Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Барабаша Артема Вадимовича

на здобуття ступеня вищої освіти Бакалавра

Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.200102.20.01.02 ПЗ

Виконав студент 4 курсу, група КБ-20-1 _____ Артем БАРАБАШ
Підпис, дата — Ініціали, прізвище

Керівник к.т.н, доц. _____ Віктор ЧЕШУН
Науковий ступінь, вчене звання — Підпис, дата — Ініціали, прізвище

Нормоконтролер старший викладач _____ Сергій МОСТОВИЙ
Науковий ступінь, вчене звання — Підпис, дата — Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата — Ініціали, прізвище

19 06.24 2024р.

Хмельницький, 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 лютого 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Барабашу Артему Вадимовичу

1 Тема роботи Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства

Керівник роботи к.т.н, доц. кафедри кібербезпеки Віктор Миколайович Чешун

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи розробити комплексну систему захисту для автоматизованого робочого місця керівника підприємства.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Загальні відомості, призначення та мета розробки комплексної системи захисту інформації. Розробка політики, плану та технічного завдання для автоматизованого робочого місця керівника підприємства. Підготовка до введення в дію комплексної системи захисту інформації.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Генеральний план об'єкту інформаційної діяльності. Ситуаційний план об'єкту інформаційної діяльності.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Артем БАРАБАШ

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства»

Автор роботи: Барабаш Артем Вадимович.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 68 сторінок, 10 додатків, 10 рисунків, 40 джерел.

Графічна частина: 3 плакати, 12 презентаційних слайдів.

КОМЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ КЕРІВНИКА, ТЕХНІЧНЕ ЗАВДАННЯ, ПЛАН ЗАХИСТУ ІНФОРМАЦІЇ, АКТ.

Метою роботи є розробка комплексної системи захисту інформації для автоматизованого робочого місця керівника підприємства.

В роботі визначено мету та призначення проєктованої комплексної системи захисту інформації, розроблено політики безпеки, план захисту інформації та технічне завдання, а також здійснена підготовка до введення комплексної системи захисту інформації.

В кваліфікаційній роботі здійснено розробку комплексної системи захисту інформації для автоматизованого робочого місця керівника підприємства та надано комплект супровідної документації.

17.06.2024

ABSTRACT

Subject of qualification work: "Complex system of information protection of the automated workplace of the head of the enterprise"

Author: Barabash Artem Vadimovich.

Head of work: Cheshun Viktor Nikolaevich.

Explanatory note: 68 pages, 10 appendices, 10 fig., 40 sources.

Graphic part: 3 drafts, 2 presentation slides.

COMPLEX INFORMATION PROTECTION SYSTEM, AUTOMATED WORKPLACE OF THE HEAD, TERMS OF REFERENCE, INFORMATION PROTECTION PLAN.

The purpose of the work is to develop a comprehensive information protection system for the automated workplace of the head of the enterprise.

The purpose and purpose of an integrated information protection system were determined, security policies, an information protection plan and terms of reference were developed, and preparations were made for the introduction of an integrated information protection system.

In the qualification work, a comprehensive information protection system was developed for the automated workplace of the head of the enterprise.

17.06.2024

ЗМІСТ

Зм.	Арк.	№докум.	Підпис	Дата	КРБКБ.200102.20.01.02 ПЗ		
Виконав		Барабаш А.В.		17.06.24	Комплексна система захисту інформації автоматизованого робочого місяця керівника підприємства Пояснювальна записка	Літера	Аркуш 6 / Аркушів 68
Перевір.		Чешун В.М.		17.06.24			
Н.контр.		Мостовий С.В.		18.06.24		ХНУ, КБ-20-1	
Затвер.		Кльоц Ю.П.		19.06.24			

