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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента ***Бардака Ігоря Андрійовича***

академічної групи ***УБіт–15–1***

напряму підготовки ***6.170103 Управління інформаційною безпекою***

спеціалізації[1]

за освітньо–професійною програмою

на тему ***"Розробка політики безпеки інформації інформаційно–телекомунікаційної системи ТОВ «Акварель»"***

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

Дніпро
2019

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Бардаку Ігорю Андрійовичу*** **академічної групи** ***УБіт–15–1***
(прізвище ім'я по–батькові) (шифр)

напряму підготовки *6.170103 Управління інформаційною безпекою*
(код і назва спеціальності)

на тему ***"Розробка політики безпеки інформації інформаційно–телекомунікаційної системи ТОВ «Акварель»"***

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Аналіз основних проблем забезпечення захисту інформації.	20.03.2019
Розділ 2	Проведення аналізу загроз та вразливостей ТОВ «Акварель».	30.05.2019
Розділ 3	Економічне обґрунтування впровадження елементів політики безпеки інформації ТОВ «Акварель».	15.06.2019

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 17.06.2019р.

Прийнято до виконання _____ Бардак І.А.
(підпис студента) (прізвище, ініціали)

.

РЕФЕРАТ

Пояснювальна записка: 84 с., 26 табл., 4 рис., 9 додатків, 19 джерел.

Об’єкт розробки: інформаційно–телекомунікаційна система ТОВ «Акварель».

Предмет розробки: розробка елементів політики безпеки інформації інформаційно–телекомунікаційної системи ТОВ «Акварель».

Мета кваліфікаційної роботи: проведення обстеження об’єкту інформаційної діяльності, виявлення потенційних загроз та вразливостей, розробка елементів політики безпеки інформації та подальше її впровадження, розрахунок вартості грошових витрат на впровадження політики безпеки.

У першому розділі проведений аналіз нормативно–правової бази у сфері захисту інформації, озвучено стан загроз захисту інформації у країні та безпосередньо у портовій діяльності.

У другому розділі була описана необхідність створення комплексної системи захисту інформації, опис сфери діяльності підприємства, виконаний акт обстеження об’єкту інформаційної діяльності. Під час виконання другого розділу був проведений аналіз загроз та вразливостей, згідно із отриманими даними були розроблені елементи політики безпеки інформації, які направлені на мінімізацію загроз втрат важливих ресурсів компанії

В економічній частині проведений розрахунок капітальних витрат на впровадження створених елементів політик безпеки інформації.

Практична значимість роботи полягає у розробці та впровадженні політик безпеки інформації, які підвищать рівень захисту інформації.

ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, ДЖЕРЕЛА ЗАГРОЗ, ВРАЗЛИВОСТІ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ.

РЕФЕРАТ

Пояснительная записка: 84 с., 26 табл., 4 рис.,9 додатків ,19 источников

Объект разработки: информационно–телекоммуникационная система ООО «Акварель».

Предмет разработки: разработка элементов политики безопасности информации информационно–телекоммуникационной системы ООО «Акварель».

Цель квалификационной работы: проведение обследования объекта информационной деятельности, обнаружение потенциальных угроз и уязвимостей, разработка элементов политики безопасности информации, расчёт стоимости внедрения политики безопасности.

Первый раздел дипломной работы посвящён анализу нормативно–правовой базы в сфере защиты информации, осуществлено описание состояния угроз информации в стране и в портовой деятельности.

Второй раздел дипломной работы состоит из описания необходимости создания комплексной системы защиты информации, описания сферы деятельности предприятия, проведён акт обследования объекта информационной деятельности. В процессе выполнения второго раздела был проведён анализ угроз и уязвимостей, в соответствии с полученными данным после анализа были составлены элементы политики безопасности информации.

Экономическая часть квалификационной работы направлена на расчёт капитальных затрат на внедрение элементов политики безопасности информации.

Практическая значимость работы заключается в разработке и внедрении политик безопасности информации, которые направлены на повышение уровня защищённости информации.

ЗАЩИТА ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИСТОЧНИК УГРОЗЫ, УЯЗВИМОСТИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ, МОДЕЛЬ УГРОЗ.

ABSTRACT

Explanatory note: 84 p., 26 tables, 4 figures, 9 supplements, 19 sources.

Object of study: information and telecommunication system LTD "Aquarelle".

Subject of research: the development elements of information security policy information and telecommunication systems LTD "Aquarelle".

The purpose of the qualification work: the inspection of the object of information activities, the detection of potential threats and vulnerabilities, the development of information security policy and calculation of the cost of implementing a security policy elements.

The first section of the qualification work is devoted to the analysis of the regulatory framework in the field of information protection, also first selection studying description of the state of information threats in the country and in port activities is carried out.

The second section of the qualification work consists of a description of the need to create an integrated information protection system, a description of the scope of the enterprise, and a study of the object of activity. Analysis of threats and vulnerabilities, in accordance with the data obtained after the analysis were made information security policies elements.

The economic part of the qualification work is aimed at calculating the capital costs of implementing information security policy elements.

KEYWORDS: INFORMATION PROTECTION, INFORMATION SECURITY, SOURCE OF THREAT, VULNERABILITY, INFORMATION SECURITY POLICY, MODEL OF THREAT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДТЗС – допоміжні технічні засоби і системи;

ЗОТ – засоби обчислювальної техніки;

ЗУ – Закон України;

ІЗоД – інформація з обмеженим доступом;

ІКСМ – інформаційно–комунікаційні системи та мережі;

ІП – інформаційний поток;

ІТ – інформаційні технології;

КСЗІ – комплексна система захисту інформації;

КС – комп’ютерна система;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ОІД – об’єкт інформаційної діяльності.

ЗМІСТ с.

ВСТУП

Морські порти є складовою частиною транспортної і виробничої інфраструктури держави з огляду на їх розташування на шляхах міжнародних транспортних коридорів. Від ефективності функціонування морських портів, рівня їх технологічного та технічного оснащення, відповідності системи управління та розвитку інфраструктури сучасним міжнародним вимогам залежить конкурентоспроможність вітчизняного транспортного комплексу на світовому ринку.

Стрімкий розвиток інформаційних технологій створив велику кількість засобів для кращої ефективності, тому використання мережі Інтернет, комп'ютерних мереж, новітніх програмних продуктів автоматизації бізнес–процесів для порту являється основою розвитку. Стратегічна мета інформаційних технології являється сприяння керуванню транспортної інфраструктури, реагувати на динаміку ринку, створювати та підтримувати конкурентні переваги. Виконання цього завдання вимагає створення інформаційно–технологічних систем, які мають такі атрибути, як: маневреність прикладних програм, можливість отримання доступу до інформаційно технологічних ресурсів та доступність інформаційного об'єкту одночасно багатьом. Наявність великої кількості критично важливої для підприємств та організацій інформації, що зберігається і обробляється в комп'ютерних системах, призвела до створення єдиної інфраструктури. Використання даної інфраструктури дозволяє отримати доступ до інформації найбільших бібліотек і світових баз даних, оперативно виконувати складні розрахунки, швидко обмінюватися інформацією з іншими респондентами мережі незалежно від їх віддаленості один від одного – в межах міста, країни або світу. Така кількість точок доступу у значній мірі підвищує загрозу інформаційній безпеці обробки і передачі даних. Особливо вразливими виявляються дані, що передаються в глобальних телекомунікаційних мережах.

Але водночас із розвитком інформаційних технології формуються сучасні джерела загроз та вразливості, які становлять небезпеку для діяльності кожної сфери держави, в тому числі і транспортної. Тому сучасне підприємство повинне вміти належним чином будувати політику безпеки, а саме займатися розробкою та ефективним впровадженням превентивних заходів по захисту інформаційних ресурсів. При формуванні політики інформаційної безпеки важливо звернути увагу на розміри підприємства, фінансові можливості, поточний рівень інформаційної безпеки та стадію розвитку фірми.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Ми живемо у вік інформаційних технологій. Майже кожна людина не здатна явити власне життя без різних технологій, таких як, Інтернет, низка гаджетів та сервісів. Чим швидше відбувається розвиток подібних технологій, тим швидше змінюються оточуюче середовище навколо людини. В епоху таких швидких змін бізнес не здатний працювати по застарілим моделям, адже задля того, щоб не відставати від конкурентів бізнес повинен впроваджувати новітні технології. Тому компанії повинні впроваджувати новітні розробки, алгоритми роботи та застосовувати процес нововведень у бізнес, тобто глибокого трансформування самого бізнесу, включаючи використання інформаційних технологій, впровадження автоматизації бізнес–процесів та поліпшення досвіду роботи із клієнтом. Водночас із розвитком IT активно розвиваються і кіберзагрози. Кількість виявлених злочинів у сфері кібербезпеки збільшується в середньому на 2,5 тисячі кожного року. За останні 5 років Україна зазнала низку найбільших в історії держави кібератак:

– Травень 2014 року

DDoS–атака та злом сайту ЦВК під час президентських виборів, унаслідок чого на сайті з’явилась недостовірні результати всенародного голосування

– Червень 2014 року

На серверах приватних компаній Україні та країн НАТО були виявлені шкідливі програмні засоби, які використовувалися для шпигунства. Використовувалися такі програми Turla, Uroburos, Snake, RedOctober.

– Грудень 2015 року

Кібератака при якій використовувалась програма BlackEnergy3,призвела до того, що було відключено від мережі 30 підстанцій Прикарпаттяобленерго. Внаслідок даної атаки близько 200 тисяч людей залишились без електроенергії

протягом 5–7 годин. Подібні атаки були на підстанції Київобленерго та Чернівціобленерго.

– Червень 2017 року

Масштабна кібератака за допомоги вірусної програми Petya.A, яка порушила працездатність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, Ощадбанк, Укрзалізниця, Укрпошта, Укртелеком, ДТЕК, Нова пошта, Кредобанк, Укргазбанк, Кредобанк, низка українських телеканалів та мобільних операторів. Вірус шифрував внутрішні файли, тим самим блокував доступ до використання системи після чого на екрані відображувалося повідомлення із грошовою вимогою для дешифрування даних. Основною ціллю даної кібератаки була не фінансова вигода, а дестабілізація інфраструктури України [1].

Серед найбільш розповсюджених загроз, які були зафіксовані, являється вірусна атака та шкідливе програмне забезпечення, втрата даних через зовнішні та внутрішні загрози, вразливості ПЗ, втрата персональних даних та фішинг. Дані наведені у рисунку 1.

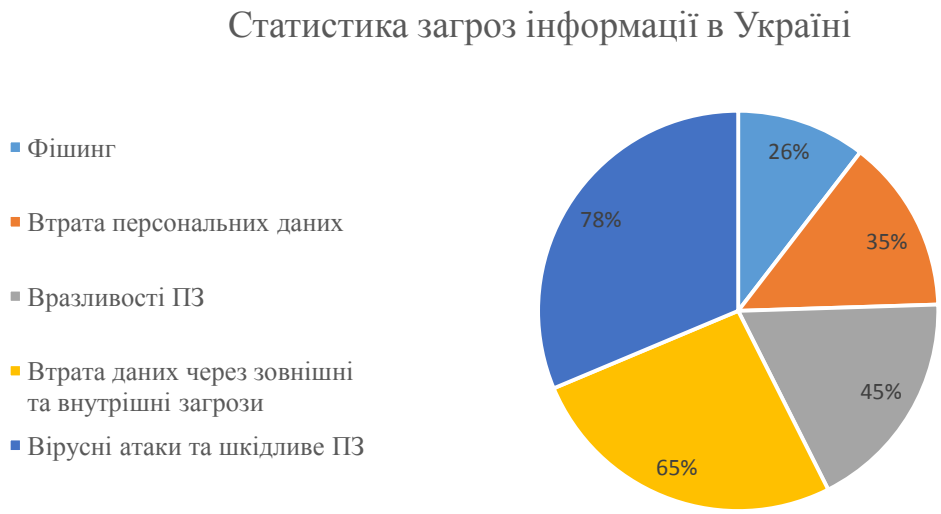


Рисунок 1 – Загрози інформації в Україні

Морський транспортний комплекс є багатофункціональною структурою, що задовольняє потреби національної економіки у транспортному забезпеченні, сприяє розвитку міжнародної торгівлі та реалізує зобов'язання України як морської держави. Водний транспорт, що обслуговується у морських портах, є найдешевшим та відносно екологічним у порівнянні з іншими видами транспорту, що робить його конкурентним всередині країни для цілей внутрішньої та міжнародної торгівлі. Морські порти є складовою частиною транспортної і виробничої інфраструктури держави з огляду на їх розташування на шляхах міжнародних транспортних коридорів. Від ефективності функціонування морських портів, рівня їх технологічного та технічного оснащення, відповідності системи управління та розвитку інфраструктури сучасним міжнародним вимогам залежить конкурентоспроможність вітчизняного транспортного комплексу на світовому ринку [2] .

