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 ***Мацайтіса Дмитра Ігоровича***

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 "ГРЕЙНФІЛД"»***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н. доц Герасіна О.В.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
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 ***Мацайтісу Дмитру Ігоровичу*** **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 "ГРЕЙНФІЛД"»***

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

Розділ	Зміст	Термін виконання
Розділ 1	Провести аналіз щодо актуального стану безпеки інформації в світі та Україні. Провести аналіз нормативно – правової бази в сфері захисту інформації.	20.03.2019
Розділ 2	Провести категоріювання підприємства. Провести аналіз ІТС підприємства. Проаналізувати ризики та ймовірних порушників безпеки інформації в ІТС.	30.05.2019
Розділ 3	Провести економічне обґрунтування доцільності елементів політики безпеки та провести розрахунок витрат на розробку елементів політики безпеки інформації	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 _____ Мацайтіс Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 сторінка., 4 рисунка, 24 таблиці, 7 додатків, 17 джерел.

Об’єкт розробки: інформаційно - телекомунікаційна система підприємства ТОВ “Грейнфілд”.

Предмет розробки: впровадження елементів політики безпеки інформації в інформаційно-телекомунікаційної системи підприємства.

Мета кваліфікаційної роботи: підвищення рівня захищеності ІТС підприємства.

У першому розділі кваліфікаційної роботи приведено аналіз щодо актуального стану безпеки інформації в світі та Україні.

У другому розділі кваліфікаційної роботи обґрунтовано необхідність створення комплексної системи захисту інформації. Проведено категоріювання підприємства. Наведено загальні відомості про об’єкт інформаційної діяльності та проведено обстеження інформаційно - телекомунікаційної системи. Обрано профіль захищеності. Розроблена модель загроз та модель порушника. Розроблено основні елементи політики безпеки інформаційно - телекомунікаційної системи підприємства. Наведено аналіз і ранжування загроз до і після впровадження елементів політики безпеки.

У третьому розділі кваліфікаційної роботи розраховано економічну доцільність впровадження та використання розроблених елементів політики безпеки.

ІНФОРМАЦІЙНО - ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБЬЕКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ ЗАГРОЗ, ПОЛІТИКИ БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, РАНЖУВАННЯ ЗАГРОЗ

РЕФЕРАТ

Пояснительная записка: 81 страниц, 4 рисунка., 24 таблицы, 7 приложений, 17 источников.

Объект разработки: информационно - телекоммуникационная система предприятия ООО "Грейнфилд".

Предмет разработки: внедрение элементов политики безопасности информации информационно-телекоммуникационной системы предприятия.

Цель квалификационной работы: повышение уровня защищенности информационно - телекоммуникационной системы предприятия.

В первом разделе квалификационной работы приведен анализ относительно актуального состояния безопасности информации в мире и Украине.

Во втором разделе квалификационной работы обоснована необходимость создания комплексной системы защиты информации. Проведено категорирование предприятия. Приведены общие сведения об объекте информационной деятельности и проведения обследования информационно - телекоммуникационной системы. Определен профиль защищенности. Разработана модель угроз и модель нарушителя. Разработаны основные элементы политики безопасности информационно - телекоммуникационной системы предприятия. Проведен анализ и ранжирование угроз до и после внедрение элементов политики безопасности.

В третьем разделе квалификационной работы рассчитаны экономическую целесообразность внедрения и использования разработанных элементов политики безопасности.

ИНФОРМАЦИОННО - ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, ОБЭКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ, ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, РАНЖИРОВАНИЕ УГРОЗ

ABSTRACT

Explanatory note: 81 pages., 4 figures, 24 tables, 7 supplements, 17 sources.

Object of study: Information system of the enterprise "GREYNFILD" LLC.

Subject of development: development of information security policy for the information and telecommunication system of “Greynfild” LLC.

The goal is to increase the level of security of the information – telecommunication system of enterprise.

The first section of the qualifying work provides an analysis of the current state of information security in the world and Ukraine.

In the second section of qualification work, the necessity of creating an integrated information protection system is justified. An enterprise categorization has been carried out. Provides general information about the object of information activities and a survey of information - telecommunication system. Defined security profile. A threat and intruder model have been developed. The basic elements of the security policy of the information and telecommunication system of the enterprise have been developed. The analysis and ranking of threats is done.

In the third section of qualification work, the economic feasibility of introducing and using the developed elements of the security policy is calculated.

INFORMATION SYSTEM, INFORMATION TELECOMUNICATION SYSTEM, COMPLEX SYSTEM OF INFORMATION SECURITY, RISKS ANALYSIS, SECURITY POLICY, THREAT MODEL, VIOLATOR MODEL, THREATS RANKING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO - Міжнародна організація зі стандартизації;

АС - Автоматизована система;

ДСТУ - Державний стандарт України;

ІТ - Інформаційні технології;

ІТС - Інформаційно - телекомунікаційна система;

ІБ - Інформаційна безпека;

КСЗІ - Комплексна система захисту інформації;

КЗ - Контрольована зона;

НД ТЗІ - Нормативний документ у сфері технічного захисту інформації;

ОІД - Об’єкт інформаційної діяльності.

ЗМІСТ с

ВСТУП

У наш час інформаційні технології та аграрна промисловість тісно пов’язані. Використання комп'ютерних мереж, інтернету, програмних продуктів наскрізної автоматизації всіх бізнес-процесів та загалом функціоналу підприємства - не просто питання лідерства але і висока конкурентоспроможність між фірм як в Україні, так і за кордоном. Інформаційна ера в аграрній промисловості зустрічається повсюдно - від дронів для моніторингу врожаю та добрив до автоматизованих систем зрошування та висушування зернових культур, їх транспонування до ларів.[1]

Для досягнення найліпшого результату, потрібного для впровадження автоматизованих інформаційних систем управління для агропромислових комплексів є повсюдна автоматизація , яка дає змогу приймати величезні обсяги товару в найкоротші терміни.

З урахуванням особливостей ведення бізнесу в Україні, в агропромислових комплексах виникають загрози безпеці інформації, які можуть фатально вплинути на імідж та бізнес компанії. Інформація, яка оброблюється в ІС, потребує значного рівня захищеності, тому що містить конфіденційну інформацію та дані комерційної таємниці, службову інформацію підприємства, персональні дані клієнтів, як фізичних так і юридичних осіб . Для забезпечення достатнього рівня захисту потрібно не тільки реагувати на виникаючи інциденти, але й вчасно запобігати їм. Можливість спрогнозувати загрози ІБ та своєчасно запобігти виникненню порушень безпеки є пріоритетом спеціалістів з безпеки інформації.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Поточний стан проблеми забезпечення безпеки інформації

Більшість організацій усвідомлює роль IT в бізнес-цілях. IT-інфраструктури тісно пов'язані між собою і працюють в середовищі з постійно зростаючим рівнем небезпеки, що характеризується безперервним збільшенням кількості атак і постійного посилення щодо вимог на запобігання. Найчастіше організації нездатні передбачити небезпеку. Управління безпекою інфраструктури організації (і створюваної завдяки цій інфраструктурі бізнес-цінності) стало одним з головних завдань спеціалістів служби безпеки інформації.

Процес управління інформаційною безпекою дозволяє агропромисловим підприємствам домогтися поєднання максимальної економічної ефективності і надає зрозумілий і не суперечливий метод організації та розмежування пріоритетів на ресурси для реалізації управління ризиками. Реалізація управління інформаційною безпекою дозволяє організаціям запровадити ефективний контроль, що знижує ризик до прийнятного рівня.

Визначення прийнятного ризику і підхід до управління інформаційною безпекою залежать від конкретної організації - всі мають різні моделі загроз та підходи. Кожна модель пропонує індивідуальну методику захисту інформації, та основана на суб’єктивному рішенні спеціаліста тому важливо створити особливий підхід до менеджменту як безпеки інформації, так і ризиків, задля ідентифікації організаційної потреби щодо відповідності вимогам конкретного підприємства.

В Україні агропромисловість являє собою галузь з дуже високим рівнем конкуренції. Будь-який сучасний елеватор – комплекс з багатьма функціонуючими підрозділами. Від злагодженості роботи цього комплексу залежить успішність існування підприємства на ринку, тому важливо

максимально вірно забезпечити та налагодити його роботу завдяки підвищенню рівня інформаційного захисту підприємства за допомогою покращення політики безпеки в інформаційно - телекомунікаційній системі (далі ІТС).

Дослідження проблеми забезпечення безпеки інформації на поточний момент широко висвітлена у різноманітних аналітичних звітах, наприклад згідно з дослідженнями корпорації Ernst & Young (далі E&Y) [2] - британської аудиторсько - консалтингової компанії, яка входить до великої четвірки було виведено такі показники :

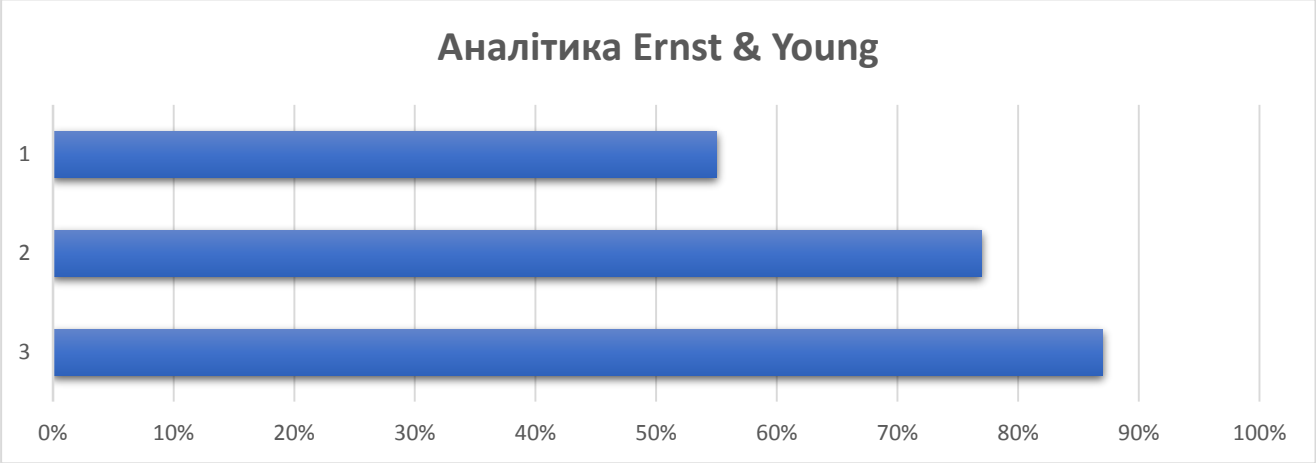


Рисунок 1.1 – Аналітика Ernst & Young

1 55% керівників не розглядають інформаційну безпеку як стратегічний пріоритет розвитку організації;

2 77% респондентів наразі мають базовий рівень інструментів із забезпечення інформаційної безпеки;

3 87% організацій стверджують, що не мають достатньо ресурсів для реалізації заходів із забезпечення інформаційної безпеки.

Після серії масштабних кібератак минулих років (WannaCry, VPNFilter, Mirai, Stuxnet та ін.) на організації і взаємних звинувачень держав у втручанні в кіберпростір, дослідження E&Y[2] показують, що інформаційна безпека залишається важливим питанням для всіх організацій.

Результати опитування показують, що 55% організацій не розглядають захист інформації як частину загальної бізнес-стратегії підприємства. 87%

мають обмежений бюджет на забезпечення необхідного рівня кібербезпеки, проте бюджети виділені на інформаційну безпеку зростають - великі компанії планують витратити більше вже в цьому (63%) і наступному роках (67%), менші компанії - 50% і 66% відповідно.

Опитування показало, що 78% великих і 65% малих організацій впевнені, що безпека інформації підприємства частково задовольняє їхні потреби, і лише 8% респондентів вважають, що функція в повній мірі відповідає потребам компанії, тому організації продовжують працювати над впровадженням базових елементів кібербезпеки, а також знаходяться в пошуку нових підходів та стратегій захисту.

Також неможливо не згадати минуле дослідження компанії PwC (Price water house Coopers) [3] - міжнародна мережа компаній, що пропонує професійні послуги у сфері консалтингу та аудиту.