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

АРМ – Автоматизоване робоче місце

АС – Автоматизовна система

ДТЗ – Допоміжні технічні засоби

ДСТУ – Державний стандарт України

ЗЗІ – Засоби захисту інформації

ЗУ – Закон України

ІзОД – Інформація з обмеженим доступом

ІС – Інформаційна система

ІКС – Інформаційно – комунікаційна система

КСЗІ – Комплексна система захисту інформації

НД ТЗІ – Нормативний документ системи технічного захисту інформації

ОІД – Об’єкт інформаційної діяльності

ОТЗ – Основні технічні засоби

ПЗ – Програмне забезпечення

ПІБ – Політика інформаційної безпеки

ПП – Приватне підприємство

ТЗІ – Технічний захист інформації

ЦАЗІ – Центр антивірусного захисту інформації

ВСТУП

З розвитком технологій у сучасному світі інформація, як ресурс, набувала досить масштабного значення у всіх сферах людського життя, зокрема і на підприємствах. Будь-яке спотворення, знищення, несанкціонована передача може мати колосальні наслідки на репутації організації, а також може призвести до фінансових збитків. Особливу увагу потрібно приділяти інформації, яка обробляється за використанням автоматизованого робочого місця керівника підприємства.

Автоматизоване робоче місце (АРМ) – це комплекс програмно-технічного забезпечення, який автоматизує роботу людини. Одними з основних функцій АРМ є введення, зберігання, пошук за ознаками інформації [1]. АРМ керівника містить різного роду інформацію як і для службового користування, так і конфіденційну інформацію, а в залежності від організації може містити інформацію з грифом секретності «таємно», «цілком таємно», «особливої важливості». Тому, враховуючи ці особливості, захист інформації в АРМ керівника є одним з пріоритетних завдань служби інформаційної безпеки на підприємстві. Тому для захисту даних необхідно розробити комплекс заходів спрямованих на безпеку інформації.

Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, а також програмно-апаратних засобів, використовуючи які можна забезпечити захист інформації в автоматизованій системі. Головною метою створення КСЗІ є об’єднати в цілісну систему усі критично важливі заходи та засоби, які забезпечують захист інформації від різноманітного роду загроз на всіх етапах життєвого циклу автоматизованої системи [2].

Основою для визначення важливості розроблення та впровадження КСЗІ є норми та вимоги діючого законодавства України, відповідно до яких державні інформаційні ресурси або ж інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна обробляти в системі з використанням

комплексної системи захисту інформації. Зокрема, одними з таких нормативно-правових документів є: закон України «Про інформацію», закон України «Про захист інформації в інформаційно-комунікаційних системах», Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 №373 тощо [1].

Аналіз нормативних та законодавчих актів та документів необхідний для того, щоб визначити як можна обмежити чи заборонити доступ до певного виду інформації, а також як захистити дані за відповідними критеріями. На підставі проведеного аналізу приймається рішення про необхідність створення комплексної системи захисту інформації в організації [1].

Основною метою комплексної системи захисту інформації для автоматизованого робочого місця керівника є забезпечення безпеки інформації, яка є важливою для підприємства. Однак, 100% захист неможливий, але для захисту від певних ризиків і втрат для приватної організації ці заходи можуть врятувати компанію, тому дане питання є актуальним.

Метою даної кваліфікаційної роботи є розробка комплексної системи захисту інформації автоматизованого робочого місця керівника підприємства, реалізація даного проєкту підвищить рівень захищеності інформації.

1 ЗАГАЛЬНІ ВІДОМОСТІ, ПРИЗНАЧЕННЯ ТА МЕТА РОЗРОБКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Огляд нормативних документів для створення комплексної системи захисту інформації

Основними нормативно-правовими документами які використовуються при створенні системи захисту в комплексній системі захисту інформації є [1]:

– Закон України «Про інформацію»;

– Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

– НД ТЗІ 1.1-002-99: «Загальні положення з захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

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

– НД ТЗІ 2.5-004-99: «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;

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

– НД ТЗІ 3.7-001-99: «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;

– НД ТЗІ 3.7-003-05: «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі».

Найважливішим законом у сфері захисту інформації є Закон України «Про інформацію». Даний закон регулює відносини, які пов'язані зі розробкою, колекціонуванням, отриманням, використанням, поширенням, зберігання, захистом інформації. Стаття 1 даного закону стверджує, що інформація – це

перелік відомостей або/та дані, які зберігають на фізичних носіях або які можна відобразити у електронному вигляді [3].

Відповідно до цієї ж статті захист інформації – це сукупність дій, зокрема адміністративних, організаційних, технічних та правових, виконуючи які можна забезпечити безпеку, цілісність та належний доступ до інформації [3].

Стаття 2 ЗУ «Про інформацію» визначає основні принцип інформаційних відносин, які зображені на рисунку 1.1.