Морські порти вважаються критично важливими об'єктами для економіки держави, оскільки порушення їх послуг здатне нанести збиток державній економіці. За останній період портові комплекси стали об'єктом посиленої уваги міжнародних груп та груп національної безпеки, які у свою чергу роблять все можливе для посилення контролю та запобігання можливих загроз, тому як дана сфера стикається з низкою ризиків. Загальним інтересом безпеки портових комплексів у світі, в тому числі і в Україні, являється забезпечення безпечного транспортування та стоянка судна із вантажем. Відомо, що контейнери являються засобом для транспортування заборонених засобів, мігрантів, тому перевірка контейнера на порушення являється основною задачею забезпечення безпеки функціонування діяльності портового комплексу. Також присутні загрози захисту інформації,

Можна виділити низку загроз захисту інформації:

– програмні (кіберзлочинність);

– технічні (перехоплення інформації, пошкодження роботи радіосигналу);

– режимні (несанкціонований доступ до інформаційних ресурсів);

– антропогенні (відсутність кваліфікаційного рівня персоналу).

Необхідно розуміти важливість високого рівня інформаційної безпеки. Із зростанням рівня кіберзлочинності ступінь поінформованості зростає так само і тому керівництво портових комплексів повинно з більшою відповідальністю ставитися до створення компетентного та конкурентоспроможного рівня інформаційної безпеки. Сучасне підприємство повинне вміти належним чином будувати політику інформаційної безпеки, а саме займатися розробкою та ефективним впровадженням превентивних заходів по захисту інформаційних ресурсів. При формуванні політики інформаційної безпеки важливо звернути увагу на розміри портового комплексу, фінансові можливості, поточний рівень інформаційної безпеки та стадію розвитку фірми. Захист інформації в системі обробки інформації повинен базуватися за принципами: системності, комплексності, розумової достатності, відкритості алгоритму та простоти застосування захисних заходів та 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 [3]. При виконанні комплексного принципу фахівці із забезпечення інформаційної безпеки застосовують широкий спектр заходів, методів, та засобів захисту комп'ютерних систем. Головним аспектом використання комплексного принципу являється узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації загроз і не містить слабких місць на стиках окремих її компонентів. Принцип розумової достатності базується на вірному виборі рівня захисту при якому витрати, ризик і розмір можливого збитку були б прийнятними. Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не

повинен забезпечуватися тільки за рахунок обмеження доступу до структурної організації та алгоритмів функціонування її підсистем. Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових трудовитрат при звичайній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (введення декількох паролів та імен і т. д.).

Тому до питання забезпечення інформаційної безпеки необхідно ставитися серйозно, адже воно являється вкрай важливим. Провідні галузі країни потребують забезпечення кваліфікаційного та конкурентоспроможного рівня безпеки. Дане забезпечення являється основою ефективного функціонування усіх сфер держави, у тому числі і сфері вантажообігу.

1.2 Аналіз нормативно–правового забезпечення захисту інформації

Питання забезпечення захисту інформації знаходяться під постійним контролем та регулюванням, як зі сторони держави, так і зі сторони структур керування підприємствами. Нормативно – правова база для вирішення питань безпеки інформації являється у першу чергу вимогою чинного українського законодавства, яка визначає обов’язковість захисту інформації із обмеженим доступом, у тому числі персональні дані громадян, усіма суб’єктами інформаційних відносин на всій території України.

На території України чинності набувають наступні нормативно–правові акти та Закони України:

– Закон України «Про інформацію»

Цей Закон закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності [4] .

– Закон України «Про захист інформації в інформаційно–телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах [5].

– Концепція національної безпеки України

Цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони [6] .

– Закон України «Про державну таємницю»

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. [7]

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно–апаратних засобів слід керуватися низкою нормативно–правових документів та актів. Базовими нормативними документами при організації та побудови комплексної системи захисту інформації ІКСМ є:

– НД ТЗІ 1.1–002–99: Загальні положення з захисту інформації в комп’ютерних системах від НСД;

Цей нормативний документ технічного захисту інформації визначає методологічні основи (концепцію) вирішення завдань захисту інформації в

комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання: визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу, створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу, оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача [8] .

– НД ТЗІ 1.1–003–99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов'язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації [9] .

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

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі – "Положення про службу захисту інформації в автоматизованій системі" [10] .

– НД ТЗІ 2.5–005–99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу [11] .

Захист інформації на підприємстві здійснюється із використанням міжнародного підходу на основі документів серії ДСТУ серії номер 27:

– ДСТУ ISO/IEC 27001:2015 викладає вимоги до методів захисту системи управління інформаційною безпекою. Містить в собі інформацію для визначення сфери застосування системи управління інформаційною безпекою

та оцінювання ризиків інформаційної безпеки та їх обробку, оцінку, моніторинг, вимірювання та аналіз результативності [12] .

–ДСТУ ISO/IEC 27002:2015 викладає методики захисту та звід практик щодо заходів інформаційної безпеки, вимоги до її забезпечення, категорії безпеки, принципи її управління та політики інформаційної безпеки. Регламентує управління ресурсами СУІБ, відповідальність за її ресурси [13] .

– ДСТУ ISO/IEC 27005:2017 Цей стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації [14].

Нормативно–правова база, яка регулює питання відносин між людьми в сфері захисту інформації постійно оновлюється та вдосконалюється. Оновлення документів засвідчує факт того, що із розвитком технологій, необхідно модернізувати юридичну базу. Враховуючи перелік документів формується розуміння того, що сфера захисту інформації являється достатньо великою та потребує більших сил для ведення правового урегулювання, сам тому документи повинні оновлюватись частіше на цілісніше.

1.3 Постановка задачі

На період виконання кваліфікаційної роботи були сформовані та поставлені наступні задачі:

- проведення аналізу нормативно–правового захисту інформації;
- виконання акту обстеження об’єкта інформаційної діяльності;
- детальне обґрунтовування необхідності створення КСЗІ;
- проведення аналізу ризиків;
- розробка елементів політики безпеки;
- аналізу ризиків після впровадження політик безпеки інформації;
- розрахування трудоємності та затрат на створення та впровадження політики безпеки.

1.4 Висновок

У першому розділі дипломного проекту був описаний стан питання забезпечення інформаційної безпеки у портовій діяльності, огляд основних проблем із забезпеченням захисту інформації. Проведений аналіз нормативно–правового забезпечення захисту інформації та постановка задачі для подальшої роботи.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Обґрунтування необхідності створення КСЗІ

Інформація, яка являється власністю держави та інформація з обмеженим доступом підлягають обов'язковому захисту згідно чинного законодавства України і вимог окремих нормативних документів ЗУ, а саме:

– Закон України «Про захист персональних даних» [14];

– Закон України «Про захист інформації в інформаційно–телекомунікаційних системах» [5].

Згідно Законів України «Про захист інформації в інформаційно–телекомунікаційних системах» ст.4 п.1 та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Власник інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, у разі відсутності суперечності чинному законодавству. У відділі експлуатації та інформаційному відділі комплексу «Акварель» циркулює інформація з обмеженим доступом (база даних клієнтів, база даних прийому та відправки товарів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності

здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

У процес створення КСЗІ залучаються такі сторони:

- організація, для якої здійснюється побудова КСЗІ (Замовник);
- організація, що здійснює заходи з побудови КСЗІ (Виконавець);
- Адміністрація Державної служби спеціального зв'язку та захисту інформації України;
- організація, що здійснює державну експертизу КСЗІ;
- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник) [15].

2.2 Загальні відомості про підприємство

Об’єктом дослідження являється портовий комплекс «Вантажний термінал ООО “Акварель”», м. Дніпро (далі «комплекс»). Комплекс був введений в експлуатацію у травні 2010 року та знаходиться у центральному регіоні України на водяній артерії країни – ріки Дніпро. Комплекс зафіксований у єдиному реєстрі портів України. Наявність у даному реєстрі надає можливість приймати судна класу «ріка–море», які працюють як під українським прапором, так і під прапорами іноземних держав. Комплекс являється генеральним агентом єдиної в Україні контейнерної лінії «Tavria Line», володіючи двома власними суднами–контейнеровозами та парком власних контейнерів. Єдність цих двох компаній успішно працювала за турецьким напрямком, здійснюючи регулярні рейси між портами Туреччини та Дніпропетровська. На сьогоднішній день логістичний комплекс займає міцну позицію серед ринку транспортування вантажу в Україні та продовжує набирати стрімкі обороти розвитку.

Організаційна структура комплексу побудована за лінійно–функціонально ознакою. Організаційна структура комплексу наведена у рисунку 2. До штату компанії входить 12 людей. На території офісу присутні 4 представники охоронної компанії. Один екіпаж фізичної охорони (2 людини), два співробітника відділу моніторингу камер відеоспостереження. Комплекс функціонує згідно із чинним законодавством України.

1 Керівництво (начальник порту, заступник начальника порту) – 2 людини. Координують роботу усіх відділів.

2 Відділ служби внутрішньої безпеки (керівник відділу, 2 співробітника) – займаються перевіркою документації, відповідають за дотриманням безпеки вантажу, забезпечують безпеку всередині організації (шахрайство, крадіжки), формують акти проведення робіт. Звітують керівництву порту.

3 Інформаційний відділ (керівник відділу,2 співробітника) – формують зворотній зв'язок із постачальником вантажу та адресатом, забезпечують ведення комп'ютерних баз даних та адмініструють АС .

4 Відділ експлуатації (керівник, 2 людини) – відповідальні за прийом та розміщення вантажу, оформлення належних документів. Звітують керівництву порту та відділу служби безпеки.

5 Фінансово–економічний відділ (керівник фінансово–економічного відділу, 2 людини) – розробляють бухгалтерський та фінансовий облік, а також проводять інші економічні розрахунки. Звітують керівництву порту.

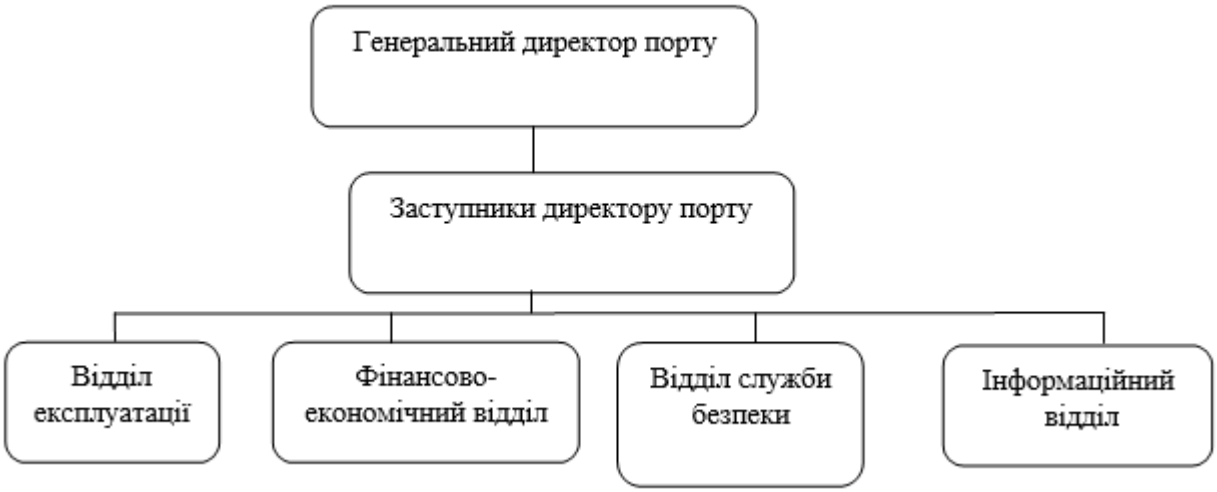


Рисунок 2.1 – Організаційна структура комплексу «Акварель»

Аналіз оброблюваної інформації

Співробітниками оброблюється та зберігається велика кількість інформації, що має обмежений доступ: бази даних постачальників, відомості товару, маршрути кораблів, фінансова звітність та інше. Всі документи створюються відповідними працівниками на своїх робочих станціях за допомогою встановленого ПЗ та роздруковуються на принтерах чи розмножуються. Електрона копія зберігається або на робочий станції працівника або в спеціально відведеному місці (папка на диску) на сервері для документів, роздрукований паперовий варіант зберігається в столі. Після втрати необхідності документа він знищується. Облік місця та режиму зберігання носіїв інформації а також їх переміщення на обстежуваному ОІД не ведеться.

