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 *Гуні Владислава Олеговича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		Рейтинговою	інституційною	
кваліфікаційної роботи	доц. Галушко О. М.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро

2021

ЗАТВЕРДЖЕНО:

завідувач кафедри

безпеки інформації та телекомунікацій

_____ д.т.н., проф. Корнієнко В.І.

« » 20 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Гуні Владиславу Олеговичу* **академічної групи** *125-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи*

Затверджено наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Виконати аналіз нормативно-правової бази в сфері захисту інформації, визначити актуальність проблеми захисту інформації в ІТС, визначити постановку задачі на розробку основних елементів КСЗІ для ОІД.	20.05.2021
Розділ 2	Обстежити ОІД, проаналізувати середовища функціонування, проаналізувати ризики, розробити основні елементи КСЗІ.	30.05.2021
Розділ 3	Обґрунтувати економічну доцільність впровадження політики безпеки, розрахувати витрати та ефект впровадження політики безпеки.	07.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 11.01.2021

Дата подання до екзаменаційної комісії: 10.06.2021

Прийнято до виконання: Гуня В.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 64 с., 8 рис., 16 табл., 6 додатків, 15 джерел.

Об'єктом дослідження є відділ бухгалтерії дитячо-юнацької спортивної школи.

Предметом дослідження є інформаційно-телекомунікаційна система відділу бухгалтерії.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи.

Перший розділ кваліфікаційної роботи описує стан питання, аналізуються основні нормативно-правова база. Також у першому розділі кваліфікаційної роботи сформульована постановка задачі кваліфікаційної роботи.

У другому розділі було описано: типове підприємство, його організаційна структура; обчислювальну систему. Було проаналізовано інформацію, що оброблюється на ІТС. За результатами було складено модель порушника загроз. Також в цьому розділі кваліфікаційної роботи розглянуто необхідність розробки комплексної системи захисту інформації, стан забезпечення безпеки інформації. Окрім цього, у другому розділі наведено загальні відомості про об'єкт інформаційної діяльності. Проведено обстеження об'єкту інформаційної діяльності та виконано категоріювання об'єкта інформаційної діяльності, обрано профіль захищеності. З метою реалізаці вимог до захисту інформації були запропоновані програмно-апаратні та організаційні методи щодо захисту інформації.

У третьому розділі було розраховано витрати на створення комплексу засобів захисту та щорічні експлуатаційні витрати на його підтримку. Також було доведено економічну доцільність створення комплексної системи захисту інформації.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОСЛУГИ БЕЗПЕКИ, ОПЕРАЦІЙНІ СИСТЕМИ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ

РЕФЕРАТ

Пояснительная записка: 64 стр., 8 рис., 16 табл., 6 прил., 15 источников.

Объектом исследования является отдел бухгалтерии детско-юношеской спортивной школы.

Предметом исследования является информационно-телекоммуникационная система отдела бухгалтерии.

Целью квалификационной работы является разработка комплексной системы защиты информации информационно-телекоммуникационной системы отдела бухгалтерии детско-юношеской спортивной школы.

Первый раздел квалификационной работы описывает состояние вопроса, анализируются основные нормативно-правовая база. Также в первой главе квалификационной работы сформулирована постановка задачи квалификационной работы.

Во втором разделе описано: типичное предприятие, его организационная структура. Было проанализировано информацию, которая обрабатывается на ИТС. По результатам был составлен модель нарушителя угроз. Также в этом разделе квалификационной работы рассмотрена необходимость разработки комплексной системы защиты информации. Кроме этого, во второй главе приведены общие сведения об объекте информационной деятельности. Проведено обследование объекта информационной деятельности и выполнено категорирование объекта информационной деятельности., выбран профиль защищенности. Были предложены программно-аппаратные и организационные методы по защите информации.

В третьем разделе было рассчитано затраты на создание комплекса средств защиты и ежегодные эксплуатационные расходы на его поддержку. Также было доказано экономическую целесообразность создания комплексной системы защиты информации.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОПЕРАЦИОННЫЕ СИСТЕМЫ, МОДЕЛЬ НАРУШИТЕЛЯ, МОДЕЛЬ УГРОЗ

ABSTRACT

Explanatory note: _64_ p., _8_ fig., _16_ tab., _6_ additions, _15_ sources.

The object of the study is the accounting department of the children's and youth sports school.

The subject of the study is the information and telecommunications system of the accounting department.

The purpose of the qualification work is to develop a comprehensive information security system of information and telecommunications system of accounting department of children's and youth sports school.

The first section of the qualification work describes the status of the issue, analyzes the main regulatory framework. Also in the first chapter of the qualification work formulates the statement of the problem of qualification work.

The second section describes a typical enterprise, its organizational structure, computing system. The information that is processed on the ITS was analyzed. Based on the results, a model of a threat actor was compiled. Also in this section of the qualification work, the need to develop a comprehensive information security system and the state of information security have been considered. In addition, the second chapter provides general information about the object of information activities. A survey of the object of information activity was carried out and a categorization of the object of information activity was performed. The software-hardware and organizational methods of information protection for the purpose of of realization of requirements to information protection were offered.

In the third section the expenses for creation of complex of protection means and annual operational expenses for its support were calculated. It was also proved economic feasibility of creating an integrated information protection system.

Practical value of the project is to increase the level of information security in information processing in automated systems.

INTEGRATED INFORMATION SECURITY SYSTEM, OPERATING SYSTEMS, INTRUDER MODEL, THREAT MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ - державний стандарт України;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КЗЗ – комплекс засобів захисту;

ІТ - інформаційні технології;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ІТС – інформаційно-телекомунікаційна система;

КЗ– контрольована зона;

ОС - операційна система;

КЗЗ - комплекс засобів захисту;

ВП - внутрішній порушник;

ДТЗ – допоміжні технічні засоби;

ТЗІ – технічний захист інформації;

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації);

GDPR - General Data Protection Regulation (Загальний регламент про захист даних);

НД ТЗІ – нормативний документ із технічного захисту інформації

ОС – обчислювальна система

КСЗІ – комплексна система захисту інформації.

ЗМІСТ

ВСТУП

У сучасному світі процес інформатизації охоплює більшість сфер людської діяльності: соціальну, економічну, освітні, тощо. Інформація стрімко набуває значимості, і це пов’язано з розвитком технологій.

Сьогодні, всі основні етапи покращення роботи бюджетних установ припадає на комп’ютерні системи. Але для безпечного функціонування підприємства потрібно забезпечувати безпеку інформації. За оцінками експертів, за швидкістю та об’ємами забезпечення безпеки інформації Україна, маючи для цього великий потенціал та досвідчених спеціалістів, демонструє порівняно не достатньо гарні результати порівняно з країнами Європи. Також, на даному етапі, кількість викликів пов'язаних з модернізацією системи кібербезпеки та потребами у модернізації цифрової економіки та суспільства, не зменшується. В бюджетних установах України відчувається дефіцит відповідного забезпечення, особливо на тлі розвинених країн. Нині держава має чинний закон «Про основні засади забезпечення кібербезпеки України», та стратегію кібербезпеки України на 2021 рік.

Сьогодні в кожній інформаційній системі циркулює інформація, розголошення якої призведе до збитків. Тому створення заходів захисту інформації є одним з найбільш актуальних питань.

Захист інформації — це певна діяльність яка направлена на запобігання та унеможливлення витоку інформації, розкрадання інформації у цілях збуту, втрати важливої інформації, модифікації (підробки) інформації, несанкціонованих і ненавмисних впливів на захищену інформацію.

Досить тривалий час методи захисту інформації розроблялися лише державними органами влади, і впровадження методів захисту інформації розглядалось тільки як виключне право органів влади.

Для запобігання витоку інформації під час її обробки в автоматизованій системі використовують комплекси засобів захисту та операційні системи з засобами захисту. Комплекс засобів захисту забезпечує реалізацію політики безпеки, що регламентує порядок захисту інформації.

Об’єктом дослідження є відділ бухгалтерії дитячо-юнацької спортивної школи.

Предметом дослідження є інформаційно-телекомунікаційна система відділу бухгалтерії.

Метою кваліфікаційної роботи є розробка комплексної-системи захисту інформації інформаційно-комунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи.

Так як бюджетні установи нашої країни не мають досить налагодженої комплексної-системи захисту інформації, що в свою чергу становить високу ймовірність атак зловмисників. Як наслідок, конфіденційна інформація, що обробляється в ІТС є недостатньо захищеною. Через це кваліфікаційна робота є актуальною.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

В кожній інформаційній системі (ІС) циркулює інформація, розголошення якої може спричинити значні збитки власнику інформації або особі, до якої ця інформація відноситься. Інформація, яка обробляється в автоматизованій системі (АС), що являє собою організаційно-технічну систему – поєднання обчислювальної системи (ОС), фізичного середовища, персоналу та оброблюваної інформації.

У 2020 році в Україні зафіксували близько 1 мільйона випадків кіберінцидентів. Найпоширеніші з кіберінцидентів - мережеві атаки рівня, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення [1].

Офіційно підтверджено, що зловмисники проводили дії незаконного характеру, що перешкоджало роботі бюджетних установ, бухгалтерських операцій, системі звітностей.

Темпи кіберзлочинності зростають та на жаль, випереджають розвиток кіберіндустрії в Україні. Кількість кібератак в Україні збільшується з кожним роком.

В цьому році менше бюджетних організацій виявляють порушення або атаки, ніж в 2020 році, Це може бути результатом зниження активності підприємств під час пандемії, що могло ненавмисно зробити деякі підприємства тимчасово менш помітними для зловмисників в цьому році.

Однак інші кількісні та якісні дані, отримані в ході дослідження, свідчать про те, що рівень ризику по COVID-19 потенційно вище, ніж будь-коли, і що бюджетним організаціям складніше застосовувати заходи кібербезпеки під час пандемії. Наприклад, в даний час менше бюджетних організацій розгортають засоби моніторингу безпеки або здійснюють моніторинг користувачів в будь-якій формі. Таким чином, таке скорочення серед підприємств, можливо, говорить про те, що вони просто менше, ніж раніше, обізнані про порушення і атаках, з якими стикаються їх співробітники.

Positive Technologies [2] представила звіт з актуальних кіберзагрозам за IV квартал 2020 року. У порівнянні з попереднім кварталом кількість інцидентів зросло на 3,1%. Зберігається тенденція до збільшення частки хакінгу в атаках на організації: частка цього методу в IV кварталі збільшилася на 6 процентних пунктів і становить 36%. В атаках на приватних осіб, навпаки, відзначено різкий сплеск застосування технік соціальної інженерії: їх частка зросла з 67% в III кварталі до 86% в четвертому. Частка шифрувальників серед усіх атак з використанням шкідливого ПО склала 56%.

Ці цифри поступово змінюються з плином часу - частка тих, хто відчуває негативні наслідки або вплив у 2021 році, значно нижче, ніж в 2019 і попередніх роках. Це не пов'язано з тим, що порушення або атаки стали відбуватися рідше - в цьому році помітних змін в їх частоті не відбулося. Навпаки, частково це може бути пов'язано з тим, що після введення в 2018 році Загального регламенту захисту даних (GDPR) все більше організацій впроваджують базові заходи кібербезпеки.

Бюджетні установи в Україні – це одна з найважливіших баз у сфері електронного документообігу. Для забезпечення нормальної працездатності таких бюджетних установ використовують велику кількість одиниць техніки. В залежності від розмірів окремих підприємств, кількість одиниць техніки може варіюватися від 5 до 50+ одиниць техніки.

Тому особливу важливість відіграє правильно впроваджена комплексна система захисту інформації для кожного з підприємств.

При створенні комплексної системи захисту інформації ураховують розміри підприємства, фінансовий стан підприємства, стан інформаційної безпеки підприємства. При створенні інформаційної безпеки та її впровадженні, слід дотримуватися головних критеріїв: системність, комплексність, адекватність, відкритість алгоритму, простота у реалізації цієї безпеки на самому підприємстві.

