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 ***Палія Вадима Володимировича***

академічної групи ***УБіт-15-1***

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

спеціалізації[1]

за освітньо-професійною програмою ***бакалавр***

на тему ***«Розробка політики безпеки інформаційно-телекомунікаційної системи ТОВ «Дніпропресс Сталь»»***

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

Дніпро
2019

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Палію Вадиму Володимировичу*** **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 інформаційно-телекомунікацінйної системи ТОВ «Дніпропресс Сталь»»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2019 № 771-л

Розділ	Зміст	Термін виконання
Розділ 1	Проведено аналіз безпеки інформації в інформаційно - телекомунікаційних системах	20.03.2019
Розділ 2	Обстеження інформаційно-телекомунікацийної системи ТОВ "Дніпропресс Сталь", ранжування загроз та розробка елементів політики безпеки	30.05.2019
Розділ 3	Економічне обґрунтування доцільності елементів політики безпеки та проведено 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 _____ Палій В.В.
(підпис студента) (підпис та ініціали)

РЕФЕРАТ

Пояснювальна записка: 103 с., 5 рис., 24 табл., 7 додатки, 13 джерел.

Об'єкт розробки: інормаційно-телекомунікаційна система відділу головного енергетика товариство з обмеженою відповідальністю «Дніпропресс Сталь»

Предмет розробки: впровадження елементів розробки політики безпеки в інформаційно-телекомунікаційну систему відділу головного енергетика.

Мета кваліфікаційної роботи: розробка елементів політики безпеки для інформаціно-телекомунікаційної системи відділу головного енергетика

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем інформаційної безпеки світу на України, розглянуто стан інформаційної безпеки в металургійній галузі.

В другому розділі кваліфікаційної роботи розглянуто необхідність розробки політики безпеки, стан інформаційної безпеки на теперішній час. Наведено загальні відомості про об’єкт інформаційної діяльності та підприємство. Проведено акт обстеження об’єкту інформаційної діяльності, категоріювання інформаційно-телекомунікаційної, підібрано профіль захищеності. Розраховано коефіцієнти ймовірності реалізації загроз, розроблено політики інформаційної безпеки.

В третьому розділі кваліфікаційної роботи розраховано доцільність використання розробки політки безпеки, та економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об’єкті інформаційної діяльності

ІТС, ОІД, АКТ ОБСТЕЖЕННЯ, ПБ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗА

РЕФЕРАТ

Объяснительная записка: 103 с., 5 рис., 24 табл., 7 прилож., 13 источ.

Объект разработки: информационно телекоммуникационная система отдела главного энергетика общества с ограниченной ответственностью «Днепропресс Сталь»

Предмет разработки: внедрение элементов разработки политики безопасности в информационно-телекоммуникационную систему отдела главного энергетика.

Цель квалификационной работы: разработка политики безопасности для информационно-телекоммуникационной системы отдела главного энергетика

В первом разделе квалификационной работы приведено общий анализ проблем информационной безопасности мира и Украины, рассмотрено состояние информационной безопасности в металлургической отрасли.

Во втором разделе квалификационной работы рассмотрено необходимость разработки политики безопасности, состояние информационной безопасности в настоящее время. Приведено общие сведенья про объект информационно деятельности и предприятие. Проведен акт обследования объекта информационной деятельности, категорирование информационно-телекоммуникационной системы, подобран профиль защищённости. Рассчитан коэффициент вероятности реализации угроз, разработаны политики для информационной безопасности.

В третьем разделе квалификационной работы рассчитана целесообразность использования разработки политики безопасности и экономическую эффективность внедрения её элементов в ИТС на ОИД

ИТС, ОИД, АКТ ОБСЛЕДОВАНИЯ, ПБ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УГРОЗА

ABSTRACT

Explanatory note: 103 p., 5 images, 24 tables, 7 supplements, 13 resources.

Object of study: information and telecommunication system in chief power engineer department of “Dnipropress Steel” Limited liability company.

Subject of development: implement developed elements of information securite policy for information and telecommunication system in chief power engineer department

The goal is to develop elements of information security policy for information and telecommunication system in chief power engineer department

First section of qualification work describes general analysis of information security problems in the world and in Ukraine, analyzed status of information security in metallurgical industry.

Second section of qualification work describes necessary of development SP in object of information activity, status of information security at this time. Generally described object of information activity and enterprise. Conducted survey of the object of information activity. Provided categorization of information and telecommunication system in object of information activity, according to categorization selected security profile. Calculated realization chance of threads and developed policies for security policy in object of information activity.

The third section of qualification work contains calculated coefficient information security policy usage expediencies and economic efficiency of implementation of information security policy.

ITS, ISP, OIA, SURVEY OF OIA, THREAD, INFORMATION SECURITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO – Міжнародна організація зі стандартизації

АС – Автоматизована система

ІБ – Інформаційна безпека

КЗ – Контрольована зона

КСЗИ – Комплекс системи захисту інформації

НД ТЗІ – Нормативний документ технічного захисту інформації

ОІД – Об’єкт інформаційної діяльності

ОС – Обчислювана система

ПЗ – Програмне забезпечення

ТЗ – Технічне завдання

ЗМІСТ с

ВСТУП

У зв’язку зі стрімким розвитком інформаційних технологій, за останні роки, стало очевидним, що жоден бізнес, не здатен до існування, якщо в нього не має інформаційного ресурсу та виходу до мережі Інтернет. Металургійна галузь стала однією з перших, що почала переходити до автоматизації процесів.

Автоматизація процесів у металургійній галузі дозволила розробляти більше високоякісних сплавів, адже для їх розробки та виготовлення потребується акуратність та точність якої людина не може досягти ніколи.

Впровадження автоматизованих систем значно зменшує вплив людини на виробництво та людську технічну помилку, а тому зменшується ризик створення ситуацій, що можуть загрожувати життю оточуючих.

Проте беручи до уваги специфіки виробництва у металургійній галузі неможливо остаточно відмовитися від людського фактору на виробництві. Металургійна галузь в Україні є однією з найбільших, а тому монополізація, неможлива у цій сфері, що призводить до існування конкурентів. Присутність людського фактора та відкритість ринкових відносин можуть стати однією із складових створення кримінальних ланок, що намагатимуться привласнити підприємства.

Обумовленість існування факторів, відкритість ринкових відносин, людський фактор на підприємстві, є достатніми аби підприємство мало інформацію із обмеженим доступом, як приклад: персональні дані робітників, власні розробки у сфері функціонування підприємства. А тому ця інформація потребує захищеності, а тому потрібно швидко реагувати на зміни в інформаційному середовищі та інциденти, що можуть трапитися у сфері інформаційної безпеки підприємства для найефективнішого реалізації потенціалу підприємства.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Інформаційні технології за останні роки перетворилися з науки про розрахунки математичних формул за допомогою комп’ютерів до однієї з найвпливовіших сфер людської діяльності.

Вплив інформаційних технологій зараз помітний повсюди; жодна людина зараз не може представити своє життя без Інтернету, соціальних мереж та потокових сервісів. Але найбільший вплив інформаційні технології мають в індустріальній сфері та економічній. Інформаційно-технічний вплив змінив характер та способи ведення бізнесу. Це призвело до його тотальної перебудови, а також швидкого економічного росту, зростання прибутків та збитків, що залежать від теперішнього стану інформаційної середи, а також технологій, що використовуються.

Підняття рівня в економічній сфері завжди супроводжується зростанням кримінального фактору, а також факторів шкідливого впливу, що можуть призвести до збитків завданими, явними або неявними, порушниками. Це обумовлює зростання кількості та тяжкості кібератак за останні роки:

− Внаслідок кібератаки кракерів проти партії «УДАР» наприкінці листопада 2013 року в руках зловмисників опинилися база електронної пошти партійної прес-служби, а також доступ до облікових записів у соціальних мережах Facebook і ВКонтакте лідера «УДАРу» Віталія Кличка. Відповідальність за акцію взяло на себе угрупування Anonymous Ukraine.[1]

− Внаслідок кібератаки кракерів проти партії «УДАР» наприкінці листопада 2013 року в руках зловмисників опинилися база електронної пошти партійної прес-служби, а також доступ до облікових записів у соціальних мережах Facebook і ВКонтакте лідера «УДАРу» Віталія Кличка. Відповідальність за акцію взяло на себе угрупування Anonymous Ukraine.[1]

− 2014 рік. 21–25 травня відбулися DDoS-атаки і злам сайту Центральної виборчої комісії під час президентських виборів. Внаслідок них на сайті з'явилися помилкові результати. Незважаючи на повідомлення української ЦВК про атаку, саме ці дані були оприлюднені в новинах на російському «Першому каналі» як реальні результати виборів в Україні.[1]

− Кібератака на енергетичні компанії України в грудні 2015 року. Найбільше постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy. Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. Загальний недовідпуск електричної енергії становив — 73 МВт·год (0.015 % від добового обсягу споживання України).[1]

− Кібератака на Укренерго 17-18 грудня 2016 року. Електроенергія була відсутня протягом 1 години 15 хвилин. Вимкнено струм у північній частині Києва на правому березі і частині прилеглих районів Київської області.[1]

− 6 грудня 2016 року хакерська атака на урядові сайти (Держказначейства України та інших) і на внутрішні мережі держорганів призвела до масштабних затримок бюджетних виплат. Вже 7 грудня (досить оперативно, як для державних органів) Кабмін виділив 80 млн гривень для захисту від хакерів.[1]

− 14 квітня 2017 року з'явилось перше відоме оновлення програми M.E.Doc уражене бекдором. Завдяки йому 18 травня 2017 року сталась перша масова кібератака вірусом XData. 27 червня 2017 року сталась друга масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80 % підприємств в Україні а також перекинулась на підприємства закордоном. Бекдор тривалий час дозволяв зловмисникам викрадати інформацію з підприємств та відкривав доступ зловмисникам до комп'ютерних мереж. На думку всіх п'яти країн Five Eyes, Данії та України відповідальність за атаку лежить на російській владі.[1]

Найчастішими були вірусні атаки та атаки на програмне забезпечення (далі ПЗ), втрата даних через зовнішні та внутрішні загрози, вразливості ПЗ, фішинг та втрата персональних даних через ПЗ з розрахунку на 1000 кібератак.

Металургійна галузь є однією з найстаріших та найрозвиненіших галузей, що існують на території України. Ця галузь також є однією з основних, адже створює близько 30% ВВП та забезпечую 40% валютних надходжень в економіку України.[2]

Складовою цієї галузі є металургійні заводи. Металургійний завод має інформаційну систему, що перебуває під постійним контролем і в разі відмови може загрожувати життєдіяльності людини. Металургійні заводи є складовою інтересів національної безпеки, оскільки на території цих заводів, а також у процесах виробництва використовуються речовини, що можуть спричинити техногенні катастрофи у районах їх розташування. Тому загальним інтересом безпеки України, органів місцевого самоврядування є запобігання викрадення небезпечних речовин з території заводів, недопущення збоїв у роботі. Тому на підприємствах слід виділити загрози інформаційній безпеці, що можуть привести до порушення нормальної працездатності комплексу, а саме можна виділити:

- Програмні
- Технічні
- Режимні
- Антропогені
- Природні

Наявність небезпечних для життєдіяльності речовин, що можуть спричинити техногенні катастрофи, їх облік та дотримання є вкрай вразливою інформацією, тому ця галузь є вразливою до загроз викрадення матеріального обладнання, порушення робочого процесу, а також кібератак. На таких підприємствах слід розуміти важливість високого забезпечення рівня інформаційної безпеки. Із розвитком технологій, а також інформаційних

ресурсів у відкритому доступі, інформованість про діяльність та наявність матеріального забезпечення підприємств такого типу стало майже загально доступним, саме тому власники таких підприємств повинні намагатися створювати компетентні та конкуренто спроможний рівень інформаційної безпеки. Саме тому розробка політики безпеки повинна бути одним із ключових факторів побудови систем інформаційного захисту на підприємствах такого типу, повинні бути якомога ефективніше використані інформаційні ресурси та інформаційне забезпечення підприємств. Під час формування політики безпеки слід розраховувати на розміри підприємства, фінансовий стан, та теперішній рівень інформаційної безпеки. Побудова комплексу системи захисту інформації повинно дотримуватися основних критеріїв: системності, комплексності, адекватності, відкритості алгоритму, простоти реалізації її на підприємстві. Системність означає необхідність обліку всіх взаємозалежних, взаємодіючих і періодичних умов і факторів що є необхідними для реалізації інформаційної безпеки. Принцип комплексності забезпечує широкий спектр методологій, заходів, засобів, що використовуються для проведення аналізу та захисту комп'ютерних систем (далі КС) підприємства. Узгоджене використання різних методів та засобів надасть змогу якнайкраще забезпечити знаходження або/та перекриття каналів витоку інформації, слабких місць у побудові систем захисту. Адекватність побудови передбачає, що комплекс системи безпеки не буде порушувати норми виробництва, розміри і можливості реалізації збитків були прийнятними. Відкритість алгоритму реалізації полягає у тому, що навіть при тому, що порушник знає алгоритм це не призводить до можливості реалізації загрози витоку інформації, або реалізації потребує стільки часу, що інформація стає неактуальною. Механізми захисту повинні бути простими і інтуїтивно зрозумілими, не базуватися лише на принципах розподілення доступу або вимагати додаткових навичок від співробітників підприємства, додаткових затрат при виконанні роботи, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій.