У дослідженні глобальних тенденцій безпеки інформації PwC [3] 2018 року, 40% респондентів з організацій які використовують автоматизовані системи, стверджують що порушення операцій буде найбільш критичним наслідком кібератак на ці системи, опираючись на це можемо зробити висновок, що багато компаній дотепер не підготовлені до реальної протидії загрозам.

У зв’язку з тенденціями безпеки інформації в Україні та світі існує висока потреба в побудові ефективних систем захисту інформації.

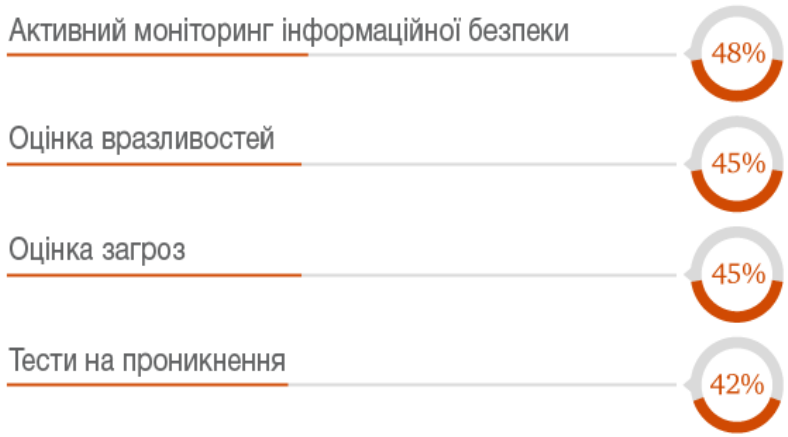


Рисунок 1.2 – Дослідження глобальних тенденцій інформаційної безпеки PWC 2018 року

Підсумки досліджень показують, що в цілому ринок ІБ в Україні виріс дуже незначно: загальний приріст не перевищить 10% в порівнянні з показниками минулого року. При цьому позитивну динаміку ринок отримує за рахунок запуску окремих проектів в області оцифрування державного рівня (наприклад, переведення міського господарства на нові технології, появи розумних міст, розумного транспорту, державних сервісів), а також за рахунок ряду найбільших гравців вітчизняного ринку, які обрали для себе шлях цифрової трансформації і розуміють необхідність безпеки та розділяють підхід, заснований не тільки на відбитті атак, але і на попередньому виявленні загроз.

1.2 Аналіз нормативно правової бази в сфері захисту інформації

Існують підходи до забезпечення безпеки інформації як на базі міжнародних так і вітчизняних стандартів, нормативної документації та законодавчих норм. Міжнародні документи дозволяється використовувати у частині, що не протирічить вітчизняним.

Розглянемо основні з них:

Закон України “Про інформацію” [4] регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Класифікація інформації:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;

– соціологічна інформація;

– інші види інформації.

Закон України “Про захист персональних даних” [5] - регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Закон України “Про доступ до публічної інформації” [6] визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” [7] регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі ІТС). Регламентує положення да доступ інформації в системі, умови її обробки та повноваження державних органів в ІТС.

Закон України “Про електронний цифровий підпис” [8] визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

Якщо міжнародним договором, згода на обов’язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Забезпечення безпеки інформації на підприємстві з використанням міжнародного підходу рекомендується складати з використанням стандартів, з яких можна виділити основні - ДСТУ 27-мої серії.

ДСТУ ISO/IEC 27001:2015 [9] 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.

ДСТУ ISO/IEC 27002:2015 [10] 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.

ДСТУ ISO/IEC 27005:2017 [11]

Цей стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації.

Рекомендації призначені, щоб допомогти реалізувати достатню інформаційну безпеку, засновану на підході менеджменту ризиками та є придатним до всіх типів організацій (наприклад, комерційні підприємства, урядові агентства, некомерційні організації), які мають намір здійснювати менеджмент ризиками, які ставлять під загрозу інформаційну безпеку організації.

Безпека інформації на об’єктах інформаційної діяльності в Україні створюється з необхідністю реалізації комплексної системи безпеки інформації (далі КСЗІ).

КСЗІ створюється відповідно до вимог, викладених в НД ТЗІ. НД ТЗІ 3.7-003 [12] регламентує порядок створення комплексної системи захисту інформації.

На підприємстві повинна бути створена служба захисту інформації згідно НДТЗІ 1.4-001.[13]

За допомогою НД ТЗІ 2.5-004 [14] можливо відібрати критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого

доступу та надає змогу розподілити такі критерії як цілісність, доступність та спостережність.

НД ТЗІ 2.5-005 [15] надає змогу класифікувати автоматизовану систему підприємства залежно від призначення автоматизованої системи та визначити функціональний профіль захищеності оброблюваної інформації від НСД.

1.3 Постановка задачі

Згідно зі станом безпеки інформації в інформаційно-телекомунікаційних системах підприємств та безпеки інформації у світі, та спираючись на аналіз нормативно - правової бази в сфері захисту інформації, приходимо до висновку, що створення комплексних систем захисту інформації для підприємств зі значними вимогами до забезпечення захисту інформації є необхідністю.

1.4 Висновок

В першому розділі розглянута проблематика безпеки інформації в інформаційно - телекомунікаційних системах. Проведено аналіз нормативно правової бази в сфері інформаційної безпеки та розглянуто основні закони та нормативні документи які пов’язані із захистом інформації. Проаналізовано ситуацію в Україні та світі у сфері розвитку інформаційних технологій в агропромисловому комплексі, а також описано проблему забезпечення безпеки інформації.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Балівський елеватор «Грейнфілд» (повна назва - Товариство з обмеженою відповідальністю Компанія «Грейнфілд») знаходиться в с Партизанське Дніпропетровської області. Елеватор розпочав свою діяльність в 1973 році. Входить до складу Корпорації «Алеф». На сьогоднішній день Корпорація «Алеф» є потужною бізнес-структурою, штат якої становить 15 тис. співробітників. Агродепартамент корпорації «Алеф» до якого входить елеватор, займається виробництвом, вирощуванням та реалізацією сільськогосподарської продукції. До її складу входять такі компанії, як ТОВ «Торговий Дім «Агроальянс», ТОВ «АГРОПЕРСПЕКТИВА 2008», ПрАТ «Агроком» і ТОВ «Виробничо-комерційна фірма «Укрсільгоспром». Агродепартамент має власний IT відділ з фахівцями інформаційної безпеки.

Тип елеватора - лінійний, тип зберігання - бетонні силоси (147000 тон.) Підприємство має 2 зерносушарки Sukup TE 2452 E (США) та CFCAI LAW SBC 219 LE (Франція), потужність яких при знятті 10% вологи по кукурудзі складає 38+47 тон/год (паливо - газ) Обладнання для очистки - Сепаратори БСХ-300, Buhler (Швейцарія), потужністю 200 т/год.

Загальна потужність елеватора для одночасного зберігання становить 147000 тон, потужність ліній автозавантаження складає 3000 т/добу, потужність автовідвантаження - 900 т/добу. Географічне розташування елеватора поблизу залізничної станції «Балівка» Придніпровської ЗД (455702) дає змогу здійснювати з/д завантаження із потужністю 1500 тон/добу та відвантаження на залізничні зерновози із потужністю 2000 тон/добу. Потужність транспортного обладнання - 150 тон/годину.

Торгово-виробнича корпорація «Алеф» була створена в 1995 році. Елеватор видає складські квитанції, які є підтвердженням якості та кількості

прийнятої продукції, а також дає можливість продавати продукцію, як у повному обсязі або частково через інструменти електронних торгів на AGROXY як на внутрішньому ринку так і на експорт.

2.2 Категоріювання об’єкта інформаційної діяльності

За допомогою 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” визначаємо, що підприємство відноситься до четвертої категорії. [16]

“Об’єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.” Створення КСЗІ для цієї категорії не є обов'язковим, але відповідно з постановкою задачі, керівництвом підприємства було прийнято рішення створити Комплексну систему захисту інформації - далі КСЗІ для інформаційно - телекомунікаційної системи підприємства. Згідно до наказу [ДОДАТОК Ґ.] від 17.01.19.

2.3 Обґрунтування необхідності створення КСЗІ

Комплексна система захисту інформації - сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку й несанкціонованого доступу. [17]

Головною метою створення КСЗІ є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у галузі захисту інформації: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

Для конкретної інформаційно-телекомунікаційної системи склад, структура та вимоги до КСЗІ визначаються властивостями та актуальними

загрозами безпеки оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС відповідно до нормативних документів з захисту інформації.

Комплексна система захисту інформації складається з організаційних та інженерно-технічних заходів. Створення полягає в розробці інструкцій для користувачів та обслуговуючого персоналу, правил адміністрування інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів, розробці планів дій у разі несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації, навчанні правилам безпеки інформації користувачів тощо.

Щодо інженерно-технічних заходів, то це сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Суб’єктами комплексної системи захисту інформації є 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 (Адміністрація Держспецзв’язку) (Контролюючий орган), організація, що здійснює державну експертизу КСЗІ (Організатор експертизи), організація, що, у разі необхідності, залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник). [17]

Об’єктом захисту КСЗІ є інформація в будь-якому її вигляді.

Впровадження комплексної системи захисту інформації складається з етапів: підготовки організаційно-розпорядчої документації, обстеження інформаційної інфраструктури Замовника, розробки “Технічного завдання на створення КСЗІ”, розробки “Плану захисту інформації”, розробки “Технічного проекту на створення КСЗІ”, приведення інформаційної інфраструктури Замовника у відповідність до “Технічного проекту на створення КСЗІ”,

розробки “Експлуатаційної документації на КСЗІ”, впровадження КСЗІ, випробування КСЗІ, проведення державної експертизи КСЗІ і отримання “Атестата відповідності”, а також підтримки й обслуговування КСЗІ.

2.4 Обстеження об’єкту інформаційної діяльності

Обстеження фізичного середовища

Об’єктом інформаційної діяльності є інформаційно - телекомунікаційна система підприємства ТОВ “ГРЕЙНФІЛД” - далі елеватор.

Елеватор розташований за адресою с Партизанське, вул. Заводська, буд.18А. Паркування для автомобілів знаходиться на території об’єкту. Відносно ОІД по сусідству розміщені: В 150 метрах на південь від ТОВ “ГРЕЙНФІЛД” Філіал «Агротехсервіс» АО «Промарматура», а також в 750 - 800 метрах на південь - схід від обстежуваного ОІД - придорожнє кафе “СМАКОТА” та філіал Нової Пошти.

Елеватор працює пн-сб з 9:00 до 20.00, нд з 12.00 до 18.00. Без перерви та вихідних. Прибирання приміщення проводиться кожний четвер з 8 до 9 години ранку. Охорона цілодобова - надаються послуги приватної охорони.

Охорона функціоную цілодобово та виконує регулярні нічні обходи. Охорона і тільки вона має ключі від серверної тому повністю відповідає за його фізичну цілісність. Дистанційно до серверу має доступ системний адміністратор, який контролює цілісність інформації на всіх її етапах, та робить зміни у базах даних згідно з наказом генерального директора та його заступника. Агродепартамент дистанційно веде відеоспостереження та має доступ до серверу і інформації на ньому.

Вхід на територію 1 Вхід на офісну територію - 1.(ДОДАТОК В)

Опис ситуаційного плану

Зовнішні стіни будівлі виконані з бетону, фундамент будівлі - подушка з щебню. При купівлі території будівництво було відновлено та удосконалено.

Дах виконаний з гідроізоляційної мембрани Onduline та згодом буде замінена на металочерепицю .Територія навколо будівлі з обстежуваним ОІД заасфальтована на задньому дворі. Вхідні двері центрального входу металопластикові, складаються з 2 блоків та мають магнітний замок. Автомобільна стоянка співробітників знаходиться на території. Паркування сторонніх осіб заборонено (окрім клієнтів).

Данні ситуаційного плану приведені в таблиці 2.1.

Ситуаційний план - ДОДАТОК В.

Ситуаційний план розроблений під час проходження переддипломної практик

Таблиця 2.1 - Прилеглі будівлі відносно КЗ ТОВ «ГРЕЙНФІЛД»

№	Тип споруди	Адреса	Кількість поверхів	Розташування відносно КЗ	Мін. відстань від КЗ до споруди (в метрах)
1	Офіс «Нова пошта»	вул. Стаханівська	3	Північ-схід	850
2	Кафе «Смакота»	вул. Стаханівська	2	Північ-схід	750
3	Філіал «Агротехсервіс»	-	5	Південь	250
4	Залізнична станція «Балівка»	-	1	Південь-схід	550

Дані по прилеглим об’єктам приведено в таблиці 2.2.