Детальний перелік інформації, її правовий режим, вид зберігання та вимогу до захисту зображений в таблиці 2.1. Схема зображення інформаційних потоків наведена у рисунку 2.2. В таблиці 2.2 вказано, як авторизовані користувачі мережі можуть здійснювати керування інформацією.

Таблиця 2.1 – Оброблювана інформація

№	Інформація	Вид зберігання	Режим доступу	Вимоги до захисту
1	База даних клієнтів (постачальників)	Електронний	ІЗоД	КЦД
2	Документи виробничої діяльності	Електронний, паперовий	ІЗоД	КЦД
3	Фінансова звітність	Електронний	ІЗоД	КЦД
4	База даних прийому та відправки товарів	Електронний	ІЗоД	КЦД
5	Розпорядження про алгоритм прийому товарів	Електронний, паперовий	ІЗоД	КЦД

Продовження таблиці 2.1

№	Інформація	Вид зберігання	Режим доступу	Вимоги до захисту
6	База даних партнерів компаній	Електронний	Відкрита	–
7	Формування та ведення реєстру форм звітних документів	Електронний	ІЗоД	КЦД
8	Внутрішня документація	Електронний	ІЗоД	КЦД
9	Розпорядження про алгоритм охорони товарів	Електронний	ІЗоД	КЦД
10	Інформація про діяльність порту	Електронний	Відкрита	–
11	Акт роботи відділу ВСБ	Електронний, паперовий	ІЗоД	КЦД
12	Акт роботи інформаційного відділу	Електронний, паперовий	ІЗоД	КЦД
13	Акт роботи експлуатаційного відділу	Електронний, паперовий	ІЗоД	КЦД
14	Акт роботи фінансово–	Електронний,	ІЗоД	КЦД

	економічного відділу	паперовий		

Згідно до таблиці:

К – вимоги до конфіденційності;

Ц – вимога до цілісності;

Д – вимога до доступності;

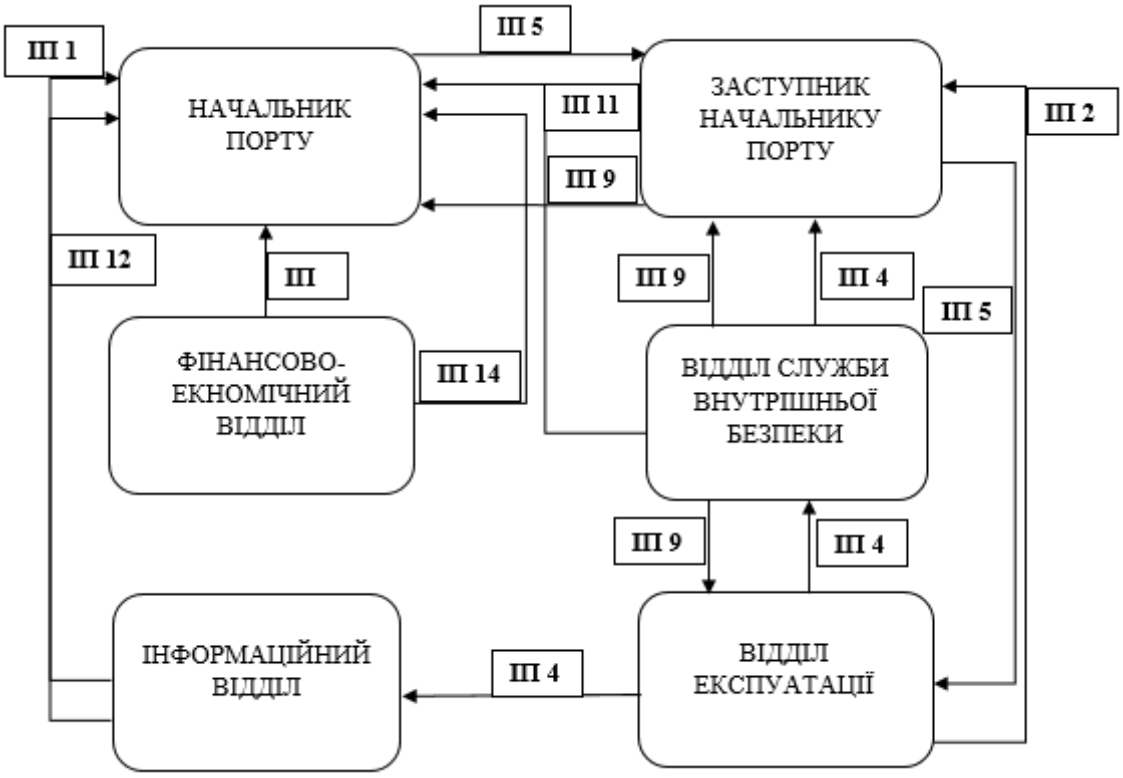


Рисунок 2.2 – Інформаційні потоки ТОВ “Акварель”

Функціональний профіль захищеності

У комплексі використовується АС класу 3 – розподілений багатомашинний комплекс, з підвищеними вимогами до забезпечення

конфіденційності, цілісності і доступності оброблюваної інформації. Де є необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. [17] Згідно із НДТЗІ 1.6, а саме п.5.16 комплексу присвоюється четверта категорія.[16] Керівництвом комплексу було узгоджено створити КСЗІ для ІТС підприємства. Згідно до наказу [ДОДАТОК Е] від 16.01.19.Стандартний функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = КД–2, КО–1, КВ–1, ЦД–1, ЦО–1, ЦВ–1, ДР–1, ДВ–1, НР–2, НИ–2, НК–1, НО–2, НЦ–2, НТ–2, НВ–1

КД–2 – базова довірча конфіденційність. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КО–1 – Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КВ–1 – Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

ЦД–1 – Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Користувача і захищеного об'єкта користувача і захищеного об'єкта.

ЦО–1 – Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

ЦВ–1 – 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.

ДР–1 – Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

ДВ–1 – 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.

НР–2 – КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

НИ–2 – Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути.

НК–1 – Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО–2 – Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора.

НЦ–2 – Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

НТ–2 – Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

НВ–1 – 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.

Таблиця 2.2 – Матриця доступу до інформації

Інформація	Посада											
	НП	ЗНП	ГФВ	ПФВ	ГСВБ	ПСВБ	ПСВБ	ГІВ	ПІВ	ПІВ	ГВЕ	ПВЕ
1	П,З,М	П	П	П	П	П	П	П,М	П	П	П	П
2	П.Д	П	П,М	П	–	–	–	–	–	–	–	–
3	П,Д	П	П,Д,М,З	П,М	П	П	П	–	–	–		
4	П,З,М	П,М	П	–	П	П	П	П,М	П	П	П,М,Д	П
5	П,З,М,Д	П	–	–	П,Д	П	П	–	–	–	П,Д,М	П
6	П,М	П	П	П	П	П	П	П,М,Д	П,М	П,М	П	П
7	П,М	–	–	–	П	П	П	П,М	П	П	П	–
8	П,М,З	П	П	П	П	П	П	П	П	П	П	П
9	П	П	–	–	П,М,З	П	П	П	–	–	–	–
10	П,Д,З	П	П	П	П	П	П	П	П	П	П	П
11	П,Д,З	П	–	–	П,М,З	П	П	–	–	–	–	–
12	П,Д,З	П	–	–	–	–	–	П,М,З	П,М	П,М	–	–
13	П,Д,З	П	–	–	–	–	–	–	–	–	П,Д,М	П
14	П,Д,З	П	П,Д,М	П,М	–	–	–	–	–	–	–	–

П – перегляд інформації; М – модифікація інформації; З – знищення інформації, Д– друк

2.3 Обстеження об’єкта інформаційної діяльності

Офіс комплексу розташований за адресою м. Дніпро, вул. Верстова, 43а., офісне приміщення займає два поверхи будинку. Графік понеділок–п’ятниця с 09:00 до 20:00. Субота та неділя вихідні дні. В офісі розташований пульт пожежної сигналізації. Прибирання відбувається один раз у чотири дні. Графік прибирання клінінгової компанії з 09:20 до 10:00. Послуги охорони надаються сервісом «Охорона–ОКО». Офіс підключений до ЦПО «Охорона–ОКО». Графік роботи охорони з 09:00 до 20:00 та з 20:00 до 09:00. На території порту присутній один екіпаж фізичної охорони (2 людини), також дві людини займаються моніторингом камер відеоспостереження, знаходячись в офісному приміщенні. На КЗ знаходиться 5 камер відеоспостереження. Доступом до камер відеоспостереження володіють працівники охоронного агентства, начальник порту та начальник відділу служби безпеки. Офіс оснащений системою контролю і управління доступом. Кожний працівник компанії має магнітну карту завдяки якій здатний увійти до офісного приміщення. Пропуск сторонніх осіб на територію КЗ здійснюється лише із узгодженням з керівництвом порту. Територія портового комплексу має зовнішній контрольно–пропускний пункт із залізними воротами та шлагбаумом на заході.

Перелік організацій, що розташовані біля офісу:

СТО «Пегас» – західний напрямок

ТОВ НВП «Укроагрокомплекс» – північно–західний напрямок

ТД «Ельба»– східний напрямок

Опис ситуаційного плану

Контрольована зона визначена наказом начальника порту №556 від 28.05.2015 р. та складає 9654 м^2. На КЗ знаходиться 4 камери відеоспостереження. Дві камери на вході до офісного приміщення. Одна КПП. Одна біля розвантажувальної точки. Ситуаційний план наведений у додатку А. Прилеглі споруди відносно КЗ вказані у таблиці 2.3

Таблиця 2.3 – Прилеглі споруди відносно ОІД

Тип споруди	Назва	Місце знаходження від ОІД	Мін. відстань від ОІД	Кількість поверхів
Промислова	СТО «ПЕГАС»	Північно–західний напрямок	35 м.	1
Промислова	ТОВ НВП «УКРАГРОКОМ»	Північно–західний напрямок	100 м.	5
Промислова	ТБ «ЕЛЬБА»	Північний напрямок	200 м.	6

Прилеглі вулиці відносно КЗ вказані у таблиці 2.4

Таблиця 2.4 – Прилеглі вулиці відносно КЗ

Назва вулиці	Описання
Мілова	Відносно ОІД вулиця знаходиться у західній стороні. Рух автомобілів малоактивний (10–30 автомобілів на годину). Ширина проїжджої частини 7 метрів. Пішохідна зона 10 метрів.

Комунікаційні системи КЗ вказані у таблиці 2.5

Таблиця 2.5 – Комунікаційні системи

Вид комунікацій	Характеристика
Система опалення	Підключена до міської мережі опалення «Теплоенерго», знаходиться за межами КЗ.

Продовження таблиці 2.5

Вид комунікацій	Характеристика
Електроживлення	Підключено до трансформаторної підстанції ТП № 91 «ДТЕК Дніпровські Електромережі», котра обслуговує сторонніх споживачів і виходить за межі КЗ.
Система водопостачання	Підключена до міського водоканалу «Водоканал», котрий виходить за межі КЗ
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ.
Система заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.
Мобільний зв'язок	Мобільна лінія «Київстар». На всіх співробітників виділені мобільні номера. Виходить за межі КЗ.
Лінія постачання мережі Інтернет	Підключена до Інтернет–провайдеру «Sata–group», знаходиться за межами КЗ.