Отже, питання інформаційної безпеки стоїть гостро на великих та середніх галузевих підприємствах, оскільки від спроможності надати достатній рівень захищеності залежить не тільки спроможність підприємства бути конкуренто спроможнім, а також можливість попередження антропогенних катастроф та людських жертв, особливо в теперішній час, коли кібератаки йдуть не тільки на фінансові ринки, а також на ринки енергетики на галузевих підприємств для нанесення збитків та реалізації загроз

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Нормативно правова база у сфері інформаційної безпеки забезпечується наступними нормативно-правовими актами:

- Закон України «Про інформацію»

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

- Закон України «Про захист інформації в автоматизованих системах»

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

- Концепція національної безпеки України

Цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий

спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.[6]

− Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Базові нормативно правові акти, що регулюють побудову комплексу системи захисту інформації:

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

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

− визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

− створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

− оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.[7]

− НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;

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

− Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.[8]

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

− Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”.[9]

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

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

− Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

Цей стандарт установлює об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Для розробки ефективного комплексу системи захисту інформації однією із складових є вибір профілю захищеності згідно з НД ТЗІ 2.5-005-99. Основними вимогами на підприємствах такого типу є збереження цілісності та доступності інформації. Нормативно-правова база у сфері інформаційних відносин не є сталою і постійно обновлюється, тому з плином часу необхідно модернізувати базу та вдосконалювати згідно неї комплекс систем захисту інформації.[10]

1.3 Постановка задачі

На період виконання дипломного проекту були сформовані та поставлені наступні задачі:

− виконання обстеження ОІД;

- аналіз ризиків;
- детальне обґрунтовування необхідності створення КСЗІ;
- розробка політики безпеки;
- розрахування трудомісткості та затрат на створення та впровадження політики безпеки.

1.4 Висновки до першого розділу

У першому розділі дипломного проекту було описано стан інформаційної захищеності в галузі та в країні в цілому, наведені статистики та найбільші кібератаки за останні роки, приведений перелік документів, що регулюють відносини у сфері інформаційних відносин у державі, була зроблена постановка задачі для подальшої роботи дипломного проекту.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Підприємство «Дніпропресс Сталь» було створено на основі заводу важких гідравлічних пресів «НПО Дніпропресс», котре було засноване у 1955 році.

Можливості заводу забезпечують повний цикл виробництва від виплавки до механічної обробки та зборки великогабаритних вузлів і машин.

Площа цехів підприємства складає понад 500 тисяч квадратних метрів, територія, що займається 57 Га.

З 2014 року на заводі було проведено масштабну реконструкцію. Введено в експлуатацію конвертер гозокисневого рафінування ємкістю 15тн, проведено модернізацію нагрівачів і термічних печей, проведена глибока модернізація і повна автоматизація преса з зусиллям 1250 тс, встановлено обладнання для механічної обробки готових виробів. Технічне переозброєння допомогло випускати нержавіючу, жаростійку сталь і сплави, також використовувати ковку титану та його сплавів.

Завод «Дніпропресс Сталь» постійно проводить научно-технічні досліди, має технології для виробництва високопробних виробів з конструкційних, нержавіючих сталей і сплавів із титану.

Об’єктом дослідження є відділ головного енергетика підприємства ООО «Дніпропресс Сталь», м. Дніпро (надалі «ОІД»), комплекс системи захисту на підприємстві є інтеграційним.

2.2 Обґрунтування необхідності створення КСЗІ

Інформація з обмеженим доступом підлягає обов’язковому захисту згідно чинного законодавства України і вимог окремих нормативних документів ЗУ, а саме:

- Закон України «Про захист персональних даних»
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
- Закон України «Про захист персональних даних»
- Згідно Законів України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації. Володілець інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, у разі відсутності суперечності чинному законодавству.

На підприємстві «Дніпропресс Сталь» циркулює інформація з обмеженим доступом (персональні дані, база даних клієнтів, розробки оптимальних планів виробництва, звітність аналізів збою мереж) , вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником.

Інформація, з обмеженим доступом повинна оброблятися в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Організаційні заходи включають в себе:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

− розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

− навчання правилам інформаційної безпеки користувачів.

2.3 Організаційна структура підприємства

Рисунок 2.1 – Структура підприємства «Дніпропресс Сталь»

Структура заводу «Дніпропресс Сталь» збудована за лінійно-функціональною ознакою. Штат працівників налічує понад 2000 тисячі осіб з них близько 200 є працівниками адміністративного відділу заводу. За забезпечення фізичної охорони відповідає представники охоронної компанії, які підпорядковуються і входять до адміністративного відділу заводу. Завод функціонує згідно із чинним законодавством.

1) Адміністративний відділ – відповідає за координацію роботи усіх цехів та за злагоджену роботу відділів підприємства.

2) Цех механічної обробки – відповідає за первинну механічну обробку, та інші види механічної обробки сировини, що прибуває на підприємство.

3) Сталеплавний цех – відповідає за виплавку, сплавку, окислення сплавів виготовлення вторинної сировини.

4) Ковальсько-термічний цех – відповідає за термічну обробку та інші види обробки.

Оскільки комплекс системи захисту інформації на заводу «Дніпропресс сталь» є інтеграційним та типовим то достатньо розглядати один з відділів підприємства для огляду повної системи захисту.

В даному разі об’єктом інформаційної діяльності є відділ головного енергетика заводу «Дніпропресс Сталь»(далі ОІД). ОІД є складовою адміністративного відділу, що можна побачити на рисунку №2.3.

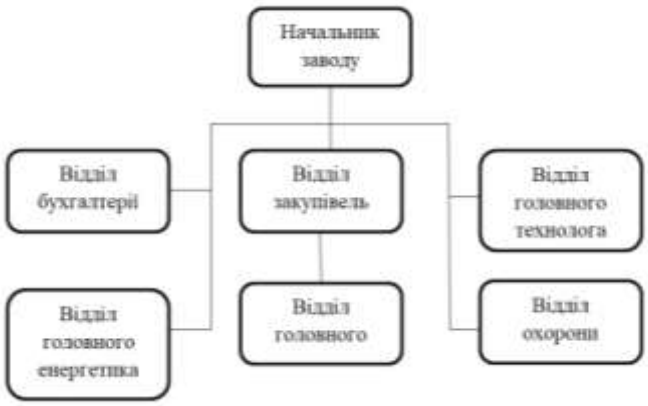


Рисунок 2.2 – Структура адміністративного відділу «Дніпропресс Сталь»

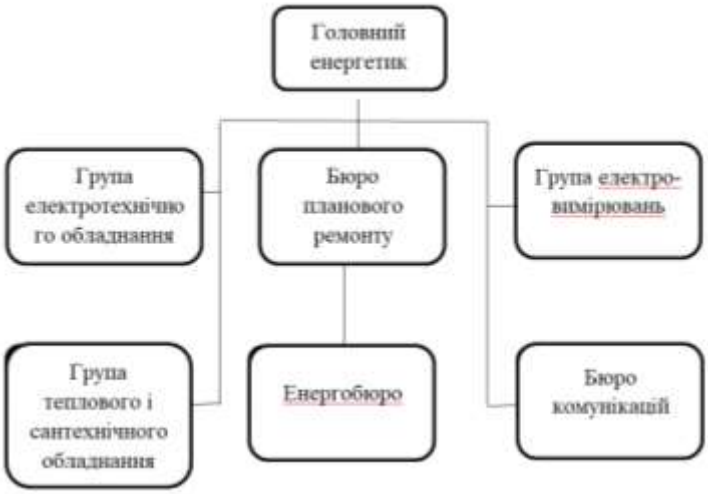


Рисунок 2.3 – Структура відділу головного енергетика

Склад та службові обов’язки відділу головного енергетика:

1) Головний енергетик – 1 людина, координує роботу всіх своїх підлеглих, є відповідальною особою за робото здатність систем на підприємстві. Звітує директору заводу.

2) Енергобюро – 2 людини, є відповідальними за регулювання, та підрахунок спожитого пального та енергії на підприємстві. Звітують головному енергетику.

3) Група теплового і сантехнічного обладнання – 2 людини, є відповідальними за ремонт, установку, демонтування обладнання теплових та сантехнічних мереж. Звітують головному енергетику.

4) Бюро комунікацій – 1 людина, є відповідальною, за встановлення безперервного зв’язку між усіма підпорядкованими відділами з головним енергетиком. Звітують головному енергетику.

5) Група електровимірювань – 1 людина, є відповідальною, за проведення замірів, розрахунку потужностей на енерго витратному обладнанні. Звітують головному енергетику.

6) Бюро планового ремонту – 4 людини, є відповідальними за проведення планових технічних робіт. Звітують головному енергетику.

7) Група електротехнічного обладнання – 2 людини, є відповідальним за розробку планів, щодо вдосконалення, реконструкції електротехнічного обладнання на підприємстві.

2.4 Аналіз оброблюваної інформації

У відділі співробітниками оброблюється інформація з обмеженим доступом: розробки планів оптимізації електроживлення, плани технічних робіт, результати замірів, звіти щодо закупівель обладнання та матеріалів, плани перспективного розвитку та інші. Вся документація існує у двох видах матеріальному та електронному, остання створюється працівниками на робочих станціях з інстальованим ПЗ, матеріальні копії створюються на основі

електронних шляхом розмноження на принтері або ксероксі. Електроні копії зберігаються на робочій станції працівника та на робочій станції головного енергетика. Після втрати чинності документи знищуються, облік місця та режиму зберігання носіїв інформації, а також її переміщення на підприємстві не відстежується.

Детальний перелік інформації, правовий режим, вид зберігання та вимогу до захисту наведено у таблиці 2.1.

Зображення інформаційних потоків наведено на рисунку 2.4.

К – вимоги до конфіденційності
Ц – вимога до цілісності
Д – вимога до доступності

Таблиця 2.1 – Інформація, що оброблюється в ОІД

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
1	Розробки планів оптимізації електроспоживання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
2	Плани оптимізації електроспоживання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
3	Плани робіт бюро планових робіт	Електронний, паперовий	ІЗоД	Службова	КЦД
4	Звітність бюро планових робіт	Електронний, паперовий	ІЗоД	Службова	КЦД
5	Звітність бюро комунікацій	Електронний, паперовий	ІЗоД	Службова	КЦД

Продовження таблиці 2.1

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
6	Звітність групи електровимірювань	Електронний, паперовий	ІЗоД	Службова	КЦД
7	Звітність групи електротехнічного обладнання	Електронний, паперовий	ІЗоД	Службова	КЦД
8	Звітність групи теплового і сантехнічного обладнання	Електронний, паперовий	ІЗоД	Службова	КЦД
9	Звітність енергобюро	Електронний, паперовий	ІЗоД	Службова	КЦД
10	Плани розробки перспективного розвитку підприємства	Електронний, паперовий	ІЗоД	Службова	КЦД
11	Акти про реконструкцію електромережі цехів	Електронний, паперовий	ІЗоД	Службова	КЦД
12	Акти про технічне переобладнання підприємства	Електронний, паперовий	ІЗоД	Службова	КЦД
13	Технічні завдання по проектуванню нових енерго об’єктів	Електронний, паперовий	ІЗоД	Службова	КЦД

Продовження таблиці 2.1

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
14	Технічні завдання по реконструкції діючих енерго об’єктів	Електронний, паперовий	ІЗоД	Службова	КЦД
15	Висновки по розробленим проектам	Електронний, паперовий	ІЗоД	Службова	КЦД
16	Акти про прийом енергоустановок	Електронний, паперовий	ІЗоД	Службова	КЦД
17	Акти про проходження іспитів енергоустановок	Електронний, паперовий	ІЗоД	Службова	КЦД
18	Акти про перевірку зв’язку, сигналізації.	Електронний, паперовий	ІЗоД	Службова	КЦД
19	Договір про постачання електроенергії	Паперовий	ІЗоД	Службова	КЦД
20	База даних енергообладання на підприємстві	Електронний	ІЗоД	Службова	КЦД
21	Інформація про діяльність відділу головного енергетика	Електронний, паперовий	Відкрита	-	-