Таблиця 2.2 - Прилеглі вулиці відносно КЗ ТОВ «ГРЕЙНФІЛД»

№	Назва вулиці	Опис
1	Вул. Стаханівська	Знаходиться на північному сході відносно ОІД, в 400 метрах від ОІД, інтенсивність руху - 30-50 автомобілів в годину, ширина проїжджої частини - 5 метрів (односмугова в північному напрямі), ширина пішохідної частини - 2 метри (2 метри ліворуч та 2 метри праворуч відносно вулиці).

Продовження таблиці 2.2

№	Назва вулиці	Опис
2	Вул. Заводська	Знаходиться на півночі відносно ОІД, в 2 метрах від ОІД, проїжджої частини немає, ширина пішохідної частини - 10 метрів.
3	Шосе Полтавське Т0441	Відстань до шосе 200 м.

Системи електропостачання КЗ підключені до трансформаторної підстанції (ТП) №110 - «ЦЕК Центральна Енергетична Компанія» і з'єднуються з міською системою електропостачання надземним способом.

Лінії електроживлення проведені від ТП до головного розподільного щитка, що розташований на 1 поверсі офісного приміщення КЗ. Від цього щитка лінії електропостачання під'єднані до КЗ.

Каналізаційні системи будівлі КЗ підключені до каналізаційних систем міста підземним способом. Ці системи обслуговуються ОСМД.

Системи водопостачання будівлі КЗ підключені до систем водопостачання міста підземним способом та обслуговуються постачальником "Східний". З'єднання регулюється в підвальному приміщенні за межами КЗ.

Матеріал труб - поліетиленові.

Стрижні заземлення вкопані у внутрішньому дворі. Заземлені на загальний контур заземлення, який є замкнутим і виходить за межі КЗ.

У кожного працівника є особистий номер телефону з тарифним планом "корпоративний."

Послуги надаються Інтернет-провайдером «LAnet» через оптоволоконне з'єднання за допомогою повітряних ліній.

Опис генерального плану

Генеральний план 1,2 поверх - ДОДАТОК Г;

Генеральний план був розроблений під час проходження переддипломної практики.

Склад зовнішніх стін - цеглина. Товщина - 0.5м.

Висота перекриття - 2.5м.

Склад внутрішніх стін - оштукатурений гіпсокартон.

Стеля - залізобетонна монолітна заливна;

Пол - монолітна бетонна стяжка;

Покриття підлоги - ламінована підлога;

Вікна (11 шт. - металопластикові з двокамерним склопакетом. На вікнах знаходиться жалюзі.

Внутрішні двері (10 шт.) Terminus;

Зовнішні - 1 шт. Металеві. Iron Sight;

Магнітні замки - 2 шт.

Контрольована зона (КЗ) обмежена першим та другим поверхами офісної будівлі. Офіс обладнано системою пожежної сигналізації та контролю доступу. Опис основних технічних засобів приведено в таблиці 2.3.

Таблиця 2.3 - Опис основних технічних засобів

Тип	Ім’я	Інвентарний номер	Місце розташування та № на генеральному плані	Мін. відстань до ОІД (в метрах)
Принтер	HP LaserJet 1919	20043929001	На столі; 1	1
Комутатор	CiscoCatalyst 2960X-24PS	20043929002	На столі; 2	1
Маршрутизатор x2	Mikrotik Cloud Core Router; RJ-45 1gb/s : 7.	20043929003	На столі; 3	1
Системний блок x2	CompPLine H700	20043929004-05	На підлозі. №4,5	1.5
Системний блок x2	CompPLine H700	20043929006-07	На підлозі; №6,7	1.5
Системний блок x2	CompPLine H700	20043929008-09	На підлозі; №8,9	3
Системний	CompPLine	20043929010-11	На підлозі;	3

блок x2	H700		№10,11	

Продовження таблиці 2.3

Системний блок	CompPLine H700	20043929012	На підлозі; №12	2
Системний блок	CompPLine H700	20043929013	На підлозі; №13	2
Монітор x2	LG 23MP55	200439290021-22	На столі; №1,2	2
Монітор x2	LG 23MP55	20043929031-32	На столі; №3,4	2
Монітор x2	LG 23MP55	20043929041-42	На столі; №5,6	1
Монітор x2	LG 23MP55	20043929051-52	На столі; №7,8	1
Монітор	LG 23MP55	20043929071	На столі; №9	1
Монітор	LG 23MP55	20043929081	На столі; №10	1
Ip камера	SpeedDome ActiveCAM AC-D5024	20043929091	На стелі; №16	1
Ip камера	SpeedDome ActiveCAM AC-D5024	20043929101	На стелі; №17	1
Ip камера	SpeedDome ActiveCAM AC-D5024	20043929111	На стелі; №18	1
Сервер	Dell PowerEdge R720XD	20043929112	На підлозі;	1
Медіа конвертер оптичний	Allied Telesis AT-GS2002/SP	20043929113	На столі;	1

На ОІД функціонують наступні ДТЗС - данні приведено в таблиці 2.4.

Таблиця 2.4 - Опис елементів ДТЗС ТОВ «ГРЕЙНФІЛД»

Тип	Ім’я	Інвентарний номер	Місце розташування	Мінімальна відстань до кордонів ОІД (в метрах)	Положення відносно ОІД
Безперебійник	APC Smart-UPS	20043929110	На підлозі - серверна	1.5	ОІД (серверна)
Датчик диму	Zamel CDB 0-1	20043929111	На стелі	3	Суміжне приміщення (хол)
Датчик диму	Zamel CDB 0-1	20043929112	На стелі	3	Суміжне приміщення (хол)
ПКП	Тирас 8П-1	20043929113	На стіні	1.5	Суміжне приміщення (хол)
Магнітний замок	Shield 19in	20043929114	На двері	1	Вхідні двері офісу
Магнітний замок	Shield 19in	20043929115	На двері	2	Двері серверної

Облік та контроль переносних засобів та портативних носіїв інформації не ведеться.

1 Аналіз обчислювальної системи

2.1 Характеристика ІТС ТОВ «ГРЕЙНФІЛД»

Монітори LG 23MP55 - 11 шт.

Сервер - 1шт. На сервері знаходяться резервні копії усієї документації (баз даних, планів, рахунків, тощо). Доступ до серверу має агродепартамент та системний адміністратор - дистанційно. Ключ від приміщення серверу для фізичного доступу знаходяться у генерального директора та заступника генерального директора.

Інвентарна відомість автоматизованих засобів в ІТС наведено в таблиці 2.6.

Інвентарну відомість ПЗ ІТС наведено в таблиці 2.5.

Таблиця 2.5 - Інвентарна відомість ПЗ ІТС

№	Назва	Місце встановлення	Тип ліцензії	Дата закінчення ліцензії
1	Nvidia GeForce Experience build 3.19.04	PC1-PC10	Відкрита	-
2	Google Chrome 75.0	PC1-PC10	Відкрита	-
3	Skype 7.1	PC1-PC10	Відкрита	-
4	WhatsApp Desktop 7.2	PC1-PC10	Відкрита	-
5	Telegram Desktop 8.2	PC1-PC10	Відкрита	-
6	Microsoft Office 2016 SP1 Standart build 19.03	PC1-PC10	Відсутня	-
7	Avast Antivus Premium build 19.03	PC1-PC10	Відсутня	-
8	Notepad++ Build 8.124	PC1-PC10	Відкрита	-
9	1С Бухгалтерія build 8.0	PC9-PC10	Комерційна	
10	Windows 10 Pro build 1903	PC1-PC10	Відсутня	-

Таблиця 2.6 - Інвентарна відомість апаратних засобів ІТС

№	Назва	Характеристика	Ім'я в ІТС	Місце розташування та номер на плані	IP адреса	MAC адреса	Відповідальна особа
1	CompPLine H700	I5 5600k; Nvidia 1050; 16gb ОЗП; БЖ Chieftec 600W; Жорсткий диск Seagate Barracuda 1tb; Материнська плата AS rock 320P; Корпус Qube.	PC-1	Відділ менеджменту №4;	DHCP	F1-7B-8F-EC-97-2E	Системний адміністратор
			PC-2	Відділ менеджменту №5;		28-61-0D-99-D4-FF	
			PC-3	Відділ менеджменту №6;		24-9C-02-DE-FE-BA	
			PC-4	Відділ менеджменту №7;		58-5A-B5-47-EA-D5	
			PC-5	Бухгалтерія №8;		DF-6B-86-FA-D9-DE	

Продовження таблиці 2.6

№	Назва	Характеристика	Ім'я в ІТС	Місце розташування та номер на плані	IP адреса	MAC адреса	Відповідальна особа
1	CompPLine H700	I5 5600k; Nvidia 1050; 16gb ОЗП; БЖ Chieftec 600W; Жорсткий диск Seagate Barracuda 1tb; Материнська плата AS rock 320P; Корпус Qube.	PC-6	Бухгалтерія №9;	DHCP	68-A6-E1-53-72-3D	Системний адміністратор
			PC-7	Каб. заступника Ген.Дир.№10;		FF-66-50-C3-A7-83	
			PC-8	Секретар №11;		A1-EF-49-70-7A-62	
			PC-9	Каб.Ген.Директора №12		34-A8-24-72-F0-E2	
			PC-10	Каб.Системного адміністратора		EA-27-EA-1A-79-7E	
2	Маршрутизатори x2	Mikrotik Cloud Core Router; RJ-45 1gb/s : 7ports	R1 - R2	Каб.Сис.Адміністратора	172.16.2.6 30.32.86.72	FC-DC-9F-3F-A3-00, 98-2E-F0-BD-3B-C4	Системний адміністратор
					172.16.2.4		
3	Свіч	Cisco Catalyst 2960X-24PS - 24 lan	SW-1	Каб.Сис.Адміністратора	172.16.2.5	9F-08-5C-FD-84-E4	Системний адміністратор

Продовження таблиці 2.6

№	Назва	Характеристика	Ім'я в ІТС	Місце розташування та номер на плані	IP адреса	MAC адреса	Відповідальна особа
4	Сервер	Dell PowerEdge R720XD/ 2 x XEON	S-1	Серверна	172.16.2.10	F1-7B-8F-EC-97-2E	Системний адміністратор
5	Медіаконвертер оптичний	Allied Telesis AT-GS2002/SP	M-1	Каб.Сис.Адміністратора	-	-	Системний адміністратор
6	Монітори x10	LG 23MP55 IPS	PC 1-10	ОІД, у кожному кабінеті.	-	-	Системний адміністратор
7	Клавіатура, мишка x10	Logitech g130	PC1-PC10	ОІД, у кожному кабінеті.	-	-	Системний адміністратор
8	IP camera x3	SpeedDome ActiveCAM AC-D5024	Cam 1 - Cam 3	На території КЗ, 1 поверх - 2 камери. 2 поверх - 1 камера.	172.16.2.1 172.16.2.2 172.16.2.3	4E-17-2F-BF-DA-6C, 4A-21-EE-05-22-7F, 9B-59-C3-92-52-41	Системний адміністратор

2.2 Топологія мережі

Тип з’єднання : локальна мережа фізично має архітектуру «зірка».

Пристрої : 2 маршрутизатори, 1 свіч, 1 сервер, 1 медіаконвертер оптоволоконної лінії.

Маршрутизатор R2 займається збором даних с камер відеоспостереження. Маршрутизатор R1 - забезпечення маршрутизації, фаєрвола та VPN каналу для доступу з агродепартаменту.

Сервер SW1 виконує роль DHCP, DNS, сховища даних та контролеру домену- вся актуальна інформація, бази даних покупців та продукції та ін. зберігаються на сервері як резервні копії.