Рисунок 1.1 – Основні принципи інформаційних відносин

Наступним законом який відіграє важливу роль у сфері захисту інформації є Закон України «Про захист інформації в інформаційно-комунікаційних системах» який забезпечує реалізацію прав особи на інформації, вільний доступ до цієї інформації, захист цієї інформації від спотворення, неправомірного використання, розголошення, знищення, несанкціонованого доступу, а також створення правових та організаційних засад захисту інформації в автоматизованих системах тощо. Дія даного закону розповсюджується на весь перелік інформації, що буде оброблятися в автоматизованій системі [4].

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі» визначає основні елементи організації та процесу виконання завдань із захисту інформації в інформаційно-комунікаційних системах (ІКС) – процес прийняття рішень щодо складу комплексної системи захисту інформації залежно від умов функціонування ІКС та видів оброблюваної інформації, визначення обсягу та змісту завдань, поетапності виконання завдань, основних завдань та процесу виконання завдань в інформаційно-комунікаційних системах, визначення обсягу та змісту завдань, поетапності виконання завдань, основних завдань та процесу виконання завдань в інформаційно-комунікаційних системах [5].

Цей НД ТЗІ поширюється лише на ІКС, в яких інформація обробляється автоматично. Отже, всі законодавчі та нормативні документи, що стосуються створення автоматизованих систем та захисту інформації в автоматизованих системах, поширюються на ці КСЗІ. НД ТЗІ не встановлює нових стандартів, а систематизує в одному документі вимоги, стандарти та правила, які прямо чи опосередковано випливають з положень чинних нормативних документів [5].

Цей НД ТЗІ організовано у вигляді посібника, в якому перелічено роботи та зроблено посилання на відповідні нормативні документи, згідно з якими ці роботи повинні виконуватися. Якщо певні етапи або види робіт не стандартизовані, надається короткий опис робіт та отриманих результатів [5].

НД ТЗІ призначено для суб'єктів інформаційних відносин (власників або розпорядників КСЗІ, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в КСЗІ, постачальників компонентів КСЗІ, а також фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації з метою забезпечення її відповідності вимогам ТЗІ [5].

Порядок, викладений у цій НД ТЗІ, є обов'язковим для всіх суб'єктів системи ТЗІ України незалежно від їх організаційно-правової форми та форми власності, в КСЗІ яких обробляється інформація, що є власністю держави, належить до

державної або іншої таємниці чи окремих видів інформації, вимога щодо захисту якої встановлена законом. У разі обробки в КСЗІ інших видів інформації суб'єкти системи захисту критичної інфраструктури можуть керуватися вимогами цього нормативного документа [5].

НД ТЗІ 3.7-001-99: «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». Цей нормативний документ визначає вимоги до процесу розроблення, складу та змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання та передавання інформації з обмеженим доступом або інформації, захист якої гарантується державою. [6].

НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» - документ визначає принципи класифікації автоматизованих систем та створення стандартних функціональних профілів для захисту інформації від несанкціонованого доступу [7].

Цей документ призначений для постачальників (розробників), споживачів (замовників, користувачів) автоматизованих систем, що використовуються для обробки (у тому числі збирання, зберігання, передавання тощо) критичної інформації (інформації, яка потребує захисту), а також органів, які здійснюють контроль за обробкою цієї інформації [7].

Метою цього документа є створення правових та методичних засад для вибору та реалізації вимог щодо захисту інформації в автоматизованій системі.

Цей керівний документ визначає основні принципи та положення організації захисту інформації для кожного етапу життєвого циклу комплексної системи захисту інформації [7].

1.2 Автоматизоване робоче місце керівника підприємства як об’єкт інформаційної діяльності

Перед початком створення комплексної системи захисту інформації необхідно ознайомитися з об’єктом інформаційної діяльності на якому буде здійснюватися захист інформації.

Приватне підприємство «SBS» - це компанія, яка надає послуги у сфері інформаційних технологій. Основними напрямками роботи компанії є:

– розробка програмного забезпечення;

– консультації у сфері IT;

– хмарні рішення та послуги;

– технічна підтримка та обслуговування.

Організаційна структура підприємства має наступну архітектуру:

1. Керівництво: керівник підприємства, фінансовий директор, технічний директор.

2. Відділ розробки програмного забезпечення, який складається з команди розробників, тестувальників та аналітиків.