Опис генерального плану

Розташування кімнат та їх розмір, технічних засобів вказаний на генеральному плані. Генеральний план першого та другого поверху наведений у додатку Б. Перелік технічних засобів вказаний у таблиці 2.6

Таблиця 2.6 – Технічні засоби

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування
1	Системний блок	DELL Vostro 3668	SP000001	На столі
2	Системний блок	DELL Vostro 3668	SP000002	На столі
3	Системний блок	DELL Vostro 3668	SP000003	На столі
4	Системний блок	DELL Vostro 3668	SP000004	На столі
5	Системний блок	DELL Vostro 3668	SP000005	На столі
6	Системний блок	DELL Vostro 3668	SP000006	На столі
7	Системний блок	DELL Vostro 3668	SP000007	На столі
8	Системний блок	DELL Vostro 3668	SP000008	На підлозі
9	Системний блок	DELL Vostro 3668	SP000009	На підлозі
10	Системний блок	DELL Vostro 3668	SP0000010	На підлозі
11	Системний блок	DELL Vostro 3668	SP0000011	На підлозі
12	Системний блок	DELL Vostro 3668	SP0000012	На підлозі
13	Монітор	Asus VP228DEC	MO111111	На столі

Продовження таблиці 2.6

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування
14	Монітор	Asus VP228DEC	MO111112	На столі
15	Монітор	Asus VP228DEC	MO111113	На столі
16	Монітор	Asus VP228DEC	MO111114	На столі
17	Монітор	Asus VP228DEC	MO111115	На столі
18	Монітор	Asus VP228DEC	MO111116	На столі
19	Монітор	Asus VP228DEC	MO111117	На столі
20	Монітор	Asus VP228DEC	MO111118	На столі
21	Монітор	Asus VP228DEC	MO111119	На столі
22	Монітор	Asus VP228DEC	MO1111110	На столі
23	Монітор	Asus VP228DEC	MO1111111	На столі
24	Монітор	Asus VP228DEC	MO1111112	На столі
25	Відеокамера	Uniview– IPC26	CAM999991	На стіні
26	Відеокамера	Uniview– IPC26	CAM999992	На стіні
27	Відеокамера	Uniview– IPC26	CAM999993	На стіні
29	Відеокамера	Uniview– IPC26	CAM999994	На стіні
30	Відеокамера	Uniview– IPC26	CAM999995	На стовпу
31	Проектор	ZelCaw	WI0000001	На стіні
32	Принтер	HP–Deskjet1515	HP00000001	На столі
33	Комутатор	Tenda TEF1126P	CM0000001	На столі
34	Маршрутизатор	TP–Link–WRN841	MR00000001	На столі
35	Сервер	Dell PowerEdge R410 LFF	SV000001	На столі
36	Сервер	Dell PowerEdge R410 LFF	SV0000001	На столі
37	Моноблок	Asus Vivo AiO V222UBK	AS00001SEC	На столі
38	Моноблок	Asus Vivo AiO V222UBK	AS00002SEC	На столі

Опис ДТЗС вказані у таблиці 2.7 та 2.8

Таблиця 2.7 – ДТЗС у суміжних зонах з ОІД

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування
39	Мікрохвильова піч	Mastex GV–1234	MG00001	На столі
40	Електрочайник	Goop NJ–132	GH000001	На столі

Таблиця 2.8 – Допоміжні технічні засоби та системи у зоні ОІД

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування
41	Кондиціонер	LG CN–4921	CC000001	На стіні
42	Кондиціонер	LG GoldnF2145	CC000002	На стіні
43	Клавіатура	BRAVIS JK–4	KD00000001	На столі
44	Клавіатура	BRAVIS JK–4	KD00000002	На столі
45	Клавіатура	BRAVIS JK–4	KD00000003	На столі
46	Клавіатура	BRAVIS JK–4	KD00000004	На столі
47	Клавіатура	BRAVIS JK–4	KD00000005	На столі
48	Клавіатура	BRAVIS JK–4	KD00000006	На столі
49	Клавіатура	BRAVIS JK–4	KD00000007	На столі
50	Клавіатура	BRAVIS JK–4	KD00000008	На столі
51	Клавіатура	BRAVIS JK–4	KD00000009	На столі
52	Клавіатура	BRAVIS JK–4	KD000000010	На столі
53	Клавіатура	BRAVIS JK–4	KD000000011	На столі
54	Клавіатура	BRAVIS JK–4	KD000000012	На столі
55	Комп’ютерна мишка	Logitech KH12	MB000001	На столі
56	Комп’ютерна мишка	Logitech KH12	MB000002	На столі
57	Комп’ютерна мишка	Logitech KH12	MB000003	На столі
58	Комп’ютерна мишка	Logitech KH12	MB000004	На столі
59	Комп’ютерна мишка	Logitech KH12	MB000005	На столі
60	Комп’ютерна мишка	Logitech KH12	MB000006	На столі
61	Комп’ютерна мишка	Logitech KH12	MB000007	На столі
62	Комп’ютерна мишка	Logitech KH12	MB000008	На столі
63	Комп’ютерна мишка	Logitech KH12	MB000009	На столі
64	Комп’ютерна мишка	Logitech KH12	MB0000010	На столі
65	Комп’ютерна мишка	Logitech KH12	MB0000011	На столі
66	Комп’ютерна мишка	Logitech KH12	MB0000012	На столі
67	Датчик диму	Lofasar 98Z	SMK120001	На стелі

Продовження таблиці 2.8

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування
68	Датчик диму	Lofasar 98Z	SMK120002	На стелі
69	Датчик диму	Lofasar 98Z	SMK120003	На стелі
70	Датчик диму	Lofasar 98Z	SMK120004	На стелі
71	Датчик диму	Lofasar 98Z	SMK120005	На стелі
72	Датчик диму	Lofasar 98Z	SMK120006	На стелі
73	Датчик диму	Lofasar 98Z	SMK120007	На стелі
74	Датчик диму	Lofasar 98Z	SMK120008	На стелі
75	Магнітний замок	BlockForce–1322	BH000000001	На стіні
76	Магнітний замок	BlockForce–1322	BH000000002	На стіні
77	Магнітний замок	BlockForce–1322	BH000000003	На стіні
78	Магнітний замок	BlockForce–1322	BH000000004	На стіні
79	Магнітний замок	BlockForce–1322	BH000000005	На стіні
80	Магнітний замок	BlockForce–1322	BH000000006	На стіні

Характеристика обчислювальних систем вказані у таблиці 2.8 та 2.9.

Таблиця 2.8 – Характеристики ОС DELL Vostro 3668

Тип	Повна назва	Серійний номер	Потужність
Процесор	Intel Core i5–7400 (Kaby Lake	SP000001-12	–
Материнська плата	Gigabyte GA–H110M–S2	SP000001-12	–
ОЗП	Kingstone RAM	SP000001-12	4 ГБ
Графічний відеоадаптер	Intel HD Graphics 630	SP000001-12	1 ГБ
ПЗП (SSD)	Moosnstone Losy	SP000001-12	1 ТБ
Блок живлення	Aerocool VX 500 Plus	SP000001-12	500 Вт

Таблиця 2.9 – Характеристики ОС Asus Vivo AiO V222UBK

Тип	Повна назва	Серійний номер	Потужність
Процесор	AMD RYZEN 3	AS00001SEC	–
Материнська плата	Gigabyte ZN–BZ0M–S2	AS00001SEC	–
Графічний відеоадаптер	GeForce MX110	AS00001SEC	1 ГБ

Продовження таблиці 2.9

Тип	Повна назва	Серійний номер	Потужність
ОЗП	Kingstone RAM	AS00001SEC	2 ГБ
ПЗП (SSD)	Moosnstone Losy ZN	AS00001SEC	1 ТБ
Блок живлення	ChieftekVX 500 Plus	AS00001SEC	500 Вт

Характеристики програмного забезпечення вказані у таблицях 2.10 та 2.11.

Таблиця 2.10 – Програмне забезпечення ОС DELL Vostro 3668

Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
Opera	Прикладне	1.1	Не потребує	12
Telegram	Прикладне	1.6	Не потребує	12
Google Chrome	Прикладне	5.6	Не потребує	11
Notepad++	Прикладне	9.1	Не потребує	12
Windows 10 Enterprise	Системне	1803	–	12
Skype	Прикладне	6.5	Не потребує	12
IntelDriverPACK	Системне	23.55	+	12
Microsoft Office 2013	Прикладне	333.553	–	12
Lightshot	Прикладне	435.55	+	12
MindManager	Прикладне	6756.55	–	12
GackOffice	Прикладне	1.11	+	12
AdobeAcrobatDC	Прикладне	6.1	+	12

Таблиця 2.11 – Програмне забезпечення ОС Asus Vivo AiO V222UBK

Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
Opera	Прикладне	1.1	Не потребує	2
Telegram	Прикладне	1.6	Не потребує	2
Skype	Прикладне	6.5	Не потребує	2
CamView	Прикладне	3.0	Не потребує	2
Notepad++	Прикладне	9.1	Не потребує	2
Windows 10	Системне	1803	+	2
MPC HC	Прикладне	1.9	Не потребує	2

Продовження таблиці 2.11

Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
Microsoft Office 2013	Прикладне	333.553	+	2
CameraPAD	Прикладне	1.10	Не потребує	2

Топологія мережі

Локальна мережа має архітектуру «зірка». Вихід комп'ютерів до мережі Інтернет забезпечується за допомогою встановленого комутатору під'єднаного до провайдера «SATA–GROUP». IP камери підключені до сигналу WiFi,

Точка підключення знаходиться за межами КЗ, обладнання провайдера складається із оптоволоконного Ethernet кабелю.

Перелік обладнання, що приймає участь в обробці інформації на ОІД:

1 Комп'ютер начальника порту (КНП);
2 Комп'ютер заступника начальника порту (КЗНП);
3 Комп'ютер голови фінансово–економічного відділу (КГФВ);
4 Комп'ютер працівника фінансово–економічного відділу (КПФВ);
5 Комп'ютер голови служби внутрішньої безпеки (КГСБ);
6 Комп'ютер працівника служби внутрішньої безпеки (КПСВБ);
7 Комп'ютер працівника служби внутрішньої безпеки (КПСВБ);
8 Комп'ютер голови інформаційного відділу (КГІВ);
9 Комп'ютер працівника інформаційного відділу (КПІВ);
10 Комп'ютер працівника інформаційного відділу (КПІВ);
11 Комп'ютер голови відділу експлуатації (КГВЕ);
12 Комп'ютер працівника відділу експлуатації (КПВЕ);
13 Моноблок співробітника відділу моніторингу (МСВМ);
14 Моноблок співробітника відділу моніторингу (МСВМ).

Комп'ютери штатних працівників належать до єдиної робочої групи «AQAWORK». Співробітникам охоронної компанії, які займаються

моніторингом камер відеоспостереження доступ до робочої групи не надається. Функціональна схема комп'ютерної мережі наведена рисунку 2.1

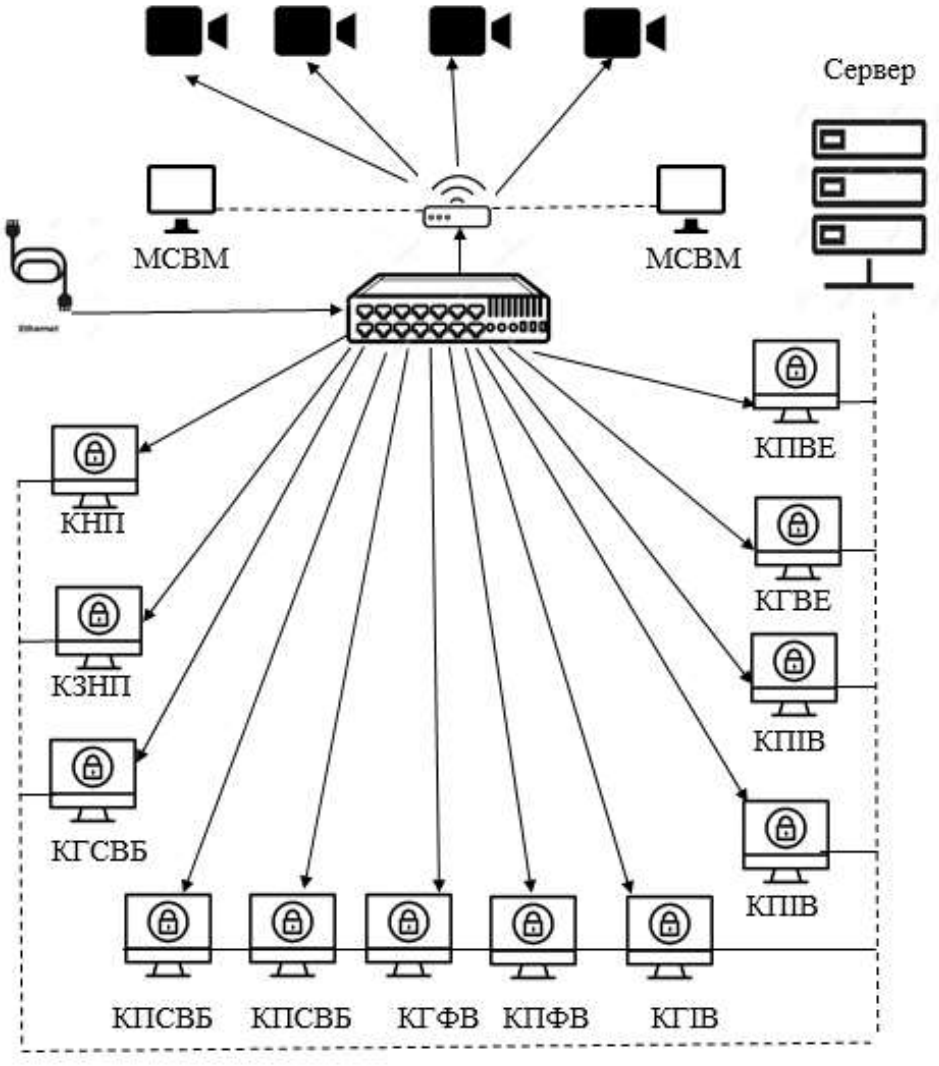


Рисунок 2.1 – Схема комп'ютерної мережі комплексу

2.4 Аналіз загроз та вразливостей

Забезпечення захисту інформації повинно носити комплексний характер та базуватися на глибокому аналізі можливих негативних наслідків. Під час проведення такого аналізу дуже важливо не упустити істотні аспекти. Аналіз негативних наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз, факторів, які сприяють їх прояву та, як наслідок, зазначення актуальних загроз безпеки інформації [18,19].

