або поганої якості обслуговування в системі і, отже, потенційно впливатиме на достовірність і своєчасність доставки платіжних документів.

На рисунку 2.4 наведена модель реалізації загроз з урахуванням джерел загроз, вразливостей та методів реалізації загроз інформаційній безпеці.

Загрози інформаційним ресурсам виявляються у вигляді:

– розголошування конфіденційної інформації;

– витоків конфіденційної інформації через технічні засоби забезпечення виробничої діяльності різного характеру і виконання;

– несанкціонованого доступу до відомостей, що охороняються, з боку конкурентних організацій і злочинних формувань.

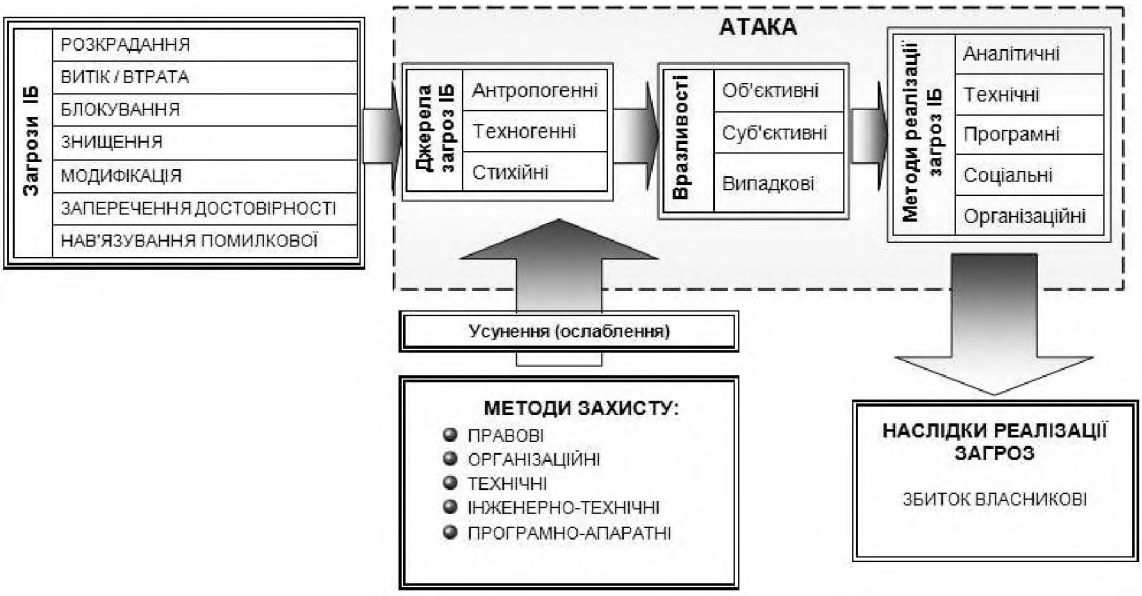

Рисунок 2.5 – Модель реалізації загроз

Здійснення загроз інформаційним ресурсам може бути проведене:

– шляхом неофіційного доступу і знімання конфіденційної інформації;

– шляхом підкупу або шантажу осіб, що працюють в компанії або структурах, безпосередньо пов'язаних з його діяльністю;

– шляхом перехоплення інформації, циркулюючої в засобах і системах зв'язку і обчислювальної техніки за допомогою технічних засобів розвідки і знімання інформації, несанкціонованого доступу до інформації і навмисних програмно-математичних дій на неї в процесі обробки і зберігання;

– шляхом підслуховування конфіденційних переговорів, що ведуться в службових приміщеннях, службовому і особистому автотранспорті і т.д.;

За ознакою джерела загрози безпеці компанії вирізняються:

– загрози з боку конкурентів, які прагнуть до посилення власних позицій на відповідному ринку шляхом використання заходів недобросовісної конкуренції,

наприклад економічного шпіонажу, переманювання висококваліфікованих співробітників, дискредитації суперника в очах партнерів та держави;

– загрози з боку кримінальних структур і окремих зловмисників, що прагнуть до досягнення власних цілей, які знаходяться в протиріччі з інтересами конкретного банку, наприклад, захоплення контролю над ним, розкрадання власності, нанесенню іншого збитку;

– загрози з боку нелояльних співробітників банку, які усвідомлено наносять збиток заради досягнення власних цілей, наприклад, поліпшення матеріального становища, кар'єрного росту, помсти працедавцю за реальні або уявні образи та ін.

За видами можливих джерел загроз ІБ компанії виділяються наступні класи загроз:

– загрози, пов'язані з навмисними або ненавмисними діями осіб, що мають доступ до ІС, включаючи користувачів ІС, що реалізовують погрози безпосередньо в ІС (внутрішній порушник);

– загрози, пов'язані з навмисними або ненавмисними діями осіб, що не мають доступу до ІС, що реалізовують погрози з зовнішніх мереж зв'язку загального користування.

За видами несанкціонованих дій, здійснюваних з інформаційними ресурсами виділяються наступні класи загроз:

– загрози, що призводять до порушення конфіденційності інформаційних ресурсів (копіюванню або несанкціонованому розповсюдженню при реалізації яких не здійснюється безпосередньої дії на зміст інформації;

– загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на зміст інформації, в результаті якого здійснюється зміна інформаційних ресурсів або їх знищення;

– загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на програмні або програмно-апаратні елементи ІС, в результаті якого здійснюється блокування інформаційних ресурсів.

2.6.3 Моделі загроз і порушника

Моделі загроз і порушників ІБ розробляються, як правило, для компанії в цілому, але при необхідності можлива розробка для окремих процесів при цьому ступінь деталізації параметрів моделей загроз і порушників ІБ може бути різна.

Відповідно до вимог до забезпечення інформаційної безпеки автоматизованої системи компанії визначені наступні моделі загроз:

– навмисні програмно-технічні впливи (дії) з метою порушення цілісності (знищення, спотворення) інформації в процесі її обробки, передачі і зберігання в ІС компанії;

– порушення санкціонованої доступності інформації в ІС компанії, за рахунок порушення працездатності програмного забезпечення, комунікаційного устаткування і маршрутизаторів ІС компанії або їх перепрограмування (дефекти, збої, аварії і відмови апаратно-програмних комплексів);

– витік і спотворення конфіденційної інформації за рахунок несанкціонованого доступу до неї через технічні засоби ІС компанії, витік конфіденційної інформації по технічних каналах;

– розголошування конфіденційної інформації і неправомірні дії з боку осіб, що мають право доступу до конфіденційної інформації і реалізовують загрози в рамках своїх повноважень і за їх межами.