3. IT-відділ, який складається з адміністраторів система, спеціалістів з мережевої безпеки, хмарних технологій та спеціалістів підтримки користувачів.

Керівник підприємства відповідає за загальне управління компанією, стратегію розвитку та прийняття стратегічних рішень. Фінансовий директор відповідає за фінансові аспекти діяльності компанії, включаючи бюджетування, фінансовий аналіз та фінансове планування. Технічний директор керує технічними аспектами бізнесу, враховуючи розробку та розгортання технологій, інфраструктури та програмного забезпечення.

Відділ розробки програмного забезпечення створює програмне забезпечення враховуючи вимоги клієнтів, здійснює тестування даного програмного забезпечення, а також розробляють концепції програмних рішень за вимогами клієнтів.

ІТ-відділ забезпечує підтримку інформаційних систем, безпеку мережі та даних компанії, впроваджує та керує хмарними послугами, а також надає технічну підтримку та консультацію користувачам.

Враховуючи організаційну структуру зрозуміло, що найвищу місце в ієрархії підприємства займає керівник підприємства, який визначає загальні цілі та стратегію розвитку компанії та взаємодіє з усіма подальшими структурами. Керівник підприємства має власне автоматизоване робоче місце для кращої організації роботи підприємства.

Автоматизоване робоче місце – це робоче місце працівника, яке обладнане засобами обчислювальної техніки де здійснюється обробка та відображення робочої інформації. [8]

1.3 Мета та призначення створення комплексної системи захисту інформації

Автоматизоване робоче місце керівника підприємства створюється відповідно до законодавства України «Про захист прав споживачів». Основне завдання керівника підприємства – забезпечення ефективного управління, прийняття рішення на основі доступних даних, а оскільки розглядається система керівника, у нього наявні абсолютно вся інформація, що стосується підприємства [3].

Основними функціями АРМ керівника підприємства є [1]:

– збір та аналіз даних – це означає, що система повинна забезпечувати можливість збору та обробки різноманітної інформації з різного роду джерел;

– звіт та аналітика даних - це означає, що використовуючи автоматизоване робоче місце керівника потрібно формувати звіти та аналітичні звіти на основі даних, які було зібрано про проаналізовано;

– керування процесами – це означає, що АРМ керівника допомагає йому налаштувати роботу різних процесів, наприклад виробничих процесів чи бізнес-процесів;

– керування персоналом – це означає, що використовуючи АРМ керівник підприємства може налаштувати зв’язок з персоналом, планувати графік, вести облік робочого часу, відслідковувати продуктивність тощо;

– підтримка прийняття рішень – використовуючи структуроване АРМ керівник може швидше та простіше аналізувати дані, а отже і приймати відповідні рішення.

Метою створення комплексної системи захисту інформації є здійснення заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також цілісності та доступності відкритої інформації, яка важлива для тих, хто нею володіє та її використовує [9].

Зростання загроз інформації, викликане такими факторами, як лібералізація, кризовий стан економіки, використання технічних засобів обробки інформації та засобів зв'язку, поширення засобів несанкціонованого доступу до інформації та впливу на неї, призвело до необхідності побудови та розробки відповідних інтегрованих систем захисту інформації.

Комплексна система захисту інформації – це комплекс організаційно-технічних заходів, програмно-технічних засобів, що забезпечують захист інформації на АС [9].

Для забезпечення всебічного захисту конфіденційної інформації необхідно провести ретельний аналіз каналів витоку, каналів і методів несанкціонованого впливу на інформацію. Отже, основною метою КСЗІ є інтеграція всіх необхідних заходів та інструментів для захисту інформації від різноманітних загроз безпеці протягом усього життєвого циклу АС [9].

Напрямки захисту автоматизованого робочого місця керівника можна поділити на правові, організаційні та програмно-апаратні заходи [10].

До правових заходів можна віднести такі заходи, як дотримання нормативно-правових документів державної політики в сфері захисту та контроль за захищеністю інформації, яка є власністю держави.

До організаційних заходів можна віднести розробку політики безпеки,

встановлення режимних заходів, встановлення контролю за виконання та ефективністю впроваджених заходів щодо безпеки інформації.