Дистанційно до серверу доступ має інспектор безпеки з агр

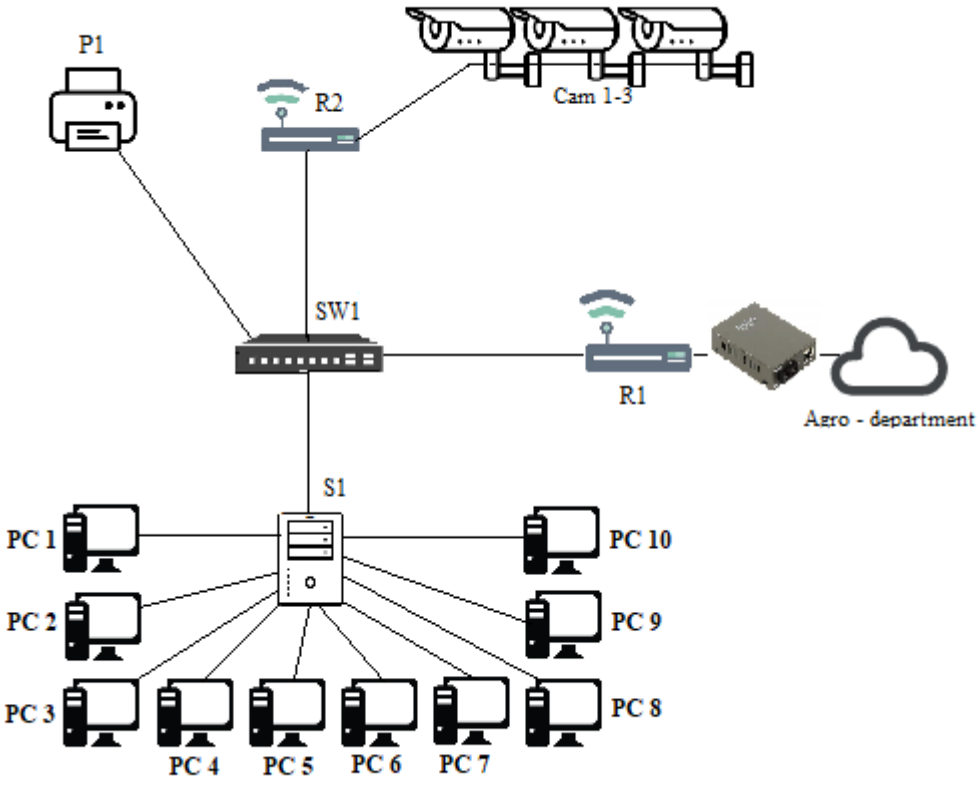


Рисунок 2.1 - Функціональна схема мережі

PC1 - Комп’ютер директора;

PC2 - Комп’ютер заступника директора;

PC3 - Комп’ютер секретаря;

PC4 - Комп’ютер системного адміністратора;

PC5 - Комп’ютер менеджера з закупівлі;

PC6 - Комп’ютер менеджера з закупівлі;

PC7 - Комп’ютер менеджера з продажу;

PC8 - Комп’ютер менеджера з продажу;

PC9 - Комп’ютер бухгалтера;

PC10 - Комп’ютер бухгалтера;

R1 - Маршрутизатор 1;

R2 - Маршрутизатор 2;

SW1 - Свіч;

Cam 1-3 - Ip камера x3;

P1 - Принтер;

M1 - Медіаконвертер.

Особливості мережі

Комп’ютери директора, заступника генерального директора, бухгалтерів, менеджерів з продажу та закупівлі, секретаря із системним адміністратором, сервер, принтер, маршрутизатор (1-10; сервер, принтер, 2 маршрутизатори) підключені до свіча за допомогою кабелю UTP cat. 5e.

Основна інформація знаходиться на персональних комп’ютерах робітників.

Маршрутизатор R2 - забезпечення маршрутизації, фаєрвола та VPN каналу.

Сервер виконує роль DHCP, DNS, сховища даних та контролеру домену-вся актуальна інформація, бази даних покупців та продукції та ін. зберігаються на сервері як резервні копії.

Дистанційно до серверу має доступ агродепартамент та системний адміністратор.

Дистанційний доступ та керування відеокамерами спостереження, під'єднаних до маршрутизатора по Wi-Fi мережі має співробітники агродепартаменту - служба безпеки інформації підприємства. Всі комп’ютери належать до одного домену - GFD.

Аналіз інформаційного середовища

В ТОВ «ГРЕЙНФІЛД» оброблюється та зберігається інформація з обмеженим доступом - БД постачальників, БД клієнтів, фінансові звіти, платіжні данні клієнтів. Неправомірний доступ або втрата інформації може привести до втрати клієнтів, погіршення фінансового положення та втрати іміджу. Саме тому необхідно забезпечити захист інформаційних ресурсів від несанкціонованих дій.

Оброблювана інформація представлена в таблиці 2.7.

Таблиця 2.7 - Оброблювальна інформація

№	Інформація	Носій	Правовий режим	Режим доступу	Вимоги до захисту
1	Робочий план	Електронний, паперовий	Комерційна таємниця	ІзОД	К–1, Ц,–1 Д–1
2	Бухгалтерський звіт	Електронний, паперовий	-	Відкрита	Ц–1,Д–1
3	Звіт діяльності підприємства	Електронний, паперовий	Комерційна таємниця	ІзОД	К–2,Ц–2,Д–2
4	База даних покупців	Електронний	Комерційна таємниця	ІзОД	К–2,Ц–2,Д–2
5	База даних продукції	Електронний	Комерційна таємниця	ІзОД	К–2,Ц–2,Д–2
6	Системний звіт	Паперовий, електронний	Комерційна таємниця	ІзОД	К–3,Ц –2,Д –2
7	Реклама	Електронний	-	Відкрита	Ц –2,Д,–2
8	Банківські дані підприємства (о/р, ЄДРПОУ та ін.)	Електронний, паперовий	-	Відкрита	Ц –2,Д –2

Продовження таблиці 2.7

№	Інформація	Носій	Правовий режим	Режим доступу	Вимоги до захисту
9	Зарплатні відомості	Електронний, паперовий	Комерційна таємниця	ІзОД	К,–1,Ц,–1,Д,–2
10	Перелік співробітників (посада, кількість робочих годин, тощо.	Електронний, паперовий	Комерційна таємниця	ІзОД	К,–2,Ц,–1,Д,–2

К - вимоги до конфіденційності;
Ц - вимога до цілісності;
Д - вимога до доступності.

Рівні конфіденційності:

К1– рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Використовується АС класу 3 згідно з пунктом 5.7 НД ТЗІ 2.5-005-99 [17] розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Профіль захищеності

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Для стандартних функціональних профілів захищеності не вимагається ні зв'язаної з ними політики безпеки, ні рівня гарантій, хоч їх наявність і допускається в разі необхідності

Згідно з нормативними документами НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-005-99 [18] на досліджуваному ОІД АС належить до третього класу, а вимоги до захисту інформації (конфіденційність, цілісність та доступність), то обраний профіль має вигляд:

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}

Функціональний профіль захищеності приведено в таблиці 2.8.

Таблиця 2.8 - Профіль захищеності

Критерії	Пояснення
КО-1. Повторне використання об'єктів	Виконуються, так як інформація, що знаходиться на звільненому об'єкті не стає недосяжною для інших користувачів.
КВ-1. Мінімальна конфіденційність при обміні	Виконується, якщо відомо, що при обміні інформацією використовуються захищені (зашифровані) лінії передачі.
ЦД-1. Мінімальна довірча цілісність	Виконується, так як користувач сам ранжує інформацію.
ЦО-1. Обмежений відкат	Виконується тому, що користувачу дозволяється відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.
ЦВ-1. Мінімальна цілісність при обміні	Виконується автоматично в певних механізмах системи (наприклад: оновлення ОС, антивірусу).
ДР-1. Квоти	Виконується, так як користувач з правами адміністратора контролює кількість виділених ресурсів.
ДВ-1. Ручне відновлення	Повинні існувати ручні процедури, за допомогою яких мож

	на безпечним чином повернути КС до нормального функціонування.
НР-2. Захищений журнал	Виконується, так як для доступу до журналу треба мати права адміністратор, щоб потрапити до реєстру.

Продовження таблиці 2.8

Критерії	Пояснення
НК-1. Однонаправлений достовірний канал	Реалізується, так як використовується користувачем логін і пароль для входу в систему. Зв’язок з використанням даного каналу відбувається виключно користувачем, а не роботом.
НО-1. Виділення адміністратора	Реалізується, так як визначаються ролі адміністратора і звичайного користувача.
НЦ-2. КЗЗ з гарантованою цілісністю	Виконується, тому що КЗЗ має власного домену для підтримання захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.
НТ-2. Самотестування при старті	Реалізується, бо йде перевірка файлів при запуску системи.
НВ-1: Автентифікація вузла	Виконується, так як йде оновлення операційної системи з офіційних серверів постачальника ОС.
КД-2. Базова довірча конфіденційність	Є розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

Технологія обробки інформації.

Обробка інформації відбувається поетапно, спочатку генеральний директор або його заступник контактують з потенціальною фірмою - партнером або з приватним підприємством з приводу придбання або продажу зернової продукції. Після узгодження загальної інформації, потенційного клієнта контактують з менеджером згідно з їх бажанням, оформлюють документи за здійснюють перевірку оплати.

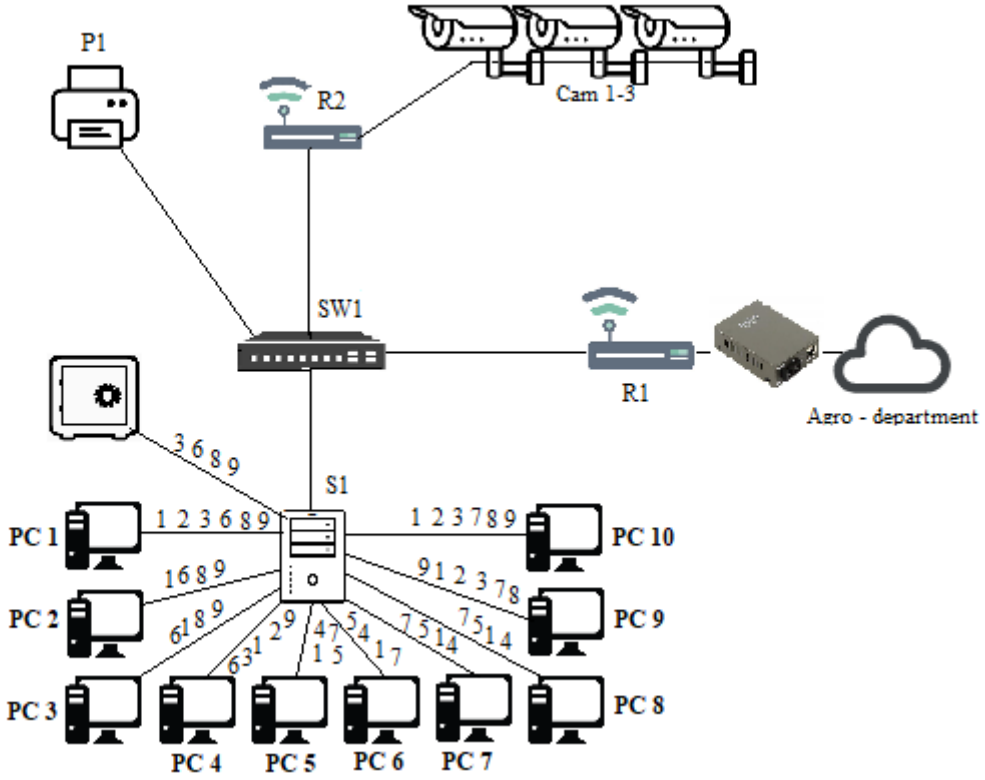


Рисунок 2.2 – Модель інформаційних потоків

1 Обробка робочого плану;

2 Підготовка бухгалтерського звіту;

3 Формування звіту діяльності підприємства;

4 Обробка бази даних покупців;

5 Обробка бази даних продукції;

6 Обробка системний звіт;

7 Передача банківських даних підприємства (о/р, ЄДРПОУ та ін.);

8 Формування зарплатних відомостей;

9 Формування відомісті по співробітникам (посада, кількість робочих годин, тощо).

Аналіз середовища користувачів представлено в таблиці 2.9.