Механізми комплексної системи захисту інформації повинні бути простими та зрозумілими, механізми не повинні базуватися тільки на загальних принципах розподілення доступу і не повинні вимагати особливих навичок від співробітників цього підприємства, не повинні виникати додаткові витрати при виконанні робіт на

реалізацію політики інформаційної безпеки, а також, не повинні ставити за мету виконувати співробітникам підприємства незрозумілих та/або малознайомих їм операцій.

Серед основних задач захисту інформації в бюджетних установах України є задача захисту персональних даних співробітників, захисту персональних даних підприємств які таким чи іншим чином мають зв'язок з таким установами, захисту інформації з обмеженим доступом.

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Забезпечення захисту інформації базується на нормативно-правових актах держави

Розроблення комплексної системи захисту інформації базується на вимогах чинного законодавства України, а також на основі нормативного-правових документів.

В Законі України «Про Інформацію» визначає інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі.

Згідно зі статтею 1 Закону України «Про Інформацію», інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У Законі України «Про Інформацію» докладно описується інформація; види інформації, серед яких слід виділити інформацію з обмеженим доступом.

Згідно зі статтею 8 Закону України "Про захист інформації в ІТС", Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності, який акредитовано:

- національним органом України з акредитації;
- чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов:

1. Підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

2. Використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

3. Жоден з елементів системи не може бути розташований на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України "Про санкції", та на територіях держав, які входять до митних союзів з такими державами;

4. виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Згідно зі статтею 9 Закону України "Про захист інформації в ІТС", відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

В НД ТЗІ 1.1-003-99 розглядається термінологія та визначення понять в 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.

Для кожного поняття встановлено один термін. Застосування синонімів терміну не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. №53);

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". НД ТЗІ призначений для суб'єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов'язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах. Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту інформації впродовж всього життєвого циклу автоматизованих систем в державних органах, на підприємствах, в установах та організаціях усіх форм власності (далі – організаціях).

НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999р.№22).

НД ТЗІ 2.5-004-99 встановлює критерії оцінки захищеності інформації, яка обробляється в комп'ютерних системах від несанкціонованого доступу. Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010

Стандарт ДСТУ ISO/IEC 27001:2015 визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стра-тегічним рішенням для організації. На проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації. Очікують, що всі ці чинники змінюються з часом.

Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. Важливо, щоб система управління інформаційною безпекою була частиною та інтегрувалася в процеси організації та загальну структуру управління, щоб інформаційну безпеку розглядали в процесах розроблення, інформаційних системах і заходах безпеки. Очікують, що впровадження сис-теми управління інформаційною безпекою буде масштабованим відповідно до потреб організації. Цей стандарт може бути використано зацікавленими внутрішніми та зовнішніми сторонами для оцінки можливості організації відповідати власним вимогам щодо інформаційної безпеки. Послідовність, з якою вимоги надано в цьому стандарті, не відображає їх важливості чи по-слідовності, з якою їх має бути впроваджено. Перелік пунктів понумеровано лише для цілей за-безпечення посилань. ISO/IEC 27000 надає огляд і словник систем управління інформаційною безпекою з посиланням на сімейство стандартів щодо систем управління інформаційною

безпекою (охоп-люючи ISO/IEC 27003, ISO/IEC 27004 та ISO/IEC 27005), з пов'язаними термінами та ви-значеннями.

ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

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

Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям і процесам, зазначеним в ISO / IEC 27001. Ці рекомендації призначені, щоб допомогти реалізувати достатню інформаційну безпеку, засновану на підході менеджменту ризиками.

Для закінченого розуміння цього стандарту важливо знайомство з поняттями, моделями, процесами і термінологією, описаної в ISO/IEC 27001 та ISO/IEC 27002.

Цей міжнародний стандарт є придатним до всіх типів організацій (наприклад, комерційні підприємства, урядові агентства, некомерційні організації), які мають намір здійснювати менеджмент ризиками, які ставлять під загрозу інформаційну безпеку організації.

Стандарти ДСТУ ISO/IEC, що засновані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;

НД ТЗІ 1.6-005-2013 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

Згідно з пунктом 5 НД ТЗІ 1.6-005-2013 об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного

захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи - власника (розпорядника, користувача) об'єкта.

Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.

Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися ІІІ категорія.

Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності.

1.3 Постановка задачі

Основою для необхідності створення комплексної системи захисту інформації є проблеми, які були проаналізовані у пункті 1.1. У якості задачі визначено необхідність розробки комплексної системи захисту інформації.

Для розробки комплексної системи захисту інформації потрібно:

- ознайомитись з особливостями підприємства;
- проаналізувати фізичні характеристики об’єкту;
- проаналізувати інформацію, що обробляється на об'єкті;
- обрати профіль захищеності;

- на основі обраного профілю захищеності надати програмні та апаратні засоби захисту;

Висновки першого розділу

У розділі 1 кваліфікаційної роботи було проаналізовано стан інформаційної безпеки в бюджетних установах України, наведена статистика кібератак. У розділі 1 були перелічені нормативно-правові документи в сфері захисту інформації. Серед документів були більш детально розглянуті документи НД ТЗІ та їх галузі використання, стандарти ISO, закони України, основні положення та накази.

Обґрунтовано потребу у створенні та розробці комплексної системи захисту інформації інформаційно-телекомунікаційної системи дитячо-юнацької спортивної школи.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про типове підприємство

У якості типового об’єкта дослідження є Комунальний позашкільний навчальний заклад "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради, більш детально розглядається бухгалтерський відділ Комунального позашкільного навчального закладу "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради. Всі дані про заклад були частково змінені на вимогу керівництва підприємства в цілях забезпечення анонімності підприємства.

Заклад займається спортивним вихованням дітей, юнаків, та підготовкою їх до змагань. Сьогодні підприємство розташоване у м. Дніпро.

2.2 Обґрунтування необхідності створення КСЗІ

Основним приводом для необхідності створення КСЗІ є нормативно-правові акти, які були розглянуті в Розділі 1. В цьому розділі були вказані вимоги, які встановлюють обмеження для доступу до певних видів інформації. Згідно з актом категоріювання об'єкта (ДОДАТОК А), директором підприємства було прийняте рішення щодо створення КСЗІ та видано наказ "Наказ на створення КСЗІ" (ДОДАТОК Б).

На підприємстві наявна інформація, яка потребує захисту та забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, розглянутих у Розділі 1.

2.3.1 Організаційна структура підприємства

Комунальний позашкільний навчальний заклад "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради налічує близько 40 співробітників. Заклад має одну будівлю на території міста Дніпро, додаткових споруд/будівель на території міста Дніпро та за його межами заклад не має.

Підприємство складається з таких відділів:

- Головне управління;

- Відділ бухгалтерії;
- Відділ художньої гімнастики;
- Відділ футболу;

Так як об’єктом інформаційної діяльності (ОІД) є відділ бухгалтерії, розглянемо його більш детально.

Штат відділу складає 2 співробітників, які мають чітке розподілення обов’язків. Відділ бухгалтерії не має структурних підрозділів. Основні задачі відділу:

- ведення бухгалтерського обліку Комунального позашкільного навчального закладу "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради, та складання звітності;
- відображення у документах достовірної та у повному обсязі інформації про всі операції і результати діяльності, необхідної для оперативного управління бюджетними призначеннями та фінансовими і матеріальними (нематеріальними) ресурсами;
- ведення бухгалтерського обліку відповідно до національних положень (стандартів) бухгалтерського обліку в нормативно-правових актах щодо ведення бухгалтерського обліку, в тому числі з використанням уніфікованої автоматизованої системи бухгалтерського обліку та звітності;
- складення на підставі даних бухгалтерського обліку фінансової та бюджетної звітності, а також державної статистичної, зведеної та іншої звітності в порядку, встановленому законодавством;
- своєчасне та у повному обсязі перерахування податків і зборів (обов'язкових платежів) до відповідних бюджетів;

2.3.2 Аналіз підприємства

У бухгалтерському відділі Комунального позашкільного навчального закладу "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради обробляється інформація з обмеженим доступом: персональні дані співробітників та учнів, трудові договори, інформація про документи підприємства, інформація про стан мережі та інші.

Вся документація підприємства існує у двох видах: паперовому та електронному. Електронний вид документації створюється працівниками підприємства на робочих комп'ютерах з інстальованим програмним забезпеченням. Копії паперових документів здійснюються завдяки: принтерам, ксероксам. Електронні копії документів зберігаються на робочих станціях директора та бухгалтерів.

Класифікація інформації, що обробляється на ОІД та потреби до К, Ц, Д наведено у таблиці 2.1.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступу

Таблиця 2.1 Класифікація інформації, що обробляється на ОІД

Вид інформації	По режиму доступності	По режиму секретності	Вид представлення в ІТС	Потреби до К,Ц,Д			
				К	Ц	Д	
Персональні дані співробітників, їх посадові інструкції	З обмеженим доступом	Персональні дані	Паперовий Електронний	3	2	2	0,4
Персональні дані учнів	З обмеженим доступом	Персональні дані	Паперовий Електронний	3	2	2	0,4
Інформація про діяльність підприємства	Відкрита	Відкрита	Паперовий Електронний	1	2	2	0,15
Інформація про графік роботи підприємства	Відкрита	Відкрита	Паперовий Електронний	1	2	2	0,15

Продовження таблиці 2.1

Вид інформації	По режиму доступності	По режиму секретності	Вид представлення в ІТС	Потреби до К,Ц,Д			
				К	Ц	Д	
Статутні документи підприємства	Відкрита	Відкрита	Паперовий Електронний	1	3	2	0,15
Трудові договори	З обмеженим доступом	Конфіденційна	Паперовий	1	3	2	0,3
Інформація про документи підприємства (Службові записки, накладні, накази, розпорядження)	З обмеженим доступом	Конфіденційна	Паперовий Електронний	3	2	3	0,6
Інформація про фінансову діяльність підприємства	Відкрита	Відкрита	Паперовий Електронний	3	2	2	0,4
Інформація про стан мережі і її компоненті в	З обмеженим доступом	Конфіденційна	Електронний	3	3	2	0,6
Фото/Відео архів	З обмеженим доступом	Конфіденційна	Електронний	3	3	2	0,6

- К1 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків в разі розкриття інформації особам, які не мають допуску до неї;

- К2 - рівень конфіденційності інформації, при якому організація пізнає відчутних збитків в разі розкриття інформації особам, які не мають допуску до неї;
- К3 - рівень конфіденційності інформації, яка може призвести до значних матеріальних втрат у разі розкриття інформації особам, які не мають допуску до неї;
- Ц1 - рівень цілісності інформації, при якому компанія зазнає незначних збитків в разі втрати цілісності інформації;
- Ц2- рівень цілісності інформації, при якому організація відчуває від-чутних збитків в разі втрати цілісності інформації;
- Ц3 - рівень цілісності інформації, яка може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Д1 - рівень доступності інформації, при якому компанія відчуває не-значні збитки в разі втрати доступності інформації;
- Д2 - рівень доступності інформації, при якому організація несе відчутних збитків в разі втрати доступності інформації;
- Д3 - рівень доступності інформації, яка може призвести до значних матеріальних втрат у разі втрати доступності інформації;

2.3.3 Обстеження об’єкту інформаційної діяльності.

Назва підприємства – Комунальний позашкільний навчальний заклад "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради.

Адреса – вулиця Перемоги 3А.

Робочі години з 9:00 до 20:00.

Адреса, суміжні вулиці були змінені на вимогу керівництва закладу.