Таблиця 2.2 – Загальна модель загроз безпеці інформаційних ресурсів

Джерело загрози	Рівень реалізації загрози	Типи об'єктів середовища	Загроза
1	2	3	4
Комп'ютерні зловмисники, що здійснюють цілеспрямовану деструктивну дію	Рівень операційних систем	Файли даних з КІ	Порушення конфіденційності, цілісності, доступності
	Рівень систем управління базами даних	Бази даних з КІ	Порушення конфіденційності, цілісності, доступності
	Рівень банківських технологічних додаткових програм і сервісів	Прикладні програми доступу і обробки КІ, АРМ	Порушення конфіденційності цілісності

Продовження табл. 2.2

1	2	3	4
Постачальники програмно-технічних засобів, витратних матеріалів, послуг і тому подібне і підрядчики, що здійснюють монтаж, пуско-налагоджувальні роботи устаткування і його ремонт	Рівень операційних систем	Файли даних з КІ	Порушення конфіденційності цілісності
	Рівень систем управління базами даних	Бази даних з КІ	Порушення конфіденційності цілісності
	Рівень банківських технологічних додаткових програм і сервісів	Прикладні програми доступу і обробки КІ, АРМ	Порушення конфіденційності цілісності
Співробітники, що діють в рамках наданих повноважень	Фізичний рівень	Лінії зв'язку, апаратні і технічні засоби, сервера, фізичні носії інформації	Порушення конфіденційності цілісності
	Мережевий рівень	Маршрутизатори, комутатори, концентратори	Порушення конфіденційності, цілісності, доступності
	Рівень мережевих додаткових програм і сервісів	Програмні компоненти передачі даних по комп'ютерних мережах (мережеві сервіси)	Порушення конфіденційності, цілісності, доступності
	Рівень операційних систем	Файли даних з КІ	Порушення конфіденційності, цілісності, доступності
	Рівень систем управління базами даних	Бази даних з КІ	Порушення конфіденційності, цілісності, доступності
	Рівень банківських технологічних додаткових програм і сервісів	Прикладні програми доступу і обробки КІ, АРМ	Порушення конфіденційності, цілісності, доступності

Продовження табл. 2.2

1	2	3	4
Співробітники, що діють поза рамками наданих повноважень	Рівень операційних систем	Файли даних з КІ	Порушення конфіденційності, цілісності
	Рівень систем управління базами даних	Бази даних з КІ	Порушення конфіденційності, цілісності
	Рівень банківських технологічних додаткових програм і сервісів	Прикладні програми доступу і обробки КІ, АРМ	Порушення конфіденційності, цілісності

Основними критичними елементами засобів автоматизації ІС компанії (в порядку спадання їх важливості) є:

– сервера баз даних і додаткових програм;

– комунікаційне устаткування (компоненти) системи передачі даних (маршрутизатори, концентратори, модеми);

– спеціалізовані АРМ з встановленими СКЗІ;

– робочі станції користувачів банку.

Об'єктами захисту засобів автоматизації є:

– програмно-технічний комплекс АС компанії в цілому як автоматизована система, що оброблює конфіденційну інформацію;

– сервера баз даних і додаткових програм;

– спеціалізованих АРМ зі встановленими СКЗІ;

– канали зв'язку, за допомогою яких здійснюється інформаційний обмін в ІС компанії;

– приміщення, в яких розташовується серверна частина програмно-технічних комплексів і робочі станції кінцевих користувачів (залежно від оброблюваної інформації).

Система інформаційної безпеки ІС компанії будується відповідно до певного характеру загроз і основних елементів системи, на які ці загрози розповсюджуються.

Джерелами загроз НСД в ІС можуть бути:

– порушник;

– носій шкідливої програми;

– апаратна закладка.

Зовнішніми порушниками можуть бути:

– розвідувальні служби держав;

– кримінальні структури;

– конкуренти (конкуруючі організації);

– недобросовісні партнери;

– зовнішні суб'єкти (фізичні особи).

Зовнішній порушник має наступні можливості:

– здійснювати несанкціонований доступ до каналів зв'язку, що виходять

– за межі службових приміщень;

– здійснювати несанкціонований доступ через автоматизовані робочі місця, підключені до мереж зв'язку загального користування;

– здійснювати несанкціонований доступ до інформації з використанням спеціальних програмних дій за допомогою програмних вірусів, шкідливих програм, алгоритмічних або програмних закладок;

– здійснювати несанкціонований доступ через елементи інформаційної інфраструктури ІС, які в процесі свого життєвого циклу (модернізації, супроводу, ремонту, утилізації) виявляються за межами контрольованої зони;

– здійснювати несанкціонований доступ через інформаційні системи взаємодіючих відомств, організацій і установ при їх підключенні до ІС.

Внутрішніми порушниками можуть бути:

– особи, що мають санкціонований доступ в контрольовану зону, але не мають доступу до інформаційних ресурсів;

– зареєстрований користувач інформаційних ресурсів, що має обмежені права доступу до ІС з робочого місця;

– користувачі інформаційних ресурсів, що здійснюють віддалений доступ до інформаційних ресурсів по ЛОМ;

– зареєстрований користувач з повноваженнями системного адміністратора ІС;

– зареєстрований користувач з повноваженнями адміністратора безпеки ІС;

– програмісти-розробники прикладного ПО і осіб, що забезпечують його супровід в ІС;

– розробники і особи, що забезпечують постачання, супровід в ІС.

Можливості внутрішнього порушника істотним чином залежать від тих, що діють в межах контрольованої зони режимних і організаційно-технічних заходів захисту, зокрема по допуску фізичних осіб до інформаційних ресурсів і контролю порядку проведення робіт.

В залежності від можливостей, внутрішніх потенційних порушників можна представити у вигляді наступної ієрархії рівнів (кожний наступний рівень включає в себе функціональні можливості попереднього):

– перший рівень – визначається можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

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

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

– четвертий рівень – визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІС, аж до включення до складу ІС власних засобів з новими функціями обробки інформації.