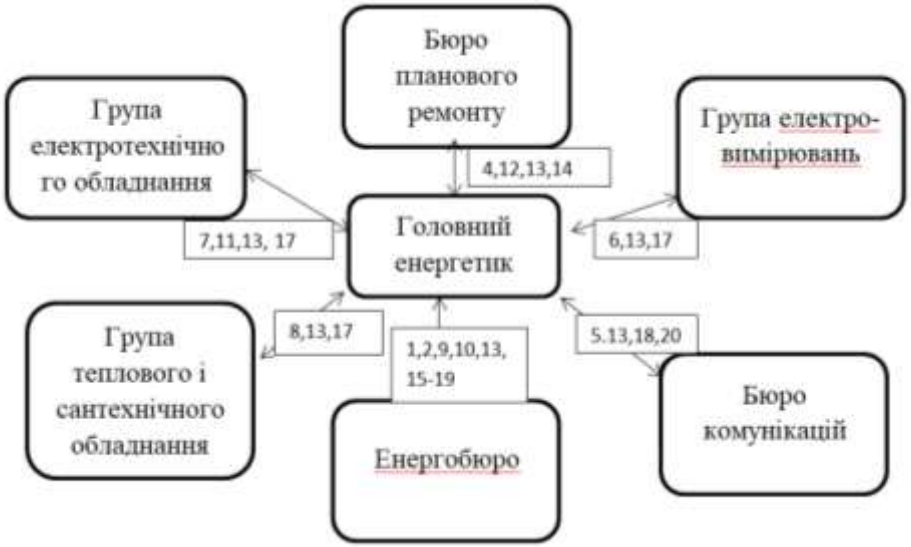


Рисунок 2.4 – Інформаційні потоки в ОІД

Таблиця 2.2 - Матриця доступу до інформації

Інформація	Посада										
	НВ	НГЕ	РГЕ	СЕБ	РЕБ	АД	СЕВ	СПР	РПР	СТС	РТС
1	CRWD	-	-	CRWD	CWR	-	-	-	-	-	-
2	CRWD	-	-	CRWD	CWR	-	-	-	-	-	-

Продовження таблиці 2.2

Інформація	Посада										
	НВ	НГЕ	РГЕ	СЕБ	РЕБ	АД	СЕВ	СПР	РПР	СТС	РТС
3	RD	-	-	CRW	R	-	-	-	-	-	-
4	RD	-	-	-	-	-	-	CRW	R	-	-
5	RD	-	-	-	-	CRW	-	-	-	-	-
6	RD	-	-	-	-	-	CRW	-	-	-	-
7	RD	CRW	R	-	-	-	-	-	-	-	-
8	RD	-	-	-	-	-	-	-	-	CRW	R
9	RD	-	-	CRW	R	-	-	-	-	-	-
10	RD	-	-	CRWD	RW	-	-	-	-	-	-
11	RD	CRW	CRW	-	-	-	-	-	-	-	-
12	RD	-	-	-	-	-	-	CRW	RW	-	-
13	CRWD	R	R	R	R	R	R	R	R	R	R
14	CRWD	-	-	-	-	-	-	WR	R	-	-
15	WR	-	-	R	R	-	-	-	-	-	-
16	CRWD	-	-	RW	RW	-	-	-	-	-	-

Продовження таблиці 2.2

Інформація	Посада										
	НВ	НГЕ	РГЕ	СЕБ	РЕБ	АД	СЕВ	СПР	РПР	СТС	РТС
17	RD	-	-	R	R	-	CRW	-	-	-	-
18	RD		-	-	-	CRW	-	-	-	-	-
19	CWRD	-	-	WR	R	-	-	-	-	-	-
20	R	-	-	-	-	CRWD	-	-	-	-	-
21	CWRD	R	R	R	R	R	R	R	R	R	R

C – create (право на створювання); R – read (право на зчитування); W – write (право на редагування); D – delete (право на видалення).

Пояснення до таблиці 2.2

НВ – Начальник відділу головного енергетика

НГЕ – старший робітник групи електротехнічного обладнання

РГЕ – робітник групи електротехнічного обладнання

СЕБ – старший робітник енергобюро

РЕБ – робітник енергобюро

АД – адміністратор бюро комунікацій

СЕВ – старший робітник групи електровимірювань

СПР – старший робітник бюро планового ремонту

РПР – робітник бюро планового ремонту

СТС – старший робітник групи теплового і сантехнічного обладнання

РТС – робітник групи теплового і сантехнічного обладнання

2.5 Обстеження об’єкту інформаційної діяльності

Відділ головного енергетика (далі ОІД) – є об’єктом інформаційної діяльності, що досліджується в кваліфікаційній роботі. ОІД є складовою адміністративного відділу заводу «Дніпропресс Сталь», за адресою проспект Богдана Хмельницького, 148А у місті Дніпро. Приміщення ОІД знаходиться на 3 поверсі Адміністративної будівлі, займає 6 приміщень

Робочі години: з 8:00 до 18:00

Перерва: з 12:00 до 13:00

Робочі дні: понеділок – п’ятниця

За фізичну охорону ОІД відповідає приватна охорона фірма, що забезпечує фізичну охорону на території всього заводу. Графік роботи фізичної охорони складається з трьох змін:

- Перша зміна з 9:00 до 17:00
- Друга зміна з 17:00 до 01:00
- Третя зміна з 1:00 до 9:00

На території заводу присутні декілька екіпажів охоронної фірми. На поверсі де знаходиться ОІД розташовані декілька камер в коридорах. Також кожна кімната підключена до пульту управління і сповіщення сигналізації. Кожному працівникові видається унікальний ідентифікатор, за допомогою, якого він може потрапити на територію заводу.

Територія заводу має зовнішні контрольно-пропускні пункти.

Поруч з територією заводу знаходяться:

- СТО «ЗІГФРІД»
- ГП «ДОСЖТ»
- Автосервіс шино монтаж «Колесо»

- Дніпро, металобаза 7ФВ Метал Груп
- Ветеринарна клініка «Панда»

Відстань до залізничної колії у західному напрямку – 665 метрів, відстань до промислових об’єктів – 1,5 км (ЗАТ «Дніпрошина), відстань до житлових будинків по вул. Героїв Сталінграду – 540 м в північно-східному напрямку. Найменша відстань від елементів ПНО до котельні міських теплових мереж - 50 метрів

Місце розташування ОІД зображено на додатку А

Контрольована зона визначена наказом начальника порту №137 від 06.08.2014 р. і охоплює територію заводу (0,57 га). Ситуаційний план наведений у додатку Б.

Таблиця 2.3 - Прилеглі споруди відносно ОІД

Тип споруди	Назва	Місцезна-ходження від ОІД	Мін.відстань від ОІД	Кіль-сть поверхів
Промислова	СТО «ЗІГФРІД»	Південно-західний напрямок	210 м.	3
Промислова	Дніпро, металобаза 7ФВ Метал Груп	Південно - західний напрямок	250 м.	3
Промислова	Австосервіс шино монтаж «Колесо»	Західний напрям	50 м.	2

Продовження таблиці 2.3

Тип споруди	Назва	Місцезна-ходження від ОІД	Мін.відстань від ОІД	Кіль-сть поверхів
Офісна будівля	ГП «ДОСЖТ»	Південний напрям	80 м.	5
Промислова	Ветеринарна клініка «Панда»	Західний напрямок	60 м.	2

Прилеглі вулиці відносно КЗ вказані у таблиці 2.4

Таблиця 2.4 - Прилеглі вулиці відносно ОІД

Назва вулиці	Описання
Проспект Богдана Хмельницького	Відносно ОІД вулиця знаходиться у західній стороні. Рух автомобілів активний (150-200 автомобілів на годину). Ширина проїжджої частини 30 метрів. Пішохідна зона 10 метрів.

Комунікаційні системи КЗ вказані у таблиці 2.5

Таблиця 2.5 - Комунікаційні системи

Вид комунікацій	*Характеристика*
Система опалення	Підключена до міської мережі опалення «Теплоенерго», знаходиться за межами КЗ.
Електроживлення	Підключено до трансформаторної підстанції ТП № 83 «ДТЕК Дніпровські Електромережі», котра обслуговує сторонніх споживачів і виходить за межі КЗ.

Продовження таблиці 2.5

Вид комунікацій	*Характеристика*
Система водопостачання	Підключена до міського водоканалу «Водоканал», котрий виходить за межі КЗ
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ.
Система заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.
Телефонний зв'язок	Телефонія надана компанією "Binotel". Вижодить за межі КЗ
Лінія постачання мережі Інтернет	Підключена до Інтернет-провайдеру «Kyivstar», знаходиться за межами КЗ.

Опис технічних засобів, що використовуються на підприємстві наведений у таблиці 2.6

Таблиця 2.6 - Технічні засоби

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
1	Системний блок	Acer RockPrime3 50Z	37613488944	На столі	193 см
2	Системний блок	Acer RockPrime3 50Z	37613488945	На столі	217 см
3	Системний блок	Acer RockPrime3 50Z	37613488946	На столі	217 см

Продовження таблиці 2.6

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
4	Системний блок	Acer RockPrime 350Z	37613488947	На столі	185 см
5	Системний блок	Acer RockPrime 350Z	37613488948	На столі	185 см
6	Системний блок	Acer RockPrime 350Z	37613488949	На столі	228 см
7	Системний блок	Acer RockPrime 350Z	37613488950	На столі	228 см
8	Системний блок	Acer RockPrime 350Z	37613488951	На столі	271 см
9	Системний блок	Acer RockPrime 350Z	37613488952	На столі	271 см
10	Системний блок	Acer RockPrime 350Z	37613488953	На столі	254 см
11	Системний блок	Acer RockPrime 350Z	37613488954	На столі	245 см

Продовження таблиці 2.6

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
12	Системний блок	Acer RockPrime350Z	37613488955	На столі	254 см
13	Системний блок	Acer RockPrime 350Z	37613488956	На столі	213 см
14	Монітор	Samsung SyncMaster E1920	75142490125	На столі	193 см
15	Монітор	Samsung SyncMaster E1920	73894592797	На столі	217 см
16	Монітор	Samsung SyncMaster E1920	81552952056	На столі	217 см
17	Монітор	Samsung SyncMaster E1920	47006941971	На столі	185 см
18	Монітор	Samsung SyncMaster E1920	75231068045	На столі	185 см

Продовження таблиці 2.6

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
19	Монітор	Samsung SyncMaster E1920	12631319995	На столі	228 см
20	Монітор	Samsung SyncMaster E1920	80673141073	На столі	228 см
21	Монітор	Samsung SyncMaster E1920	59652705567	На столі	271 см
22	Монітор	Samsung SyncMaster E1920	59249941759	На столі	271 см
23	Монітор	Samsung SyncMaster E1920	32854231317	На столі	254 см
24	Монітор	Samsung SyncMaster E1920	35252622766	На столі	245 см
25	Монітор	Samsung SyncMaster E1920	99987920585	На столі	254 см

Продовження таблиці 2.6

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
27	Монітор	Samsung SyncMaster E1920	26444551086	На столі	213 см
28	Роутер	TP LINK TL 840n	39266555089	На стіні	20 см
29	Роутер	TP LINK TL 840n	39317214237	На стіні	20 см
30	Роутер	TP LINK TL 840n	79107129732	На стіні	20 см
31	Роутер	TP LINK TL 840n	12431341950	На стіні	20 см
32	Роутер	TP LINK TL 840n	43685409045	На стіні	20 см
33	Комутатор	Tenda TEF1126P	40087688857	На стіні	20 см

Засоби ДТЗС для зон, що є суміжними з ОІД вказані у таблиці 2.7, ДТЗС у зоні ОІД вказані у таблиці 2.8.

Таблиця 2.7 - ДТЗС у суміжних зонах з ОІД

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
1	Датчик диму	Altronics	13502013776	На стелі	60 см
2	Датчик диму	Altronics	13502013777	На стелі	60 см
3	Датчик диму	Altronics	13502013778	На стелі	90 см
4	Датчик диму	Altronics	13502013779	На стелі	490 см
5	Камера відеоспостереження	Hiseeu FH-1C 1080 P	76919682768	На стіні	60 см
6	Камера відеоспостереження	Hiseeu FH-1C 1080 P	76919682769	На стіні	800 см
7	Кондиціонер	HYUNDAI ARN07HQBUA/ARU07HQBUA	80908964086	На стіні	30 см
8	Кондиціонер	HYUNDAI ARN07HQBUA/ARU07HQBUA	80908964087	На стіні	30 см
9	Кондиціонер	HYUNDAI ARN07HQBUA/ARU07HQBUA	80908964088	На стіні	30 см

Таблиця 2.8 - ДТЗС у зоні ОІД

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
1	Клавіатура	Acer RockPrime3 50Z	38277742600	На столі	193 см
2	Клавіатура	Acer RockPrime3 50Z	38277742601	На столі	217 см
3	Клавіатура	Acer RockPrime3 50Z	38277742602	На столі	217 см
4	Клавіатура	Acer RockPrime3 50Z	38277742603	На столі	185 см
5	Клавіатура	Acer RockPrime3 50Z	38277742604	На столі	185 см
6	Клавіатура	Acer RockPrime3 50Z	38277742605	На столі	228 см
7	Клавіатура	Acer RockPrime3 50Z	38277742606	На столі	228 см
8	Клавіатура	Acer RockPrime3 50Z	38277742607	На столі	271 см

Продовження таблиці 2.8

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
9	Клавіатура	Acer RockPrime3 50Z	38277742608	На столі	271 см
10	Клавіатура	Acer RockPrime3 50Z	38277742609	На столі	254 см
11	Клавіатура	Acer RockPrime3 50Z	38277742610	На столі	245 см
12	Клавіатура	Acer RockPrime3 50Z	38277742611	На столі	254 см
13	Клавіатура	Acer RockPrime3 50Z	38277742612	На столі	213 см
14	Комп’ютерна мишка	A4tech OP-720 USB (Black)	69959106782	На столі	193 см
15	Комп’ютерна мишка	A4tech OP-720 USB (Black)	96033017804	На столі	217 см
16	Комп’ютерна мишка	A4tech OP-720 USB (Black)	29566299778	На столі	217 см