До програмно-апаратних заходів можна віднести захист інформації від витоку технічними каналами, від несанкціонованого доступу, встановлення антивірусного програмного забезпечення, налаштування автентифікації та авторизації користувача, проведення аудиту, розробку комплексу захисту інформації, впровадження системи безперебійного електроживлення, встановлення камер відеоспостереження тощо.

Враховуючи вище наведений аналіз приймається рішення про необхідність створення комплексної системи захисту інформації.

Комплексна система захисту інформації створюватиметься для того, аби використовуючи ряд інженерно-технічних заходів забезпечити доступність, цілісність та конфіденційність інформації.

КСЗІ повинна забезпечувати виконання таких задач, як [11]:

– обмеження та контроль доступу до ресурсів АС організації відповідно до повноважень користувачів організації;

– реєстрація подій, що відбуваються в системі, та даних, що стосуються інформаційної безпеки;

– підтримання цілісності середовища установи та прикладних програм, інформації та даних, що обробляються в системі;

– виявлення вразливостей операційної системи;

– захист від атак з боку порушників безпеки;

– захист від впровадження та розповсюдження комп'ютерних вірусів;

– захист інформації при передачі телекомунікаційними засобами;

– функціональне управління КСЗІ.

Наступним етапом після ознайомлення з організацією та визначення необхідності створення КСЗІ є безпосередньо створення відповідних нормативних документів. Першим найважливішим документом є Наказ про створення КСЗІ, що зображений на рисунку 1.2.

Наказ про створення КСЗІ зобов'язує на об'єкті впровадити комплексну систему захисту інформації. Даний документ містить ряд важливих елементів, зокрема підстави для створення КСЗІ, а також визначення відповідальної особи за створення КСЗІ.

Важливим етапом при створенні КСЗІ є визначення категорії важливості інформації. Отже, наступним розробленим документом є Наказ про створення комісії з категоріювання та обстеження об’єктів інформаційної діяльності (рисунок 1.3). Метою даного наказу є визначення відповідальних осіб, які будуть проводити категоріювання та обстеження об’єкту та створювати відповідні нормативні документи [12]. Завданням цієї комісії є визначити категорію інформації, яка буде оброблятися в автоматизованій системі керівника. В акт обстеження комісія повинна описати приміщення об’єкту та вказати всі можливі данні, які є важливими для забезпечення захисту інформації [13].

Акт категоріювання – документ, що визначає категорію, тобто важливість об’єкта та визначає необхідний рівень захисту цієї інформації. Акт категоріювання повинен розроблятися відповідно до 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» [13].

Інформація за рівнем важливості поділяється на чотири категорії [14]:

– перша категорія – «особливої важливості»;

– друга категорія – «цілком таємно»;

– третя категорія – «таємно»;

– четверта категорія – «Для службового користування», конфіденційна, державні інформаційні ресурси, відкрита інформація.

Перші три категорії містять державну таємницю і мають особливий рівень захисту, четверта категорія не відноситься до державної таємниці, проте теж повинна захищатися.

НАКАЗ

10.02.2024 Київ №9

Про створення комплексної
системи захисту інформації

Відповідно до закону України «Про захист інформації в інформаційно-комунікаційних системах» №80/94-ВР від 05.07.1994 (зі змінами), Положення про технічний захист інформації в Україні №1229/99 від 27.09.1999 та Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах №373 від 29.03.2006

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації (далі КСЗІ) в АС класу «1» інв. № 1129384, в якій передбачається обробка інформації з грифом обмеження доступу «Для службового користування» для ПП «SBS».
2. Відповідальним за створення КСЗІ та впровадження заходів із захисту інформації призначити керівника центру цифрових технологій Верещука А.С.
3. Контроль за виконанням наказу залишаю за собою.

Керівник ПП «SBS» Верещук А.С.

Рисунок 1.2 – Наказ про створення КСЗІ для ПП «SBS»

НАКАЗ

10.02.2024 Київ №9

Про утворення комісії з категоріювання та обстеження
об'єктів інформаційної діяльності

Відповідно до законів України «Про інформацію» №2657-XII від 02.10.1992, «Про захист інформації в інформаційно-комунікаційних системах» №80/94-ВР від 05.07.1994 (зі змінами), Тимчасове положення по категоріювання об'єктів №35 від 10.07.95, Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці №215 від 15.04.2013, НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Переддипломні роботи»

НАКАЗУЮ:

1. Утворити комісію з категоріювання та обстеження автоматизованої системи класу 1 у складі:

ГОЛОВА:

Верещук Андрій Сергійович - керівник приватного підприємства «SBS»;

ЧЛЕНИ КОМІСІЇ:

Кимчук Віктор Костянтинович - заступник керівника приватного підприємства «SBS».