За рівнем знань про ІС всіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості ІС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації ІС;

– володіють інформацією про функції та механізм дії засобів захисту.

Класифікація порушників за рівнем можливостей та рівнем знань наведена згідно НД ТЗІ 1.4-001-2000 Типового положення про службу захисту інформації.

2.6.4 Аналіз загроз витоків інформації

В кваліфікаційній роботі модель загроз буде розглянута в межах найбільш значної загрози витокам інформаційних ресурсів в компанії, яку представляють навмисні або ненавмисні дії внутрішніх порушників.

В таблиці 2.3 наведено опис станів безпеки відповідно збиток від атаки та ймовірність її виникнення.

Таблиця 2.3 – Збиток від атаки та ймовірність її виникнення

Стан безпеки	Ймовірність реалізації загрози	Небезпека загрози	Опис
Безпека	Відсутня	0	Розкриття інформації принесе мінімальний моральний і фінансовий збиток
	Рідше ніж 1 раз на рік	1	Збиток від атаки є, але він незначний, основні фінансові операції не зазнають впливу
Ризик	1 раз на рік	2	Операції не ведуться протягом певного часу, але становище компанії на ринку змінюється мінімально
Загроза	1 раз на місяць	3	Значні втрати репутації та прибутку
Небезпека	1 раз на тиждень	4	Дуже значні втрати, компанія втрачає становище на ринку. Потрібні додаткові витрати.
	Більше ніж 1 раз на тиждень	5	Компанія припиняє існування

В таблиці 2.4 представлена модель загроз безпеці інформаційних ресурсів компанії, джерелом яких є навмисні та ненавмисні дії персоналу компанії.

Таблиця 2.4 – Модель загроз безпеці інформаційним ресурсам

Перелік загроз	Ймовірність реалізації загрози	Небезпека загрози	Ризик
1	2	3	4
Загрози несанкціонованого доступу до інформації			
Загрози знищення, розкрадання носіїв інформації шляхом фізичного доступу до елементів ІС			
Крадіжка носіїв інформації	2	4	8
Крадіжка ключів доступу	3	4	12
Крадіжки, модифікації, знищення інформації.	3	4	12
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	1	3	3
Несанкціоноване відключення засобів захисту	3	3	9
Загрози навмисних дій внутрішніх порушників			
Витік даних від порушення експлуатації програмного забезпечення	3	4	12
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	3	3	9
Передача конфіденційної інформації, з використанням електронної пошти	3	4	12
Витік даних від неавторизованого використання обладнання/програмного забезпечення	3	4	12
Передача нешифрованої інформації, що захищається, в зовнішню мережу	3	4	12
Передача зашифрованої інформації, що захищається, в зовнішню мережу	3	3	9
Витік інформації за рахунок запису інформації, що захищається на знімні носії (USB-накопичувачі, flash-носії і т. д.)	3	4	12
Компрометація інформації за допомогою розкриття/продажу інформації працівниками компанії	3	4	12

Продовження табл. 2.4

1	2	3	4
Витік інформації за рахунок друку документів, які містять конфіденційну інформацію	3	4	12
Компрометація інформації за допомогою нелегального оброблення даних	3	4	12
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	3	4	12
Компрометація інформації за рахунок підробки прав доступу до інформації	3	4	12
Доступ, модифікація, знищення інформації особами, не допущеними до її обробки	3	4	12
Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	4	4	16
Загрози ненавмисних дій користувачів і порушень безпеки функціонування			
Витік даних від недбалості персоналу	3	4	12
Витік даних від порушення експлуатації обладнання/ програмного забезпечення	2	3	6
Витік даних від неавторизованого використання обладнання/програмного забезпечення	2	3	6
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	3	3	9
Втрата ключів доступу	3	4	12
Ненавмисна модифікація (знищення) інформації співробітниками	3	3	9
Ненавмисне відключення засобів захисту	3	3	9
Разом (середнє значення)			10,5

Функція імовірності реалізації певної загрози, виду і величини завданих збитків визначає ризик для безпеки інформаційних ресурсів компанії.

Процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС визначається як аналіз ризику.

2.7 Політика безпеки

«ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

1 Загальні положення

З метою мінімізації ризиків СЗІ забезпечує виконання вимог цілісності, конфіденційності та доступності інформації.

Розробкою вимог і контролем їх виконання займається СЗІ.

Дані вимоги є обов'язковими до виконання всіма працівниками структурних підрозділів, відділів і служб.

Всі вимоги щодо забезпечення інформаційної безпеки застосовні до кожного працівника, а також до будь-якій третій особі, включаючи осіб, які працюють за договорами цивільно-правового характеру та прикомандированих працівників, що мають доступ до інформації та її інформаційних ресурсів.

Кожен працівник, а також будь-яка третя особа, включаючи осіб, які працюють за договорами цивільно-правового характеру та прикомандированих працівників, що мають доступ до інформації та її інформаційних ресурсів визнає право на здійснення контролю їх діяльності при роботі з інформаційними засобами та інформацією.

Вся ділова інформація в будь-якій формі, придбана або отримана, використовувана для підтримки його законною виробничо-господарської діяльності, або розроблена його працівниками в ході виробничо-господарської діяльності, належить компанії. Це право власності поширюється на голосову та факсимільний зв'язок з використанням апаратури, на ліцензійне і розроблене програмне забезпечення та окремі програми, на електронні поштові скриньки, а

також на паперові та електронні файли всіх бізнес-напрямків, бізнес-функцій, і на всіх працівників.

Забороняється використання інформації та інформаційних засобів в особистих цілях.

2 Цілі і завдання системи забезпечення інформаційної безпеки

2.1 Мета системи забезпечення інформаційної безпеки - створення і постійне дотримання умов, при яких ризики, пов'язані з порушенням безпеки інформаційних активів, постійно контролюються і виключаються, або знаходяться на допустимому (прийнятному) рівні залишкового ризику.

Процеси забезпечення інформаційної безпеки є складовою і невід'ємною частиною процесів управління інформаційними технологіями та супутніми операційними ризиками і здійснюються на основі циклічної моделі: «планування - реалізація - перевірка вдосконалення - планування - ...».