Продовження таблиці 2.8

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
17	Комп’ютерна мишка	A4tech OP-720 USB (Black)	48203865871	На столі	185 см
18	Комп’ютерна мишка	A4tech OP-720 USB (Black)	12383634573	На столі	228 см
19	Комп’ютерна мишка	A4tech OP-720 USB (Black)	26169710941	На столі	228 см
20	Комп’ютерна мишка	A4tech OP-720 USB (Black)	26771691065	На столі	271 см
21	Комп’ютерна мишка	A4tech OP-720 USB (Black)	47882476571	На столі	185 см
22	Комп’ютерна мишка	A4tech OP-720 USB (Black)	48159393332	На столі	271 см
23	Комп’ютерна мишка	A4tech OP-720 USB (Black)	25742441276	На столі	254 см
24	Комп’ютерна мишка	A4tech OP-720 USB (Black)	47015668925	На столі	245 см

Продовження таблиці 2.8

№	Тип засобу	Назва та марка	Інвентарний номер	Розташування	Мін.відстань до кордонів ОІД
25	Комп'ютерна мишка	A4tech OP-720 USB (Black)	36226873459	На столі	254 см
26	Комп'ютерна мишка	A4tech OP-720 USB (Black)	17707187167	На столі	213 см
27	МФУ	Canon i-SENSYS MF633Cdw (1475C007)	78497167287	На підлозі	150 см

2.6 Опис обчислювальної системи

Опис обчислювальних систем, що використовуються на ОІД наведено в таблиці 2.9

Таблиця 2.9 - Опис обчислювальної системи

Назва	Характеристика		Серійний номер
Acer RockPrime350Z	Процесор	Intel(R) Core(TM) i3 CPU 540@ 3.07GHz	-
	ОЗУ	4,00 ГБ	-
	Вінчестер	500 ГБ	8383106
	Оптичний привід	DVD ROM ASUS	3088686

Продовження таблиці 2.9

Назва	Характеристика		Серійний номер
	Відокарта	NVIDIA GeForce 9600, 1ГБ	5899536
	Материнська плата	ASRock Socket 1155 Z77M	9355469

Програмне забезпечення обчислювальних систем наведено у таблиці 2.10

Таблиця 2.10 - Програмне забезпечення ОС Acer RockPrime350Z

Повна назва	Тип ПЗ	Версія ПЗ	Наявність ліцензії	Кількість ПЗ
Telegram	Прикладне	1.6	Не потребує	13
Skype	Прикладне	6.5	Не потребує	13
Google Chrome	Прикладне	5.6	Не потребує	13
Windows 10 Enterprise	Системне	1221.45	+	13
IntelDriverPACK	Системне	23.55	+	13
ADOBE PDF Reader	Прикладне	DC(2015.0)	+	13
Microsoft Office 2013	Прикладне	333.553	+	13

Топологія мережі

Для локальної мережі на ОІД використовується топологія типу «дерево». Кожний підпорядкований відділ, група або бюро має власний роутер. Доступ в

Інтернет відбувається через оптоволоконний кабель Ethernet ,котрий заходить на територію ОІД з за меж КЗ. Підключення оптоволоконного Ethernet кабелю відбувається до комутатора. Усі комп'ютери в мережі мають власні іменна та робочі групи. Підключення МФУ відбувається бездротовим шляхом, доступ до нього мають усі користувачі мережі відділу.

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

1. Комп'ютер головного енергетика (ME)
2. Комп'ютер голови енергобюро (CEB)
3. Комп'ютер робітника енергобюро (WEB)
4. Комп'ютер старшого в бюро планового ремонту (CPR)
5. Комп'ютер робітника бюро планового ремонту (WPR1)
6. Комп'ютер робітника бюро планового ремонту (WPR2)
7. Комп'ютер робітника бюро планового ремонту (WPR3)
8. Комп'ютер старшого групи електровимірювань (CES)
9. Комп'ютер старшого групи електротехнічного обладнання (CEQ)
10. Комп'ютер робітника групи електротехнічного обладнання (WEQ)
11. Комп'ютер старшого групи теплового і сантехнічного обладнання (CET)
12. Комп'ютер робітника гри теплового і сантехнічного обладнання (WET)
13. Комп'ютер адміністратора зв'язку (COM)

Комп'ютери усіх працівників розділені по робочим групам відповідно до бюро, відділу або групи якому вони належать.

Відповідність групи та комп'ютерів наведено в таблиці 2.11

Таблиця 2.11 - Відповідність робочих станцій робочим групам

Назва групи	Робоча станція
EBUR-G ROUP	ME
	CEB
	WEB
PLANBUR-GROUP	CPR
	WPR1
	WPR2
	WPR3
ELESTM-GROUP	CES
ELTECH-GROUP	CEQ
	WEQ
SANTECH_GROUP	CET
	WET
COMUNE_GROUP	COM

Функціональна схема мережі наведена на рисунку 2.5

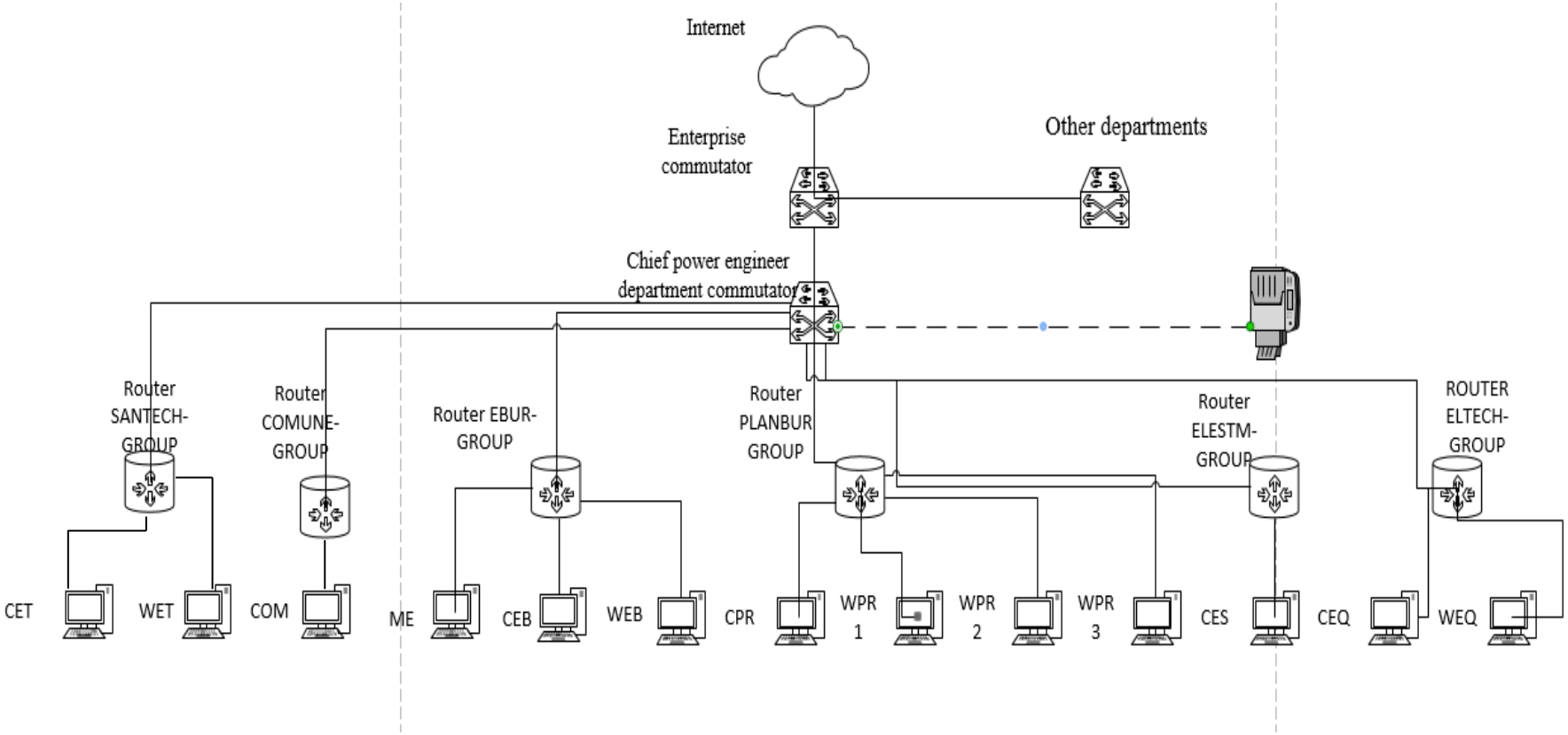


Рисунок 2.5 – Функціональна схема мережі ОІД

2.6 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 2.5-00599 на досліджуваному ОІД АС належить до третього класу. Згідно із НДТЗІ 1.6-005-99, а саме п.5.16 комплексу присвоюється четверта категорія[15]. 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} [ДОДАТОК Е]

2.7 Аналіз загроз та вразливостей

Забезпечення стану захищеності інформації потребує виконання певного комплексу дій, що передбачають глибинний аналіз негативних наслідків, які можуть реалізуватися. Цей комплекс дій включає в себе ідентифікацію можливих джерел, можливих загроз, факторів, що можуть їх спричинити. Як результат виконання комплексу дій є визначення актуальних загроз безпеці інформації.

Усі джерела інформаційної безпеки можуть бути виділені в три основні категорії:

- Антропогенні (обумовлені діями суб’єкта)
- Техногенні (обумовлені технічними засобами)

- Стихійні

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

$$К_{неб} = \frac{К1 \times К2 \times К3}{125}$$

125- це максимальне число добутку показників $К_{неб}$

Розглянемо перелік антропогенних джерел загроз та вразливостей:

Для антропогенних джерел:

К1 – ступінь доступності до об’єкту;

К2 – ступінь кваліфікації і мотивації;

К3 – рівень наслідків (фатальність).

Таблиця 2.12 – Перелік можливих антропогенних джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Начальник відділу головного енергетика	5	1	5	25	0,2
Старший робітник групи електротехнічного обладнання	3	2	4	24	0,192
Робітник групи електротехнічного обладнання	3	3	4	36	0,288
Старший робітник енергобюро	4	2	4	32	0,256
Робітник енергобюро	4	3	4	48	0,384
Адміністратор бюро комунікацій	4	3	4	48	0,384
Старший робітник групи електровимірювань	3	3	5	45	0,36

Продовження таблиці 2.12

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Старший робітник бюро планового ремонту	3	2	4	24	0,192
Робітник бюро планового ремонту	3	3	4	36	0,288
Старший групи теплового і сантехнічного обладнання	3	2	4	24	0,192
Робітник групи теплового і сантехнічного обладнання	3	3	4	36	0,288
Допоміжний персонал(прибиральниця, охоронець)	1	3	2	6	0,048
Конкуренти	2	5	5	50	0,4
Хакери	2	4	4	32	0,256
Кримінальні ланки	2	5	4	40	0,32

Критерії класифікації вразливостей:

К1 – ступінь впливу вразливості на незворотність наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз

К3 – кількість елементів об’єкту.