2. Контроль за виконання цього наказу залишаю за собою.

Рисунок 1.3 – Наказ про створення комісії з категоріювання та обстеження ОІД

На автоматизованому робочому місці керівника підприємства буде оброблятися інформація четвертої категорії: для службового користування, конфіденційна та відкрита інформація. А саме автоматизоване робоче місце являтиме собою автоматизовану систему класу «1». Акт визначення ступеня обмеження доступу до інформації, яка циркулюватиме на ОІД представлено у додатку Ж.

Також акт категоріювання містить наступну інформацію: підстава для категоріювання ОІД, тобто які накази були видані, вид категоріювання, що виконуватиметься з інформацією на ОІД, а також зазначається ступінь обмеження доступу до інформації [15].

Розроблений акт категоріювання зображено на рисунку 1.4.

Акт обстеження – документ, який описує всі об'єкти, що знаходяться в приміщенні ОІД. Акт обстеження повинен розроблятися відповідно до НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи». Передпроєктна робота ОІД є першим кроком у розробці комплексу ТЗІ, де передбачється [16]:

- проведення обстеження існуючої ОІД;
- розробка моделі загроз для ІзОД або доповнення до існуючої моделі;
- загрози відповідно до положень НД ТЗІ;
- розробка технічного завдання на створення комплексної ТЗІ.

Метою обстеження є підготовка вихідних даних, необхідних для визначення вимог до створення комплексу ТЗІ. Обстеження на ОІД проводиться комісією, склад якої затверджується керівником установи-замовника відповідно до затвердженої програми [16]. Акт обстеження ОІД представлено у додатку З.

Наступним етапом є визначення переліку відомостей, що відноситься до конфіденційної інформації автоматизованого робочого місця керівника. Наказ про затвердження Переліку відомостей представлений у Додатку Е. Такий перелік наведено у таблиці 1.1.

«**ЗАТВЕРДЖУЮ**»
Керівник приватного
підприємства «SBS»
_____ Верещук А.С.
«10» березня 2024 р.
М.П.

АКТ
категоріювання автоматизованої системи класу 1 інв. № 114656 кабінету керівника
(найменування об'єкта категоріювання)

1. Підстава для категоріювання наказ №9 від 10.02.2024 про створення КСЗІ
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
зміна ознаки, за якою була встановлена категорія об'єкта, тощо;
наказ №9 від 13.04.2024 про утворення комісії з категоріювання та обстеження об'єктів інформаційної діяльності
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
інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (персональні дані)
(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 IV (четверта)

Голова комісії _____ А.С. Верещук
(підпис) (ініціали, прізвище)
Члени комісії: _____ В.К. Кимчук
(підпис) (ініціали, прізвище)

Рисунок 1.4 – Акт категоріювання

Таблиця 1.1 – Перелік відомостей, що відноситься до конфіденційної інформації автоматизованого робочого

№	Інформація	Гриф обмеження доступу
1	Інформація про фінансові звіти підприємства, про прибуток і збиток, бюджетні дані, бухгалтерія, інвестиції.	Для службового користування
2	Інформація про послуги та товари	Для службового користування
3	Відомості про організацію, реагування та дій у разі виникнення надзвичайної ситуації	Для службового користування
4	Технічні заходи щодо захисту конфіденційної інформації та для службового користування	Для службового користування
5	Нормативна та експлуатаційна документація щодо технічних рішень, прийнятих у спеціальних проектах та проектах захисту організації, політика безпеки організації	Для службового користування
6	Відомості про клієнтську базу підприємства	Конфіденційно
7	Публічна інформація про проєкти підприємства	Відкрита
8	Публічна фінансова інформація	Відкрита
9	Відомості про загальнодоступні події	Відкрита
10	Відомості про працівників підприємства	Конфіденційно
11	Відомості про стан та ефективність роботи організації	Конфіденційно
12	Дані, що стосуються стратегічного розвитку підприємства, його плани, проєкти, аналіз ринку та конкурентів	Конфіденційно

Визначення даного переліку відомостей, опис об’єктів які входять в автоматизоване робоче місце керівника є необхідним для ефективного впровадження КСЗІ, а отже і для ефективної роботи підприємства.