Джерела загроз інформаційній безпеці поділяються на три основні групи:

– Антропогенні (зумовлені діями суб’єкта)

– Техногенні (зумовлені технічними засобами)

– Стихійні

Загрози визначаються коефіцієнтом рівня небезпеки $К_{небезпеки}$ наступною формулою:

$$К_{небезпеки} = \frac{К1 * К2 * К3}{125} \quad (2.1)$$

125 – це максимальне число добутку показників $К_{небезпеки}$

Антропогенні суб’єктивні та об’єктивні джерела загроз та вразливості.

Розрахунок відбувається за формулою 2.1 :

де К1 – ступінь доступності до об’єкту;

К2 – ступінь кваліфікації і мотивації;

К3 – рівень наслідків (фатальність).

Перелік можливих антропогенних джерел загроз вказаний у таблиці 2.12

Таблиця 2.12 – Перелік можливих антропогенних джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Начальник порту	5	1	5	25	0,20
Заступник начальнику порту	5	1	5	25	0,20
Керівник фінансово–економічного відділу	4	3	3	36	0,30
Співробітник фінансово–економічного відділу	3	2	3	18	0,14
Керівник відділу служби внутрішньої безпеки	4	3	4	48	0,39

Продовження таблиці 2.12

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Співробітники відділу служби внутрішньої безпеки	3	3	3	27	0,21
Керівник інформаційного відділу	4	5	4	80	0,64
Співробітники інформаційного відділу	4	2	3	24	0,19
Керівник відділу експлуатації	4	3	3	36	0,29
Співробітник відділу експлуатації	4	3	2	24	0,19
Допоміжний персонал (охорона, прибиральниця)	1	3	1	3	0,02
Конкуренти	4	3	4	48	0,38
Хакери	4	4	5	80	0,64

Коефіцієнт вразливостей розраховується за формулою 2.1 :

де К1 – ступінь впливу вразливості на не усунення наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз;

К3 – кількість елементів об’єкту.

Перелік ймовірних об’єктивних та суб’єктивних вразливостей наведений у таблиці 2.13 та 2.14

Таблиця 2.13 – Перелік об’єктивних антропогенних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Вразливості, що активізуються					
Монтаж прослуховуючих пристроїв	2	4	2	12	0,10
Шкідливе програмне забезпечення	3	3	3	27	0,21
Вразливості, які об’єктом захисту					
Пряма зона перегляду видимості об’єкту	2	2	2	8	0,06

Таблиця 2.14 – Перелік антропогенних суб’єктивних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Помилки					
Встановлення та використання неліцензійного програмного забезпечення	4	4	4	64	0,51
Помилки при використані засобів обміну інформацією	4	4	4	64	0,51
Порушення					
Обміну, збереження та розповсюдження документів	3	4	3	36	0,29

Взаємозв’язок джерел загроз і властивостей відображено у таблиці 2.15 та 2.16

Значення коефіцієнтів:

К1 – коефіцієнт небезпеки для джерел загроз;

К2 – коефіцієнт небезпеки для вразливостей;

К3 – коефіцієнт взаємозв’язку джерела загрози та вразливості.

Таблиця 2.15 – Взаємозв’язок джерел загроз і суб’єктивних антропогенних вразливостей

Джерело загроз	К1	Вразливість	К2	К3
Начальник порту	0,20	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,10
		Помилки при використані засобів обміну інформацією	0,51	0,10
		Порушення обміну, збереження та розповсюдження документів	0,29	0,03
Заступник начальнику порту	0,20	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,10

		Помилки при використані засобів обміну інформацією	0,51	0,10
		Порушення обміну, збереження та розповсюдження документів	0,29	0,03

Продовження таблиці 2.15

Джерело загроз	К1	Вразливість	К2	К3
Керівник фінансово–економічного відділу	0,30	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,15
		Помилки при використані засобів обміну інформацією	0,51	0,15
		Порушення обміну, збереження та розповсюдження документів	0,29	0,07
Співробітник фінансово–економічного відділу	0,14	Помилки при використані засобів обміну інформацією	0,51	0,07
		Встановлення та використання неліцензійного програмного забезпечення	0,51	0,07
		Порушення обміну, збереження та розповсюдження документів	0,29	0,04
Керівник відділу служби внутрішньої безпеки	0,39	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,19
		Помилки при використані засобів обміну інформацією	0,51	0,19
		Порушення обміну, збереження та розповсюдження документів	0,29	0,10
Співробітники відділу служби внутрішньої безпеки	0,21	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,10
		Помилки при використані засобів обміну інформацією	0,51	0,10
		Порушення обміну, збереження та розповсюдження документів	0,29	0,06
Керівник інформаційного відділу	0,64	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,32
		Помилки при використані засобів обміну інформацією	0,51	0,32

		Порушення обміну, збереження та розповсюдження документів	0,29	0,18

Продовження таблиці 2.15

Джерело загроз	К1	Вразливість	К2	К3
Співробітники інформаційного відділу	0,19	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,09
		Порушення обміну, збереження та розповсюдження документів	0,29	0,05
		Помилки при використані засобів обміну інформацією	0,51	0,09
Керівник відділу експлуатації	0,29	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,14
		Помилки при використані засобів обміну інформацією	0,51	0,14
		Порушення обміну, збереження та розповсюдження документів	0,29	0,08
Співробітник відділу експлуатації	0,19	Встановлення та використання неліцензійного програмного забезпечення	0,51	0,09
		Помилки при використані засобів обміну інформацією	0,51	0,09
		Порушення обміну, збереження та розповсюдження документів	0,29	0,05
Допоміжний персонал	0,02	Режиму використання носіїв інформації	0,29	0,01
		Встановлення та використання неліцензійного програмного забезпечення	0,51	0,01
		Помилки при використані засобів обміну інформацією	0,51	0,01
Хакери	0,64	Порушення обміну, збереження та розповсюдження документів	0,29	0,18
		Встановлення та використання неліцензійного програмного забезпечення	0,51	0,32

		Помилки при використані засобів обміну інформацією	0,51	0,32

Продовження таблиці 2.15

Джерело загроз	К1	Вразливість	К2	К3
Конкуренти	0,38	Порушення обміну, збереження та розповсюдження документів	0,29	0,11
		Встановлення та використання неліцензійного програмного забезпечення	0,51	0,19
		Помилки при використані засобів обміну інформацією	0,51	0,19

Таблиця 2.16 – Взаємозв’язок джерел загроз і об’єктивних вразливостей

Джерело загроз	К1	Вразливість	К2	К3
Начальник порту	0,20	Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
		Шкідливе програмне забезпечення	0,21	0,04
		Монтаж прослуховуючих пристроїв	0,10	0,04
Заступник начальнику порту	0,20	Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
		Шкідливе програмне забезпечення	0,21	0,04
		Монтаж прослуховуючих пристроїв	0,10	0,04
Співробітник фінансово–економічного відділу	0,14	Шкідливе програмне забезпечення	0,21	0,02
		Монтаж прослуховуючих пристроїв	0,10	0,01
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
Керівник фінансово–економічного відділу	0,30	Шкідливе програмне забезпечення	0,21	0,06

		Монтаж прослуховуючих пристроїв	0,10	0,03
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01

Продовження таблиці 2.16

Джерело загроз	К1	Вразливість	К2	К3
Керівник відділу служби внутрішньої безпеки	0,39	Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
		Монтаж прослуховуючих пристроїв	0,10	0,03
		Шкідливе програмне забезпечення	0,21	0,08
Співробітники відділу служби внутрішньої безпеки	0,21	Шкідливе програмне забезпечення	0,21	0,04
		Монтаж прослуховуючих пристроїв	0,10	0,02
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
Керівник інформаційного відділу	0,64	Шкідливе програмне забезпечення	0,21	0,14
		Монтаж прослуховуючих пристроїв	0,10	0,06
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,03
Співробітники інформаційного відділу	0,19	Шкідливе програмне забезпечення	0,21	0,03
		Монтаж прослуховуючих пристроїв	0,10	0,01
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
Керівник відділу експлуатації	0,29	Шкідливе програмне забезпечення	0,21	0,06
		Монтаж прослуховуючих пристроїв	0,10	0,02
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
Співробітник відділу експлуатації	0,19	Шкідливе програмне забезпечення	0,21	0,03

		Монтаж прослуховуючих пристроїв	0,10	0,01
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01

Продовження таблиці 2.16

Джерело загроз	К1	Вразливість	К2	К3
Допоміжний персонал	0,02	Шкідливе програмне забезпечення	0,21	0,01
		Монтаж прослуховуючих пристроїв	0,10	0,01
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,01
Хакери	0,64	Шкідливе програмне забезпечення	0,21	0,14
		Монтаж прослуховуючих пристроїв	0,10	0,06
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,03
Конкуренти	0,38	Шкідливе програмне забезпечення	0,21	0,07
		Монтаж прослуховуючих пристроїв	0,10	0,03
		Наявність прямої зони перегляду видимості об’єкту	0,06	0,02

Загрози, з коефіцієнтом нижче 0,1 вважаються неактуальними через малу вірогідність їх реалізації на об’єкті дослідження.

Стихійні джерела загроз та стихійні вразливості.

Для класифікації джерел загроз визначаються такі коефіцієнти:

К1 – особливості місцевості;

К2 – наявність необхідних умов;

К3 – рівень наслідків (фатальність).

Для класифікації вразливостей визначаються наступні критерії:

К1 – ступінь впливу вразливості на не усунення наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз

К3 – кількість елементів об’єкту.

Перелік можливих стихійних джерел загроз та вразливостей вказаний у таблицях 2.17 та 2.18.

Таблиця 2.17 – Перелік можливих стихійних джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Пожежа	2	1	1	2	0,01
Повінь	5	4	1	20	0,16
Землетрус	4	2	2	16	0,12
Ураган	1	2	1	2	0,01

Таблиця 2.18 – Перелік випадкових вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{небезпеки}$
Пошкодження					
Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	2	2	3	12	0,09
Зовнішнє огородження території	2	2	2	8	0,06

У таблиці 2.19 відображений взаємозв’язок стихійних джерел загроз та вразливостей.

Таблиця 2.19 – Взаємозв’язок стихійних джерел загроз та вразливостей

Джерело загроз	К1	Вразливість	К2	К3
Пожежа	0,01	Пошкодження життєзабезпечуючих комунікацій (електро,водо,газо,теплопостачання)	0,09	0,01
Повінь	0,16	Пошкодження життєзабезпечуючих комунікацій (електро,водо,газо,теплопостачання)	0,09	0,05
		Зовнішнє огородження території	0,06	0,03
Землетрус	0,12	Пошкодження життєзабезпечуючих комунікацій	0,09	0,03

		(електро,водо,газо,теплопостачання)		
		Зовнішнє огородження території	0,06	0,01
Ураган	0,01	Пошкодження життєзабезпечуючих комунікацій (електро,водо,газо,теплопостачання)	0,09	0,01
		Зовнішнє огородження території	0,06	0,01

Загрози, з коефіцієнтом нижче 0,1 вважаються неактуальними через малу вірогідність їх реалізації на об’єкті дослідження.

Розглянемо техногенні джерела загроз та вразливості.

Для техногенних джерел використовуються наступні коефіцієнти:

К1 – ступінь віддаленості від об’єкту захисту (можливість виникнення);

К2 – наявність необхідних умов;

К3 – рівень наслідків (фатальність).

Для класифікації вразливостей визначаються наступні критерії:

К1 – ступінь впливу вразливості на не усунення наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз;

К3 – кількість елементів об’єкту.