Таблиця 2.9 - Аналіз середовища користувачів

№	Посада	ПІБ	Кабінет	Обчислювальна техніка	Робочі обов’язки	Контактні дані
1	Генеральний директор	Коліченко Дмитро Тарасович	Кабінет генерального директора (2 поверх)	PC1	Координує функціонування всіх відділів на всіх етапах.	+380972516651
2	Заступник генерального директора	Нечай Аркадій Вікторович	Кабінет заступника генерального директора (2 поверх)	PC2	Виконує обов’язки генерального директора у час його відсутності	+380972516652
3	Секретар	Бондар Вікторія Сергіївна	Кімната секретаря (2 поверх)	PC3	Виконує доручення керівництва.	+380972516653

Продовження таблиці 2.9

№	Посада	ПІБ	Кабінет	Обчислювальна техніка	Робочі обов'язки	Контактні дані
4	Системний адміністратор	Гірков Олег Ігорович	Кабінет системного адміністратора (1 поверх)	PC4	Виконує адміністрування АС підприємства.	+380972516654
5,6	Менеджери з закупівлі	Коваль Василь Несторович	Відділ менеджменту (1 поверх)	PC5 - PC6	2 менеджери з продажу займаються залученням клієнтів.	+380972516655 +380972516656
7,8	Менеджери з продажу	Сейсмічний Олександр Володимирович	Відділ менеджменту (1 поверх)	PC 7 - PC 8	2 Менеджери з закупівлі -пошук вигідних пропозицій.	+380972516657 +380972516658
9,10	Бухгалтерія	Вутін Петро Олегович	Бухгалтерія (2 поверх)	PC 9 - PC 10	Ведуть бухгалтерський та фінансовий облік підприємства.	+380972516659 +380972516660
		Фрутін Миколай Афанасьєвич				

Контактні дані та ПІБ працівників змінено за вимогою підприємства.

Матрицю доступу до інформації приведено в таблиці 2.10.

Матрицю доступу до ПЗ приведено в таблиці 2.11.

Таблиця 2.10 – Матриця доступу до інформації

Інформація	Посада						
	1	2	3	4	5,6	7,8	9,10
1	RWD	RWD	RP	R	R	R	R
2	R	R	-	-	-	-	RWD
3	R	R	-	-	-	-	-
4	R	R	-	-	-	-	RWD
5	R	R	-	RWDP	RWDP	-	-
6	R	R	-	RWDP	-	RWDP	-
7	R	R	-	-	-	-	-
8	RWD	RWD	RWD	R	-	-	-
9	R	R	-	RWDP	RWD	-	RWPD
10	R	R	-	RWDP	RWD	-	RWPD

R - перегляд інформації; W - модифікація інформації; D - знищення інформації; P - друк.

Таблиця 2.11 – Матриця доступу до ПЗ

ПЗ	Посада						
	1	2	3	4	5,6	7,8	9,10
1.	IW	IW	W	IWDU	W	W	W
2.	IW	IW	W	IWDU	IW	IW	W
3.	IW	IW	W	IWDU	IW	IW	IW
4.	IW	IW	W	IWDU	W	W	W
5	IW	IW	W	IWDU	W	W	W
6.	IW	IW	W	IWDU	W	-	-
7.	IW	IW	W	IWDU	W	W	W
8.	1	2	3	4	5,6	7,8	9,10
9.	-	-	-	IWDU	-	-	-
10.	W	W	W	IWDU	W	W	W

I - інсталяція ПЗ; W - використання ПЗ; D - деінсталяція ПЗ; U - оновлення.

2.5 Аналіз ризиків

Для аналізу інформаційних ризиків застосуємо модель їх ранжування та класифікації. Джерела загроз можна розділити на антропогенні, техногенні та стихійні, яким можна визначити коефіцієнтом рівня небезпеки $К_А$.

Для антропогенних джерел:

К1 - ступінь доступності до об’єкту;

К2 - ступінь кваліфікації і мотивації;

К3 - рівень наслідків (фатальність).

Для техногенних джерел:

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

К2 - наявність необхідних умов;

К3 - рівень наслідків (фатальність).

Для стихійних джерел:

К1 - особливості місцевості;

К2 - наявність необхідних умов;

К3 - рівень наслідків (фатальність).

Кожному критерію привласнюється оцінка від 1 до 5, після чого для джерела можна порахувати коефіцієнт $К_А$ за допомогою формули:

$$К_А = \frac{К1 \times К2 \times К3}{125} \quad (2.1)$$

де 125 - максимальне число добутку показників К.

Для створення політики безпеки потрібно створити модель загроз та модель порушника, виявивши джерела загроз з найвищім коефіцієнтом.

Найбільш ймовірні джерела загроз приведено в таблиці 2.12.

Таблиця 2.12 – Найбільш ймовірні джерела загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	А
Генеральний директор	5	1	2	10	0.08
Заступник генерального директора	5	1	2	10	0.08
Секретар	2	1	1	2	0.01
Системний адміністратор	4	1	3	12	0.09
Менеджери з продажу	2	1	1	2	0.01
Менеджери з закупівлі	2	1	1	2	0.01
Бухгалтерія	3	1	3	9	0.07
Ймовірний порушник	1	5	5	25	0.2

Джерела загроз, з коефіцієнтом нижче 0.01 вважаються неактуальними.

Найбільш небезпечні загрози теоретично можуть надходити від ймовірного порушника.

Найбільш небезпечні вразливості можна розділити на об’єктивні, суб’єктивні і випадкові.

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.

А - коефіцієнт небезпеки джерел загроз

Б - коефіцієнт небезпеки вразливостей

В - загальний коефіцієнт небезпеки

Коефіцієнт небезпеки вразливостей визначається так само, як і коефіцієнт небезпеки джерела загроз (формула 1).

Об’єктивні вразливості приведено в таблиці 2.13.

Суб’єктивні вразливості приведено в таблиці 2.14.

Виконаємо ранжування вразливостей.

Таблиця 2.13 – Об’єктивні вразливості

Вразливість	К1	К2	К3	К1*К2*К3	Б
1. Вразливості, що активізуються					
Програмні закладки	3	2	3	18	0.14
Неліцензійне або шкідливе ПЗ	5	4	3	60	0.48
2. Вразливості, які обумовлені особливостями захищеного об’єкту					
Наявність прямої видимості об’єктів	1	1	1	1	0.008

Таблиця 2.14 – Суб’єктивні вразливості

Вразливість	К1	К2	К3	К1*К2*К3	Б
1. Помилки					
Помилки користувачів системи	1	3	2	6	0.04
Помилки при підготовці та використанні програмного забезпечення	1	3	2	6	0.04
Помилки при експлуатації технічних засобів обміну інформацією	2	1	1	2	0.01
2. Порушення					
Порушення режиму використання інформації (сервер)	5	5	1	25	0.2
Порушення режиму конфіденційності працівниками в неробочий час	1	1	5	5	0.04

Проаналізуємо взаємозв’язок джерел загроз і вразливостей.

Дані взаємозв’язку джерел загроз і об’єктивних вразливостей приведено в таблиці 2.15.

Таблиця 2.15 – Взаємозв’язок джерел загроз і об’єктивних вразливостей

Джерело загроз	А	Вразливість	Б	В
Генеральний директор	0.08	Програмні закладки	0.14	0,01
		Неліцензоване або шкідливе ПЗ	0.48	0,03
		Наявність прямої видимості об’єктів	0.008	0,006
Заступник генерального директора	0.08	Програмні закладки	0.14	0,01
		Неліцензоване або шкідливе ПЗ	0.48	0,03
		Наявність прямої видимості об’єктів	0.008	0,006

Продовження таблиці 2.15

Джерело загроз	А	Вразливість	Б	В
Секретар	0.01	Програмні закладки	0.14	0.01
		Неліцензоване або шкідливе ПЗ	0.48	0.04
		Наявність прямої видимості об’єктів	0.008	0,008
Системний адміністратор	0.09	Програмні закладки	0.14	0.01
		Неліцензоване або шкідливе ПЗ	0.48	0.04
		Наявність прямої видимості об’єктів	0.008	0.007
Менеджери з продажу	0.01	Програмні закладки	0.14	0.01
		Неліцензоване або шкідливе ПЗ	0.48	0.04
		Наявність прямої видимості об’єктів	0.008	0,008
Менеджери з закупівлі	0.01	Програмні закладки	0.14	0.01
		Неліцензоване або шкідливе ПЗ	0.48	0.004
		Наявність прямої видимості об’єктів	0.008	0,008
Бухгалтерія	0.07	Програмні закладки	0.14	0.09
		Неліцензоване або шкідливе ПЗ	0.48	0.03
		Наявність прямої видимості об’єктів	0.008	0.005
Ймовірний порушник	0.2	Програмні закладки	0.14	0.02
		Неліцензоване або шкідливе ПЗ	0.48	0.09
		Наявність прямої видимості об’єктів	0.008	0,01

Дані взаємозв’язку джерел загроз і суб’єктивних вразливостей приведено в таблиці 2.16.

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

Джерело загроз	А	Вразливість	Б	В
Генеральний директор	0.08	Помилки користувачів системи	0.04	0.032
		Помилки при експлуатації технічних засобів обміну інформацією	0.04	0.032
		Порушення режиму використання інформації(сервер)	0.2	0.016

Продовження таблиці 2.16

Джерело загроз	А	Вразливість	Б	В
Генеральний директор	0.08	Порушення режиму конфіденційності працівниками в неробочий час	0.04	0.032
Заступник генерального директора	0.08	Помилки користувачів системи	0.04	0.032
		Помилки при експлуатації технічних засобів обміну інформацією	0.01	0,008
		Порушення режиму використання інформації (сервер)	0.2	0.016
		Порушення режиму конфіденційності працівниками в неробочий час	0.04	0.032
Секретар	0.01	Помилки користувачів системи	0.04	0.04
		Помилки при експлуатації технічних засобів обміну інформацією	0.01	0.01
		Порушення режиму використання інформації(сервер)	0.2	0.02
		Порушення режиму конфіденційності працівниками в неробочий час	0.04	0,004
Системний адміністратор	0.09	Помилки при експлуатації технічних засобів обміну інформацією	0.04	0.03
		Порушення режиму використання інформації(сервер)	0.01	0.009
		Порушення режиму конфіденційності працівниками в неробочий час	0.2	0.01
Менеджери з продажу	0.01	Помилки при експлуатації технічних засобів обміну інформацією	0.04	0.04
		Порушення режиму використання інформації(сервер)	0.04	0.04
		Порушення режиму конфіденційності працівниками в неробочий час	0.01	0,001
		Помилки користувачів системи	0.2	0,2

Продовження таблиці 2.16

Джерело загроз	А	Вразливість	Б	В
Менеджери з закупівлі	0.01	Помилки при підготовці та використанні програмного забезпечення	0.04	0.04
		Помилки при експлуатації технічних засобів обміну інформацією	0.01	0.04
		Порушення режиму використання інформації(сервер)	0.2	0,001
		Порушення режиму конфіденційності працівниками в неробочий час	0.04	0,02
Бухгалтерія	0.07	Помилки при підготовці та використанні програмного забезпечення	0.04	0,02
		Помилки при експлуатації технічних засобів обміну інформацією	0.01	0,07
		Порушення режиму використання інформації(сервер)	0.2	0,01
		Порушення режиму конфіденційності працівниками в неробочий час	0.04	0,02
		Помилки користувачів системи	0.04	0,02
Ймовірний порушник	0.2	Помилки при експлуатації технічних засобів обміну інформацією	0.01	0,02
		Порушення режиму використання інформації(сервер)	0.2	0,04
		Порушення режиму конфіденційності працівниками в неробочий час	0.04	0,08

Загрози, з коефіцієнтом нижче 0,1 вважаються неактуальними.

Розглянемо стихійні джерела загроз та стихійні вразливості:

Для стихійних джерел:

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 приведено в таблиці 2.17.

Таблиця 2.17 – Перелік можливих стихійних джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	А
Пожежа	1	1	1	1	0,08
Повінь	1	1	1	1	0,08
Ураган	1	1	1	1	0,08

Перелік випадкових вразливостей приведено в таблиці 2.18.

Таблиця 2.18 - Перелік випадкових вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	А
Пошкодження					
Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	1	1	1	1	0,08
Зовнішнє огородження території	1	1	1	1	0,08

Дані взаємозв’язку джерел стихійних загроз та випадкових вразливостей приведено в таблиці 2.19

Таблиця 2.19 – Взаємозв’язок джерел стихійних загроз та випадкових вразливостей

Джерело загроз	А	Вразливість	Б	В
Пожежа	0,08	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,08	0,06
Повінь	0,08	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,08	0,06
		Зовнішнє огородження території	0,08	0,06
Ураган	0,08	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,08	0,06
		Зовнішнє огородження території	0,08	0,06

Загрози, з коефіцієнтом нижче 0,1 вважаються не актуальними.