2.2 Безпека інформаційних активів оцінюється і забезпечується за кожним з таких аспектів:

- доступність,
- цілісність,
- конфіденційність.

При цьому критерієм оцінки є ймовірність, розмір і наслідки нанесення компанії будь-якого виду шкоди (невиконання наявних перед партнерами зобов'язань, фінансові втрати, втрата репутації та ін.).

Стан інформаційної безпеки безпосередньо впливає на операційні ризики діяльності в зв'язку з чим будь-який факт (інцидент) порушення інформаційної безпеки розглядається як важлива подія.

2.3 Завданнями системи забезпечення інформаційної безпеки є:

- зниження операційних ризиків, пов'язаних з використанням інформаційних технологій;
- оптимізація витрат на забезпечення інформаційної безпеки;
- своєчасне виявлення нових загроз;

– контроль стану інформаційної безпеки на всіх етапах життєвого циклу автоматизованих систем;

– мінімізація втрат Організації при виникненні загроз інформаційній безпеці;

– забезпечення життєдіяльності та безпеки його інформаційних активів в умовах несприятливих подій (економічні та політичні кризи, природні та техногенні катастрофи, терористичні загрози та ін.).

3 Основні принципи забезпечення інформаційної безпеки

3.1 Поінформованість про ризик інформаційної безпеки

Процеси забезпечення інформаційної безпеки зачіпають кожного працівника, що використовує його інформаційні активи, і накладають на нього відповідні обов'язки і обмеження.

3.2 Персональна відповідальність

Відповідальність за порушення вимог інформаційної безпеки покладається безпосередньо на працівників, які допустили порушення, та керівника структурного підрозділу, відділу, служби, в якому порушення допущені.

3.3 Обмеження повноважень

Будь-якому співробітникові доступ до інформаційних активів надається тільки в тому обсязі, який необхідний йому для виконання службових обов'язків. Всі операції з надання доступу або призначенням повноважень здійснюються строго у відповідності до встановлених процедур (Процедура отримання індивідуального доступу).

3.4 Комплексність захисту

Заходи щодо забезпечення безпеки інформаційних активів приймаються за всіма ідентифікованим видам загроз з урахуванням результатів оцінки ризиків інформаційної безпеки.

3.5 Адекватність захисту

Заходи, що вживаються забезпечення інформаційної безпеки ефективні і відповідні мають місце ризиків інформаційної безпеки.

3.6 Безперервність процесів контролю та вдосконалення системи забезпечення інформаційної безпеки

Постійний моніторинг і аудит системи забезпечення інформаційної безпеки, за результатами яких здійснюється аналіз ефективності вжитих заходів забезпечення інформаційної безпеки з урахуванням змін IT-середовища, появи нових загроз, інцидентів і проблем, плануються і впроваджуються додаткові заходи захисту.

3.7 Контроль з боку керівництва

Керівництво на регулярній основі розглядає звіти про стан інформаційної безпеки в структурних підрозділах, відділах, службах і фактах порушень встановлених вимог, а також загальні та приватні питання інформаційної безпеки, пов'язані з використанням технологій підвищеного ризику або істотно впливають на бізнес-процеси.

3.8 Цільове фінансування заходів щодо забезпечення інформаційної безпеки

Бюджет передбачає витрати на забезпечення інформаційної безпеки.

4 Загальні вимоги щодо забезпечення інформаційної безпеки

В основі процесів управління інформаційною безпекою лежать такі загальні вимоги:

4.1 Призначення і розподіл ролей, і забезпечення довіри до персоналу

«Рольове» управління є основним механізмом управління повноваженнями користувачів і адміністраторів в автоматизованих системах.

Ролі формуються з урахуванням принципу мінімальності повноважень.

Критичні технологічні процеси повинні бути захищені від помилкових і несанкціонованих дій адміністраторів. Штатні процедури адміністрування, діагностики та відновлення повинні виконуватися через спеціальні ролі в автоматизованих системах без безпосереднього доступу до даних.

Посадові обов'язки співробітників і трудові договори передбачають обов'язки персоналу щодо виконання вимог щодо забезпечення інформаційної безпеки, включаючи зобов'язання щодо нерозголошення інформації, що становить комерційну таємницю.

Накази і розпорядження, актуальна інформація з питань забезпечення інформаційної безпеки, в тому числі за виявленими порушеннями, доводяться до всіх співробітників під розпис.

Періодично перевіряється і оцінюється рівень компетентності та інформованості працівників в питаннях інформаційної безпеки.

4.2 Управління життєвим циклом автоматизованих систем

Процедури по забезпеченню інформаційної безпеки передбачаються на всіх стадіях життєвого циклу автоматизованих систем: при розробці (придбання), експлуатації, модернізації, зняття з експлуатації.

У контрактах зі сторонніми розробниками на поставку систем передбачається їх відповідальність за наявність в системах прихованих недокументованих можливостей, а також дотримання умов конфіденційності.

Системи сторонньої розробки перевіряються на відповідність вимогам інформаційної безпеки. У разі невідповідності поточної версії ПО вимогам інформаційної безпеки, вказане ПО оновлюється або закуповується нове.

При виведенні АС з експлуатації або заміні входить до її складу обладнання здійснюється обов'язкове гарантоване видалення інформації з відповідних машинних носіїв і з пам'яті комп'ютерів.

4.3 Антивірусний захист

Кожен працівник зобов'язаний виконувати правила експлуатації антивірусного ПО і вимоги антивірусної безпеки щодо зовнішніх джерел і носіїв інформації, а також мережі Інтернет, негайно припиняти роботу і інформувати служби автоматизації і безпеки при підозрах на вірусне зараження.

Антивірусні засоби повинні бути встановлені на всі робочі місця працівників і сервера в режимі постійного захисту.

Забороняється відключати антивірусне ПЗ, без узгодження зі СЗІ.

Користувачі на робочих місцях не повинні мати адміністративні прав. Наявність адміністративних прав на робочих місцях дозволяється лише користувачам, які виконують спеціальні функції по управлінню автоматизованою системою за погодженням зі СЗІ.

Все ПО встановлюється на робочі станції системним адміністратором з погодженням зі СЗІ. Встановлюється ПО повинно бути ліцензійним. Забороняється самостійна установка ПО користувачами.