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

Таблиця 2.13 – Перелік об’єктивних антропогенних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
1. Вразливості, що активізуються					
1.1 Апаратні закладки	2	4	2	12	0,100
1.2 Програмні закладки	2	3	4	24	0,192
2. Вразливості, що визначаються особливостями елемнтів					
2.1 Апарати з електроакустичним перетворенням	1	3	2	6	0,048
3. Визначені особливостями захищеністю об’єкту					
3.1 Наявність прямої видимості об’єктів	2	2	1	4	0,032

Таблиця 2.14 – Перелік антропогенних суб’єктивних вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
1. Помилки					
1.1 Помилки при експлуатації ПЗ	2	4	3	24	0,192
1.2 Помилки при інсталяції та завантаженні ПЗ	3	5	3	45	0,360
1.3 Помилки при експлуатації технічних засобів	3	4	2	24	0,192
2. Порушення					
2.1 Порушення експлуатації технічних засобів	3	3	4	36	0,288

Зв’язок між джерелами загроз і вразливостями наведено у таблицях 2.15, 2.16

Таблиця 2.15 – Взаємозв’язок між джерелами загроз і об’єктивних антропогенних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
Начальник відділу головного енергетика	0,2	Апаратні закладки	0,100	0,02
		Програмні закладки	0,192	0,038
		Апарати з електроакустичним перетворенням	0,048	0,009
		Наявність прямої видимості об’єктів	0,288	0,056
Старший робітник групи електротехнічного обладнання	0,192	Апаратні закладки	0,100	0,019
		Програмні закладки	0,192	0,036
		Апарати з електроакустичним перетворенням	0,048	0,009
		Наявність прямої видимості об’єктів	0,288	0,055
Робітник групи електротехнічного обладнання	0,288	Апаратні закладки	0,100	0,028
		Програмні закладки	0,192	0,055
		Апарати з електроакустичним перетворенням	0,048	0,013

Продовження таблиці 2.15

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Наявність прямої видимості об’єктів	0,288	0,08
Старший робітник енергобюро	0,256	Апаратні закладки	0,100	0,025
		Програмні закладки	0,192	0,049
		Апарати з електроакустичним перетворенням	0,048	0,012
		Наявність прямої видимості об’єктів	0,288	0,07
Робітник енергобюро	0,384	Апаратні закладки	0,100	0,038
		Програмні закладки	0,192	0,073
		Апарати з електроакустичним перетворенням	0,048	0,018
		Наявність прямої видимості об’єктів	0,288	0,110
Адміністратор бюро комунікацій	0,384	Апаратні закладки	0,100	0,038
		Програмні закладки	0,192	0,073

Продовження таблиці 2.15

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Апарати з електроакустичним перетворенням	0,048	0,018
		Наявність прямої видимості об’єктів	0,288	0,110
Старший робітник групи електровимірювань	0,36	Апаратні закладки	0,100	0,036
		Програмні закладки	0,192	0,069
		Апарати з електроакустичним перетворенням	0,048	0,017
		Наявність прямої видимості об’єктів	0,288	0,103
Старший робітник бюро планового ремонту	0,192	Апаратні закладки	0,100	0,019
		Програмні закладки	0,192	0,036
		Апарати з електроакустичним перетворенням	0,048	0,009
		Наявність прямої видимості об’єктів	0,288	0,055
Робітник бюро планового ремонту	0,288	Апаратні закладки	0,100	0,028

Продовження таблиці 2.15

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Програмні закладки	0,192	0,055
		Апарати з електроакустичним перетворенням	0,048	0,013
		Наявність прямої видимості об’єктів	0,288	0,08
Старший групи теплового і сантехнічного обладнання	0,192	Апаратні закладки	0,100	0,019
		Програмні закладки	0,192	0,036
		Апарати з електроакустичним перетворенням	0,048	0,009
		Наявність прямої видимості об’єктів	0,288	0,055
Робітник групи теплового і сантехнічного обладнання	0,288	Апаратні закладки	0,100	0,028
		Програмні закладки	0,192	0,055
		Апарати з електроакустичним перетворенням	0,048	0,013

Продовження таблиці 2.15

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Наявність прямої видимості об’єктів	0,288	0,08
Допоміжний персонал(прибиральниця, охоронець)	0,048	Апаратні закладки	0,100	0,004
		Програмні закладки	0,192	0,009
		Апарати з електроакустичним перетворенням	0,048	0,002
		Наявність прямої видимості об’єктів	0,288	0,013
Конкуренти	0,4	Апаратні закладки	0,100	0,020
		Програмні закладки	0,192	0,076
		Апарати з електроакустичним перетворенням	0,048	0,018
		Наявність прямої видимості об’єктів	0,288	0,112
Хакери	0,256	Апаратні закладки	0,100	0,025
		Програмні закладки	0,192	0,049

Продовження таблиці 2.15

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Апарати з електроакустичним перетворенням	0,048	0,012
		Наявність прямої видимості об’єктів	0,288	0,070
Кримінальні ланки	0,32	Апаратні закладки	0,100	0,032
		Програмні закладки	0,192	0,061
		Апарати з електроакустичним перетворенням	0,048	0,015
		Наявність прямої видимості об’єктів	0,288	0,092

Таблиця 2.16 – Взаємозв’язок між джерелами загроз і суб’єктивних антропогенних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
Начальник відділу головного енергетика	0,2	Помилки при експлуатації ПЗ	0,192	0,038
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,072

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Помилки при експлуатації технічних засобів	0,192	0,038
		Порушення експлуатації технічних засобів	0,288	0,056
Старший робітник групи електротехнічного обладнання	0,192	Помилки при експлуатації ПЗ	0,192	0,036
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,069
		Помилки при експлуатації технічних засобів	0,192	0,036
		Порушення експлуатації технічних засобів	0,288	0,055
Робітник групи електротехнічного обладнання	0,288	Помилки при експлуатації ПЗ	0,192	0,055
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,103
		Помилки при експлуатації технічних засобів	0,192	0,055

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Порушення експлуатації технічних засобів	0,288	0,082
Старший робітник енергобюро	0,256	Помилки при експлуатації ПЗ	0,192	0,049
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,092
		Помилки при експлуатації технічних засобів	0,192	0,049
		Порушення експлуатації технічних засобів	0,288	0,073
Робітник енергобюро	0,384	Помилки при експлуатації ПЗ	0,192	0,073
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,138
		Помилки при експлуатації технічних засобів	0,192	0,073
		Порушення експлуатації технічних засобів	0,288	0,110

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
Адміністратор бюро комунікацій	0,384	Помилки при експлуатації ПЗ	0,192	0,073
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,138
		Помилки при експлуатації технічних засобів	0,192	0,073
		Порушення експлуатації технічних засобів	0,288	0,110
Старший робітник групи електровимірювань	0,36	Помилки при експлуатації ПЗ	0,192	0,06
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,129
		Помилки при експлуатації технічних засобів	0,192	0,069
		Порушення експлуатації технічних засобів	0,288	0,103
Старший робітник бюро планового ремонту	0,192	Помилки при експлуатації ПЗ	0,192	0,036

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,069
		Помилки при експлуатації технічних засобів	0,192	0,036
		Порушення експлуатації технічних засобів	0,288	0,055
Робітник бюро планового ремонту	0,288	Помилки при експлуатації ПЗ	0,192	0,055
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,103
		Помилки при експлуатації технічних засобів	0,192	0,055
		Порушення експлуатації технічних засобів	0,288	0,082
Старший групи теплового і сантехнічного бладнання	0,192	Помилки при експлуатації ПЗ	0,192	0,036
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,069

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Помилки при експлуатації технічних засобів	0,192	0,036
		Порушення експлуатації технічних засобів	0,288	0,055
Робітник групи теплового і сантехнічного обладнання	0,288	Помилки при експлуатації ПЗ	0,192	0,055
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,103
		Помилки при експлуатації технічних засобів	0,192	0,055
		Порушення експлуатації технічних засобів	0,288	0,082
Допоміжний персонал(прибиральниця, охоронець)	0,048	Помилки при експлуатації ПЗ	0,192	0,009
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,017
		Помилки при експлуатації технічних засобів	0,192	0,009

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
		Порушення експлуатації технічних засобів	0,288	0,013
Конкуренти	0,4	Помилки при експлуатації ПЗ	0,192	0,076
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,144
		Помилки при експлуатації технічних засобів	0,192	0,076
		Порушення експлуатації технічних засобів	0,288	0,112
Хакери	0,256	Помилки при експлуатації ПЗ	0,192	0,049
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,092
		Помилки при експлуатації технічних засобів	0,192	0,049
		Порушення експлуатації технічних засобів	0,288	0,073

Продовження таблиці 2.16

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливості	$К_{неб\ (вр.)}$	$К_{неб}$
Кримінальні ланки	0,32	Помилки при експлуатації ПЗ	0,192	0,061
		Помилки при інсталяції та завантаженні ПЗ	0,360	0,115
		Помилки при експлуатації технічних засобів	0,192	0,061
		Порушення експлуатації технічних засобів	0,288	0,092

Загрози з коефіцієнтом нижче 0.1 вважати неактуальними

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)

Таблиця 2.17 – Можливі техногенні джерела загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Зовнішні:					
Мережа інженерних комунікацій (тепло, водо, газопостачання)	4	3	4	48	0,384

Продовження таблиці 2.17

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Внутрішні:					
Неякісні технічні засоби обробки інфромації	4	4	5	80	0,64
Неякісне програмні засоби обробки інформації	2	3	3	18	0,144
Допоміжні засоби обробки інформації	3	4	5	60	0,48

Для класифікації вразливостей визначаються наступні критерії:

К1 – ступінь впливу вразливості на незворотність наслідків;

К2 – можливість використання вразливості джерелом загроз

К3 – кількість елементів об’єкту

Таблиця 2.18 – Техногенні вразливості

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
Збій та відмова в роботі:					
Відмова та несправність роботи засобів оброки інформації	5	5	4	100	0,80
Збій програмного забезпечення	4	4	4	64	0,512
Пошкодження:					
Життєзабезпечуючих комунікацій (тепло, водо, газопостачання)	4	3	4	48	0,384

Таблиця 2.19 – Взаємозв’язок техногенних загроз та вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
ЗОВНІШНЄ ДЖЕРЕЛО ЗАГРОЗ				
Мережа інженерних комунікацій (тепло, водо, газопостачання)	0,384	Життєзабезпечуючих комунікацій (тепло, водо, газопостачання)	0,384	0,147
ВНУТРІШНЄ ДЖЕРЕЛО ЗАГРОЗ				
Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Неякісні технічні засоби обробки інфромації	0,64	Відмова та несправність роботи засобів оброки інформації	0,80	0,512
Неякісне програмні засоби обробки інформації	0,144	Збій програмного забезпечення	0,64	0,092
Допоміжні засоби обробки інформації	0,48	Відмова та несправність роботи засобів оброки інформації	0,80	0,384

Розглянемо стихійні джерела загроз та стихійні вразливості:

Для стихійних джерел:

К1 – особливості місцевості;

К2 – наявність необхідних умов;

К3 – рівень наслідків (фатальність).

Таблиця 2.20 – Джерела стихійних загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Пожежа	2	1	1	2	0,01
Повінь	4	4	3	20	0,16
Землетрус	4	2	3	16	0,12
Ураган	1	2	1	2	0,01

Для класифікації вразливостей визначаються наступні критерії:

К1 – ступінь впливу вразливості на неусунення наслідків (фатальність);

К2 – можливість (зручність) використання вразливості джерелом загроз

К3 – кількість елементів об’єкту.

Таблиця 2.21 – Класифікація вразливостей

Вразливість	К1	К2	К3	К1*К2*К3	$К_{неб}$
Пошкодження					
Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	4	4	3	48	0,38
Зовнішнє огородження території	4	4	3	36	0,28

Таблиця 2.22 – Взаємодія джерел стихійних загроз з вразливостями

Джерело загроз	$К_{неб}$ (д.з.)	Вразливість	$К_{неб}$ (вр.)	$К_{неб}$
Пожежа	0,01	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,38	>0,01
		Зовнішнє огородження території	0,28	>0,01

Продовження таблиці 2.22

Джерело загроз	$К_{неб}$ (д.з.)	Вразливість	$К_{неб}$ (вр.)	$К_{неб}$
Повінь	0,16	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,38	0,06
		Зовнішнє огородження території	0,28	0,04
Землетрус	0,12	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,38	0,04
		Зовнішнє огородження території	0,28	0,03
Ураган	0,01	Життєзабезпечуючі комунікації (електро,водо,газо,теплопостачання)	0,38	0,001
		Зовнішнє огородження території	0,28	0,003

Для визначення моделі порушника на підприємстві проведемо загальне ранжування антропогенних загроз у таблиці 2.23

Таблиця 2.23 – Загрози, що реалізуються

№	Загроза	Порушник	Коефіцієнт	Рівень загрози
1	Наявність прямої видимості об’єктів	Робітник енергобюро	0,110	4
		Адміністратор бюро комунікацій	0,110	4
		Старший робітник групи електровимірювань	0,103	3
		Конкуренти	0,112	5

Продовження таблиці 2.23

№	Загроза	Порушник	Коефіцієнт	Рівень загрози
2	Помилки при інсталяції та завантаженні ПЗ	Робітник групи електротехнічного обладнання	0,103	3
		Робітник енергобюро	0,138	4
		Адміністратор бюро комунікацій	0,138	4
		Старший робітник групи електровимірювань	0,129	4
		Робітник бюро планового ремонту	0,103	3
		Робітник групи теплового і сантехнічного обладнання	0,103	3
		Конкуренти	0,144	5
		Кримінальні ланки	0,115	5
3	Порушення експлуатації технічних засобів	Робітник енергобюро	0,110	4
		Адміністратор бюро комунікацій	0,110	4

Продовження таблиці 2.23

№	Загроза	Порушник	Коефіцієнт	Рівень загрози
		Старший робітник групи електровимірювань	0,103	3
		Конкуренти	0,112	5

2.8 Розробка політик безпеки інформації

Для забезпечення робото здатності ОІД на підприємстві, а також для забезпечення сталого функціонування відділ головного енергетика повинен бути стійким до загроз та факторів інформаційної безпеки, а саме зовнішніх та внутрішніх. Інформаційна безпека ОІД – є запорукою його сталого функціонування і стосується кожного співробітника. Політика інформаційної безпеки ОІД регламентує функціонування системі управління інформаційної безпеки згідно із законодавством України.

Політика безпеки ОІД є основою для здійснення базової захищеності іформації. Політикою встановлюютьяс основні підходи, щодо обробки, збереження, передачі та знищення інформації. Політка інформаційної безпеки є однією із запорук збереження активів підприємства на якому функціонує ОІД.

Сфера регулювання: Процес забезпечення інформаційної безпеки на ОІД, що функціонує на підприємстві, охоплює усі аспекти діяльності, застосовується до всіх бізнес процесів. Є обов’язковою для виконання усіма співробітниками ОІД.