Розглянемо техногенні джерела загроз та вразливості:

Для техногенних джерел:

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 загроз приведено в таблиці 2.20.

Таблиця 2.20 – Перелік можливих техногенних загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	А
Зовнішні:					
Мережа комунікацій життєзабезпечення (тепло, водо, газопостачання)	1	1	1	1	0,08
Інженерна комунікація (мережа інтернет)	1	1	1	1	0,08
Внутрішні:					
Неякісні технічні засоби обробки інформації	1	1	1	1	0,08

Перелік техногенних вразливостей приведено в таблиці 2.21

Таблиця 2.21 – Перелік техногенних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	А
Збій та відмова в роботі:					
Відмова та несправність роботи засобів оброки інформації	1	1	1	1	0,08
Пошкодження:					
Інженерні комунікації (тепло, водо, газопостачання)	1	1	1	1	0,08
Збій постачання мережі інтернет	1	1	1	1	0,08

Дані взаємозв’язку техногенних джерел загроз та вразливостей приведено в таблиці 2.22.

Таблиця 2.22 – Взаємозв’язок техногенних джерел загроз та вразливостей

Джерело загроз	А	Вразливість	Б	В
Зовнішнє	0,08	Інженерні комунікації (тепло, водо, газопостачання)	0,08	0,06
Мережа інженерних комунікацій (тепло, водо, газопостачання)				
Неякісні технічні засоби обробки інформації	0,08	Відмова та несправність роботи засобів обробки інформації	0,08	0,06

Ранжування загроз до впровадження елементів політики безпеки приведено в таблиці 2.23

Таблиця 2.23 – Ранжування загроз до впровадження елементів політики безпеки

№	Загроза	Порушник	Коефіцієнт небезпеки	Рівень загрози
1	Неліцензійне або шкідливе ПЗ	Ймовірний порушник,	0.09	5

Продовження таблиці 2.23

№	Загроза	Порушник	Коефіцієнт небезпеки	Рівень загрози
2	Програмні закладки	Ймовірний порушник	0.05	4
3	Порушення режиму використання інформації (сервер)	Ймовірний порушник	0.03	3

- 0.01 – 0.3 = 3 (низький рівень ризику);
- 0.03 – 0.05 = 4 (середній рівень ризику);
- 0.06 – 0.10 = 5 (високий рівень ризику);

2.6 Розробка політики безпеки

Безпека і захищеність інформації є основними передумовами для забезпечення очікуваної ефективності бізнесу, його сталого розвитку та стійкості до зовнішніх та внутрішніх загроз інформаційної безпеки. Інформаційна безпеки є невід'ємною складовою діяльності ТОВ «Грейнфілд» і стосується кожного працівника, технології, інфраструктури, продукту, процесу. Політика інформаційної безпеки ТОВ «Грейнфілд» регламентує функціонування системи управління інформаційною безпекою відповідно до законодавства України.

Ця політика є основою для загальних процесів забезпечення інформаційної безпеки в елеваторі та встановлює основний підхід до забезпечення безпеки активів елеватору: інформаційних ресурсів та систем, інфраструктури елеватору, персоналу, процесів, продуктів і послуг, що надаються клієнтам, з метою забезпечення їх конфіденційності, цілісності та доступності.

Відповідальні особи політики безпеки.

Відповідальною особою за виконання елементів політик безпеки є системний адміністратор та заступник генерального директора.

– Політика антивірусної безпеки.

Політика визначає вимоги щодо захисту інформаційно-телекомунікаційної інфраструктури ТОВ “ГРЕЙНФІЛД” від загроз інформаційній безпеці, причина виникнення яких пов'язана з поширенням шкідливого програмного забезпечення. Дані вимоги мінімізують ймовірність виникнення негативних наслідків для ІТС ТОВ “ГРЕЙНФІЛД” внаслідок відсутності захисту інформаційно-телекомунікаційної інфраструктури. Негативні наслідки можуть включати в себе розкриття або втрату чутливої та конфіденційної інформації, крадіжку інтелектуальної власності, репутаційні наслідки, а також вплив на важливі внутрішні системи.

Завжди використовуйте отримане з довіреного джерела і прийняте в якості стандарту в ТОВ “ГРЕЙНФІЛД” антивірусне програмне забезпечення. Використовуйте і підтримуйте антивірусне програмне забезпечення в актуальному стані.

Ніколи не відкривайте вкладення до повідомлень електронної пошти, отриманим з невідомих, підозрілих або недовірених джерел. Такі вкладення повинні негайно видалятися.

Електронні листи містить спам, ланцюжки повідомлень і іншу небажану пошту повинні віддалятися без пересилання, відповідно до прийнятої в ТОВ “ГРЕЙНФІЛД” Політикою допустимого використання ІС.

Не завантажуйте інформацію з невідомих чи підозрілих джерел.

Уникайте надання загального доступу до логічних дисків з правами читання / запису в разі якщо це не потрібно в рамках виконання основної діяльності.

Перш ніж використовувати носії інформації, отримані від невідомих або підозрілих джерел, сканувати їх на відсутність вірусів.

Резервуйте важливі дані і настройки системи регулярно. Резервні копії зберігайте на сервері.

У разі необхідності запуску додатка, що конфліктує з встановленим антивірусним програмним забезпеченням, необхідно виконати повну перевірку робочої станції на наявність вірусів, відключити антивірусне програмне забезпечення і запустити потрібну програму. Повинно бути достеменно відомо, що запускається програма не призведе до негативних наслідків. Після виконання завдань пов'язаних з використанням програми, відновіть роботу антивірусного програмного забезпечення. При відключеному антивірусному програмному забезпеченні забороняється запускати будь-які додатки (електронна пошта або відкриття спільного доступу до файлових ресурсів) в результаті дії яких ваша робоча станція може бути схильна до інфікування шкідливим ПЗ.

Поява нового шкідливого програмного забезпечення виявляються щодня. Періодично перевіряйте антивірусну політику на предмет необхідності внесення в неї змін.

– Політика безпеки сервера

Огляд

Незахищені та вразливі сервери продовжують залишатися основною точкою входу для загроз.

Мета

Метою цієї політики є встановлення стандартів для базової конфігурації внутрішнього серверного обладнання, що є власністю та управляється в ТОВ “ГРЕЙНФІЛД”. Ефективна реалізація цієї політики дозволить мінімізувати несанкціонований доступ до інформації та технологій ТОВ “ГРЕЙНФІЛД”.

Обсяг

Усі працівники, підрядники, консультанти, тимчасові та інші працівники ТОВ “ГРЕЙНФІЛД” та його дочірніх компаній повинні дотримуватися цієї політики. Ця політика застосовується до серверного обладнання, яке належить,

експлуатується або орендується компанією або зареєстровано під власним внутрішнім доменом.

Політика

Внутрішній сервер, розгорнутий в ТОВ“ГРЕЙНФІЛД” повинен належати операційній групі, яка відповідає за системне адміністрування. Затверджені керівництво по налаштуванню сервера повинно бути створено та підтримуватися кожною оперативною групою на основі потреб бізнесу. Операційні групи повинні контролювати відповідність конфігурації та впроваджувати політику виключення, пристосовані до їхнього середовища. Кожна оперативна група повинна встановити процес зміни керівництва та налаштування. Необхідно виконати такі елементи:

Сервери повинні бути зареєстровані в корпоративній системі управління підприємством.

Вимоги до конфігурації

Послуги та програми, які не будуть використовуватися, повинні бути дезактивовані.

Доступ до послуг повинен реєструватися та / або захищатися за допомогою методів контролю доступу, таких як брандмауер веб-додатків.

Найновіші виправлення безпеки повинні бути встановлені в системі якнайшвидше, єдиним винятком є те, що негайне застосування перешкоджатиме діловим вимогам.

Довірчі відносини між системами є ризиком для безпеки.

Не використовуйте root - права, якщо використовуєте непривілейований обліковий запис.

Сервери повинні бути фізично розташований в середовищі з керованим доступом.

Моніторинг

Всі події, пов'язані з безпекою на критичних або чутливих системах, повинні бути зареєстровані та збережені.

Винятки

Будь-які винятки з політики повинні бути заздалегідь затверджені.

Невідповідність

Працівник, який виявив, що порушив цю політику, може підлягати дисциплінарному стягненню, включаючи припинення трудових відносин.

Політика захисту паролем

Огляд.

Паролі – важливий аспект комп'ютерної безпеки. Невірно вибраний пароль може призвести до несанкціонованого доступу та / або використання ресурсів. Весь персонал, включаючи підрядників та постачальників, які мають доступ до систем ІТС ТОВ “ГРЕЙНФІЛД” несуть відповідальність за вжиття відповідних заходів, як зазначено нижче, для вибору та захисту своїх паролів.

Мета.

Метою цієї політики є створення стандарту надійних паролів та їх захисту

Обсяг.

Сфера дії цієї політики включає всіх працівників, які мають або несуть відповідальність за обліковий запис (або будь-яку форму доступу, яка підтримує або вимагає пароль) у будь-якій системі, яка знаходиться на території ОІД та має доступ до мережі ТОВ “ГРЕЙНФІЛД” або зберігає будь-яку інформацію, що не є загальнодоступною в ТОВ “ГРЕЙНФІЛД”.

Політика.

– Усі користувачі повинні створити пароль для облікового запису.

– Усі паролі на рівні користувача та системного рівня повинні відповідати інструкціям щодо створення паролів.

– Користувачі повинні використовувати окремий, унікальний пароль для кожного з своїх облікових записів, пов'язаних з роботою. Користувачі не можуть використовувати будь-які пов'язані з роботою паролі для своїх особистих облікових записів.

– Облікові записи користувачів, що мають привілеї на рівні системи, надані через членство в групах або програми, повинні мати унікальний пароль від всіх інших облікових записів, які користувач має для доступу до привілеїв на рівні системи. Крім того, дуже рекомендується використовувати для будь-яких привілейованих облікових записів деяку форму багатофакторної аутентифікації

–Усі паролі зберігаються в програмі LastPass.

– Паролі слід змінювати тільки тоді, коли є підстави вважати, що пароль був скомпрометований.

– Паролі не повинні ділитися ні з ким, включаючи керівників та колег. Корпоративна інформаційна безпека визнає, що застарілі програми не підтримують проксі-системи.

– Паролі не повинні вставлятися в повідомлення електронної пошти, справи або інші форми електронного зв'язку, а також не розголошуватися по телефонній розмові.

– Паролі можуть зберігатися тільки в "менеджерах паролів", уповноважених організацією.

– Не використовуйте функцію "Пам'ятати пароль" програм (наприклад, веб-браузери).

– Будь-який користувач, який підозрює, що його пароль може бути скомпрометований, повинен повідомити про подію та змінити всі паролі.

Багатофакторна аутентифікація

– Багатофакторна аутентифікація повинна бути створена на всіх робочих станціях ТОВ “ГРЕЙНФІЛД”

Ранжування загроз після впровадження елементів політики безпеки приведено в таблиці 2.24.

Таблиця 2.24 - Ранжування загроз після впровадження політики безпеки

№	Загроза	Порушник	Коефіцієнт небезпеки	Рівень загрози після впровадження елементів політики
1	Неліцензійне або шкідливе ПЗ	Ймовірний порушник	0.09	2
2	Програмні закладки	Ймовірний порушник	0.05	2
3	Помилки при користуванні ПЗ	Ймовірний порушник	0.03	1

2.7 Висновок

У другому розділі обґрунтовано необхідність створення КСЗІ. Проведено категоріювання підприємства та підібрано профіль захищеності. Приведено загальні відомості про ОІД, проведено обстеження ОІД та аналіз загроз. Впроваджено елементи політики безпеки інформаційно - телекомунікаційної системи підприємства. Проведено ранжування загроз до та після впровадження елементів політики безпеки інформаційно - телекомунікаційної системи підприємства.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою розділу є економічне обґрунтування доцільності розробки елементів політики безпеки для ОІД ТОВ “ГРЕЙНФІЛД”- бетонно - силосного елеватора.