Технічна можливість підключення користувачами до робочих станцій ЛВС зовнішніх накопичувачів інформації, модемів, мобільних телефонів, бездротових інтерфейсів, використання USB, CD-DVD-дисководів максимально обмежується. Забороняється підключати будь-яке обладнання без узгодження з співробітниками СЗІ.

Антивірусний захист забезпечується використанням спеціалізованого ліцензійного антивірусного програмного забезпечення.

Для зниження впливу людського фактору, виключення можливості відключення або не оновленої антивірусних засобів, контроль і управління антивірусним програмним забезпеченням, а також усунення виявлених вразливостей в системному програмному забезпеченні проводиться в автоматизованому режимі. При цьому забезпечується мінімально можливий період оновлення.

4.4 Використання ресурсів Інтернет

Використання ресурсів Інтернет дозволяється виключно у виробничих цілях.

Забороняється використання мережі Інтернет для інформаційної взаємодії між підрозділами Організації без використання засобів шифрування.

Використання канальних ресурсів Інтернет для побудови корпоративних мереж Організації допускається тільки при використанні коштів шифрування (VPN-канал).

Взаємодія з партнерами по мережі Інтернет здійснюється з використанням спеціалізованих систем і засобів захисту, атестованих на відповідність вимогам інформаційної безпеки.

Використання мережі Інтернет для обробки і зберігання інформації (в тому числі не конфіденційної) забороняється. Забороняється використання ящиків

електронної пошти, заведених нема на ресурсах Організації (зокрема використання публічних поштових серверів).

Підключення до робочих станцій ЛВС мобільних телефонів, бездротових (радіо) інтерфейсів, модемів та іншого обладнання, що дозволяє виходити в Інтернет, забороняється.

Підключення до мережі Інтернет здійснюється з використанням телефонної мережі.

Обговорення співробітниками на форумах і в конференціях мережі Інтернет питань, що стосуються їх службової діяльності, допускається тільки при наявності відповідних вказівок керівництва.

Доступ співробітників до ресурсів мережі Інтернет санкціонується керівництвом і узгоджується з Департаментом інформаційних технологій, які здійснюють контроль дотримання співробітниками вимог інформаційної безпеки, включаючи контентний аналіз повідомлень.

Робота співробітників з web-ресурсами Інтернет дозволяється тільки в режимі перегляду даних, виключаючи можливість передачі інформації компанії в мережу Інтернет.

4.5 Захист інформаційних і технологічних процесів

Технологічні процеси повинні бути максимально автоматизовані і забезпечувати можливість виконання масових і потенційно небезпечних операцій без участі персоналу за рахунок реалізації ефективних процедур контентного контролю і захисту.

Для захисту технологічних процесів за результатами аналізу ризиків інформаційної безпеки застосовуються як штатні засоби безпеки мережевих операційних систем, СУБД, так і додаткові програмні і програмно-апаратні комплекси і засоби криптографічного захисту, в сукупності, що забезпечують достатній рівень безпеки на всіх ділянках і етапах технологічного процесу.

4.6 Доступ до активів (інформаційних ресурсів)

Всі інформаційні активи ідентифікуються, категоріюються і мають своїх власників. Доступ до інформаційних активів всім співробітникам надається тільки

на підставі документально оформлених заявок, погоджених з їх власниками і СЗІ. За замовчуванням визначається відсутність доступу.

Доступ до інформаційних активів не надається (припиняється) в разі відсутності виробничої необхідності, зміни функціональних і посадових обов'язків, звільнення співробітника.

СЗІ проводиться періодичний контроль (не менше одного разу на півріччя) відповідності узгоджених і реальних прав доступу до інформаційних активів, поточного статусу користувача.

Доступ до всіх інформаційних активів здійснюється тільки після авторизації користувача. Як процедури авторизації використовується пред'явлення унікального імені та пароля. Забороняється передавати свій пароль кому-небудь. Забороняється зберігати свій пароль на будь-яких носіях інформації.

Журнали аудиту дій користувачів і адміністраторів автоматизованих систем повинні бути інформативні, захищені від модифікації і зберігатися протягом терміну, потенційно необхідного для використання при розслідуванні можливих інцидентів, пов'язаних з порушенням інформаційної безпеки.

Найбільш критичні активи можуть виділятися в окремі сегменти мережі для обмеження доступу.

4.7 Забезпечення фізичного захисту

Приміщення категоризується в залежності від критичності розміщуються в них інформаційних активів. Відповідно до категорії забезпечується технічна укріпленість приміщень, оснащення засобами відеоконтролю, контролю доступу, пожежогасіння і сигналізації.

Кожен співробітник, який отримав в користування портативний комп'ютер (Notebook), зобов'язаний вжити належних заходів щодо забезпечення його збереження, як в офісі, так і в інших місцях (наприклад, готелі, конференц-залі, автомобілі або аеропорту). У разі втрати (крадіжки) портативного комп'ютера відповідальність покладається на даного співробітника.

Портативні комп'ютери (Notebooks), повинні зберігатися в фізично захищеному місці. Для їх збереження рекомендується використовувати механічні замки (наприклад, систему Kensington Lock).

5 Організація системи забезпечення інформаційної безпеки

5.1 Загальне керівництво системою забезпечення інформаційної безпеки здійснює директор.

директор:

– стверджує і переглядає Політику інформаційної безпеки;

– організовує процес управління інформаційною безпекою, включаючи визначення підрозділів, відповідальних за управління окремими процесами забезпечення інформаційної безпеки, затвердження положень про них;

– забезпечує умови і затверджує бюджет для ефективної реалізації політики інформаційної безпеки;

– розглядає інформацію та звіти про стан інформаційної безпеки.

5.2 Всі керівники структурних підрозділів, відділів і служб відповідають за реалізацію політики інформаційної безпеки та управління процесами її забезпечення в рамках своєї компетенції:

– розробляють вимоги щодо захисту інформаційних активів в аспектах цілісності і конфіденційності та доступності на основі аналізу ризиків інформаційної безпеки;

– здійснюють контроль відповідності вимогам щодо захисту інформаційних активів на всіх стадіях життєвого циклу автоматизованих систем, від проектування до зняття з експлуатації;

– проводять розслідування інцидентів і фактів порушень інформаційної безпеки і інформують директора про результати проведеного розслідування;

– організують інструктажі працівників з питань інформаційної безпеки;

– здійснюють інструментальний контроль і моніторинг поточного стану інформаційної безпеки;

– регулярно (не рідше одного разу на півроку) інформують директора про стан інформаційної безпеки.