Перелік можливих техногенних джерел загроз та вразливостей вказаний у таблицях 2.20 та 2.21

Таблиця 2.20 Перелік можливих техногенних джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Зовнішні:					
Мережа інженерних комунікацій (тепло, водо, газопостачання, мережа інтернет)	4	2	4	32	0,25
Внутрішні:					
Неякісні технічні засоби обробки інформації	4	4	5	80	0,64

Таблиця 2.21 Перелік техногенних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
Збій та відмова в роботі:					
Знищення інформації	4	4	2	16	0,12
Пошкодження:					
Блокування доступу	3	2	2	12	0,09

У таблиці 2.22 відображений взаємозв’язок техногенних джерел загроз та вразливостей.

Таблиця 2.22 Взаємозв’язок техногенних джерел загроз та вразливостей

Джерело загроз	К1	Вразливість	К2	К3
Зовнішнє джерело загроз				
Мережа інженерних комунікацій (тепло, водо, газопостачання, мережа інтернет)	0,32	Блокування доступу	0,09	0,03
Джерело загроз	К1	Вразливість	К2	К3
Внутрішнє джерело загроз				
Неякісні технічні засоби обробки інформації	0,64	Знищення інформації	0,12	0,07

Загрози, з коефіцієнтом нижче 0,1 вважаються неактуальними через малу вірогідність їх реалізації на об’єкті дослідження.

Розглянемо наступну таблицю 2.23 враховуючи дані таблиць 2.12–2.22, та проаналізуємо загрози із найбільш високим коефіцієнтом небезпеки.

Рівень загрози у таблиці 2.23 розраховувався за наступним методом:

– від 0,10–0,20 – низький рівень;

– від 0,20–0,30 – середній рівень;

– вище 0,30 – високий рівень небезпеки.

Таблиця 2.23 – Ранжування загроз

Загроза	Коефіцієнт небезпеки	Рівень загрози
Встановлення та використання неліцензійного програмного забезпечення	0,51	1

Помилки при використані засобів обміну інформацією	0,51	1
Порушення обміну, збереження та розповсюдження документів	0,29	2
Шкідливе програмне забезпечення	0,21	2
Монтаж прослуховуючих пристроїв	0,10	3

Аналізуючи таблицю 2.23 можна побачити, що загрози «Помилки при використанні засобів обміну інформації» та «Встановлення та використання неліцензійного програмного забезпечення» мають найбільший ризик для підприємства.

У таблиці 2.24 наведений перелік джерел загроз із найбільш високим коефіцієнтом небезпеки.

Таблиця 2.24 – Ранжування джерел загроз

Джерело загроз	Коефіцієнт небезпеки
Антропогенні суб’єктивні	
Хакери	0,33
Керівник інформаційного відділу	0,32
Керівник відділу служби внутрішньої безпеки	0,19
Конкуренти	0,19
Керівник фінансово–економічного відділу	0,15
Керівник відділу експлуатації	0,14
Начальник порту	0,10
Заступник начальнику порту	0,10
Співробітники відділу служби внутрішньої безпеки	0,10
Співробітники інформаційного відділу	0,09
Співробітник відділу експлуатації	0,09
Співробітник фінансово–економічного відділу	0,07
Допоміжний персонал	0,01
Антропогенні об’єктивні	
Хакери	0,14

Керівник інформаційного відділу	0,14
Керівник відділу служби внутрішньої безпеки	0,08
Конкуренти	0,07
Керівник відділу експлуатації	0,06

Продовження таблиці 2.24

Джерело загроз	Коефіцієнт небезпеки
Антропогенні об’єктивні	
Співробітники відділу служби безпеки	0,04
Співробітники інформаційного відділу	0,04
Начальник порту	0,04
Заступник начальнику порту	0,04
Співробітник фінансово–економічного відділу	0,03
Допоміжний персонал	0,01
Техногенні	
Неякісні технічні засоби обробки інформації	0,07
Мережа інженерних комунікацій (тепло, водо, газопостачання, мережа інтернет)	0,03
Стихійні	
Повінь	0,05
Землетрус	0,03
Пожежа	0,01
Стихійні	
Ураган	0,01

Згідно із даними таблиці 2.24 найбільшу загрозу серед антропогенних джерел становлять хакери та керівник інформаційного відділу. Серед джерел стихійних загроз найбільшу небезпеку складає повінь із коефіцієнтом 0,05.

Розглядуючи техногенні джерела було зазначено, що найбільшу небезпеку складають неякісні технічні засоби обробки інформації із коефіцієнтом 0,07.

Розробка елементів політики безпеки.

Політика безпеки роботи із документами

Дана політика встановлює вимоги до змісту, копіювання, порядку обміну, збереження електронних та паперових документів, файлів та інформації всередині компанії.

Область застосування.

Дана політика охоплює усі відділи діяльність яких пов’язана із підготовкою, копіюванням, збереженням, обміном документів, інформацією, даними із використанням інформаційно–технологічних ресурсів компанії.

Правила політики.

Персонал компанії повинен дотримуватися наступних вимог щодо підготовки, копіюванню, збереженню, обміну документами, інформацією, даними та файлами.

1 За змістом:

– документи за виглядом повинні відповідати офіційному іміджу компанії, слід використовувати офіційно–ділову лексику;

– слід уникати використання слів та виразів, які можуть розкрити критичну діяльність компанії, у разі необхідних умов використовувати скорочення.

2 За збереженням електронних документів:

– документи офісних, поштових ті інших стандартних додатків повинні зберігатися у папці «Мої документи»; особисті файли, що не відносяться до діяльності компанії повинні зберігатися в окремій папці;

– критичні для компанії документи, після створення та обробки слід зберігати у загальнодоступній папці «Для обміну» на сервері в особистих підпапках;

– повний доступ до особистої папки у розділі «Для обміну» має лише власник папки, доступ на перегляд можуть мати інші користувачі у разі надання відповідного доступу;

– категорично забороняється зберігати особисті файли, які не мають відношення до діяльності організації, на сервері;

– із частотою раз у тиждень проводити аналіз документів та видаляти застаріли версії файлів із особистих папок «Для обміну» та «Мої документи»

– копіювати дані та зовнішні накопичувачі CD/DVD–RW, USB FlashDrive, FlashCard категорично забороняється, доступ для копіювання надається лише вповноваженим особам; доступ обмежується шляхом редагування реєстру.

3 За обміном електронних документів:

– внутрішньоофісний обмін файлів може здійснюватися через загальнодоступну папку на сервері;

– внутрішньоофісний обмін файлів через електронну пошту категорично забороняється.

4 За збереженням паперових документів:

– не зберігати паперові документи на столі у межах візуальної доступності у момент відсутності на робочому місці, зберігати у належному місці (шафа, стіл);

– не робити зайвих ксерокопій та печатних копій документів, не залишати документи у недозволених місцях;

– критичні та документи, що вже не випростовуються слід знищувати використовуючи відповідну техніку (наприклад, знищувач паперу).

5 За обміном паперових документів:

– пріоритетним обміном документів має бути електронний обмін;

– паперовий документ слід передавати адресату у межах офісу особисто в руки.

Затвердження політики.

Політика безпеки розробляється начальником служби внутрішньої безпеки та підписується начальником порту.

Відповідальність.

Начальник служби безпеки несе відповідальність за виконанням правил політики. До співробітника, який порушив дану політику, будуть застосовуватися дисциплінарні заходи.

Політика експлуатації ліцензованого програмного забезпечення

Дана політика встановляє вимоги встановлення та використання ліцензованого ПЗ для роботи з інформацією та безпечної роботи системи в цілому.

Область застосування.

Правила, що зазначені у політиці стосуються усіх ОС, які підключені до мережі компанії.

Політика.

1 До складу кожної ОС, яка підключена до мережі комплексу, повинен входити фіксований набір ПЗ для виконання певного виду діяльності. Кожна програма або комплекс програм повинна мати активовану та діючу ліцензію.

2 Фіксований набір програмного забезпечення затверджується між начальником інформаційного відділу та начальником порту. Програмне забезпечення, що не входить до фіксованого набору не може бути встановлено та використано діючими співробітниками без узгодження із керівництвом. Встановлення певного ПЗ для користування у особистих цілях суворо заборонено.

3 Опис ПЗ кожної ОС фіксується у внутрішній документації комплексу, що має назву «Паспорт ОС».У даному документі фіксується апаратна складова ОС та встановлене ПЗ.

4 Операції встановлення, супроводження, підтримки та видалення ПЗ виконуються начальником інформаційного відділу або вповноваженим співробітником інформаційного відділу після узгодження даної дії із керівництвом.

5 У разі виникнення потреби на отримання нового, додаткового, альтернативного ПЗ, відбувається купівля ліцензії на дане ПЗ.

6 При необхідності купівлі ліцензії ПЗ начальник інформаційного відділу створює заявку на отримання ліцензії, заявка узгоджується із головою фінансово–економічного відділу. Дане ПЗ приймається до обліку фінансово–економічного відділу.

7 Після придбання ліцензованого ПЗ відбувається процес його впровадження.

8 При роботі із програмним забезпеченням слід дотримуватися наступних правил:

– використовувати ПЗ лише для робочих цілей;

– сприяти співробітникам інформаційного відділу у встановленні, налаштуванні, виправлення несправності ПЗ;

– повідомляти співробітникам інформаційного відділу у разі виявленням порушень даної політики.

Розробка політики.

Політика безпеки розробляється начальником служби внутрішньої безпеки та підписується начальником порту.

Відповідальність.

Начальник служби внутрішньої безпеки несе відповідальність за виконанням правил політики. До співробітника, який порушив дану політику, будуть застосовуватися дисциплінарні заходи, можливе звільнення з місця роботи.

Політика забезпечення захисту приміщень у яких циркулює інформація з обмеженим доступом

Дана політика призначена для організації захисту інформації з обмеженим доступом у засобах обчислювальної техніки і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

Область застосування.

Положення даної політики розповсюджуються на весь об’єкт інформативної діяльності комплексу.

Правила політики:

1 Необхідно провести часткове екранування приміщень ОІД

2 Установити системи просторового зашумлення.

3 Замінити незахищені технічні засоби на захищенні.

4 Проводи та кабелі, які являються застарілими або вже не використовуються потрібно демонтувати або вкоротити та заземлити.

5 Проводи та кабелі необхідно покрити екранованими конструкціями

6 Кабелі ОТЗ прокладаються окремим пакетом і не повинні утворювати петлі. Перехрещення кабелів ОТЗ і ДТЗС, що мають вихід за межі КЗ,

рекомендується проводити під прямим кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

Забороняється:

1 Самостійне полагодження проводів та кабелів, у разі їх пошкодження.

2 Демонтаж та заміна проводки.

3 Самостійне полагодження засобів обчислювальної техніки у разі виходу із ладу.

У разі виявлення підозрілих засобів, які були виявлені на території КЗ або у приміщеннях ОІД слід негайно повідомити начальника служби безпеки. Для виконання монтажних робіт комплексом наймається стороння організація. Під час вибору організації необхідно звернути увагу на наявність сертифікатів та ліцензій на проведення даного типу робіт.

Розробка елементів політики безпеки.

Політика безпеки розробляється начальником служби безпеки та підписується начальником порту. До співробітника, який порушив дану політику, будуть застосовуватися дисциплінарні заходи, можливе звільнення з місця роботи.

Відповідальність.

Начальник служби безпеки несе відповідальність за виконанням правил політики.

Розглянемо таблицю 2.25 у якій вказані коефіцієнти небезпеки загроз після впровадження політик безпеки інформації

Таблиця 2.25 – Аналіз загроз після впровадження політик безпеки

Загроза	К1	К2	К3	Коефіцієнт небезпеки	Рівень загрози
Встановлення та використання неліцензійного програмного	3	3	3	0,21	2

забезпечення					
Помилки при використані засобів обміну інформацією	3	3	2	0,20	2
Порушення обміну, збереження та розповсюдження документів	2	3	3	0,14	3
Шкідливе програмне забезпечення	2	2	3	0,09	3
Монтаж прослуховуючих пристроїв	2	2	2	0,06	3

– від 0,10–0,20 – низький рівень

– від 0,20–0,30 – середній рівень

– вище 0,30 – високий рівень небезпеки

Загрози «Встановлення та використання неліцензійного програмного забезпечення» та «Помилки при використані засобів обміну інформацією», які до впровадження політики безпеки інформації мали найвищій рівень небезпеки, тепер мають інші показники.