Ціллю економічного розділу є розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення (далі об’єкт проектування). Розрахунок річних експлуатаційних витрат на утримання і обслуговування об’єкта проектування. Визначення річного економічного ефекту від впровадження об’єкта проектування. Визначення та аналіз показників економічної ефективності запропонованого в кваліфікаційному проекті проектного рішення.

3.1 Розрахунок капітальних витрат

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

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):

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

$$t = 24 + 10 + 5 + 5 + 5 + 10 + 10 = 69;$$

Де $t_{тз}$ - тривалість складання технічного завдання на розробку політики безпеки інформації;

t - загальна трудомісткість розробки елементів політики безпеки.

$t_в$ - тривалість розробки концепції безпеки інформації у організації;

$t_а$ - тривалість процесу аналізу ризиків;

$t_{вз}$ - тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ - тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ - тривалість документального оформлення політики безпеки.

3.1.2 Розрахунок витрат на створення елементів політики безпеки інформації

Витрати на розробку елементів політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації З мч:

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

$$К_{рп} = 6900+131 = 7031 \text{ грн;}$$

6900 - заробітна плата спеціаліста інформаційної безпеки

131 - витрати машинного часу

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

$$З_{зп} = t \cdot З_{іб} \text{ грн.;} \quad (3.3)$$

$$З_{зп} = 69 \cdot 100 = 6900 \text{ грн;}$$

69 - годин на розробку елементів політики безпеки;

100 - заробітна плата грн/годину;

де t - загальна тривалість розробки політики безпеки, годин;

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

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч} \text{ , грн;} \qquad (3.4)$$

$$З_{мч} = 69*1.9 = 131 \text{ грн;}$$

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

Смч - вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн;} \qquad (3.5)$$

$$С_{мч} = 1.68*0.6 + \frac{5 \cdot 0.3}{1920} + \frac{3600 \cdot 0.5}{1920} = 1.90, \text{ грн/год;}$$

де P - встановлена потужність ПК, кВт;

$С_е$ - 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 $F_р$ = 1920).

$F_р$ = 1920 - річний фонд робочого часу;

$К_{лпз}$ для одного ПК:

- Microsoft Windows 10 Pro - 1000 грн;

- Microsoft office 2018 - 800 грн;

- Avast Premiere - 500 грн;

- LastPass - 1300 грн;

Всього: 3600 грн - вартість ліцензійного програмного забезпечення, грн;

$Н_{апз}$ - 0.3 - річна норма амортизації на ліцензійне програмне забезпечення;

$Н_а$ -0.5 - річна норма амортизації на ПК;

$Ф_{зал}$ - 7000 - 6995 = 5 грн - залишкова вартість ПК на поточний рік;

Р - 0,6 кВт;

$С_е$ - 1,68 грн/кВт год.;

$С_{мч}$ = 1.9 грн/год;

3.1.3 Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

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

$$К = 36000+7031+1000 = 44031 \text{ грн};$$

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки становлять 44031 тис. грн.

де $К_{пр}$-вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн; - сторонні організації не залучалися, коефіцієнт не враховуємо.

$К_{зпз}$-вартість закупівлі ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн; - 36000 грн.

$К_{рп}$ - вартість розробки політики безпеки інформації, тис. грн; - 7031 грн.

$К_{аз}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$-витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн; Відповідний працівник вже мав кваліфікацію та знання, коефіцієнт не враховуємо.

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. - 1000 грн.

3.2 Розрахунок експлуатаційних витрат

Таблиця - Вагові частки статей витрат у сукупній вартості

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

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

- вартість Upgrade-відновлення й модернізації системи (Св);

- витрати на керування системою в цілому (Ск);

- витрати, викликані активністю користувачів системи інформаційної безпеки (Сак - "активність користувача").

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак} \text{ грн;} \quad (3.7)$$

$$С = 283976+1000 = 284976 \text{ грн;}$$

Експлуатаційні витрати С - 284976 грн;

Витрати на керування системою інформаційної безпеки $С_к$ - 283976 грн;

Витрати, викликані активністю користувачів системи інформаційної безпеки $С_{ак}$ - 1000 грн.

Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_в$) не визначаються, згідно з терміном ліцензування ПЗ - 1 рік;

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн} \quad (3.8)$$

$$С_к = 18000+72000+193536+440 = 283\ 976 \text{ грн}$$

$С_н$ - 0; - Витрати на навчання адміністративного персоналу відсутні;

$С_а$ - 36000/2 = 18000 грн;

$С_з$ - $З_{осн} + З_{дод}$ *12= 72000 грн;

$С_{ел}$ - 193 536 грн; -

$С_о$ - 0 грн;

$С_{тос}$ *1% = 440 грн.

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) (табл. Додатка).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

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

$$С_з = 5000 + 1000 = 6000 \text{ грн};$$

5000 - основна заробітна плата;

1000 - додаткова заробітна плата;

де $З_{осн}$, $З_{дод}$ - основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата - в розмірі 8-10% від основної заробітної плати.

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

$$С_{ел} = 10*Р \cdot F_p \cdot Ц_е , \text{ грн.} \quad (3.10)$$

$С_{ел}$ = 193 536 грн;

Р= 0.6 кВт;

$F_р$ = 1920;

$Ц_е$ - 1.68 грн/кВт.год;

де Р - встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ - річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$- тариф на електроенергію, грн/кВт. годин

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними табл. 1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

У кожному конкретному випадку можуть бути враховані й інші види поточних витрат, що визначаються специфікою експлуатації проектованої системи інформаційної безпеки.

3.3 Оцінка величини збитку

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

– порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);

– порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);

– порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

– порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ - час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ - заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ - заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О - обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ - вартість заміни встаткування або запасних частин, грн;

I - число атакованих вузлів або сегментів корпоративної мережі;

N - середнє число атак на рік.

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

$$U = П_п + П_в + V \quad (3.11)$$

$П_п$ - 2045 грн.;

$П_в$ - 8977 грн.;

V - 19680 грн.;

U - 30702 грн.;

$П_п$ - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

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

$$Пп = \frac{20000}{176} \cdot 18 = 2045;$$

20000грн - заробітна плата обраного вузла;

де F - місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 год).

18 - час простою внаслідок атаки.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

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

$$П_{в} = 1705+272+7000 = 8977;$$

$П_в$ - 8977 грн; Маючи всі необхідні дані ми можемо розрахувати витрати на відновлення працездатності вузла експлуатаційного відділу:

$П_{ви}$ - 1705 грн; Витрати на повторне уведення інформації, грн;

$П_{пв}$ - 272 грн; Витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ - 7000 грн. Вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

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

$$Пви = \frac{20000}{176} \cdot 15 = 1705 \text{ грн};$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \quad (3.15)$$

$$Ппв = \frac{6000}{176} \cdot 8 = 272 \text{ грн;}$$

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

$$V = \frac{О}{Fг} \cdot (t_П + t_в + t_{ви}) \quad (3.16)$$

$$V = \frac{1000000}{2080} \cdot (18+8+15) = 19680 \text{ грн;}$$

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

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

$$В = \sum_i \sum_n U \quad (3.17)$$

$$В = 4 \cdot 5 \cdot 30702 = 614040 \text{грн;}$$

кількість атакованих вузлів - 4;

кількість прогнозованих атак на рік - 5;

упущена вигода від простою атакованого вузла - 30702 грн.

3.3.1 Загальний ефект від впровадження системи інформаційної безпеки

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

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

$$E = 614040 \cdot 0.75 - 284976 = 175554 \text{ грн;}$$

Загальний ефект від впровадження системи інформаційної безпеки.

де B - загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R - очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C - щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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:

$$ROSI = \frac{E}{K} \quad (3.19)$$

$$ROSI = 175554/44031 = 3,9;$$

Е - загальний ефект від впровадження системи інформаційної безпеки, що складає 175554 грн;

К - капітальні затрати, що становлять 44031 грн.

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

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

$$\text{To} = \frac{1}{3{,}9} = 0{,}25 = 92 \text{ дні} - \text{ термін окупності.}$$

3.5 Висновок

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 44031 грн, експлуатаційні - 283 976 грн. Згідно з підрахунками, створені елементи політики безпеки є доцільними з економічної точки зору.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 614040 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 175554 грн. Згідно с коефіцієнтом ROSI який становить 3,9 - створені елементи політики безпеки є цілком доцільними. Термін окупності елементів політики безпеки становить 92 робочих дні.

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто стан інформаційної безпеки в світі та Україні. Отримані висновки було поєднано для створення загальної проблематики безпеки інформації на сучасному етапі.

Проведено аналіз нормативно правової бази в сфері захисту інформації на актуальному етапі.

За допомогою нормативної документації проведено класифікацію підприємства та визначено його функціональний профіль захищеності. Проведено аналіз ОІД підприємства. Проведено аналіз ризиків. Згідно з отриманим аналізом ризиків визначено основні, та проведено їх ранжування .

В економічній частині було розраховано вартість інформаційних ресурсів підприємства, капітальні та експлуатаційні витрати на засоби захисту для зменшення ризику. Створення елементів політики безпеки виявилось доцільним згідно с коефіцієнтом ROSI – 3.9. Термін окупності – 92 дні.

Інформація, яка стосується інвентаризаційних відомостей, контактних даних працівників, їх обов’язків та плани будівлі було частково чи повністю змінено на вимогу підприємства.

СПИСОК ЛІТЕРАТУРИ

1 Технології AI в аграрно - промислових комплексах [Електронний ресурс] - Режим доступу до ресурсу: https://www.everest.ua/ai-platform/analytics/tehnologii-ai-v-agro-kompleksi/.

2 Результати Глобального дослідження EY з інформаційної безпеки показують, що кібербезпека залишається важливим питанням порядку денного організацій [Електронний ресурс] - Режим доступу до ресурсу: https://eba.com.ua/rezultaty-globalnogo-doslidzhennya-ey-z-informatsijnoyi-bezpeky-pokazuyut-shho-kiberbezpeka-zalyshayetsya-vazhlyvym-pytannyam-poryadku-dennogo-organizatsij/.

3 Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки [Електронний ресурс] - Режим доступу до ресурсу: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html.

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 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.

6 Закон України “Про доступ до публічної інформації” від 13.01.2011 №2939-VI // Відомості Верховної Ради України. - 2011. - № 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.

7 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

8 Закон України “Про електронний цифровий підпис” від 22.05.2003 852-IV // Відомості Верховної Ради України. - 2003. - № 45. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/852-15/ed20181107.

9 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.

10 ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.

11 ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912.

12 НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. - [Чинний від 08.11.2005] - К. : ДССЗЗІ, 2005. - №125 - (Нормативний документ системи технічного захисту інформації).

13 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).

14 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. - №22 - (Нормативний документ системи технічного захисту інформації).

15 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).