Мета політики безпеки

Встановити правила регулювання потоками інформації, що циркулюють в ОІД , забезпечити необхідні умови для роботи із конфіденціальною інформацією, а саме конфіденційність, цілісність, доступність. Є обов'язковою до виконання при доступі до інформаційних ресурсів, що циркулюють в ОІД.

Область дії

Відділ головного енергетика підприємства «Дніпропресс Сталь»(ОІД), всі співробітники, що користуються цією політикою.

Відповідальні особи

Відповідальними за виконання політики безпеки на ОІД є : начальник відділу головного енергетика, адміністратор бюро комунікацій.

- Політика соціальної інженерії

Огляд:

Політика соціальної інженерії є набором правил для робітників. Для захисту активів компанії усі працівники повинні захищати конфінціальність та устрій ресурсів компанії.

Мета:

Ця політика має дві мети використання: ознайомити робітників із поняттям атаки за допомогою соціальної інженерії та процедурою їх виявлення, друга, розробка спеціальних методик для працівник у разі необхідності робити правильний вибір.

Обсяг:

Політика є дійсною для усіх робітників компанії, тимчасових робітників, частково-зайнятих робітників, що займаються роботою з клієнтами.

Політика:

Політика передбачає, що жодна важлива інформація не буде передана не авторизованому користувачеві, якщо той використовує слова або техніки, що описанні нижче:

- «Невідкладна справа».
- «Забув пароль».
- «Вірусна проблема».
- Будь яка форма імітації розпорядки від начальника.
- Використання імен, що можуть надавати вигляду ніби людина є співробітником.
- Користувач потребує видачі будь-якої інформації, що може містити пароль, серійний номер, модель ресурсів компанії.
- Техніка, коли людина використовує не зареєстрований мобільний телефон, електронну пошту, факс.
- Техніка, коли людина видає себе за підрядника з яким компанія заключила контракт нещодавно.
- Техніка, коли людина видає себе за робітника крупного медіа.
- Спроби підкупу робітників контактного сервісу, для участі у злочинному діянні

Дії для забезпечення політики:

- Усі співробітники до яких можу бути застосована ця політика повинні пройти відповідний курс.
- Якщо, трапляється один із випадків описаних в політиці, співробітник повинен ідентифікувати людину, перш ніж продовжувати.
- Якщо, неможливо ідентифікувати працівника, менеджер якому підпорядковується співробітник за якого себе видають повинен бути проінформований.

- Якщо, менеджера нема на місці, потрібно проінформувати відповідального за інформаційну безпеку.

- Якщо, людина відповідальна за інформаційну безпеку відсутня співробітник повинен негайно завершити розмову

Відповідність політиці:

Група відповідальна за інформаційну безпеку перевірить відповідність, політиці за допомогою методологій, що включать в себе створення звітів, зовнішні аудити, зворотній зв’язок з власником політики

Винятки:

Усі винятки в політиці повинні бути затвердженні групою інформаційної безпеки

Невідповідність політиці:

Якщо виявляється, що працівник порушив політику, на нього накладаються дисциплінарні стягнення або припиняється співробітництво.

- Політика прийнятного використання

Огляд:

Політика в сфері інформаційної безпеки, що стосується правил публікування, не за для накладання обмеження на розповсюдження інформації про компанію, а за для забезпечення збереження активів від навмисного або ненавмисного впливу публікації, що може розкрити конфіденційну інформацію.

Мета:

Мета цієї політики безпеки полягає у визначенні прийнятності використання службових обчислювальних систем. Правила використання

встановлюються для захисту робітників та активів компанії. Неправомірне використання створює загрозу реалізації таких загроз: вірусні атаки, компрометація мережі та сервісів компанії, проблеми законного характеру

Обсяг:

Ця політика використовується, щодо визначення використання інформації, електричних приборів, обчислювальних систем та мережевих ресурсів, що надає компанія або взаємодія із внутрішньою мережею або системою ведення бізнесу, що має ліцензію на ім’я компанії, співробітника. Усі співробітники відповідальні за доречне використання ресурсів, що належать компанії або можуть бути співвіднесені до неї із додержанням місцевих законів.

Політика:

Загальне використання та право власності:

- Уся інформація, що є власністю підприємства, була надана їй або створена нею, на електронних, твердих носіях або обчислювальних системах, залишається повністю власністю компанії.
- Відповідальність за те аби звітувати про втрату, крадіжку або виток інформації, що належить компанії.
- Дозволено ділитися інформацією, що належить підприємству, тільки з авторизованими користувачами або тими кому було надано доступ
- Робітник має право використовувати службове обладнання лише в робочому процесі, а не задля власної користі.
- Для дотримання інформаційної безпеки, деякі авторизовані користувачі можуть переглядати мережевий трафік.
- Компаніє має право на періодичний аудит ресурсів, щодо відповідності використання.

Відповідність політиці:

Група відповідальна за інформаційну безпеку перевірить відповідність, політиці за допомогою методологій, що включать в себе створення звітів, зовнішні аудити, зворотній зв’язок з власником політики

Винятки:

Усі винятки в політиці повинні бути затвердженні групою інформаційної безпеки

Невідповідність політиці:

Якщо виявляється, що працівник порушив політику, на нього накладаються дисциплінарні стягнення або припиняється співробітництво.

- Політика антивірусного захисту

Огляд

Політика визначає вимоги щодо захисту інформаційно-телекомунікаційної системи відділу головного енергетика від загроз інформаційній безпеці, причина виникнення яких пов'язана з поширенням шкідливого програмного забезпечення.

Мета

Метою політики є мінімізація ймовірності виникнення негативних наслідків для ІТС відділу головного енергетика внаслідок відсутності захисту інформаційно-телекомунікаційної системи. 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 відділу головного енергетика(ОІД).

Обсяг

Ця політика застосовується до всіх співробітників компанії та обчислювальних систем, що їй належать

Політика:

- Завжди використовуйте отримане з довіреного джерела і прийняте в якості стандарту в ОІД антивірусне програмне забезпечення.
- Ніколи не відкривайте вкладення до повідомлень електронної пошти, отриманим з невідомих, підозрілих або недовірених джерел.
- Електронні листи містить спам, ланцюжки повідомлень і іншу небажану пошту повинні віддалятися без пересилання, відповідно до прийнятої в ОІД.
- Не завантажуйте інформацію з невідомих чи підозрілих джерел.
- Уникайте надання загального доступу до логічних дисків з правами читання / запису.
- 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 політику антивірусного захисту на предмет необхідності внесення в неї змін.

Відповідність політиці:

Група відповідальна за інформаційну безпеку перевірить відповідність, політиці за допомогою методологій, що включать в себе створення звітів, зовнішні аудити, зворотній зв’язок з власником політики

Винятки:

Усі винятки в політиці повинні бути затвердженні групою інформаційної безпеки

Невідповідність політиці:

Якщо виявляється, що працівник порушив політику, на нього накладаються дисциплінарні стягнення або припиняється співробітництво.

2.9 Висновки до другого розділу

У другій частині кваліфікаційної роботи було наведено загальні відомості про підприємство та необхідність створення КСЗІ, організаційна структура і проведений аналіз оброблюваної інформацій. На основі цього проведений акт обстеження підприємства. Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства. На основі рівня загроз ОІД були розроблені елементи політики безпеки інформації, що циркулює на ОІД.

3 ЕКОНОМІЧНИЙ РОЗДІЛ.

3.1 Техніко-економічне обґрунтування дипломного проекту

Основною задачею цього розділу є техніко-матеріальне обґрунтування доцільності розробки однієї із складових комплексу системи захисту інформації підприємства, що розглядається в кваліфікаційній роботі, а саме економічну доцільність політики безпеки.

Необхідність розробки політики безпеки для об’єкту інформаційної діяльності, відділ головного енергетика «Дніпропресс Сталь», полягає у наявності інформації з обмеженим доступом, яка становить інтерес для власника інформації. В тому числі запобігання можливості реалізації загроз, що можуть дозволити порушнику отримати до неї доступ або призвести до порушення нормального функціонування підприємства

Аналізуючи запропоновані в кваліфікаційній роботі варіант впровадження політики безпеки, а також програмну та технічну її реалізацію, результатом економічного аналізу буде доцільність використання запропонованих варіантів вирішення.

3.2 Визначення витрат на розробку політики безпеки

Основою для розрахунку витрат для на розробку політики безпеки інформації є концепція сукупності вартості володіння запропонована Gartner Group. У цій моделі враховуються наступні IT-витрати: фіксовані (капітальні) вкладення і поточні витрати.

Модель від Gartner Group пропонує наступні вагові частки кожної з наведених вище статей витрат стосовно сукупної вартості, які можна використовувати для спрощеної оцінки сукупної вартості володіння.

Таблиця 3.1 - Вагові частки статей витрат у сукупній вартості

Фіксовані (капітальні) вкладення	21%
Поточні витрати, у т.ч.	79%
Керування системою	12%
Технічна підтримка й відновлення	21%
Активність користувача	46%

Розрахунок капітальних витрат

Перш за все потрібно розрахувати капітальні інвестиції та капітальні затрати у політику безпеки. За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

- вартість розробки проекту інформаційної безпеки (розробка політики безпеки інформації тощо);
- витрати на залучення зовнішніх консультантів;
- вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);
- вартість створення основного й додаткового програмного забезпечення (ПЗ);
- витрати на первісні закупівлі апаратного забезпечення;
- витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);
- витрати на навчання технічних фахівців і обслуговуючого персоналу.
- Для повного визначення розробки політики безпеки інформації з точки зору економічної доцільності спочатку необхідно і доцільно розрахувати:
- визначення трудомісткості розробки політики безпеки інформації;
- розрахунок витрат на розробку політики безпеки інформації.

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):

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

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

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{взз}$ – 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;

$t_{д}$ – 15 годин, $t_{в}$ – 20 годин, $t_{а}$ – 15 годин, $t_{взз}$ – 25 годин, $t_{озб}$ – 20 годин, $t_{д}$ – 15 годин, $t_{тз}$ – 10 годин

Отже виходячи із експертних даних та запропонованої формули:

$$t = 20+30+20+25+20+15+10 = 120 \text{ годин.}$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку 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 **Змч**:

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

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:

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

Середня заробітна плата спеціаліста достатньої кваліфікації становить 4$ на годину що за перерахунком на гривную за теперішнім курсом становить 105,5 грн/год. Отже, розрахуємо заробітну плату виконавця:

$$З_{зп} = 120*105.5 = 12\ 660$$

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

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

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot На}{F_р} + \frac{К_{лпз} \cdot На_{пз}}{F_р}, \quad \text{грн.}, \qquad (3.5)$$

Спочатку необхідно розрахувати амортизацію розраховуємо за формулою зменшення залишкової вартості: А = Ва/Т, де Ва = Вп - Вл

Вп = 18000 – начальна вартість комп’ютера

Ліквідаційна вартість – 3000 грн

Т – корисне користування комп’ютером – 2 роки

Залишкова вартість комп’ютера становить 9999,96 грн

Норма оптимизації = ½ = 0,5

Розрахуємо залишкову вартість програмного забезпечення

Вп = 8 000 грн

Т = 4 роки

Річна норма амортизації = ¼ = 0,25

$$С_{мч} = 1,7*2,73 + (9999,96*0,50)/1920 + (8000*0,25)/1920 = 8 \text{ грн. } 28 \text{ коп.}$$

Розрахуємо вартість машиного часу для розробки політики безпеки

$$З_{мч} = 120*8,28= 993 \text{ грн } 60 \text{ коп.}$$

Отже виходячи із отриманих розрахунків витрати на розробку політики безпеки будуть становити:

$$К_{рп} = 12\ 660+993,6 =13\ 653 \text{ грн. } 60 \text{ коп.}$$

Таким чином розрахуємо капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки:

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

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

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

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

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

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

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

$К_{пр}$ – 13 000 грн. – вартість залучення незалежного експерта на момент проведення аналізу ризиків підприємства;

$К_{зпз}$ – 13 000 грн – вартість закупівлі ліцензій антивірусного обладнання, 13 ліцензій ПЗ «Malwarebytes»

$К_{рп}$ – 13 249 грн 20 коп – вартість розробки політики безпеки на ОІД.

$К_{аз}$ – 6 0000 грн. – вартість закупівлі трансформаторів напруги для обладнання , датчиків диму, камер, тощо.

$К_{навч}$ – 13 000 грн – проходження курсів для співробітників та тренінгів по соціальній інженерії.

$К_{н}$ – 8 000 грн – виплата працівнику монтажнику за встановлення апаратури.

$$К = 13\,000+13\,000+13\,249{,}2+6\,000+13\,000+8\,000=77\,249 \text{ грн. } 20 \text{ коп.}$$

Розрахунок поточних експлуатаційних витрат

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

- вартість Upgrade-відновлення й модернізації системи ($С_{в}$);
- витрати на керування системою в цілому ($С_{к}$);
- витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ – "активність користувача").