5.2.1 Служба захисту інформації:

– забезпечує виконання вимог інформаційної безпеки при підключенні і адмініструванні комунікаційного обладнання, операційних систем, СУБД і систем доставки;

– проводить оновлення системного ПЗ, пов'язане з усуненням критичних вразливостей;

– забезпечує доступність інформаційних активів в умовах відмов та інших несприятливих подій в частині комунікаційного обладнання, операційних систем, СУБД і систем доставки;

– забезпечує виконання вимог інформаційної безпеки при адмініструванні автоматизованих систем;

– здійснює реєстрацію інцидентів, що мають відношення до інформаційної безпеки;

– забезпечує доступність інформаційних активів в умовах відмов та інших несприятливих подій в частині автоматизованих систем;

– бере участь у формуванні рішень, пов'язаних з організацією технологічних процесів, розробляє пропозиції щодо використання сучасних інформаційних технологій з урахуванням вимог щодо забезпечення інформаційної безпеки;

– забезпечує управління ключовими системами засобів криптографічного захисту;

– експлуатує спеціалізовані засоби забезпечення безпеки інформаційних активів і забезпечує відповідність характеристик даних коштів необхідного підрозділам рівнем доступності;

– організовує проведення єдиної антивірусної політики.

5.2.2 Підрозділи:

– спільно з СЗІ, беруть участь в оцінці ризиків реалізації загроз їх інформаційних активів;

– встановлюють в межах своєї компетенції режим і порядок доступу, правила роботи з інформаційними активами, власниками яких вони є;

– забезпечують виконання вимог і процедур інформаційної безпеки при роботі співробітників з інформаційними активами;

– сприяють при проведенні перевірок та розслідувань інцидентів безпеки.

6 Відповідальність

Співробітники несуть відповідальність за невиконання вимог щодо забезпечення інформаційної безпеки на своїх робочих місцях.

Керівники структурних підрозділів, відділів і служб несуть відповідальність за невиконання вимог щодо забезпечення інформаційної безпеки їх працівниками.

Служба автоматизації несе відповідальність за невиконання вимог щодо забезпечення інформаційної безпеки серверів, робочих станцій, обладнання.

У разі виявлення порушення вимог інформаційної безпеки до співробітника вживаються заходи, передбачені внутрішніми документами компанії, а також чинним законодавством.

2.8 Аналіз ризиків після впровадження політики безпеки

Після впровадження політики безпеки інформації в ІКС били отримані нові данні моделі загроз та аналізу ризиків, що приведено в таблиці 2.5.

Таблиця 2.5 – Модель загроз безпеці інформаційним ресурсам після впровадження політики безпеки

Перелік загроз	Ймовірність реалізації загрози	Небезпека загрози	Ризик
1	2	3	4
Загрози несанкціонованого доступу до інформації			

Загрози знищення, розкрадання носіїв інформації шляхом фізичного доступу до елементів ІС			
Крадіжка носіїв інформації	1	4	4
Крадіжка ключів доступу	2	4	8
Крадіжки, модифікації, знищення інформації.	2	4	8
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	1	3	3
Несанкціоноване відключення засобів захисту	2	3	6
Загрози навмисних дій внутрішніх порушників			
Витік даних від порушення експлуатації програмного забезпечення	2	4	8
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	2	3	6
Передача конфіденційної інформації, з використанням електронної пошти	2	4	8
Витік даних від неавторизованого використання обладнання/програмного забезпечення	2	3	6
Передача нешифрованої інформації, що захищається, в зовнішню мережу	2	3	6
Передача зашифрованої інформації, що захищається, в зовнішню мережу	2	3	6
Витік інформації за рахунок запису інформації, що захищається на знімні носії (USB-накопичувачі, flash-носії і т. д.)	2	4	8
Компрометація інформації за допомогою розкриття/продажу інформації працівниками компанії	2	4	8
Витік інформації за рахунок друку документів, які містять конфіденційну інформацію	2	4	8

Продовження табл. 2.5

1	2	3	4
Компрометація інформації за допомогою нелегального оброблення даних	2	4	8
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	2	4	8
Компрометація інформації за рахунок підробки прав доступу до інформації	2	4	8
Доступ, модифікація, знищення інформації особами, не допущеними до її обробки	2	4	8
Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	3	4	12
Загрози ненавмисних дій користувачів і порушень безпеки функціонування			
Витік даних від недбалості персоналу	2	4	8
Витік даних від порушення експлуатації обладнання/ програмного забезпечення	1	3	3
Витік даних від неавторизованого використання обладнання/програмного забезпечення	1	3	3
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	2	3	6
Втрата ключів доступу	2	4	8
Ненавмисна модифікація (знищення) інформації співробітниками	2	3	6
Ненавмисне відключення засобів захисту	2	3	6
Разом (середнє значення)			6,8

Середнє значення ризику свідчить про значне його зниження та про вдосконалення системи інформаційної безпеки в ІКС ТОВ «Фінанс-Дніпро» шляхом впровадження ПБ.

Також слід зазначити, що зниження показників ризику, в основному відбулося завдяки зменшенню показників ймовірності реалізації загроз.

2.9 Висновки до Розділу 2

У спеціальній частині кваліфікаційної роботи наведено загальні відомості про підприємство, розглянуто питання інформаційної безпеки фінансової компанії, проведено категоріювання інформаційних ресурсів та визначена структура інформаційно-комунікаційної системи. Також наведено визначення профілю захищеності ІКС, проведено аналіз загроз та їх джерел, класифікація загроз інформаційним ресурсам, моделі загроз і порушника. Розроблено та наведено політику забезпечення інформаційної безпеки та виконано аналіз ризиків після впровадження політики безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою економічного розділу є розрахунок витрат на створення та впровадження політики безпеки інформації в ІТС підприємства.

Завданням був розрахунок капітальних та експлуатаційних витрат на розробку та впровадження ПБ.