Масштаб 1:10000

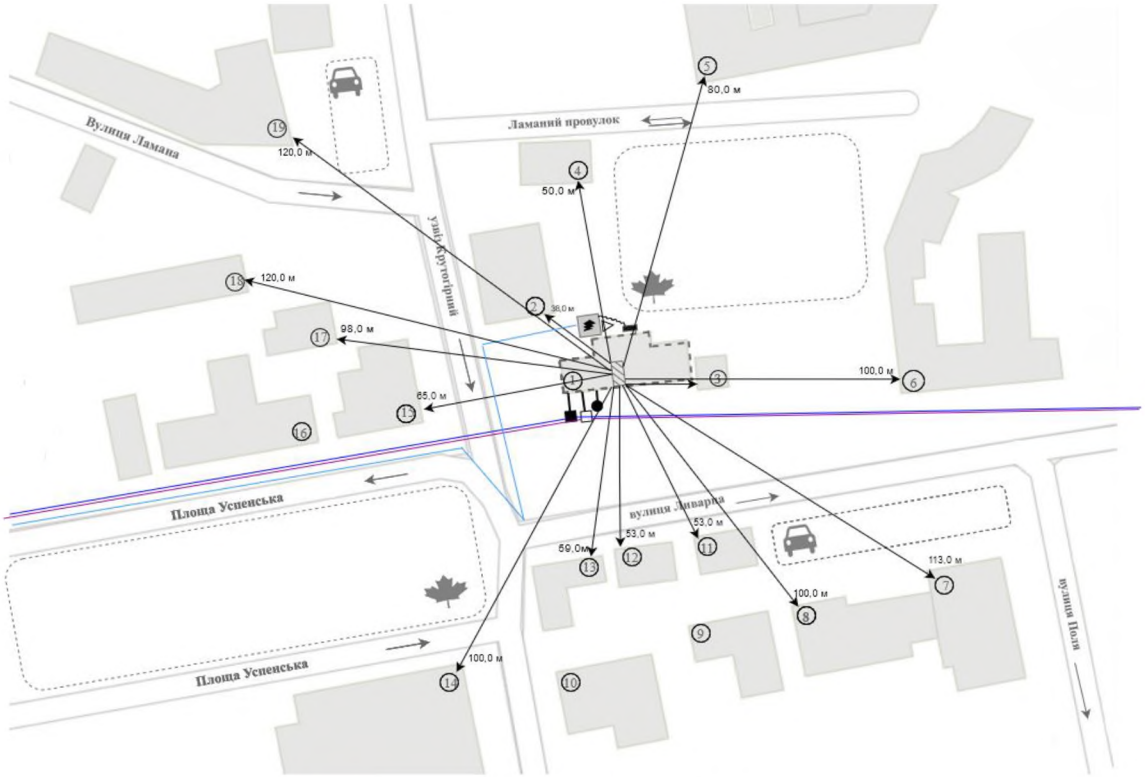
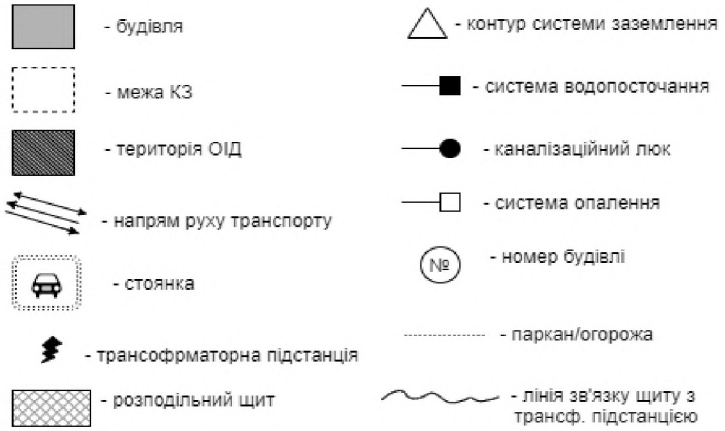


Рисунок 2.1 Ситуаційний план

Умовні позначення:



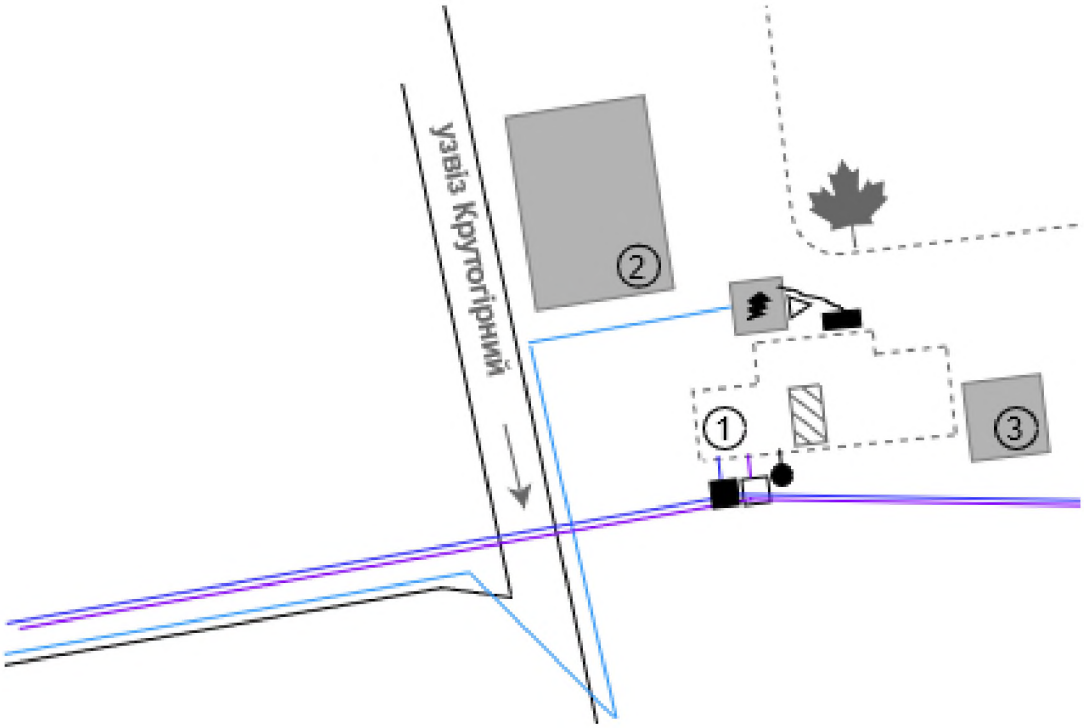
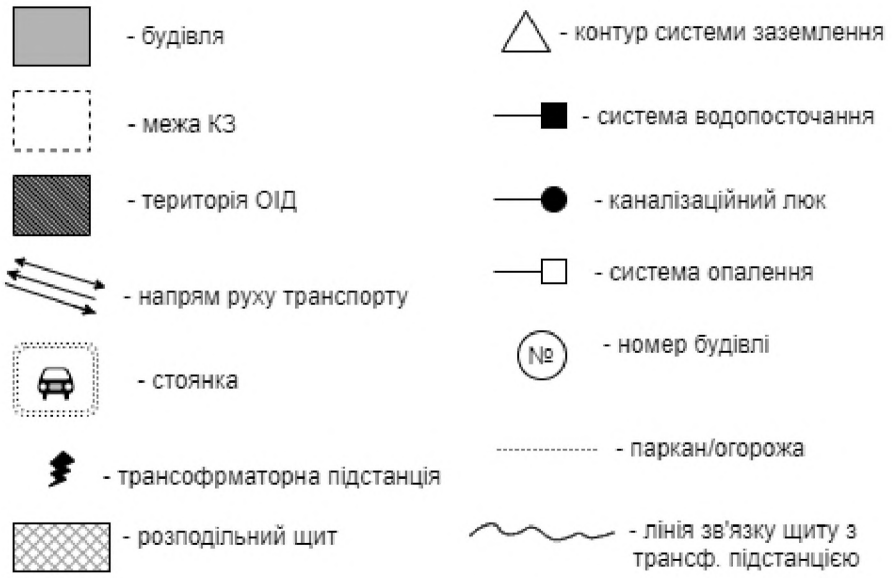


Рисунок 2.1.1 Ситуаційний план. Зовнішні комунікації

Умовні позначення:



Наявність охорони території

На території комплексу діє централізована охорона. Охоронний пункт на першому поверсі біля вхідних дверей. Контролює вхід на територію та переміщення по території.

Перепускний режим

Режим КЗ забезпечується: Територія підприємства – закрита. Вхід на територію підприємства здійснюється через вхідні двері. Вхідні двері (металеві, 55 мм.). Вхід до підприємства контролюється централізованою охороною (цілодобово).

Відомості щодо інформаційної діяльності на ОІД та категорія ОІД:

На об’єкті інформаційної діяльності (ОІД) видом інформаційної діяльності є обробка технічними засобами та озвучення інформації з обмеженим доступом.

Об’єкту встановлена четверта (IV) категорія, на якому обробляється технічними засобами та озвучується інформація з обмеженим доступом, що не становить державної таємниці (Додаток А).

Характеристика ОІД:

Тип Об’єкту Інформаційної Діяльності (ОІД) — Комунальний позашкільний навчальний заклад "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради.

Контрольована зона обмежена межами ОІД.

Ситуаційний план — Рисунок 2.1 Ситуаційний план.

Територія Контрольованої Зони (КЗ) обмежена стіною, яка суміжна з будівлею поруч з Контрольованої Зони (КЗ). Будівля Контрольованої Зони (КЗ) не обмежена парканом. Територія Контрольованої Зони (КЗ) обмежена будівлею, в якій охорона Об’єкту Інформаційної Діяльності покладається на охоронців.

Трансформаторна підстанція розміщена поруч з будівлею підприємства.

Схема (Ситуаційний план Об’єкту Інформаційної Діяльності (ОІД)) — зображено на Рисунок 2.1 Ситуаційний план.

Суміжних будівель немає.

Архітектурно-будівельні особливості ОІД:

Розміри Об'єкту Інформаційної Діяльності: 7х9м. Висота стелі 2,55м. Поверх — 1ий.

Стеля (матеріал — бетон, товщина — 0,45м); підлога (матеріал — бетон+дошки (паркет, товщина — 0,7м); стіни (матеріал — бетон, товщина 0,5м).

Вікна (кількість — 1 шт, матеріал вікна — пластик, розміри — 1,3х1,7м, встановлені решітки на вікно). Вікно виходить на вулицю Перемоги. Сектор прямої видимості — це будівлі № 11, №12, №13.

Характеристика складових ОІД:

Відомості щодо ОТЗ — див. Таблиця 2. Перелік ОТЗ. З Допоміжних Технічних Засобів і Систем зустрічаються мобільні телефони, які знаходяться на території ОІД. Опис Допоміжних Технічних Засобів і Систем надано у: Таблиця 3.Перелік ДТЗС.

Схема розташування ОТЗ та транзитних комунікацій зображено на Рисунок 1.Ситуаційний план.

Схема систем електроживлення зображено на Генеральному плані (Рисунок 3). Місце розташування трансформаторної підстанції відносно межі контрольованої зони зображено на Рисунок 1. Ситуаційний план.

Схема заземлення зображена на Ситуаційному плані Рисунок 2.1 Ситуаційний план. "Заземлення за КЗ. Підключення ДТЗС або інших технічних засобів сторонніх споживачів до заземлення відсутня. Наявність підключення до контуру заземлення ОТЗ відсутня. Розетки та інші ОТЗ і ДТЗС заземленню не підлягають.

Транзитні комунікації, які мають вихід за межі ОІД: система опалення, система каналізації та водопостачання, система електроживлення, Інтернет(комунікація ДТЗС).

Відомості про обладнання, що може впливати на показники захищеності інформації:

- За межі КЗ мають вихід: електроживлення, водопостачання, оптоволоконний кабель Інтернету.
- Система електроживлення проходить до КЗ повітрям, до ОІД проходить внутрішньо. Кабель інтернету також проходить до ОІД через перший поверх. Водопостачання проходить до КЗ через перший поверх. Система опалення проходить внутрішньо, по стіні будівлі через кімнати.
- Виявлені характерні особливості ОІД, що впливають на вибір заходів та засобів ТЗІ: системи водопостачання, каналізації проходять дуже поруч з кімнатами ОІД. відсутність лінії телефонного зв'язку; перший поверх будівлі.