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

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

Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_{в}$) можна визначити на підставі фактичних даних організації або користуючись даними табл. 1, про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

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

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

$С_н$ – витрати на навчання адміністративного персоналу

$С_а$ - річний фонд амортизаційних відрахувань

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу

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

$С_{ел}$ - вартість електроенергії

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

$З_{осн}$ в місяць для робітника дорівнює 9 тис гривень Тоді додаткова заробітна платня становить 0,1*9 = 0,9 тис грн. тобто 900 грн., тобто Сз складає 9900 грн. Річний фонд становить 900*12 = 10 800 грн

Розрахуємо вартість електроенергії, оскільки в відділі мається дві камери, сигналізація, датчики диму, та магніто-контактні датчики загальна потужність них становить 0,7 кВт/годину.

$$С_{ел} = 0,7*8760*2,73 = 16\ 740 \text{ грн } 36 \text{ коп}$$

$С_о$ - витрати на залучення сторонніх організацій для виконання деяких видів обслуговування

$С_{тос}$ – витрати на технічне і адміністративне адміністрування та сервіс

$С_н$ – 18 000 грн,

$С_а$ –9 500 грн – $А_{зпз} + А_{аз} = 0.5*К_{зпз} + 0,5*К_{аз}$

$С_з$ –10 800,

$C_е$ – 16 740.36,

$C_{ос}$ – 10 000 грн, залучення фахівців з монтажу та інсталяції ПЗ

$C_{тос}$ – 2210 грн.

C = 18 000 + 19 250 + 10 800 + 16 740,36 + 10 000 + 2210 = 54 530 грн 36 коп.

Розрахуємо витрати викликані активністю користувача системи інформаційної безпеки:

$$C_{ак} = 54\,530{,}36 * 0{,}46 = 25\,083 \text{ грн } 96 \text{ коп.}$$

3.3 Оцінка можливого збитку від атаки (злому)

Оцінка величини збитку

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

Можливі відвернені збитки можуть визначатися відповідно до створеної при розробці політики безпеки інформації моделі загроз та аналізу ризиків у вартісному вираженні.

Універсальних рецептів визначення можливого збитку від інформаційної атаки на вузол або сегмент корпоративної мережі не існує. У самому загальному виді передумова розрахунку потенційного збитку полягає в тому, що витрати на забезпечення інформаційної безпеки не повинні перевищувати вартість об'єкта, що захищається, або величину збитку, що може виникнути внаслідок атаки на об’єкт, що захищається.

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 – 5 - годин

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин – 12

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин – 8 годин

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць – 9900 грн

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць – 9500 грн

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб. - 1

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб. - 13

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік - 0

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн; - 3000 грн

І – число атакованих вузлів або сегментів корпоративної мережі – 6, оскільки усі комп’ютери пов’язані між собою за допомогою роутерів, тому достатньо вивести із ладу роутер аби вивести одразу декілька вузлів з ладу.

N – середнє число атак на рік - 2

Для розрахунку упущеної вигоди слід використовувати наступну формулу:

$$U = П_п + П_в + V, \qquad (3.11)$$

де $П_п$ – 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.

$$V = \sum E_e(кВ) * C_{ел} * (t_n + t_B + t_{Bn}) \qquad (3.12)$$

Розрахуємо втрати від зниження продуктивності атакованого вузла:

$П_П = 9500*13 * 5/176 = 3508,5$ грн

Розрахуємо витрати на відновлення працездатності вузла або сегменту корпоративної мережі:

$П_в = П_{ви} + П_{пв} + П_{зч}$,

Де:

$П_{ВИ} = 13*9500*8/176 = 5\ 613,63$

$П_{ПВ} = 9900*12/176 = 675$ грн

$V = 800 * 2.73*25 = 54\ 600$ грн

Таким чином $П_в = 5613,63+675+3000 = 6588,63$ грн

З цього можна зробити висновок, що:

$U = 6588,63+3508,5 + 54\ 600 = 64\ 697, 13$ грн.

Підрахуємо збитки які може отримати підприємство внаслідок реалізації загрози:

$$B = \sum_i \sum_n U. \qquad (3.13)$$

$B = 6*2*64\ 697.13 = 646\ 971$ грн 30 коп.

Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C, \quad (3.14)$$

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 - 0,6 од, оскілки відділ головного енергетика є життєво важливим відділом підприємства, але частота атак на підприємство не є значною ;

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

$$E = 646\,971{,}3 * 0{,}6 - 54\,530{,}36 = 592\,440{,}94$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для надання повного аналізу ефективності розробки політики безпеки, а також впровадження її у об’єкті інформаційної діяльності необхідно розрахувати коефіцієнт повернення інвестицій, а також термін окупності капітальних інвестицій.

Для розрахунку коефіцієнту ROSI необхідно знайти відношення, щодо загального ефекту впровадження системи інформаційної безпеки до капітальних інвестицій, що забезпечили цей варіант.

Вважатимемо, що бажаним результатом є значення ROSI >= 1

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.15}$$

ROSI = 592 440,94/ 77 249 = 7,66

Аналізуючи значення ROSI більше бажаного результату, це означає, що впроваджена система інформаційної безпеки не є збитковою і визнається більш економічно вигідною для інвестицій.

Розрахуємо термін окупності системі захисту інформації за формулою:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \quad \text{років.} \tag{3.16}$$

T_o = 1/7,66*12 = 1,6 місяці

Після перевірки окупності запропонованих нами рішень окупність наступить менше ніж за рік.

3.4 Висновки до економічно розділу

У третьому розділі, кваліфікаційної роботи було досліджено доцільність впровадження впровадженої системи захисту інформації на основі коефіцієнту поранення інвестицій, а також відносно швидкої окупності. При одноразових капіталовкладеннях у розмірі 77 249 грн, коефіцієнт окупності є 7,66 (ROSI), що означає окупність розробки політики безпеки вже за 1.6 місяці.
Максимальні витрати при реалізації загрози становлять 646 971 грн 30 коп.

ВИСНОВКИ

У ході проведення аналізу кібератак на території України було помічено значну тенденцію, щодо атак саме на підприємства пов’язані з промисловим виробництвом, дослідивши докладніше було виявлено, що ціллю ставали саме енерготранспортуючі вузли цих підприємств.

Тому на основі нормативно правової бази було розроблено основи для створення комплексу системи захисту інформації для підприємства ООО «Дніпропресс Сталь», а саме для відділу головного енергетика.

Зробивши аналіз об’єкту інформаційної діяльності (далі - ОІД), відділ головного енергетика, було виявлено ряд загроз інформаційній безпеці антропогенного характеру.

Як результат було розроблено ключові політики безпеки котрі, дозволяють зменшити ризик, реалізації загроз на підприємстві.

Після проведення економічних розрахунків із доцільності використання політик, було виявлено, що впровадження політик є економічно вигідним підприємству.

Слідуючи з цього для подальшого підтримання, оновлення та покращення інформаційного середовища підприємства було призначено у кожному відділі відповідального за інформаційну безпеку, на території ОІД. Відповідальним за інформаційну безпеку було назначено відділ комунікацій.

СПИСОК ЛІТЕРАТУРИ

1 NotPetya | Council on Foreign Relations INteractives [Електронний ресурс] // Cyber Operations Tracker. – 2018. – Режим доступу до ресурсу: https://www.cfr.org/interactive/cyber-operations/notpetya.

2 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ МЕТАЛУРГІЙНОЇ ГАЛУЗІ УКРАЇНИ: ФІНАНСОВІ ПОКАЗНИКИ РОЗВИТКУ, ЕКСПОРТ-ІМПОРТ ПРОДУКЦІЇ [Електронний ресурс] // НУ «Львівська політехніка». – 2016. – Режим доступу до ресурсу: http://ird.gov.ua/sep/sep20163(119)/sep20163(119)_102_FurdychkoLYe,SkvarkoYV.pdf

3 Історія підприємства ТОВ"Дніпропресс Сталь" [Електронний ресурс] // Web сторінка ТОВ "Дніпропресс Сталь" – Режим доступу до ресурсу: https://dps.com.ua/about/history/.

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

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

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

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

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

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

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

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

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

13 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).

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

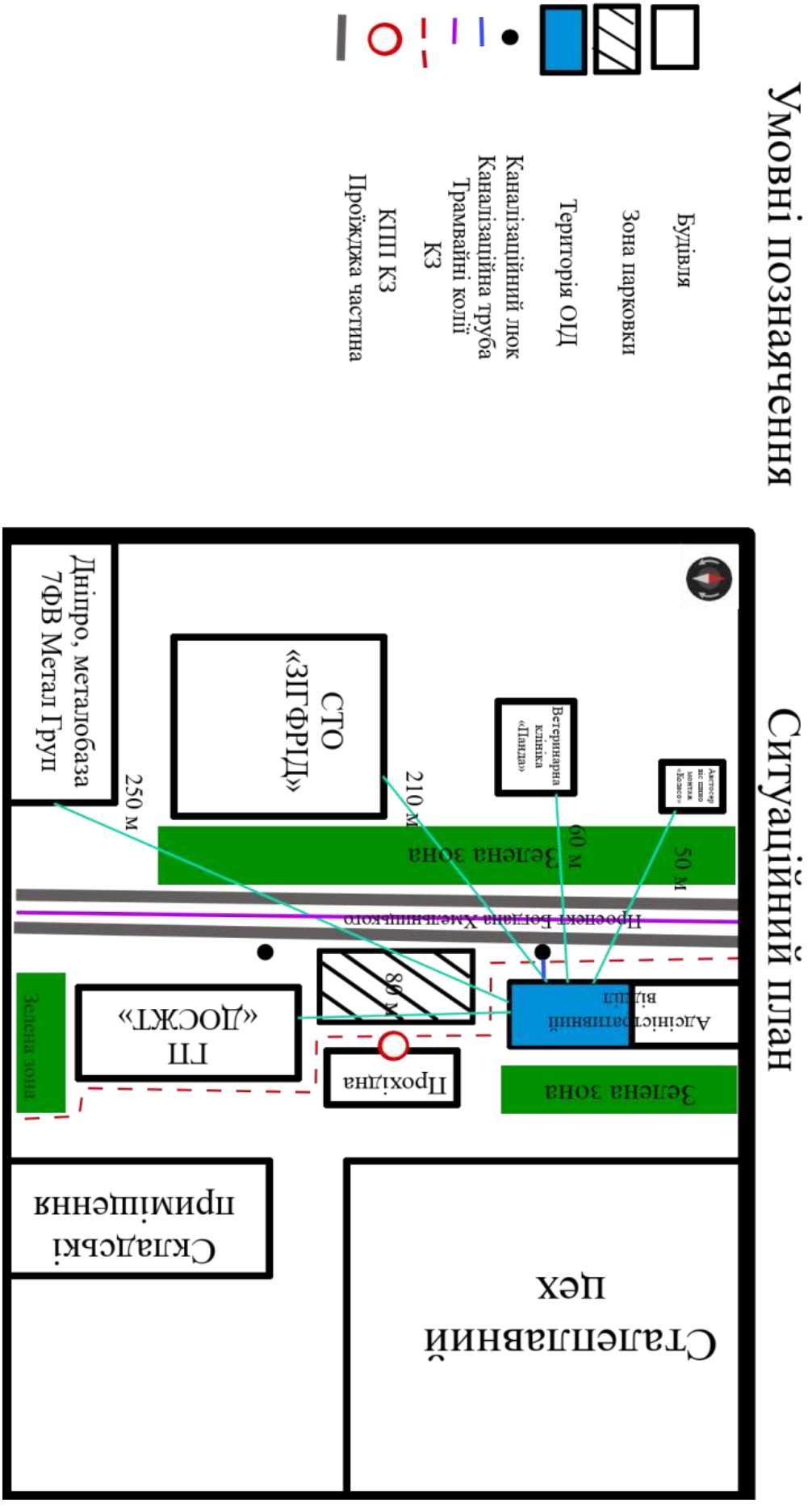
№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	8	
6	А4	Спеціальна частина	59	
7	А4	Економічна частина	11	
8	А4	Висновки	1	
9	А4	Список літератури	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	4	
14	А4	Додаток Ґ	2	
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