3.1 Визначення трудомісткості розробки системи інформаційної безпеки

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

$$t = t_{тз} + t_в + t_а + t_{пр} + t_{опр} + t_д, \text{ год.}$$

Де $t_{тз}$ = 8 год. – тривалість складання технічного завдання на розробку системи;

$t_в$ = 6 год. – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_а$ = 6 год. – тривалість розробки системи;

$t_{пр}$ = 6 год. – тривалість програмування за готовою системою;

$t_{опр}$ = 4 год. – тривалість опрацювання системи підтримки;

$t_д$ = 4 год. – тривалість підготовки технічної документації.

$$t = 8 \text{ год.} + 6 \text{ год.} + 6 \text{ год.} + 6 \text{ год.} + 4 \text{ год.} + 4 \text{ год.} = 34 \text{ год.}$$

3.2 Розрахунок витрат на створення системи інформаційної безпеки

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

$$Крп = Ззп + Змч,$$

де Крп – витрати на створення системи інформаційної безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення системи ІБ.

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

$$Ззп = t * Зіб = 34 * 250 = 8500 \text{ грн.}$$

де t – загальна тривалість розробки системи підтримки, год.;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 250 грн/год.

Вартість машинного часу для розробки системи інформаційної безпеки на ПК визначається за формулою:

$$Змч = t * Смч, \text{ грн.},$$

де t – трудомісткість розробки системи ІБ на ПК, год.;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{Fp} =$$

$$= 0,3 * 1 * 6 + (15000 * 0,5)/1920 + (12000 * 0,5)/1920 =$$

$$= 1,8 + 3,91 + 3,13 = 8,84$$

де Р- встановлена потужність апаратури інформаційної безпеки, 0,3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин, на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 6 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 15000 грн.;

На – річна норма амортизації на ПК, 0.5 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,5 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 12000 грн.;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год.).

$$Змч = t * Смч = 34 * 8,84 = 300,56 \text{ грн.}$$

Визначена таким чином вартість створення системи ІБ Крп є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

$$Крп = Ззп + Змч = 8500 + 300,56 = 8800,56 \text{ грн.}$$

3.3 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати на проєктування та впровадження проєктного варіанта системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн,$$

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 0 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, 35000 грн.;

Крп – вартість розробки політики безпеки інформації, 8800,56 грн.;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів, 85000 грн.;

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу (навчання адміністратора), 35000 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки входять, 25000 грн.

Відповідно до заданих даних розраховуємо капітальні витрати

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн =$$
$$= 35000 + 8800,56 + 85000 + 35000 + 25000 = 188800,56 \text{ грн.}$$

3.4 Розрахунок поточних експлуатаційних витрат

Поточні витрати включають:

– навчання персоналу в питаннях інформаційної безпеки;

– витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 15000 грн. – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 2000 + 1500 = 3500 \text{ грн. (в міс.)}$$

$$Сз = 3500 * 12 = 42000 \text{ грн. (рік)},$$

де Зк – додаткова заробітна плата керівника, 24000 грн. на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 18000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це,$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*12 комп'ютерів = 3,6 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 12 комп'ютерів = 23040 год. – річний фонд робочого часу системи інформаційної безпеки;

Це = 6 грн за 1 кВт/год. – тариф на електроенергію на 01.01.2024 року.

$$Се = 3,6 * 23040 * 6 = 497664 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 58800,56 * 0,02 = 1176,01 грн.$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Сз + Се + Стос =$$
$$= 15000 + 42000 + 497664 + 1176,01 = 555840,01 грн.$$

3.5 Розрахунок оцінки величини збитку

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Місячний фонд робочого часу складає 176 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 5 год.

$$Пп = (Зс/Fр) * tп = (360000/176) * 5 = 10227,27 грн.,$$

де Зс – сумарна заробітна плата персоналу, 360000 грн.

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 6 год.:

$$Пви = (120000/176) * 6 = 4090,91 грн.$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год. і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = 250 * 4 = 1000 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч =$$

$$4090,91 + 1000 + 2500 = 7590,91 \text{ грн.},$$

де Пзч = 2500 грн. - вартість для витрат на заміну частин.

О = 15750000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = O/Fp * (tп + tв + tви) = 15750000/1920 * (5 + 4 + 6) = 123046,88 \text{ грн.}$$

Fp – це річний фонд часу роботи офісу, 1920 годин;

tп – 5 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 6 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на інформаційну систему при реалізації загрози складе:

$$U = Пп + Пв + V = 10227,27 + 7590,91 + 123046,88 = 140865,06 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum i \sum n * U = 12 * 4 * 140865,06 = 6761522,88 \text{ грн.},$$

де: i- число атакованих вузлів, 12 комп'ютерів;

n – середнє число атак на рік, 4 рази.

3.6 Визначення загального ефекту від впровадження системи захисту інформації

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням B – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R – C = 6761522,88 * 0.25 - 555840,01 = 1134540,71 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій To.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

E – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

$$ROSI = E/K = 1134540,71 / 188800,56 = 6$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1/6 = 0,17 \text{ року} = 2 \text{ місяці}.$$

3.8 Висновки до Розділу 3

У цьому розділі обґрунтована економічна доцільність впровадження політики безпеки для об'єкта ОІД ТОВ «Фінанс-Дніпро». Для обґрунтування доцільності були визначені наступні фактори:

– загальні витрати на впровадження політики безпеки на підприємстві;

– передбачувані збитки за умови успішної інформаційної атаки на підприємство.

За отриманими результатами можна зробити висновок, що при атаці загальна сума збитків буде складати 6761522,88 грн. При цьому поточні експлуатаційні витрати складають 555840,01 грн, а капітальні інвестиції - 188800,56 грн., що значно менше ніж можливі збитки. Термін окупності становить 2 місяці.

Відповідно до розрахунків, виконаних в даному розділі, запропонована система захисту інформації є економічно вигідною.

ВИСНОВКИ

У вступі та в першому розділі кваліфікаційної роботи визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в ІКС, проведено огляд основних проблем захисту інформації та шляхів їх вирішення. Виконано аналіз нормативно-правової бази у сфері ЗІ та постановка задачі.