Таблиця 2.2 Характеристика будівель

№	Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
1	Комунальний позашкільний навчальний заклад "Дитячо-юнацька спортивна школа № 2" Дніпровської міської ради	2	вул. Камчатська 3А	-
2	УкрТрейдЗапчасть	1	вул. Камчатська 3	38
3	Будівля	1	вул. Камчатська 3	19
4	Будівля	1	провулок Героїв 5	50
5	Турагентство	10	провулок Ламаний 4	80
6	Будівля	7	вул. Перемоги 9	82
7	Житловий будинок	3	вул. Перемоги 6	113
8	Житловий будинок	10	вул. Перемоги 4	100
9	Житловий будинок	10	вул. Перемоги 2	77
10	Житловий будинок	10	вул. Перемоги 2	87
11	Житловий будинок	10	узвіз Ливарний 12Б	53
12	Житловий будинок	16	вул. Перемоги 2	53

Продовження таблиці 2.2

№	Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
13	Житловий будинок	12	вул. Перемоги 2Б	59
14	Будівля	2	узвіз Ливарний 21А	100
15	Торгівельний центр	2	площа Героїв Крут 11	65
16	Готель	1	площа Героїв Крут 11	88
17	Будівля	1	площа Героїв Крут 11	98
18	Будівля	1	площа Успенська 11И	120
19	Центр сімейного здоров'я та реабілітації Геліос	5	площа Успенська 11И	120

Таблиця 2.3 Комунікаційні системи

Вид комунікації	Характеристика
Система електропостачання	Підключена до трансформаторної підстанції, знаходиться за межами КЗ
Лінія Інтернету	Підключено до ІСП «Фрінет»
Кабелі комп’ютерної мережі	Кабель неекранованої мережі, вита пара
Система сигналізації	Складається з датчиків відкриття (магнітно-контактний датчик)
Система водопостачання	Підключена до мережі міста, знаходиться в межі КЗ
Система опалення	Проходить через будівлю та знаходиться в межах КЗ. Труби опалення зроблені з поліпропіленового матеріалу, що унеможливлює витік інформації по вібро-акустичному каналу
Система каналізації	Підключена до мережі міста, знаходиться в межах КЗ
Система вентиляції	Приточно-витяжна

2.3.4 Опис обчислювальної системи

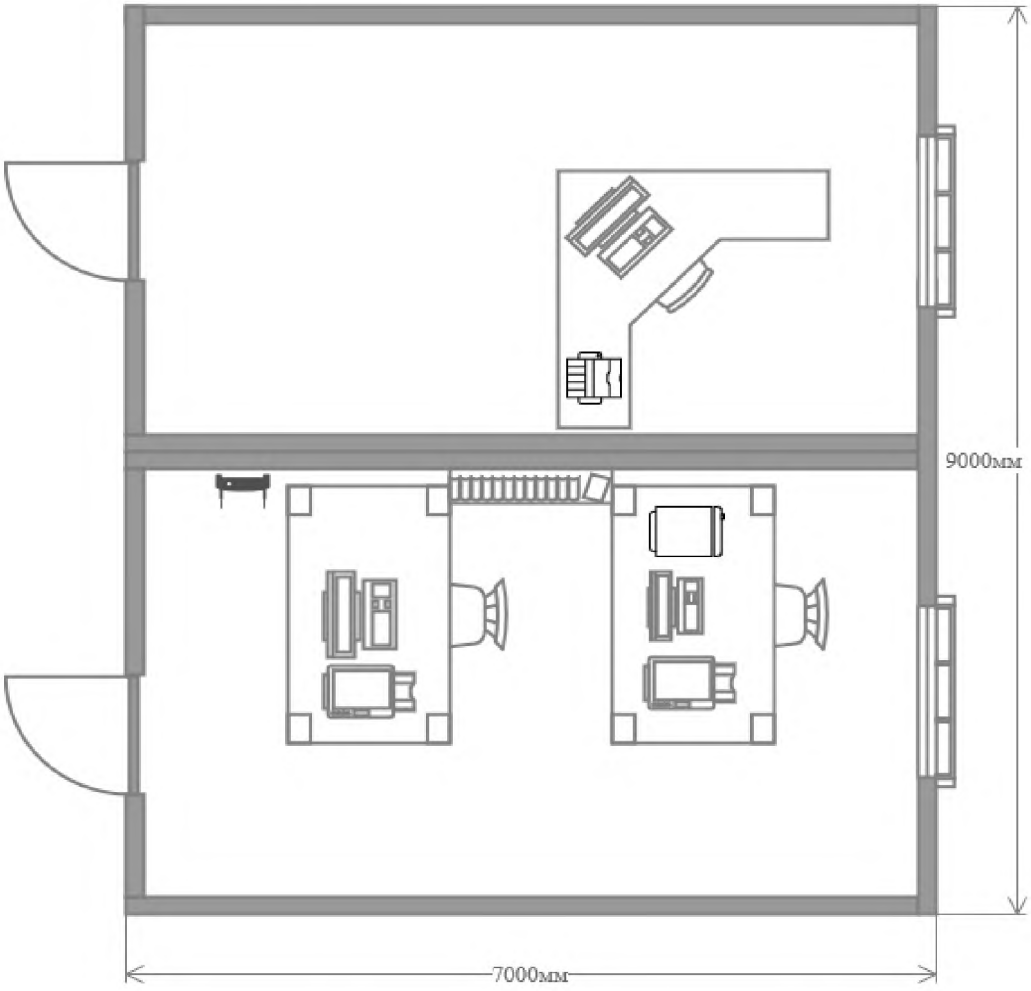


Рисунок 2.3 Генеральний план приміщення ОІД

Умовні позначення:

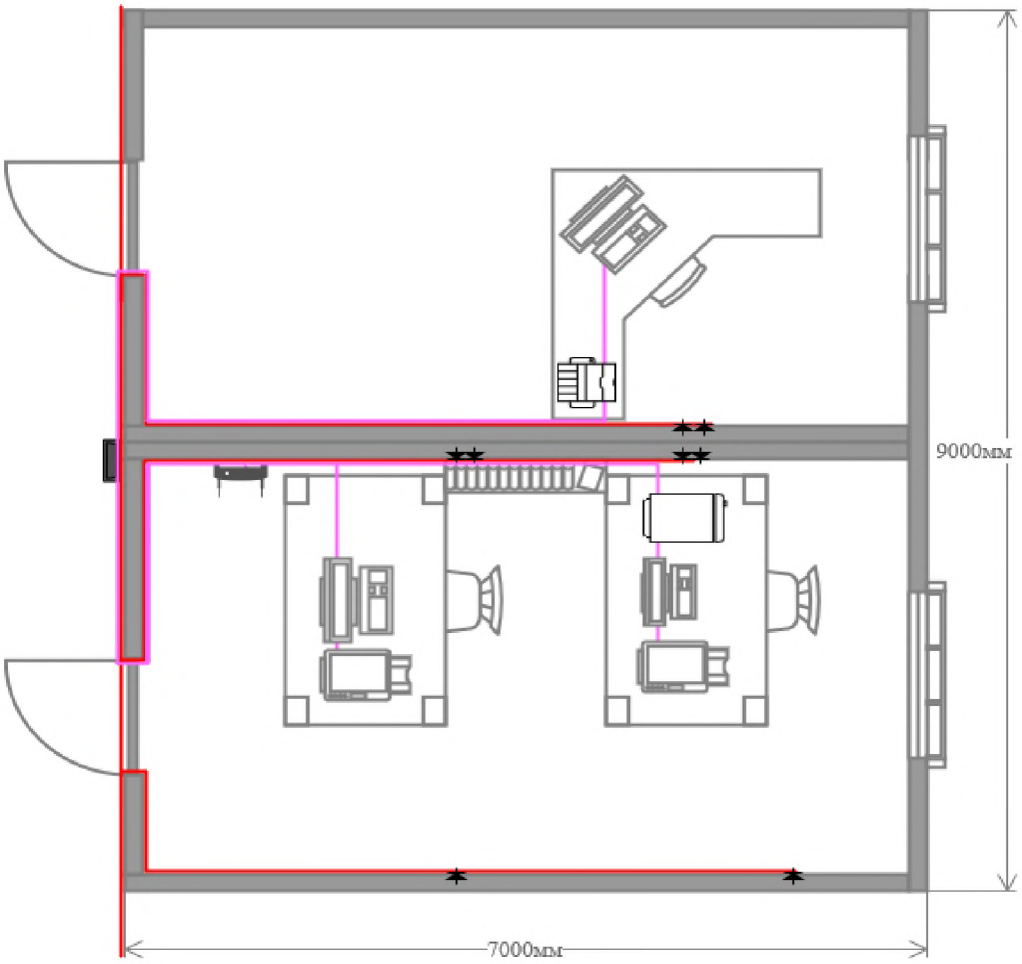


Рисунок 2.4 Генеральний план приміщення ОІД. Лінії систем електропостачання ,комп’ютерних систем

Умовні позначення:

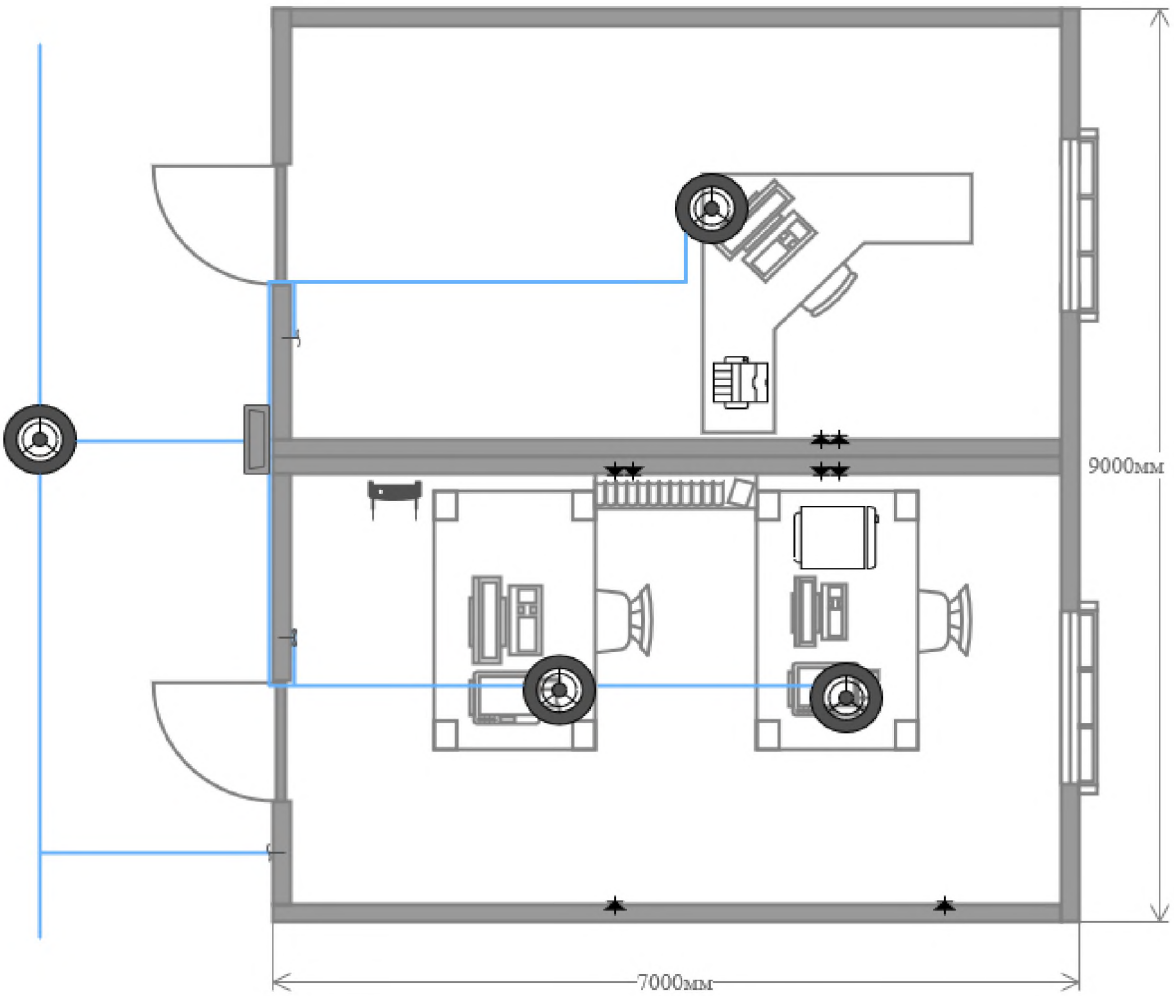
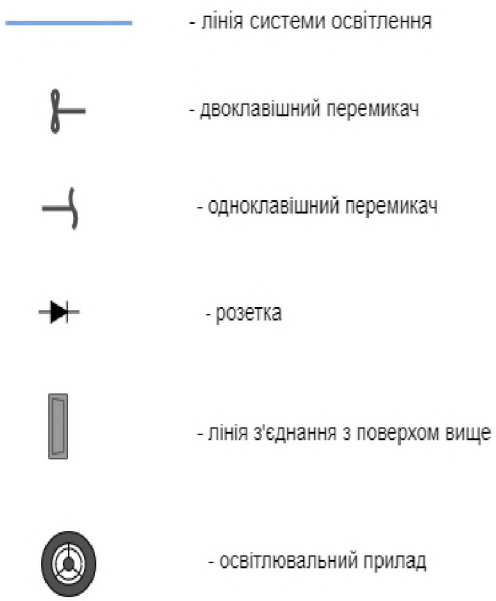