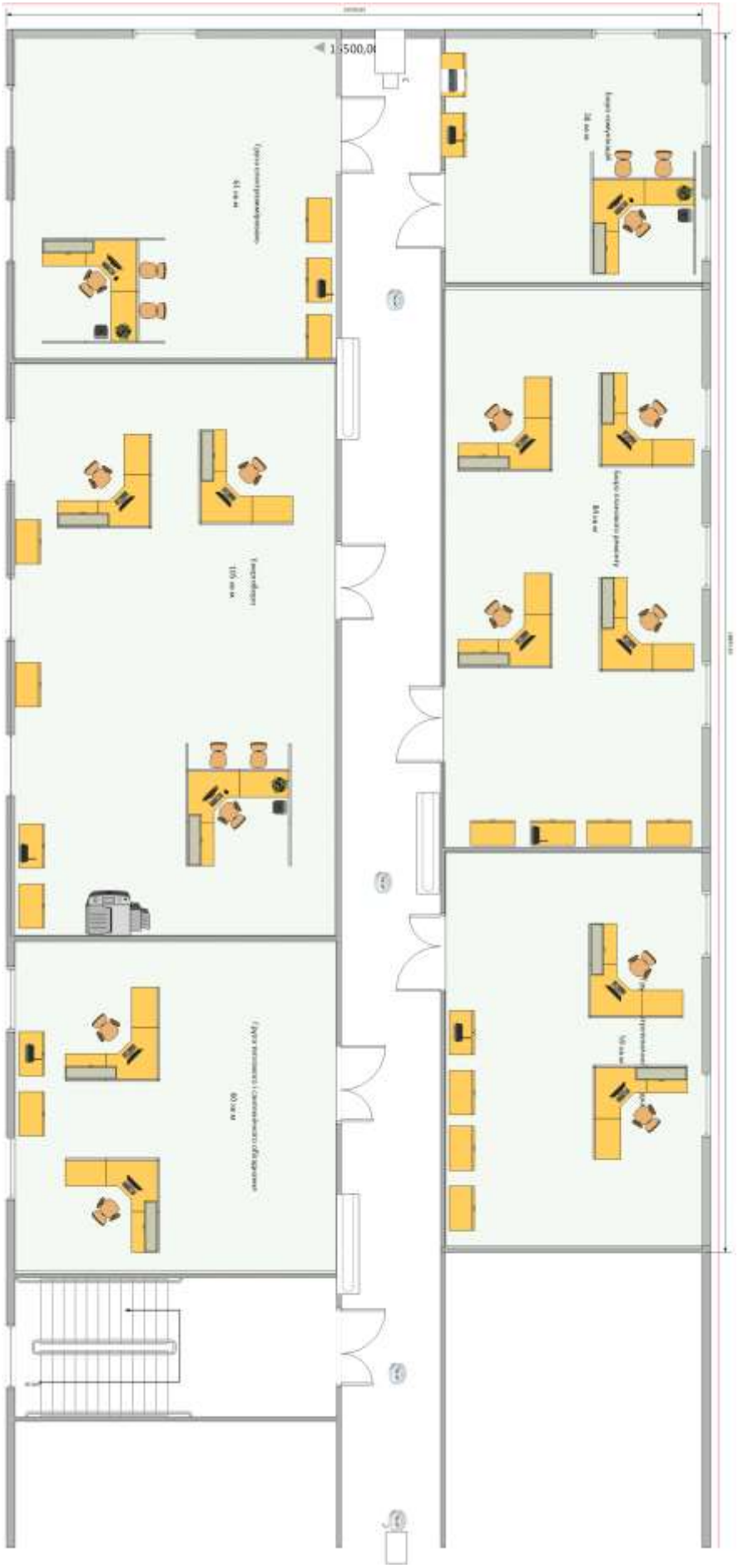
Palii V.V.Ubit-15-1.docx

Palii V.V.Ubit-15-1.pptx

ДОДАТОК В. СИТУАЦІЙНИЙ ПЛАН ОІД

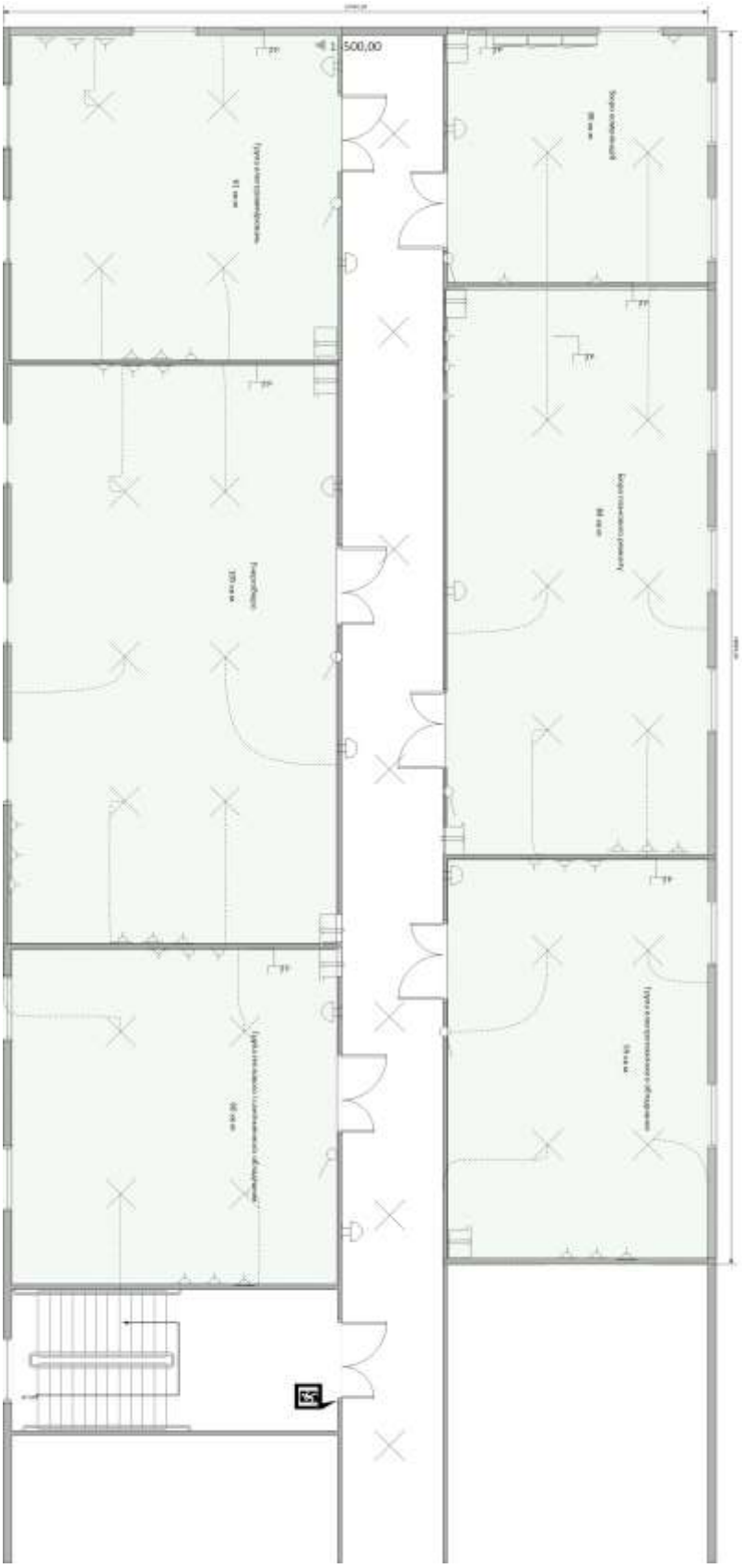


ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ПРИМІЩЕННЯ ОІД



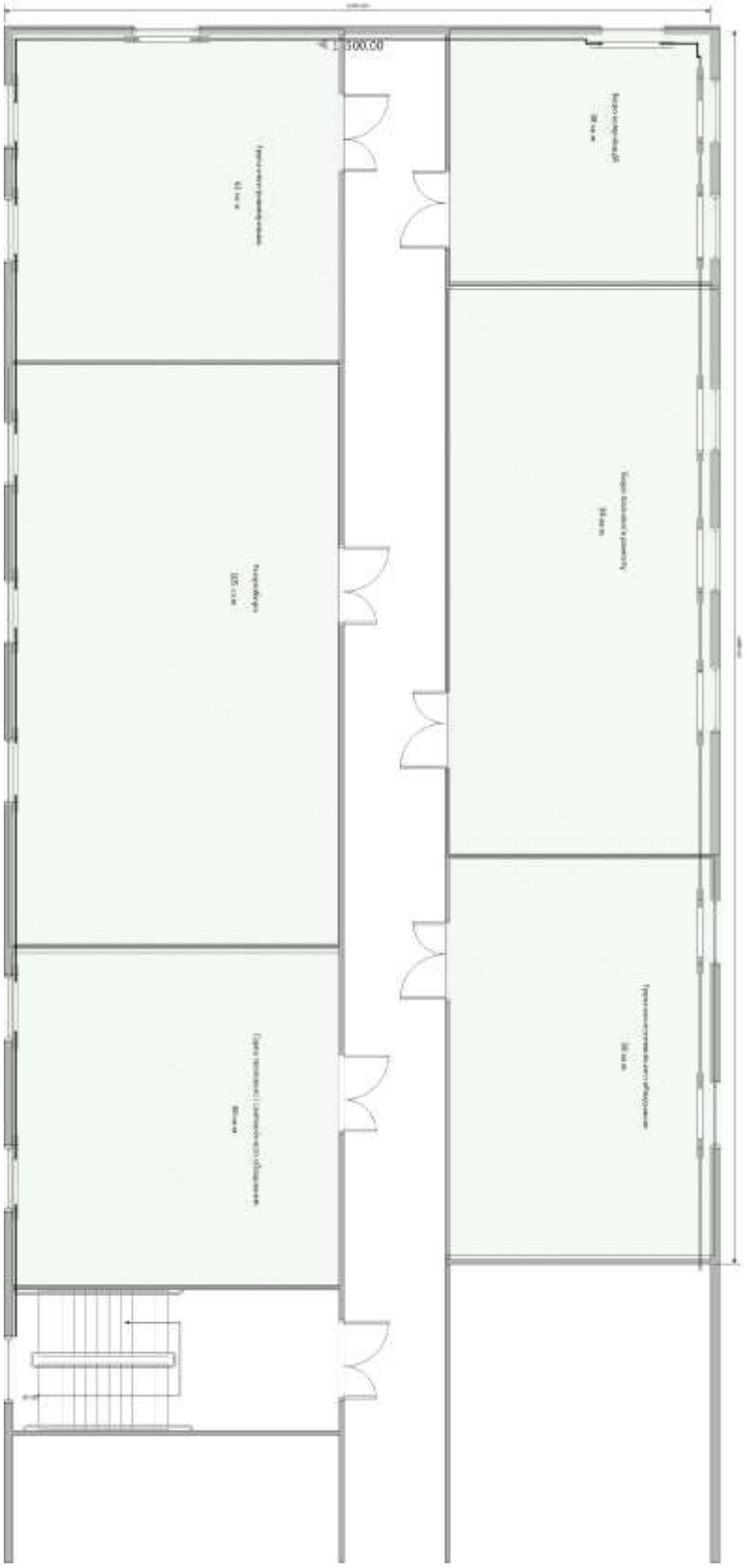
ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ПРИМІЩЕННЯ ОІД

СХЕМА ЕЛЕКТРО З’ЄДНАНЬ



ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ПРИМІЩЕННЯ ОІД

СХЕМА З’ЄДНАННЯ ОПАЛЕННЯ



ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ПРИМІЩЕННЯ ОІД

УМОВНІ ПОЗНАЧЕННЯ

ДОДАТОК Ґ. КРИТЕРІЇ ПРОФЛІЮ ЗАХИЩЕНОСТІ, ЩО РЕАЛІЗУЮТЬСЯ

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 можна безпечним чином повернути КС до нормального функціонування. Виконується автоматично системними засобами до моменту останнього оновлення.

НР-2. Захищений журнал	Виконується, так як для доступу до журналу треба мати права адміністратор, щоб потрапити до реєстру.
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.

ДОДАТОК Д. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Е. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

На кваліфікаційну роботу студента групи УБіт-15-1 Палія В.В.

на тему: «Розробка політики безпеки інформаційно-телекомунікаційної системи ТОВ «Дніпропресс Сталь»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 102 сторінках, та містить ., 5 рисунків, 24 таблиці, 7 додатків, 13 джерел.

Мета кваліфікаційної роботи є актуальною, оскільки спрямована зниження ризиків витоку інформації шляхом розробки правил політики безпеки.

При виконанні кваліфікаційної роботи автор роботи продемонстрував добрий рівень теоретичних і практичних навичок. На основі проведення акту обстеження об’єкту інформаційної діяльності було сформовано задачі, вирішенню яких присвячено спеціальний розділ. У ньому було розроблено складові політики безпеки, на основі аналізу вразливостей та загроз

Практична цінність кваліфікаційної роботи полягає в розробці інструкцій, які дозволяють враховуючи специфіку досліджуваного підприємства знизити вірогідність витоку інформації.

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

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

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

Керівник кваліфікаційного проекту,

Доктор технічних наук, доцент **Герасіна О.В.**

Керівник спеціального розділу,

ст. викл. Кафедри БІТ **Галушко С.О.**

РЕЦЕНЗІЯ

На кваліфікаційну роботу студента групи УБіт-15-1 Палія В.В.
на тему: «Розробка політики безпеки інформаційно-телекомунікаційної системи ТОВ «Дніпропресс Сталь»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 102 сторінках, та містить ., 5 рисунків, 24 таблиці, 7 додатків, 13 джерел.

Актуальність підвищення рівня захищеності інформації, що циркулює інформаційно-телекомунікаційній системі відділу головного енергетика ТОВ «Дніпропресс Сталь».

В роботі, на основі проведення акту обстеження інформаційно-телекомунікаційної системи відділу, поставлено задачі, вирішенню яких присвячено розділ 2.

Розроблені елементи політики безпеки для інформаційно-телекомунікаційної системи є ефективними.

Практична цінність кваліфікаційної роботи полягає в знижені можливості реалізації витоку інформації за рахунок імплементації елементів політики безпеки.

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

Рецензент