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

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	41	
7	А4	Економічна частина	13	
8	А4	Висновки	1	
9	А4	Список літератури	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	1	

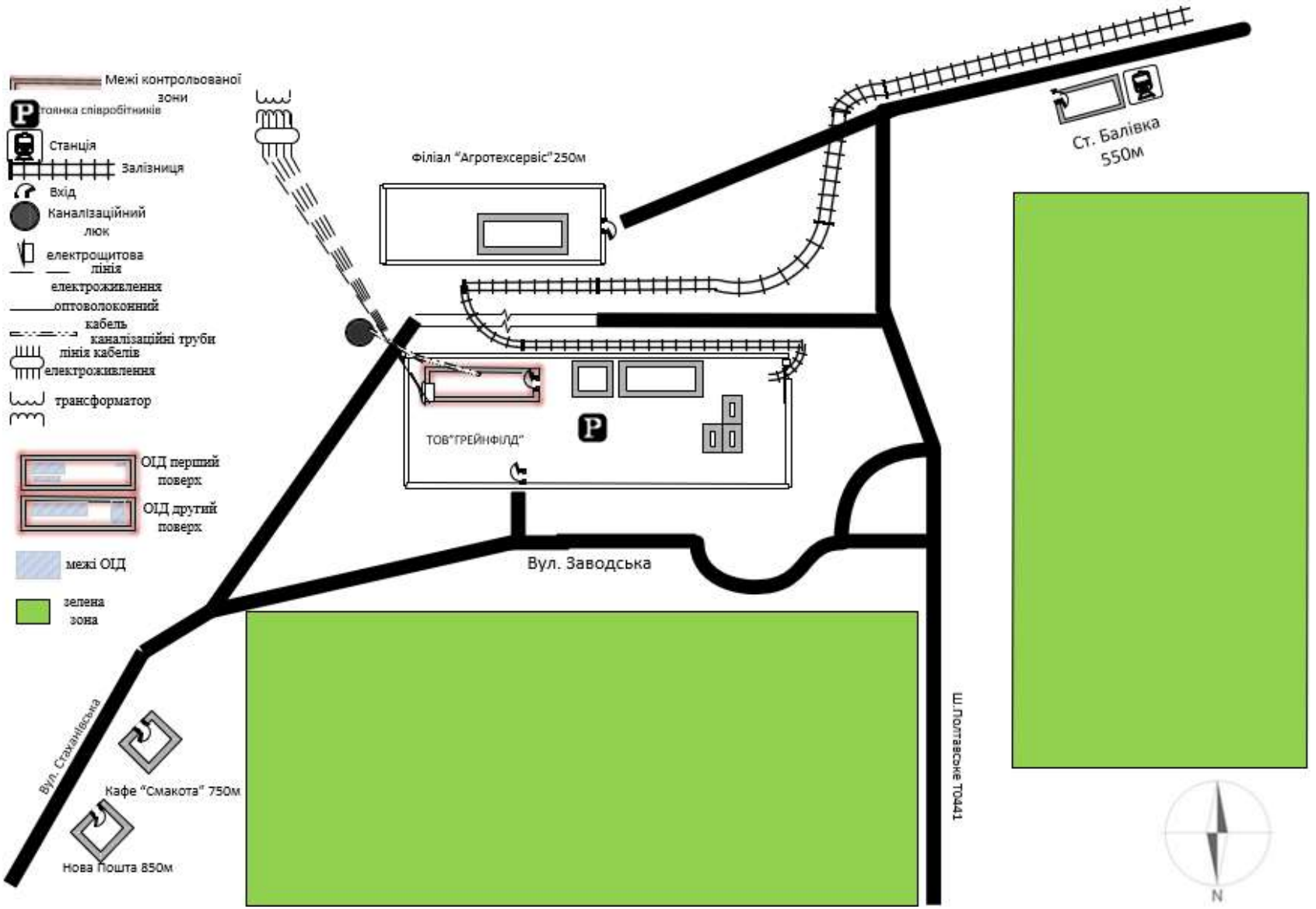
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

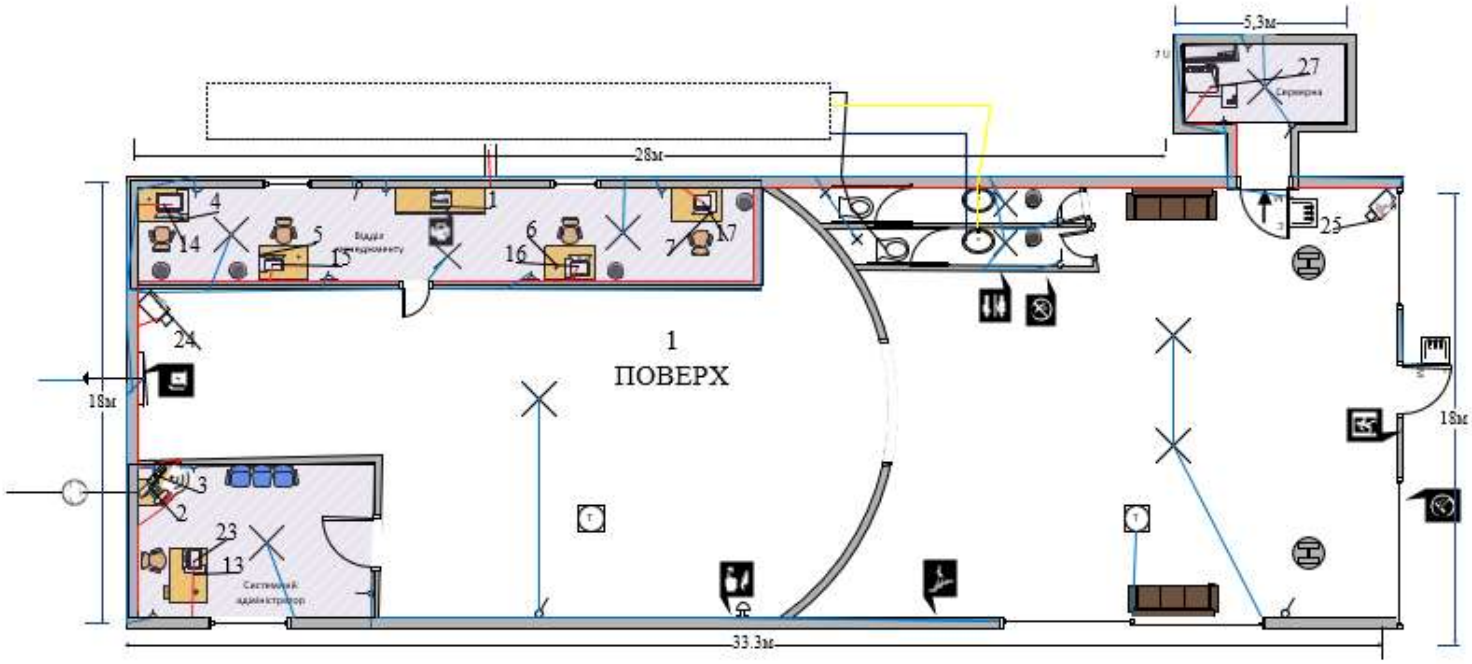
MatsaitisDIUbit151.docx

MatsaitisDIUbit151.pptx

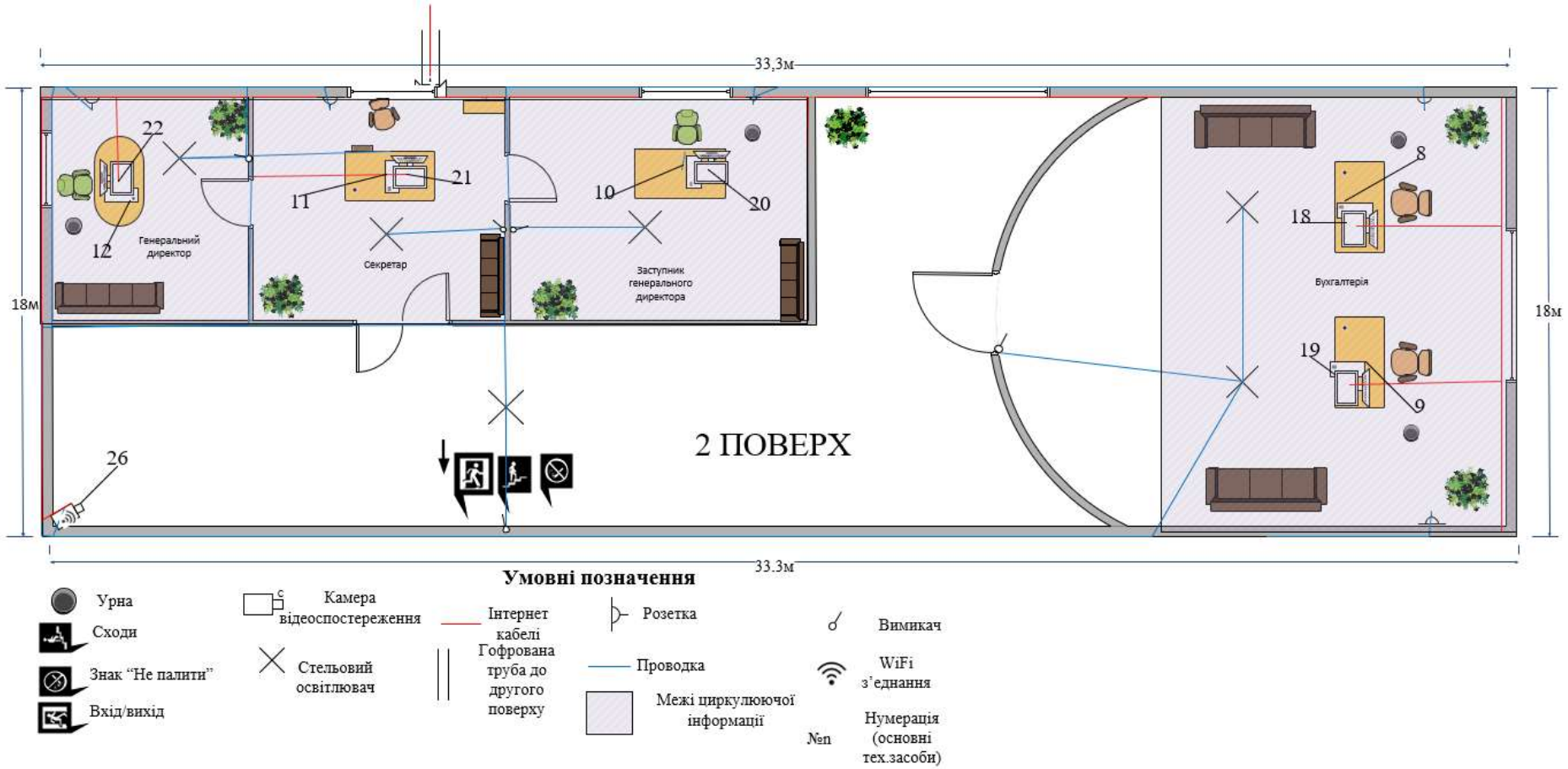
ДОДАТОК В. СИТУАЦІЙНИЙ ПЛАН ТОВ “ГРЕЙНФІЛД”



ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ПРИМІЩЕННЯ ТОВ “ГРЕЙНФІЛД”



Умовні позначення


33,3м
18м
18м
33.3м
22
12
Генеральний директор
11
21
Секретар
10
20
Заступник генерального директора
8
18
Вухгалтерія
19
9
26
2 ПОВЕРХ
Умовні позначення
Урна
Сходи
Знак “Не палити”
Вхід/вихід
Камера відеоспостереження
Стельовий освітлювач
Інтернет кабелі
Гофрована труба до другого поверху
Розетка
Проводка
Межі циркулюючої інформації
Вимикач
WiFi з’єднання
№п
Нумерація (основні тех.засоби)

ДОДАТОК Ґ. НАКАЗ НА СТВОРЕННЯ КСЗІ ДЛЯ ТОВ “ГРЕЙНФІЛД”

ТОВ “ГРЕЙНФІЛД”

НАКАЗ

«17» січня 2019 року №412

Про створення КСЗІ для
інформації в 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. Службі захисту інформації агродепартаменту створити комплексну систему захисту інформації (КСЗІ) для інформаційно - телекомунікаційної системи ТОВ “ГРЕЙНФІЛД”.

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 “ГРЕЙНФІЛД”.

3. Контроль за виконанням наказу залишаю за собою.

Директор Куплінов Д.Т.

ДОДАТОК Д. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Е. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

Метою кваліфікаційної роботи є підвищення рівня захищеності інформаційно – телекомунікаційної системи ТОВ “ГРЕЙНФІЛД”.

Тема кваліфікаційної роботи пов’язана з діяльністю спеціаліста фаху 6.170103 “Управління інформаційною безпекою”. Для досягнення поставленої мети у кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ “ГРЕЙНФІЛД”, проведення аналізу стану інформаційної безпеки з виявленням загроз; створення елементів політики безпеки ; оцінка ефективності впроваджених заходів з економічної точки зору. Практичне значення результатів кваліфікаційної роботи полягає в можливості їх використання у ТОВ “ГРЕЙНФІЛД”.

Перевагою кваліфікаційної роботи є розробка елементів політики безпеки, які дозволяють знизити рівень ризиків антропогенного характеру.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з деяким відхиленням від стандартів.

Під час виконання кваліфікаційної роботи Мацайтіс Д.І. проявив себе фахівцем, здатним майже самостійно вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи і заслуговує оцінки “добре”, а студент Мацайтіс Дмитро Ігорович присвоєння йому кваліфікації фахівець з організації інформаційної безпеки.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Керівник кваліфікаційної роботи,
кандидат технічних наук, доцент О.В. Герасіна

Керівник спеціального розділу,
старший викладач Д.С. Тимофєєв