Рисунок 2.5 Генеральний план приміщення ОІД. Лінії освітлення

Умовні позначення:



Таблиця 2.3 Перелік ОТЗ

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі ОІД
1.1	PC монітор	Samsung	D33G461G	84353	У кімнаті, на столі 1	-
1.2	Клавіатура	Logitech	G910 Orion	235925	У кімнаті, на столі 1	-
1.3	Системний блок	Expert	I5400.08.H1.1650.A320	849192	У кімнаті, на столі 1	-
3.1	Принтер	Canon	MG3640S	4522241	У кімнаті, на столі 1	-
5.1	PC монітор	DELL	N541SC1	C1W335R	У кімнаті, на столі 2	-
5.2	Клавіатура	Logitech	C44G461G	509565	У кімнаті, на столі 2	-
5.3	Системний блок	Expert	G910 Orion	01764	У кімнаті, на столі 2	-
6	Принтер	Canon	NC3450S	58434	У кімнаті, на столі 2	-
7	Сканер	Epson	VB2140D	765C1-05Y001-T504E	У кімнаті, на столі 2	-
8	Ксерокс	Canon	NH6520N	769D1-05Y001-P504E	У кімнаті, на столі 2	-

Таблиця 2.4 Перелік ДТЗС

№	Назва	Марка	Модель	Серійний номер	Розміщення
1	Мобільний телефон	Xiaomi	Redmi Note 9	8b7ed678	Переміщується по території ОІД
2	Мобільний телефон	Xiaomi	Redmi 6a	5bc23411	Переміщується по території ОІД

Продовження таблиці 2.4

№	Назва	Марка	Модель	Серійний номер	Розміщення
3	Роутер	TP-Link	TH-TR841NC	124B750102	У кімнаті, на столі
4	Клавіатура 1	A4Tech	KR-83	4711421805964	У кімнаті, на столі
5	Комп'ютерна миша 1	Logitech	B100 USB	4711421805965	У кімнаті, на столі
6	Клавіатура 2	A4Tech KR-83	KR-83	4711421805966	У кімнаті, на столі
7	Комп'ютерна миша 2	Logitech	B100 USB	4711421805967	У кімнаті, на столі

Таблиця 2.4 Встановлене програмне забезпечення

№	Призначення	Назва	Версія	Тип ліцензії
1	ОС	Windows	17763.769	Commercial
2	Браузер	Google Chrome	90.0.4430.93	Commercial
3	Антивірусне ПЗ	Avast	14.4	Commercial
4	ПЗ для роботи з документами	Microsoft Office	2019	Commercial
5	ПЗ для бухгалтерського обліку	Is-Pro	-	Commercial

Таблиця 2.5 Обстеження середовища користувачів

№	Користувач	Посада	Кількість працівників на посаді	Рівень кваліфікації
1	PC-1	Директор	1	Високо кваліфікований робітник
2	PC-2	Головний бухгалтер	1	Високо кваліфікований робітник
3	PC-3	Бухгалтер	1	Кваліфікований робітник
4	-	Системний адміністратор	1	Високо кваліфікований робітник

Продовження таблиці 2.5

№	Користувач	Посада	Кількість працівників на посаді	Рівень кваліфікації
5	-	Робітник	1	Кваліфікований робітник
6	-	Електрик	1	Кваліфікований робітник
7	-	Сантехнік	1	Кваліфікований робітник
8	-	Прибиральниця	1	Не кваліфікований робітник

Обов'язки робітників:

Директор – керівництво закладом, обробка важливих документів, підписання документів.

Головний бухгалтер – обробка інформації, підписання документів, ведення звітності.

Бухгалтер –обробка інформації, підписання документів, ведення звітності.

2.3.4 Опис обчислювальної системи.

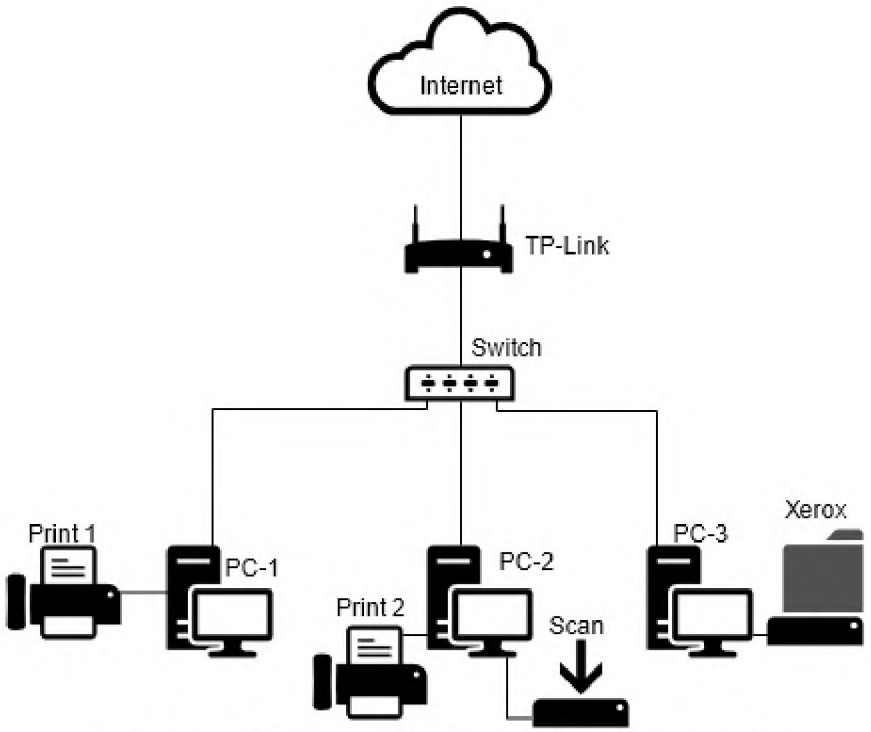


Рисунок 2.1 Схема Інформаційної Системи

Доступ в Інтернет відбувається через оптоволоконний кабель Internet, який заходить на територію ОІД з-за меж КЗ та підключений до комутатора. Усі комп'ютери в мережі мають власні імена. Підключення принтерів - дротове.

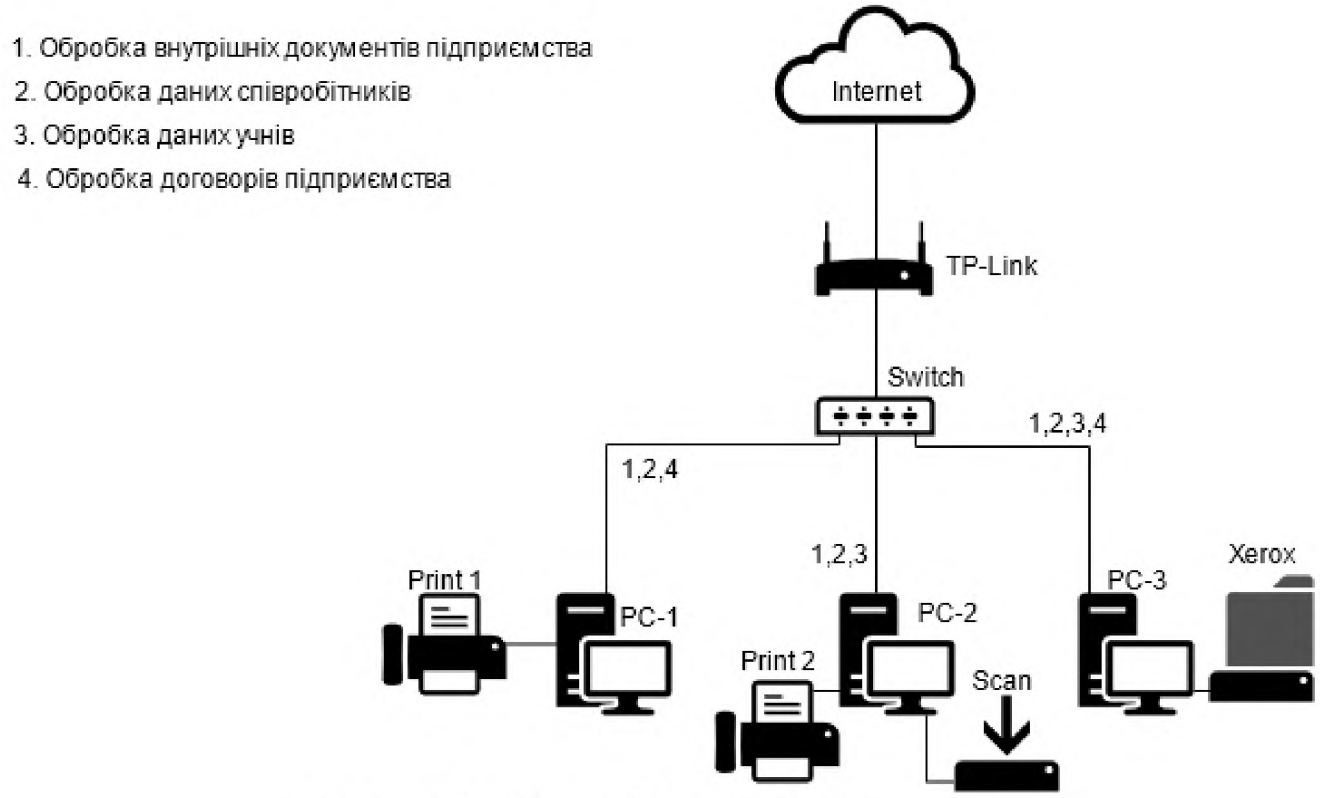


Рисунок 2.2 Схема інформаційних потоків

Здійснення аналізу ризиків (опрацювання моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) та визначення переліку суттєвих загроз є метою етапу формування завдання на створення КСЗІ.

Аналіз критичності загроз інформаційної безпеки розроблений на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2013, IDT) з урахуванням особливостей діяльності підприємства.

2.4 Модель порушника

Порушником вважається особа, яка здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Потенційними порушниками можуть бути: особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов'язаний із забезпеченням функціонування ІТС, особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД.

У таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом та місцем дії. Сукупність цих характеристик визначає профіль порушника.

Таблиця 2.6 Категорії порушників

Позначення	Визначення категорії	Потенціальний рівень загроз
П1	Авторизовані користувачі ІС, яким надано право доступу до ІзОД	5
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління ІС	4
П3	Особи, які забезпечують працездатність ІС	2
П4	Особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІС і потенційно можуть отримати доступ до ІзОД	2
П5	Особи, які знаходяться за межами ІС, мають можливість фізичного підключення до каналів зв'язку та можуть здійснити дії щодо порушення діючої в ІС	5

Таблиця 2.7 Специфікація моделі порушника за місцем дії.