2.5 Висновок

У другому розділі була описана необхідність створення КСЗІ посилаючись на чинне законодавство, а саме ЗУ «Про захист інформації в інформаційно–телекомунікаційних системах». Був створений опис основних відомостей підприємства, проведений акт обстеження об’єкту інформаційної діяльності. Проведений аналіз загроз та вразливостей вказав на незахищені місця комплексу, згідно із отриманими даними були розроблені елементи політик безпеки інформації «Політика забезпечення захисту приміщень у яких циркулює інформація з обмеженим доступом», «Політика експлуатації ліцензованого програмного забезпечення», «Політика обміну, збереження та розповсюдження документів». Після впровадження політик безпеки був проведений повторний аналіз загроз та вразливостей для перевірки змін.

3 ЕКОНОМІЧНА ЧАСТИНА

Завданням та метою цього розділу є розрахунок економічної ефективності впровадження політик безпеки інформації.

Для визначення ефективності необхідно розрахувати:

– капітальні та експлуатаційні витрати для зниження ризику за допомогою засобів захисту;

– вірогідні втрати від реалізації загроз інформації;

– термін окупності капітальних інвестицій та коефіцієнт повернення інвестицій.

3.1 Розрахунок капітальних витрат

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{тз} + t_{в} + t_{а} + t_{взз} + t_{озб} + t_{овр} + t_{д}, \text{ годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації складає 8 год.;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації складає 16 год.;

$t_{а}$ – тривалість процесу аналізу ризиків 6 год.;

$t_{взз}$ – тривалість визначення вимог до заходів, методів та засобів захисту 5 год.;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації 5 год.;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації 10 год.;

$t_{д}$ – тривалість документального оформлення політики безпеки 3 год.

$$t = 8+16+6+5+5+10+3 = 53 \text{ години}$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп визначається за наступною формулою:

$$К_{рп} = З_{зп} + З_{мч} \quad (3.2)$$

$$К_{рп} = 180 + 8215 = 8395 \text{ грн;}$$

де $З_{ЗП}$ – витрати на заробітну плату спеціаліста з інформаційної безпеки;

$З_{Мч}$ – машинний час, що необхідний для розробки політики безпеки.

Для розрахунку заробітної плати використовуємо формулу:

$$З_{зп} = t \cdot З_{іб}, \quad \text{грн}, \tag{3.3}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{ЗП} = 53*155=8299, \text{ грн}$$

Розрахунок вартості машинного часу розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, \quad \text{грн}, \tag{3.4}$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$$З_{мч} = 53 * 1{,}57 = 84, \text{ грн}$$

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

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \quad \text{грн} \tag{3.5}$$

де Р – встановлена потужність ПК, кВт;

$t_{НАЛ}$ – кількість задіяних роб.станцій при написані політики безпеки;

$С_е$ – тариф на електричну енергію, грн/кВт година;

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

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

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

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

$F_р$ – річний фонд робочого часу (за 40–годинного робочого тижня Fр = 1920)

де Р = 0,5 кВТ; (блок живлення 500 ВТ)

$С_е$ = 1,68 грн/кВт година;

$Ф_{зал}$ = 30 грн; (ціна на комплектуючи персонального комп’ютеру не змінилась за останній рік)

$Н_а$ = 0,4 ;

$Н_{АПЗ}$ = 0,5;

$К_{ЛПЗ}$ = 3500 грн;

У таблиці 3.1 вказаний перелік програмного забезпечення для одного комп’ютеру, який необхідного придбати.

Таблиця 3.1 – Перелік придбаного ліцензованого ПЗ

Назва	Вартість (грн.)
Windows 10 Enterprise	1300
Назва	Вартість (грн.)
MindManager	700
Microsoft Office 2019	875
Malwarebytes	625
Загальна сума складає 3500 грн. (на один ПК)	

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

$$С_{Мч} = 0,5*1*1,68 + \frac{0,4*30}{1920} + \frac{0,5*3500}{1920} = 1,57 \text{ грн/год;}$$

Капітальні витрати розраховуються наступним чином:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн. Стороння організація не наймалась, тому даний коефіцієнт не враховується при розрахунках;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), складає 42 000 тис. грн;

$К_{рп}$ – вартість розробки політики безпеки інформації складає 8299 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, складає 1000 тис. грн. В склад закупівлі входять листи для екранування приміщень, заміна кабелів та проводів, придбання системи просторового зашумлення;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн. Потреба у навчанні технічних фахівців відстуня.

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Монтаж та заміна проводок,кабелів, екранування приміщень та встановлення додаткового обладнання складає 1000 грн.

$$К = 42000 + 8299 + 1000 + 1000 = 52299 \text{ грн}$$

3.2 Розрахунок річних експлуатаційних витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{тис. грн} \qquad (3.7)$$

де $С_В$ – це витрати на оновлення системи

$С_{АК}$ – це витрати викликані активністю користувачів системи, що складають 800 грн.

$С_К$ – це витрати на керування інформаційною безпекою, розрахунок відбувається за наступною формулою:

$$С_К = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \qquad (3.8)$$

де $С_Н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації (персонал не потребує додаткового навчання) ;

$С_А$ – це річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ), за підрахунками він складає 21 000 грн на рік.

$С_З$ – це річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки , складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \qquad (3.9)$$

де $З_{осн}$ – основна зарплата складає 4000 грн на місяць, відповідно 48000 грн на рік.

$З_{дод}$ –додаткова заробітна плата складає 400 грн на місяць, відповідно 4800 грн на рік.

$$С_З = 48000+4800= 53600, грн$$

$С_{ЕЛ}$ – це вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = Р \cdot F_р \cdot Ц_е , грн \quad (3.10)$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0,5 Вт для одного ПК, для всього комплексу враховується повна кількість ПК та складає 12, тобто 6 кВТ;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки складає 1920 год;

$Ц_е$ – тариф на електроенергію, 1,68 грн/кВт годин

$$С_{ел} = 6*12*1920*1,68 = 232\ 224 грн;$$

$С_О$ – це витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговуючого персоналу (залучення сторонніх організацій не відбувається).

$С_{ТОС}$ – це витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає один відсоток від суми капітальних інвестиції у вигляді 523 грн.

$$С_К = 21000 + 53600 + 232224 + 523= 307\ 347 грн;$$

Маючи всі необхідні дані можемо розрахувати річні експлуатаційні витрати:

С= 307 347+800=308 147 грн;

Визначення річного економічного ефекту

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.11)$$

Втрати від зниження продуктивності співробітників атакованого вузла експлуатаційного відділу, являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad (3.12)$$

де F – місячний фонд робочого часу (при 40–а годинному робочому тижні становить 176 ч.),

$З_С$ – заробітна плата співробітників експлуатаційного відділу складає 5000 грн та 6000 грн, що складає 11 000 грн;

$Т_П$ – складає 15 годин простою атакованого сегменту.

$$П_П = (11000/176) * 15 = 938, грн$$

Витрати на відновлення працездатності вузла експлуатаційного відділу:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

Витрати на повторне введення інформації експлуатаційного відділу $П_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \quad (3.14)$$

де $З_С$ – заробітна плата співробітників експлуатаційного відділу складає 5000 грн та 6000 грн, що складає 11 000 грн;

де F – місячний фонд робочого часу (при 40–а годинному робочому тижні становить 176 ч.),

$t_{ВИ}$ = 17 годин повторного введення загубленої інформації співробітниками експлуатаційного відділу унаслідок атаки.

$$П_{ВИ} = (11000/176) * 17=1062 \text{ грн};$$

Витрати на відновлення експлуатаційного відділу $П_{пв}$ визначаються:

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_{в} \quad (3.15)$$

де $З_О$ = заробітна плата керівника інформаційного відділу, 4800 грн на місяць;

F – місячний фонд робочого часу (при 40–а годинному робочому тижні становить 176 ч.);

$t_В$ = 17 годин повторного введення загубленої інформації співробітниками експлуатаційного відділу унаслідок атаки;

$$П_{ПВ} = (4800/176)*9=260 \text{ грн};$$

$П_{зч}$ – вартість заміни устаткування або запасних частин складає 5000 грн. Мається на увазі купівля нового персонального комп’ютеру.

Маючи всі необхідні дані ми можемо розрахувати витрати на відновлення працездатності вузла експлуатаційного відділу:

$$П_в = 1062+260+5000= 6322 \text{ грн};$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла експлуатаційного визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ}) \quad (3.16)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, 2000000 грн у рік;

$F_г$ – річний фонд часу роботи організації становить близько 2080 год..;

$t_П$ – 15 годин простою експлуатаційного відділу унаслідок атаки;

$t_{ВИ}$ = 17 годин повторного введення загубленої інформації співробітниками експлуатаційного відділу унаслідок атаки;

$t_В$ = 17 годин повторного введення загубленої інформації співробітниками експлуатаційного відділу унаслідок атаки.

$$V = (2000000/2080)*(41) = 39423 \text{ грн}$$

Маючи всі необхідні дані ми можемо розрахувати упущену вигоду від простою експлуатаційного відділу:

$$U = 938+6322+13798 = 46683 \text{ грн}$$

Таким чином, загальний збиток від атаки на експлуатаційний відділ складе:

$$B = \sum_i \sum_n U \quad (3.17)$$

B = 5*5*21058=1167075 грн

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \quad (3.18)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, складає 526 450 грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі складає 0,75;

C – щорічні витрати на експлуатацію системи інформаційної безпеки складають 307 347 грн.

E=(526 450*0,75)–307 347= 567 959, грн

3.3 Аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \quad (3.19)$$

де Е – це загальний ефект від впровадження системи інформаційної безпеки, який становить 87 490 грн;

К – це капітальні затрати, які становлять 52299

ROSI = 567 959/52299 = 10.9

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \quad \text{років.} \tag{3.20}$$

T_O = 1/10.9=0.09 = 33 дня

3.4 Висновок

Під час виконання економічної частини був проведений розрахунок капітальних та експлуатаційних затрат на засоби захисту, які спрямовані для зменшення загрози ризику. Загалом капітальні витрати складають 52 299 грн., експлуатаційні витрати складають 307 347грн., загальний збиток від атаки складає 1167075 грн., ефект від впровадження системи інформаційної безпеки становить 567 959 грн.. Коефіцієнт повернення інвестицій ROSI демонструє показник 0.09, маючи вищевказані дані був проведений розрахунок терміну окупності капітальних інвестицій, що складає практично один місяць. Отримані дані вказують на доцільність впровадження створених елементів політик безпеки інформації.

ВИСНОВКИ

Об’єкти розробки кваліфікаційної роботи є інформаційно-телекомунікаційна система ТОВ «Акварель».

Під час виконання першого розділу кваліфікаційної роботи були виконані наступні завдання:

– був проведений аналіз основних проблем захисту інформації у середовищі ІТС;

– виконаний аналіз нормативно-правової документації, яка забезпечує захист інформації в Україні;

Виконання другого розділу вирішило такі питання як:

– обґрунтування необхідності створення КСЗІ;

– встановлення інформації, яка циркулює на підприємстві ТОВ «Акварель»;

– проведено обстеження об’єкту інформаційної діяльності;

– проведений аналіз загроз та вразливостей підприємства;

– сформовані елементи політики безпеки на основі аналізу загроз та вразливостей;

Виконання економічного розділу визначило капітальні та експлуатаційні витрати на впровадження розроблених елементів політики безпеки та терміну окупності самих інвестицій.

Інвентаризаційні відомості, інформація, яка циркулює на об’єкті інформаційної діяльності, найменування відділів, посадові обов’язки і т.п. були частково або повністю замінені за вимогою керівництва порту.

СПИСОК ЛІТЕРАТУРИ

1 Аналіз кіберзагроз в Україні за останні роки [Електронний ресурс] – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/29656549.html

2 Критична інфраструктура морських портів [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/

3 Аналіз нормативно–правового забезпечення захисту інформації сучасних ІКСМ [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/311654977_analiz_normativno–pravovogo_zabezpecenna_zahistu_informacii_sucasnih_iksm

4 Закон України «Про інформацію» від 02.10.1992 №2657-XII // Відомості Верховної Ради України. – 1992. – № 48. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.

5 Закон України “Про захист інформації в інформаційно–телекомунікаційних системах” від 05.07.1994 №80–VI // Відомості Верховної Ради України. – 1994. – № 80. [Електронний ресурс]. – Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

6 Постанова «Про концепцію національної безпеки України» від 16.01.1997 // Відомості Верховної Ради України. – 1997. – №10ю [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80

7 Закон України «Про державну таємницю» від від 21.01.1992 № 3855-XII //Відомості Верховної Ради України. – 1994. – № 16. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/3855–12

8 НД ТЗІ 1.1–002–99 – «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу– [Чинний від 28.04.1999] – К: ДСТСЗІ СБУ, 2000. – №22 – (Нормативний документ системи технічного захисту інформації).