У спеціальній частині кваліфікаційної роботи наведено загальні відомості про підприємство, розглянуто питання інформаційної безпеки фінансової компанії, категоріювання інформаційних ресурсів та структура інформаційно-комунікаційної системи. Також наведено визначення профілю захищеності ІКС, аналіз загроз та їх джерел, класифікація загроз інформаційним ресурсам, моделі загроз і порушника. Розроблено та наведено політику забезпечення інформаційної безпеки та виконано аналіз ризиків після впровадження політики безпеки.

У економічній частині було розраховані витрати на розробку та впровадження політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків ІБ завдяки впровадженню політики забезпечення інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

2 Про захист інформації інформаційно-телекомунікаційних системах: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

3 Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту: [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua.

4 Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навч. посібник. – К.: Юстініан, 2016. – 176 с.

5 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 2019 – 16 с.

6 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТС31 СБ України, 2019. - 26 с.

7 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» НД ТЗІ 3.7-003-2005 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

8 Міжнародній стандарт ISO / IEC 27001:2013 «Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки - Вимоги».

9 Про інформацію: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

10 Про телекомунікації: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

11 Про захист персональних даних: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

12 Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

13 «Типове положення про службу захисту інформації в автоматизованій системі» НД ТЗІ 1.4-001-2000 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

14 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» НД ТЗІ 2.5-004-99 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

15 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» НД ТЗІ 2.5-005-99 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

16 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу" НД ТЗІ 2.5-010-03 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

17 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу» НД ТЗІ 3.6-001-2000 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

18 Політика інформаційної безпеки банку [Електронний ресурс] – Режим доступу: : http://elib.lutsk-ntu.com.ua/book/fof/bs/2021/11-15/page16.html

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	1	
5	А4	Розділ 1	21	
6	А4	Розділ 2	51	
7	А4	Розділ 3	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	4	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Презентація_ Бєлоусова.ppt
2. Кваліфікаційна робота_ Бєлоусова.doc

ДОДАТОК В. Накази щодо створення КСЗІ на ОІД

ТОВ «Фінанс-Дніпро»
вул. Мануйлівська, 37, м. Дніпро, 49000, Україна.

НАКАЗ

04. 01. 2024 м. Дніпро № 10

Про створення СЗІ
ТОВ «Фінанс-Дніпро»

НАКАЗУЮ:

1. Створити СЗІ на ОІД ТОВ «Фінанс-Дніпро» у складі:

голова: заступник директора – І.І. Їжсало
члени: системний адміністратор – О.М. Панченко
юрист – Б.А. Андрійченко

2. Контроль за виконанням цього наказу залишаю за собою.

Директор _____ А.С. Гарматин

ТОВ «Фінанс-Дніпро»
вул. Мануйлівська, 37, м. Дніпро, 49000, Україна.

НАКАЗ

04. 01. 2024 м. Дніпро № 10

Про призначення комісії з категоріювання інформації на ОІД ТОВ «Фінанс-Дніпро»

НАКАЗУЮ:

1. Створити комісію з категоріювання інформації, яка циркулює на ОІД ТОВ «Фінанс-Дніпро» у складі:

голова: заступник директора – І.І. Їжсало.
члени: системний адміністратор – О.М. Панченко.
юрист – Б.А. Андрійченко.

2. Комісії в термін до 04.02.2024 провести категоріювання інформації на ОІД, підготувати та представити на затвердження результати з категоріювання.

3. Контроль за виконанням цього наказу залишаю за собою.

Директор _____ А.С. Гарматин

ТОВ «Фінанс-Дніпро»
вул. Мануйлівська, 37, м. Дніпро, 49000, Україна.

НАКАЗ

04. 01. 2024 м. Дніпро № 12

Про призначення комісії з категоріювання та обстеження ОІД ТОВ «Фінанс-Дніпро»

Згідно з вимогами чинних документів із технічного захисту інформації та на підставі «Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»

НАКАЗУЮ:

1. Створити комісію з категоріювання та обстеження ОІД ТОВ «Фінанс-Дніпро».
2. Покласти на комісію обов'язки щодо розгляду питань категоріювання ОІД.
3. Комісії в термін до 14.02.2024 провести категоріювання ОІД, підготувати та представити на затвердження відповідний Акт.
4. Комісії в термін до 18.04.2024 провести обстеження на об'єкті інформаційної діяльності та представити на затвердження відповідний Акт.
5. Контроль за виконанням цього наказу залишаю за собою.

Директор _____ А.С. Гарматин

ТОВ «Фінанс-Дніпро»
вул. Мануйлівська, 37, м. Дніпро, 49000, Україна.

НАКАЗ

04. 01. 2024 м. Дніпро № 13

Про створення комплексної системи захисту інформації на ОІД ТОВ «Фінанс-Дніпро»

НАКАЗУЮ:

1 Створити КСЗІ на ОІД ТОВ «Фінанс-Дніпро», призначену для обробки конфіденційної інформації, що не є власністю держави.

2 Контроль за виконанням цього наказу залишаю за собою.

Директор _____ А.С. Гарматин

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-20-2 Бєлоусової К.А. на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро»

Пояснювальна записка містить 99 сторінок, 5 рисунків, 5 таблиць, 5 додатків, 18 джерел.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро».

У ході виконання кваліфікаційної роботи було визначено актуальність роботи, проаналізовано стан питання інформаційної безпеки в ІКС, проведено огляд основних проблем захисту інформації та шляхів їх вирішення. Виконано аналіз нормативно-правової бази у сфері ЗІ та постановка задачі.

У спеціальній частині кваліфікаційної роботи наведено загальні відомості про підприємство, розглянуто питання інформаційної безпеки фінансової компанії, розглянуто категоріювання інформаційних ресурсів та структура інформаційно-комунікаційної системи. Також наведено визначення профілю захищеності ІКС, проведено аналіз загроз та їх джерел, надано класифікацію загроз інформаційним ресурсам, розроблено моделі загроз і порушника.

У економічній частині було розраховані витрати на розробку та впровадження політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Фінанс-Дніпро».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків ІБ завдяки впровадженню політики забезпечення інформаційної безпеки.

В якості недоліків слід відзначити окремі невідповідності вимогам при оформленні та нечітке розкриття теми аналізу ризиків.

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

В цілому робота задовольняє усім вимогам, а її авторка Бєлоусова К.А. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**