Позначення	Визначення категорії	Потенціальний рівень загроз
Д1	Усередині приміщення, але без доступу до технічних засобів ІС	3
Д2	З робочих місць користувачів та персоналу ІС, а також місць розміщення обладнання ІС, де обробляється інформація, яка підлягає захисту	4
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

Таблиця 2.8 Специфікація моделі порушника за рівнем кваліфікації та обізнаності.

Позначення	Визначення категорії	Потенціальний рівень загроз
К1	Не володіє знаннями та інформацією про порядок функціонування ІС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІС та їх недоліків.	5

Таблиця 2.9 Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз.

Позначення	Визначення категорії	Потенціальний рівень загроз
З1	Має фізичний доступ до компонентів ІС, але не є авторизованим користувачем ІС	2
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІС.	4

Таблиця 2.10 Специфікація моделі порушника за мотивами здійснення порушень.

Позначення	Визначення категорії	Потенціальний рівень загроз
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.11 Специфікація моделі порушника за часом дії.

Позначення	Визначення категорії	Потенціальний рівень загроз
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	3
Ч2	Під час функціонування ІС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	2

1) внутрішній порушник «ПВ» -варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну «Модель внутрішнього порушника політики безпеки інформації»:

Таблиця 2.12 Модель внутрішнього порушника політики безпеки інформації

Посада	Мотив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума заг-роз
Директор	М1	К4	З1	Ч1	Д2	9
Головний бухгалтер	М1	К3	З1	Ч1	Д2	8
Бухгалтер	М1	К2	З1	Ч1	Д2	7

Таблиця 2.13 Модель зовнішнього порушника

Посада	Мотив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума заг-роз
Системний Адміністратор	М1	К4	З1	Ч1	Д2	9
Електрик	М1	К1	З1	Ч1	Д2	6
Сантехнік	М1	К1	З1	Ч1	Д2	6
Прибиральниця	М1	К1	З1	Ч1	Д2	6
Працівник	М1	К2	З1	Ч1	Д1	6
Конкурент	М2	К3	З1	Ч1	Д3	10

Висновок: з останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить Конкурент, Директор та Системний адміністратор. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.5 Модель загроз

Таблиця 2.14 Модель загроз.

Вид загрози	Джерело загрози	Вразливості	Наслідки
Вірусне зараження	Користувач	Відсутність Антивірусних програмних засобів;	К, Ц
Вірусне зараження	Конкурент	Наявність неконтрольованих каналів витоку інформації.	Ц
Помилки	Користувач	Порушення, встановлених політикою безпеки, правил.	К, Ц
Ненавмисні дії користувачів	Користувач	Низький рівень кваліфікації користувачів; Відсутність спеціалістів	К, Ц
Помилки захисту	Користувач	Відсутність політики інформаційної безпеки	К, Ц, Д
Крадіжка	Конкурент	Вразлива система охорони;	Д
Несанкціонований доступ	Конкурент	Вразлива система охорони, порушення правил використання КС, відсутність системи розмежування доступом	К, Ц, Д
Копіювання ІзОД	Конкурент	Відсутність політики безпеки, яка регулює використання дозволених ПЗ	К, Д

Продовження таблиці 2.14

Вид загрози	Джерело загрози	Вразливості	Наслідки
Втручання та/або зміна ПЗ	Конкурент	Відсутність або вразливість системи розмежування прав користувачів; Піратське ПЗ; Недосконаліть системи розмежування доступом.	К, Ц, Д
Порушенні цілісності інформації	Користувач	Відсутність резервного копіювання; Використання піратських ПЗ.	Ц, Д
Повінь	-	Старе приміщення, порушення фундаменту	Ц, Д

Висновок:

1. Ненавмисні помилки користувачів, що призвели до зміни інформації на зовнішніх носіях та жорсткому диску. Це може бути можливим через низьку кваліфікацію працівника, його необізнаність та відсутності знань та навичок.

2. Порушення правил безпеки, що може призвести до пожежі. Це можливо внаслідок неакуратного використання робочого місця(вживання їжі, води, кави, чаю на робочому місці), відсутності вогнегасників, відсутності ознайомлення з технікою безпеки.

3. Порушення цілісності, конфіденційності, доступності інформації співробітниками шляхом установки стороннього ПЗ. Це може бути реалізоване, тому що не має чіткої перевірки за встановленням ПЗ та відсутністю обмеження прав на установку ПЗ.

4. Порушення конфіденційності інформації шляхом копіювання інформації на зовнішні носії. Це можливо через відсутність контролю та обліку носіїв.

5. Порушення доступності інформації шляхом крадіжки носіїв інформації. Це можливо через відсутність контролю та обліку носіїв.

2.6 Профіль захищеності.

На основі проведеного раніше аналізу загроз та вразливостей, обираємо клас системи згідно з НД ТЗІ 2.5-004-99, було обрано клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи» х.КЦД»);

Стандартний функціональний профіль захищеності в КС, що входить до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

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

Таблиця 2.15 Опис послуг профілю захищеності

№	Послуга	Назва послуги	Опис послуги
1	КД-2	Базова довірча конфіденційність	Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування. Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.

Продовження таблиці 2.15

№	Послуга	Назва послуги	Опис послуги
2	КО-1	Повторне використання об’єктів	Реалізація даної послуги забезпечує коректність повторного використання поділюваних об'єктів, гарантуючи, що в разі, якщо розділяється об'єкт виділяється новому користувачеві або процесу, в ньому не міститься інформація, яка залишилася після використання його попереднім користувачем або процесом
3	КВ-1	Конфіденційність при обміні	Реалізація даної послуги забезпечує захист від несанкціонованого ознайомлення зі змістом інформаційних об'єктів (файлів), збережених в каталогах файлової системи захищених логічних дисків, розміщених на знімних і незнімних носіях, в разі вилучення даних носіїв з під контролю коштів захисту (наприклад, в результаті розкрадання).
4	ЦД-1	Довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування.
5	ЦО-1	Відкат	Реалізація даної послуги забезпечує можливість скасування послідовності визначених операцій і повернення (відкату) захищеного об'єкта в попереднє стан. Політика даної послуги поширюється на технологічну інформацію комплексу і на послідовність операцій, що виконуються комплексом при установці захисту на каталог.
6	ЦВ-1	Цілісність при обміні	Ця послуга забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Продовження таблиці 2.15

№	Послуга	Назва послуги	Опис послуги
7	ДР-1	Квоти	Реалізація даної послуги забезпечує запобігання захоплення користувачами надмірного обсягу ресурсів
8	ДВ-1	Ручне відновлення	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС
9	НР-2	Захищений журнал	Ця послуга дозволяє контролювати небезпечні для КС дії. Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності.
10	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. Пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним.

Продовження таблиці 2.15

№	Послуга	Назва послуги	Опис послуги
11	НК-1	Однонаправлений достовірний канал	Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжуються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.
12	НО-2	Розподіл обов'язків адміністраторів	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.
13	НЦ-2	КЗЗ з гарантованою цілісністю	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування
14	НТ-2	Самотестування при старті	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження.

Продовження таблиці 2.15

№	Послуга	Назва послуги	Опис послуги
15	НВ-1	Автентифікація вузла	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжуються на підставі повноти реалізації.

КД-2. Базова довірча конфіденційність. Реалізована. Персональні фото, документи.

КО-1. Повторне використання об’єктів. Реалізована. Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КВ-1. Базова конфіденційність при обміні. Не реалізована.

ЦД-1. Довірча цілісність. Реалізована. Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

ЦО-1. Обмежений відкат. Реалізований. У системі наявна можливість відміни останніх дій у Microsoft Office 2019 Pro Plus.

ЦВ-1: Базова цілісність при обміні. Не реалізована. Електронна пошта.

ДР-1. Квоти. Реалізовано організаційними методами захисту.

ДВ-1. Ручне відновлення. Реалізована. Інтерфейся КС дозволяють виконати ручне
відновлення (параметри відновлення задаються вручну).

НР-2. Захищений журнал. Реалізована. У системі наявна можливість вибору фізичного носія, що використовується для зберігання даних реєстрації.

НИ-2. Одиночна ідентифікація та автентифікація. Реалізована. У системі наявний менеджер паролів, що задовольняє вимоги щодо захисту паролів. Реалізовано організаційними методами захисту.

НК-1. Однонаправлений достовірний канал. Реалізована.

НО-2. Розподіл обов'язків адміністраторів. Не реалізована.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізована. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

НТ-2. Самотестування при старті. Реалізована.

НВ-1. Автентифікація вузла. Реалізована.

Функції КД-2, КВ-1, КО-1, ЦД-1, ЦО-1, ДР-1, НР-2, НИ-2, НК-1, НТ-2, НВ-1 згідно з переліком засобів ТЗІ від 01.03.2021 і експертного висновку №1027, реалізовані операційною системою Windows 10 виробництва компанії Microsoft Corporation, що відповідає коректності їх реалізації згідно НД ТЗІ 2.5-004-99. Операційна система включає в себе можливості щодо реалізації вимог до функцій безпеки.

2.7. Розробка політики безпеки

В ІТС відділу бухгалтерії дитячо-юнацької спортивної школи обробляється інформація з обмеженим доступом. Згідно з цим, було обрано впровадження інформаційного захисту. Головним пріоритетом інформаційного захисту в ІТС є досягнення необхідного рівня захищеності інформації за мінімальних витрат. Для забезпечення максимального захисту, потрібно зосередитися на організаційних методах захисту. Для цього розробляються наступні політики безпеки інформації:

- Політика антивірусного захисту;
- Політика «Чистого столу»;
- Політика резервного копіювання;
- Політика паролів користувачів.

Політика антивірусного захисту

Мета політики: Створення вимог, яких повинні дотримуватися усі комп'ютери, які входять до ІТС відділу бухгалтерії дитячо-юнацької спортивної школи.

Правила політики безпеки мають виконувати усі працівники закладу.

Зміст політики. Загальна частина – встановлює наступні загальні правила, які слід виконувати для вирішення проблемі вірусу:

- завжди підтримуйте корпоративні вимоги, підтримка антивірусного ПЗ є необхідною для корпоративного вузла. Завантажте і підтримуйте поточну версію; завантажте і встановіть модифікації антивірусного програмного забезпечення;
- ніколи не відкривайте будь-які файли, що торкається електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаліть ці повідомлення негайно, потім видаліть їх за допомогою спорожнення вашого сміття;
- видаліть Spam, ланцюг і іншу електронну пошту, які не мають атрибутів вашої компанії;
- ніколи не завантажуйте файли від невідомих або підозрілих джерел;
- уникайте прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам;
- регулярно дублюйте критичні дані і системні конфігурації зберігайте їх в безпечному місці;
- Періодично перевіряйте оновлення антивірусного програмного забезпечення.

Політика «Чистого столу»

Політика "чистого столу" може стати важливим інструментом для забезпечення того, щоб всі конфіденційні / конфіденційні матеріали були видалені з робочого місця кінцевого користувача і замкнені, коли предмети не використовуються або співробітник залишає своє робоче місце. Це одна з головних стратегій, яку слід використовувати при спробі знизити ризик порушення безпеки на робочому місці. Така політика також може підвищити обізнаність співробітників про захист конфіденційної інформації.

Мета цієї політики - встановити мінімальні вимоги для підтримки "чистого столу" - коли конфіденційна / критична інформація про наших співробітників, інтелектуальної власності, наших клієнтів і постачальників зберігається в закритих приміщеннях і поза зоною доступу. Політика "чистого столу" не тільки відповідає

стандартам ISO 27001/17799, але і є частиною стандартних базових заходів контролю конфіденційності.