9 НД ТЗІ 1.1–003–99 – «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» – [Чинний від 28.04.1999] – К: ДСТСЗІ СБУ, 2000. – №22 – (Нормативний документ системи технічного захисту інформації).

10 НД ТЗІ 1.4-001 – Типове положення про службу захисту інформації в автоматизованій системі. – [Чинний від 04.12.2000] – К. : ДСТСЗІ СБУ, 2000. – №53 – (Нормативний документ системи технічного захисту інформації).

11 НД ТЗІ 2.5–005 – Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – [Чинний від 28.04.2000] – К. : ДСТСЗІ СБУ, 2000. – №22– (Нормативний документ системи технічного захисту інформації);

12 ДСТУ ISO/IEC 27001:2015 [Електронний ресурс] // ДСТУ. – 2015. – Режим доступу до ресурсу: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.

13 ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. – 2017. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=669

14 Закон України “Про захист персональних даних” від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 5. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17.

15 Етапи створення КСЗІ [Електронний ресурс] – Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.

16 НД ТЗІ 1.6-005 – Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. – [Чинний від 15.04.2013] – К. : ДССЗЗІ, 2013. – №125 – (Нормативний документ системи технічного захисту інформації).

17 НД ТЗІ 2.5–004 – Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – [Чинний від 28.04.1999] – К. : ДСТСЗІ СБУ, 1999. – №806– (Нормативний документ системи технічного захисту інформації);

18 Загрози інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: http://www.security.ase.md/publ/ru/pubru91/

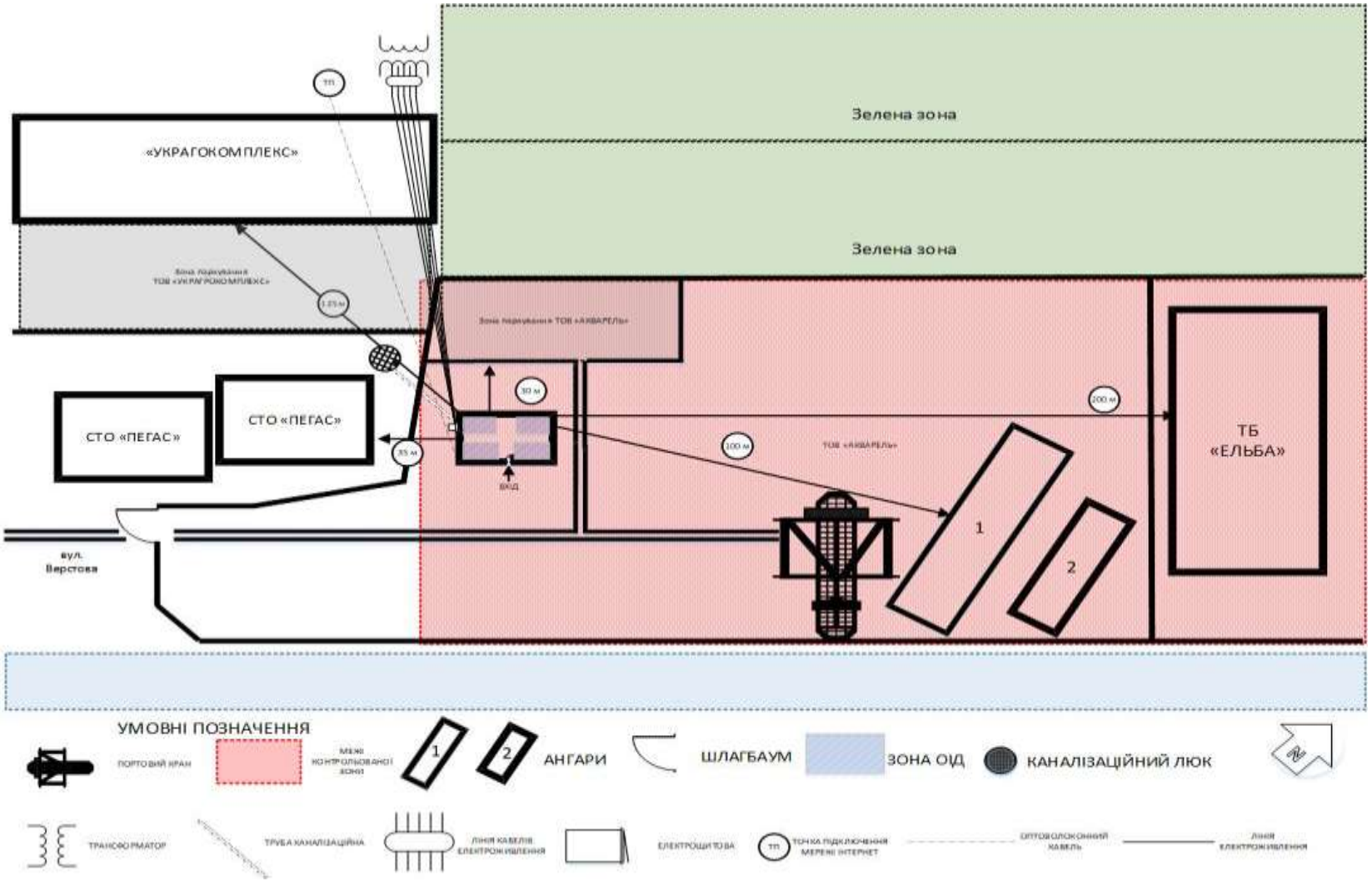
19 Опис інформаційної безпеки підприємства [Електронний ресурс] – Режим доступу до ресурсу: https://bcs.kiev.ua/infosecurity

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОГО ПРОЕКТУ

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	8	
6	А4	Спеціальна частина	39	
7	А4	Економічна частина	11	
8	А4	Висновки	1	
9	А4	Список літератури	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	5	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	

15	А4	Додаток Д	1	
16	А4	Додаток Е	1	

ДОДАТОК Б. СИТУАЦІЙНИЙ ПЛАН ТОВ «АКВАРЕЛЬ»



ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ «АКВАРЕЛЬ»

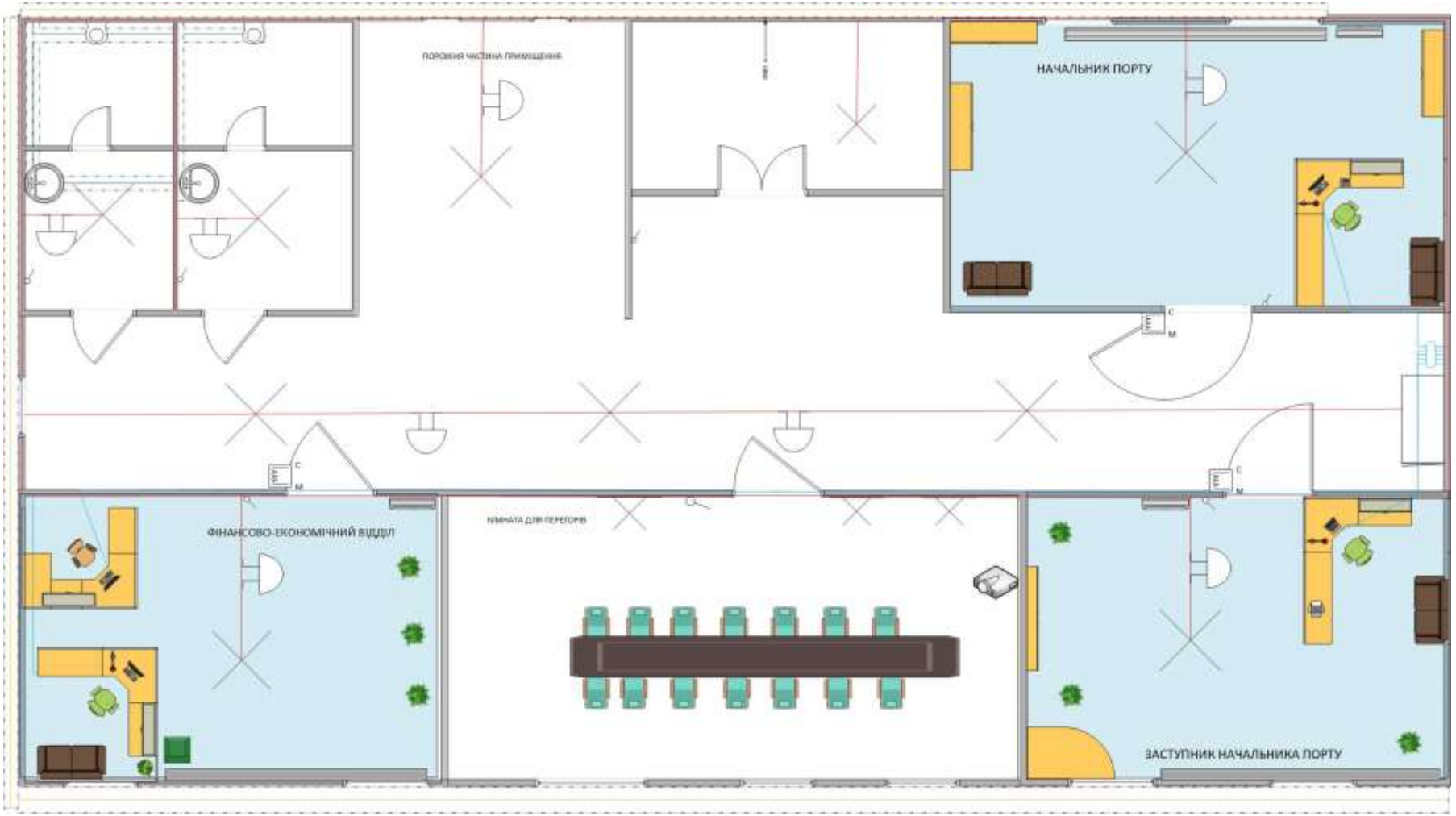
ПЕРШИЙ ПОВЕРХ

ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ «АКВАРЕЛЬ»

ПЕРШИЙ ПОВЕРХ

ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ «АКВАРЕЛЬ»

ДРУГИЙ ПОВЕРХ



ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН 1 ПОВЕРХУ ТОВ «АКВАРЕЛЬ»

ДРУГИЙ ПОВЕРХ

ДОДАТОК В. УМОВНІ ПОЗНАЧЕННЯ ГЕНЕРАЛЬНОГО ПЛАНУ

ДОДАТОК Г.ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

Бардак І.А.гр.УБіТ-15-1.docx

Бардак І.А.гр.УБіТ-15-1.pptx

ДОДАТОК Ґ. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки ТОВ «Акварель».

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності спеціаліста фаху 6.170103 «Управління інформаційною безпекою». Для досягнення поставленої мети у кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ «Акварель», проведення аналізу інформаційної безпеки з виявленням загроз; створення документів з політики безпеки та інструкцій для персоналу; оцінка ефективності впроваджених заходів та розроблених інструкцій. Практичне значення результатів кваліфікаційної роботи полягає в можливості їх використання у ТОВ «Акварель»

Перевагою кваліфікаційної роботи є розробка інструкцій які дозволяють враховуючи специфіку досліджуваного підприємства знизити вірогідність витоку інформації.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з деякими відхиленнями від стандартів.

Під час виконання кваліфікаційної роботи Бардак І.А. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи і заслуговує оцінки «_____», а студент Бардак Ігор Андрійович присвоєння йому кваліфікації фахівець з організації інформаційної безпеки.

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

Керівник кваліфікаційної роботи,
доктор технічних наук, доцент **О.В. Герасіна**

Керівник спеціального розділу,
старший викладач **С.О. Галушко**

ДОДАТОК Е. НАКАЗ НА СТВОРЕННЯ КСЗІ ДЛЯ ТОВ “АКВАРЕЛЬ”

ТОВ «АКВАРЕЛЬ»

16.01.2019 р. м. Дніпро №991-к

Про створення КСЗІ
для ІТС підприємства

З метою виконання Закону України "Про захист інформації в інформаційно–телекомунікаційних системах" (80/94–ВР) та НД ТЗІ 3.7–003–2005 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно–телекомунікаційній системі".

НАКАЗУЮ

1. Створити комплексну систему захисту інформації (КСЗІ) для інформаційно – телекомунікаційної системи ТОВ “АКВАРЕЛЬ”.
2. Службі захисту інформації у процесі створення КСЗІ в інформаційно – телекомунікаційній системі (ІТС) керуватися законами України, нормативно–правовими актами Президента України і Кабінету Міністрів України, нормативними документами ДССЗЗІ України з питань захисту інформації, державними стандартами та розпорядчими документами ТОВ “АКВАРЕЛЬ”.
3. Контроль за виконанням наказу залишаю за собою.

Начальник порту Шурутін Шурутін А.Н.