Зміст політики безпеки:

- Співробітники зобов'язані забезпечити збереження всієї конфіденційної інформації в друкованому або електронному вигляді у своїй робочій зоні в кінці робочого дня і коли очікується, що вони будуть відсутні протягом тривалого часу.
- Робочі місця повинні біля комп'ютеру повинні бути повністю виключені в кінці робочого дня.
- Будь-яка інформація обмеженого доступу повинна бути прибрана зі столу і замкнені в ящику;
- Шафи з файлами, що містять інформацію обмеженого доступу або конфіденційну інформацію, повинні бути закриті і замкнені, коли вони не використовуються або коли їх не відвідують.
- Ключі, що використовуються для доступу до інформації обмеженого доступу або чутливої інформації, не повинні залишатися на столі без нагляду.
- Ноутбуки повинні бути або закриті на блокувальний трос, або прибрані в ящик.
- Паролі можна залишати на липких записках, розміщених на комп'ютері або під ним, також їх можна залишати записаними в доступному місці.
- Роздруківки, що містять інформацію обмеженого доступу або чутливу інформацію, повинні бути негайно вилучені з принтера.
- При утилізації документи обмеженого доступу і / або конфіденційні документи повинні бути знищені в офіційних контейнерах для шредерів або поміщені в закриті конфіденційні контейнери для утилізації.
- Білі дошки, що містять інформацію обмеженого доступу і / або конфіденційну інформацію, повинні бути стерті.
- Пристрої зберігання даних, такі як CDROM, DVD або USB, слід розглядати як конфіденційні і зберігати в закритому ящику.

- Всі принтери і факси повинні очищатися від паперів після завершення друку; це допоможе забезпечити, щоб конфіденційні документи не залишалися в лотках принтерів і їх не міг забрати стороння людина.

Політика резервного копіювання

Оскільки катастрофи трапляються так рідко, керівництво часто ігнорує процес планування аварійного відновлення. Важливо розуміти, що наявність плану дій в надзвичайних ситуаціях в разі лиха дає дитячо-юнацькій спортивній школі конкурентну перевагу. Дана політика вимагає від керівництва фінансової підтримки і ретельного виконання заходів з планування на випадок стихійних лих. Лиха не обмежуються несприятливими погодними умовами. Будь-яка подія, яка може призвести до тривалої затримки обслуговування, має бути розглянуто. План аварійного відновлення часто є частиною плану забезпечення безперервності бізнесу.

Дана політика визначає вимоги до базового плану аварійного відновлення, який повинен бути розроблений і впроваджений в дитячо-юнацьку спортивну школу і описує процес відновлення IT-систем, додатків і даних після будь-якого типу лиха, що викликає серйозний збій в роботі.

Зміст політики безпеки:

- План реагування на комп'ютерні надзвичайні ситуації: З ким, коли і як слід зв'язатися? Які негайні дії повинні бути зроблені в разі певних подій?
- План наступності: Опишіть порядок передачі відповідальності, коли звичайний персонал не може виконувати свої обов'язки.
- Дослідження даних: Детально опишіть дані, що зберігаються в системах, їх критичність і конфіденційність.
- Список критичних послуг: Перерахуйте всі надані послуги та порядок їх важливості.
- Тут також пояснюється порядок відновлення в короткостроковому і довгостроковому періодах.

- План резервного копіювання та відновлення даних: Детально опишіть, які дані резервуються, на який носій вони зберігаються, де зберігаються і як часто можна створювати резервні копії. У ньому також має бути описано, як ці дані можуть бути відновлені.
- План заміни обладнання: Опишіть, яке обладнання необхідно для початку надання послуг, вкажіть, в якому порядку воно необхідне, і вкажіть, де його можна придбати.
- Управління засобами масової інформації: Хто відповідає за надання інформації засобам масової інформації?
- Також надайте деякі рекомендації щодо того, які дані слід надавати.

Після створення планів важливо, наскільки це можливо, відпрацювати їх на практиці. Керівництво повинно виділити час для перевірки виконання плану аварійного відновлення. Щорічно слід проводити тренування з використанням настільних систем. В ході цих випробувань можна виявити і усунути проблеми, які можуть призвести до збою плану, в умовах, що не мають значних наслідків.

Політика паролів користувачів

Паролі є важливим аспектом комп'ютерної безпеки. Неправильно підібраний пароль може призвести до несанкціонованого доступу і / або експлуатації наших ресурсів. Всі співробітники, включаючи підрядників і постачальників, що мають доступ до систем дитячо-юнацької спортивної школи, несуть відповідальність за прийняття відповідних заходів, описаних нижче, для вибору і захисту своїх паролів.

Мета цієї політики - встановити стандарт для створення надійних паролів і захисту цих паролів.

Зміст політики безпеки:

1. Створення паролів

- Всі паролі на рівні користувача і на рівні системи повинні відповідати Керівництву по створенню паролів.
- Користувачі повинні використовувати окремий, унікальний пароль для кожної зі своїх облікових записів, пов'язаних з роботою. Користувачі не повинні використовувати паролі, пов'язані з роботою, для своїх власних, особистих облікових записів.
- Облікові записи користувачів, які мають привілеї системного рівня, що надаються через членство в групах або програми, такі як sudo, повинні мати унікальний пароль від всіх інших облікових записів, що належать цьому користувачу, для доступу до привілеїв системного рівня. Крім того, настійно рекомендується використовувати будь-яку форму багатофакторної аутентифікації для будь-яких привілейованих облікових записів.

2. Зміна пароля

- Паролі слід міняти тільки в тому випадку, якщо є підстави вважати, що пароль був скомпрометований.
- Злом або вгадування пароля може проводитися періодично або випадково командою Infosec або її представниками. Якщо пароль буде вгаданий або зламаний під час однієї з таких перевірок, користувач повинен буде змінити його відповідно до Керівництва по створенню паролів.

3. Захист паролів

- Паролі не повинні передаватися нікому, включаючи керівників і колег. Всі паролі повинні розглядатися як конфіденційна, конфіденційна інформація дитячо-юнацької спортивної школи. Корпоративна інформаційна безпека визнає, що застарілі програми не підтримують існуючі проксі-системи. Будь ласка, зверніться до технічної довідці для отримання додаткової інформації.
- Паролі можна вставляти в повідомлення електронної пошти, ящики Alliance або інші форми електронного спілкування, а також повідомляти їх кому-небудь по телефону.

- Паролі можуть зберігатися тільки в авторизованих організацією "менеджерах паролів".
- Не використовуйте функцію "Запам'ятати пароль" в додатках (наприклад, в веб-браузерах).
- Будь-який користувач, що підозрює, що його / її пароль міг бути зламаний, повинен повідомити про це і змінити всі паролі.

4. Розробка додатків

Розробники додатків повинні переконатися, що їх програми містять такі запобіжні заходи:

- Додатки повинні підтримувати аутентифікацію окремих користувачів, а не груп.
- Додатки не повинні зберігати паролі відкритим текстом або в будь-який легко оборотної формі.
- Додатки не повинні передавати паролі відкритим текстом по мережі.
- У додатках має бути передбачено управління ролями, щоб один користувач міг взяти на себе функції іншої без необхідності знати його пароль.

5. Багатофакторна аутентифікація

Багатофакторна аутентифікація дуже рекомендується і повинна використовуватися завжди, коли це можливо, не тільки для робітників, але і для особистих акаунтів.

2.8 Розробка основних елементів КСЗІ

Так як серед інформації, що обробляється на ІТС, наявна інформація з обмеженим доступом та конфіденційна інформація, що знаходиться у власності власника ІТС, обрано принцип досягнення допустимого рівня захищеності інформації за мінімальних витрат, що є найбільш доцільним.

Спираючись на таблицю 2.15 Опис послуг профілю захищеності, де було обрано основний профіль захищеності в ІТС. Проаналізувавши обраний профіль захищеності, потрібно ввести заходи для зниження критичних загроз, які були описані в таблиці 2.14 Модель загроз. До цього відносяться: зараження антивірусним ПЗ, некомпетентність персоналу, інсталювання незнайомого ПЗ, несанкціоноване копіювання.

Для забезпечення безпеки, було запропоновано використання програмно-апаратних та організаційних методів захисту.

Антивірусне програмне забезпечення Symantec Data Loss Prevention Endpoint Discover, License, Managed Devices, Perpetual License. Призначене для захисту комп'ютерів користувачів від вірусних програм та шкідливого ПЗ, та реагуванню на виявлення даних програм та інформації, а також мережевих атак. Вартість ліцензії на одну робочу станцію - 1024 грн. Дійсний до кінця року. Не потребує навчання персоналу. Оновлення не рідше 1 разу в рік. Не підходить за пунктами підтримки та оновлення, засіб не дозволений до використання Держспецзв'язком.

Програмний продукт антивірусного захисту ESET Endpoint Antivirus Windows (EEA) версії 7.x виробництва компанії «ESET» (Словаччина). Призначений для захисту комп'ютерів користувачів від вірусних програм та шкідливого ПЗ, та реагуванню на виявлення даних програм та інформації, а також мережевих атак. Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7.x з системою централізованого керування антивірусним захистом корпоративних мереж ESET Security Management Center версії 7.x. Технічні вимоги за критеріями технічного захисту інформації». Експертний висновок №995. Дійсний з 12.07.2019 до 12.07.2022. Вартість ліцензії на одну робочу станцію - 929.05 грн. Дійсний до кінця року. Не потребує навчання персоналу. Оновлення не рідше 1 разу в рік.

На рішення щодо вибору вплинули такі фактори:

- вартість програмного засобу;
- наявність технічної підтримки з боку розробників програми;
- не потребує підвищення кваліфікації/навчання персоналу;
- стабільність версії;
- частота оновлення програмного захисту;
-програмний засіб дозволений до використання Держспецзв'язком.

Серед варіантів антивірусних програмних засобів було вирішено обрати програмний продукт антивірусного захисту ESET Endpoint Antivirus, так як він найбільше задовольняє вимогам.

Для забезпечення безпеки документообігу в компанії було обрано наступні програмні засоби, які захищають від:

- Несанкціонованого доступу до інформації;

- Контроль за документообігом;

Для забезпечення перерахованих вимог було обрано програмну систему електронної автоматизації процесів роботи підприємства документообігу та автоматизації процесів роботи підприємства Is-Pro виробництва компанії "Інтелект-Сервіс". Вартість ліцензії - безкоштовна, фінансується державною податковою службою України. Дійсна до кінця року. Потребує мінімального навчання персоналу. Оновлення не рідше 1 разу в рік.

Для забезпечення збереження/захисту паролів користувачів на підприємстві було обрано наступні програмні засоби, які захищають від:

- Злому паролів користувачів;
- Несанкціонованого доступу до паролів користувачів;
- Несанкціонованого поширення паролів користувачів.

Задля забезпечення вимог щодо захисту паролів користувачів, було обрано програмний продукт менеджер паролів користувачів "KeePass". Призначений для

захисту паролів користувачів від несанкціонованого доступу до паролів користувачів.

Безкоштовної версії програмного продукту буде достатньо задля забезпечення перерахованих вимог. Ліцензія діє до кінця року. Програмний оновлюється самостійно з боку розробників програмного продукту.

Додатково була встановлена двофакторна автентифікація пошти Gmail. Двофакторна автентифікація реалізована завдяки програмі Google Authenticator. Програма вимагає лише встановлення безкоштовного мобільного додатку на телефон працівників. Призначена для захисту пошти від НСД, регулює доступ то ІзОД.

Організаційні методи та способи їх реалізації були описані у пункті 2.11

З засобів технічного захисту було обрано :

Засіб технічного захисту інформації від несанкціонованого доступу КЗЗ «Гриф» версії 4, виробництва ТОВ «Інститут комп'ютерних технологій». Призначений для захисту від НСД до ІзОД. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні, в обсязі функцій, зазначених у документі «Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу «Гриф» версія 4. Призначений для захисту від НСД до ІзОД. Технічне завдання UA21541987.00025-01 90 01». Експертний висновок №1034. Дійсний з 24.10.2019 до 24.10.2022.

Захищає від:

- несанкціонованого доступу до ІзОД;

- регулює правила розмежування доступом.

Для забезпечення вимог використання тільки ліцензійного ПЗ, було такі програмні продукти:

Microsoft Office 2019 Pro Plus. Призначений для Вартість ліцензії на одну робочу станцію - 1350 грн. Дійсний до кінця року. Потребує мінімального навчання персоналу задля нормального користування. Оновлення не рідше 1 разу в рік.

Windows 10 Professional. Інстальоване ПЗ. Вартість ліцензії на одну робочу станцію - 4300 грн. Дійсний до кінця року. Не потребує навчання персоналу. Оновлення не рідше 1 разу в рік. Завдяки ПЗ регулюються правила розмежування доступом, захищає інформацію від НСД.

Висновки другого розділу.

У другій частині кваліфікаційної роботи було наведено загальні відомості про підприємство та необхідність розробки та впровадження комплексної системи захисту інформації, організаційна структура і проведений аналіз оброблюваної інформаціиї. На основі цього проведений акт обстеження підприємства. Результатом обстеження ОІД став аналіз загроз та було обрано профіль захищеності. На основі обраного профілю захищеності були розроблено комплексну систему захисту інформації в ІТС.

ЕКОНОМІЧНА ЧАСТИНА

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації

Метою розрахунків впровадження комплексної системи захисту інформації є економічне обґрунтування доцільності впровадження комплексної системи захисту інформації. Для цього визначена економічна ефективність використання основних впроваджень та розрахунків, що були отримані у ході виконання роботи.

Економічна доцільність визначається завдяки:

- Капітальних витрат
- Експлуатаційних витрат
- Річного економічного ефекту від впровадження комплексної системи захисту інформації.

Визначення витрат на розробку КСЗІ:

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

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

$t = tmз + tв + ta + tвз + tозб + tовр + tд$, годин,

де

$tmз$ - тривалість складання ТЗ на розробку ПБІ = 52 години;

$tв$ - тривалість розробки концепції безпеки інформації у організації = 20 години;

ta - тривалість процесу аналізу ризиків = 43 години;

$tвз$ - тривалість визначення вимог заходів, методів та засобів захисту = 26 години

$tозб$ - тривалість виробу основних рішень з забезпечення БІ = 60 години;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 120 години;

$t_{д}$ - тривалість документального оформлення ПБ = 40 години;

t = 52+20+43+26+60+120+40 = 361 години

3.1.2 Розрахунок витрат на створення КСЗІ:

Витрати на розробку комплексної системи захисту інформації $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$К_{рп} = З_{зп} + З_{мч}$ = 55 594 + 2086,58 =57 680,58 грн.

$З_{мч} = t * З_{пр}$ = 361*154 = 55 594 грн.

де t – загальна тривалість розробки політики безпеки, годин;

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

Вартість машинного часу для розробки комплексної системи захисту інформації на ПК визначається за формулою:

$З_{мч} = t * С_{мч}$ =361*3,79= 1368,19 грн.

де

$t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн;}$$

$C_{мч} = 0,6* 4 * 0,9 + ((7290*0,4)/1920) + ((2300*0,1)/1920) = 2,16+1,5187+0,1197=3,79$

Вартість ПК = 24300 грн, срок корисної служби = 42 місяці.

Мінімальний срок корисної служби = 24 місяці.

Накопичена амортизація = (24300 *42)/5*12 = 17010 грн

Залишкова вартість = 24300 – 17010 = 7290

Відповідно до розроблених рекомендацій щодо застосування розробки у інтрамережі підприємства дитячо-юнацької спортивної школи планується використання програмних засобів, які вже встановлені на підприємстві та додатково використовувати нові програмні засоби.

Таблиця 3.1 Перелік програмних засобів

Програмний засіб	Вартість, грн
Avast Business	557
Microsoft Office 2019 Pro Plus	1350
КЗЗ «Гриф» версії 4	6950
Windows 10 Professional	4300
Кількість ПК	3
Всього	(557+1350+6950+4300)*3= 39 471

Таким чином, капітальні (фіксовані) витрати на створення комплексної системи захисту інформації:

$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 20114+39\ 471+0+0+4200+6000=69\ 785$ грн.

де $К_{рп}$ – вартість розробки комплексної системи захисту інформації та залучення для цього зовнішніх консультантів, 20114 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 39 471грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, 0 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 0 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, 4200 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 6000 грн.

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$С = С_{в} + С_{к} + С_{ак}$, грн.

де $С_{в}$ - вартість відновлення й модернізації системи Св = 0;

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки = Сак = 0 грн.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}$, грн

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються $= С_{н} = 7\ 000$ грн.

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

$С_з = З_{осн} + З_{дод}$, грн.

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 13 300 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$С_з$ = (13 300*12 + 13 300*12*0,1)*0,25= (159 600+15690)*0,25=43 890 грн.

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$С_{єв}$ = 43 890 *0,22 = 9 655,8 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$С_{ел} = Р \cdot F_р \cdot Ц_е$, грн.,

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,6 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (Fр = 1920 год.);

$Ц_е$ – тариф на електроенергію, (Це = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел}$ = 0,6*1920*1,68 = 1935,36 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$С_{тос}$ = 57 680,58 *0,01=576,80 грн

Річний фонд амортизаційних відрахувань:

$С_а = К_{зпз} / 2$

$С_а$ = 21 408,15 / 2 = 10 704,08 грн.

Витрати на керування системою інформаційної безпеки визначаються:

$С_к$ = 7 000+43 890 +9 655,8 +1 935,36 +576,80 + 10 704,08 = 73 772,04 грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 73 772,04 грн.

3.2. Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку:

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

$t_{ви}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 10400 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$П_{зч}$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 3 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 6150 грн. у рік;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 3.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$U = П_п + П_в + V$,

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.

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

$П_п = ((11000 *3)/176)*1 = 187,5$ грн,

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

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

$П_в = П_{ви} + П_{пв} + П_{зч}$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$П_{ви}$ = ((9500 *3)/176)*1 =161,9 грн.

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

$П_{вп}$ = ((11750 *1)/176)*3 = 200,28 грн.

Витрати на заміни встаткування або запасних частин можуть скласти 2320,50 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$П_в$ = 161,9 + 200,28 + 2320,50 = 2682,68 грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого

вузла або сегмента корпоративної мережі визначаються виходячи із

средньогодинного обсягу прибутку і сумарного часу простою сегмента

корпоративної мережі:

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

V = (2300000/2080)* (2+3+2) = 7740,38 грн.

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

U = 2250 + 2682,68 + 7740,38 = 12 673,06 грн.

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

B = 1 * 15 * 12 673,06 = 190 095,9 грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C$$

грн.,

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 57%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 190 095,9 *0,57 – 73 772,04 = 34 582,62 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$ROSI = \frac{E}{K}$, частки одиниці,

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

ROSI = 34 582,62 / 69 785 = 0,5 частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

ROSI $> (N_{деп} - N_{інф})/100)$,

де $N_{деп}$ – річна депозитна ставка, (23%);

$N_{інф}$ – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,5 > (23 – 14)/100 = 0,5 > 0,09.

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки: Т = 1/0,5 = 2 роки.

3.4 Висновок:

Розробка та впровадження комплексної-системи захисту інформації в інформаційної-телекомунікаційній системі для дитячо-юнацької спортивної школи є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,5 грн./грн., що означає отримання 0,5 грн. економічного ефекту на кожну гривню

капітальних вкладень на розробку комплексної-системи захисту інформації в інформаційної-телекомунікаційній системі підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 2 роки (24 місяці). Капітальні витрати складають 69 785 грн.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було проаналізовано загальний стан інформаційної захищеності в комунальних підприємствах, наведена статистика кіберінцидентів. В розділі також було наведено та перелічено основні нормативно-правові документи в сфері захисту інформації, було зазначено основні положення захисту інформації. Серед нормативно-правових документів були розглянуті документі що є правовою основою забезпечення безпеки інформації України: НД ТЗІ та їх галузі використання, Закони України, головні положення.

Обґрунтовано потребу у створенні політики безпеки на підприємстві для запобігання НСД до важливих інформаційних ресурсів розглянутої інформаційно-телекомунікаційної системи. Створення комплексної системи захисту інформації віднесено відповідно до нормативної документації: обґрунтування необхідності створення КСЗІ, обстеження на ОІД, аналіз та оцінка інформаційних загроз та розробка політики безпеки, що враховує загрози найвищого рівня.

У другій частині кваліфікаційної роботи було наведено загальні відомості про підприємство та необхідність розробки та впровадження комплексної системи захисту інформації, організаційна структура і проведений аналіз оброблюваної інформації. На основі цього був проведений акт обстеження підприємства. Результатом обстеження ОІД став аналіз загроз та вразливостей підприємства. На основі рівня загроз ОІД була розроблена комплексна система захисту інформації, що циркулює на ОІД.

Розробка та впровадження комплексної-системи захисту інформації в інформаційної-телекомунікаційній системі для дитячо-юнацької спортивної школи є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,5 грн./грн., що означає отримання 0,5 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 2 роки (24 місяці). Капітальні витрати складають 69 785 грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Статистика кіберінцидентів за 2020 рік: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo/
2. Статистика кібер інцидентів за даними Positive Technologies: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020
3. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.
4. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. -2015. - Режимдоступудоресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
5. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.
6. Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
7. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
8. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герас іна, Д.С. Тимофєєв, О.В. Кручінін , Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. –47 с
9. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
10. 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. - No22- (Нормативний документ системи технічного захисту інформації).
11. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc- page.html?id_doc=66911.
12. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc- page.html?id_doc=66912.
13. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
14. 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. - No125 - (Нормативний документ системи технічного захисту інформації).
15. Політики безпеки інформації https://www.sans.org/information-security-policy/?msc=main-nav
16.

Додаток А

Гриф обмеження доступу
Прим. № ___
ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника,
користувача) об'єкта
_директор Теодорович С.В.
(посада, підпис, ініціали, прізвище)
12. 05. 2021
М.П.

АКТ
категоріювання __відділу бухгалтерії_Дитячо-юнацька спортивна школа №2__
(найменування об'єкта категоріювання)

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____первинне _____
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється __обробка інформації технічними засобами _____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті __конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).

5. Встановлена категорія___4 категорія, до четвертої категорії відносяться об'єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом_____

Голова комісії _____ _Скуйбіда В. О._____
(підпис) (ініціали, прізвище)
Члени комісії: _____ _П.А.Статива_____
(підпис) (ініціали, прізвище)
____.____. 20___

Додаток Б

Н А К А З

м. Дніпро

09.05.21
№ 101

Про створення комплексної системи захисту інформації в автоматизованій системі класу «4» ІТС Дитячо-юнацької спортивної школи №2

На виконання вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами) та п.16 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених Постановою Кабінету Міністрів України від 26.03.2006 року №373(зі змінами).

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі класу «4» для обробки інформації з обмеженим доступом.

2. Відповідальному за службу захисту інформації в автоматизованих системах Йощенко С.В., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

3. Контроль за виконанням наказу покласти на працівника – Скуйбіда В. О.

Директор

Теодорович С.В. _____
(ініціали, підпис)

ДОДАТОК В. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	10	
6	А4	2 Розділ	41	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	

ДОДАТОК Г. Перелік документів на оптичному носії

1 Диплом_Гуня_125-17-2.doc

2Диплом_Гуня_125-17-2.pdf

3 Презентація_Гуня_125-17-2.pptx

ДОДАТОК Д. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-2

Гуні Владислава Олеговича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на __64__ сторінках.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерії дитячо-юнацької спортивної школи.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз інформаційного середовища підприємства; аналіз моделі порушника та загроз.

На основі моделі загроз було розроблено елементи комплексної системи захисту інформації. Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності забезпечення безпеки інформації, за рахунок розробки політики безпеки інформації та обрання програмних засобів забезпечення захисту інформації.

За час дипломування Гуня В.О. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

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

Кваліфікаційна робота заслуговує оцінки «добре» (85).

Керівник кваліфікаційної роботи

Керівник спец. розділу