Задачі, які повинні виконуватися:

– швидко оцінювати стан апаратного та програмного забезпечення;

– ефективно управляти ресурсами підприємства;

– контроль вразливостей в системі;

– генерація регулярних або спеціальних звітів;

– оцінювання ефективності заходів безпеки.

АС являє собою сукупність інформації, персоналу та засобів автоматизації, що реалізують технічні процеси діяльності підприємства. Ця інформацію та сучасні способи обробки інформації добре поєднуються в документованій формі, якщо вважати, що документом вважається інформація, яка зафіксована на матеріальному носію інформації з реквізитами, які можуть ідентифікувати її. Тобто документ, це не лише текст, але й зображення на папері, файли на матеріальних носіях, рядок записів в базі даних [5].

Інформація загальнодоступної інформації:

– інформація про законодавство, внутрішні правила організації, актуальні трудові норми та правила техніки безпеки при роботі з технікою;

– правила внутрішнього трудового розпорядку, правила техніки безпеки при роботі з технікою;

– інформація про посаду працівника, його ім'я, прізвище та робочий телефон;

– інформація про графік роботи організації;

– база даних клієнтів;

– перелік підприємств регіону та інформація про їхніх керівників.

Список інформації обмеженого доступу:

– особиста інформація та посадові інструкції співробітників;

– інформація про постачання обладнання в організацію;

– інформація про фінансову діяльність організації;

– інформація про мережеву конфігурацію комп'ютерів і серверів;

– інформація про документацію організації.

Для опису об’єктів які містять на об’єкті інформаційної діяльності доцільно використовувати генеральний та ситуаційний плани ОІД. Генеральний план, зображений у додатку А, встановлює загальні рамки інформаційної безпеки на підприємстві, в той час як ситуаційний план, зображений у додатку Б, допомагає управляти конкретними інцидентами і відновлювати нормальну роботу після їх виникнення.

Елементами генерального плану є: зображення приміщення керівника підприємства, розташування всіх наявних об’єктів, таких як, шафа, батареї, столи, крісла, двері, вікна, комп’ютери, принтери. Елементами ситуаційного плану є: розташування будівлі в якій розміщено АС, відстані будівлі відносно до інших будівель, а також зазначено місця розташування машин.

1.4 Постановка задачі

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації для автоматизованого робочого місця керівника приватного підприємства «SBS» для забезпечення ефективності керування організацією та підвищення рівня захищеності інформації в системі.

В першому підрозділі даного розділу розглядались нормативно-правові документи, закони України та основні статті цих законів які є основою при розробці КСЗІ. В другому підрозділі було розглянуто підприємство та його ієрархію для якої розроблятиметься КСЗІ. В третьому підрозділі було визначено мету та призначення розроблюваної системи, а саме з метою розробки є забезпечення конфіденційності, цілісності та доступності даних, а також забезпечення ефективності роботи керівника підприємства. Також в третьому

підрозділі було здійснено підготовчий етап створення КСЗІ, а саме розробка наказів про створення та призначення відповідальної особи, наказ про створення комісії з категоріювання та обстеження, а також безпосередньо розроблено самі акти категоріювання та обстеження об’єкту інформаційної діяльності.

В наступних розділах, на основі вище проведеного аналізу здійснюватиметься розробка основних документів, зокрема таких:

– план захисту інформації;
– технічне завдання;
– технороботчий проєкт;
– формуляр;
– модель загроз;
– політика безпеки;
– наказ затвердження переліку відомостей;
– акт обстеження ОІД.

І важливим етапом в розробці КСЗІ для АС є впровадження її в дію та здійснення попередніх випробувань наскільки розроблена система є безпечною та надійною.

2 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Визначення потенційних загроз для інформації

При оцінці автоматизованого робочого місця керівника необхідно виявити потенційні загрози інформації, а отже, розробити модель загроз та модель зловмисника. Ці вимоги необхідно розробляти відповідно до таких нормативних документів, як НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в інформаційних системах від несанкціонованого доступу», НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», НД ТЗІ 3.7-003-05 «Порядок впровадження комплексної системи захисту інформації в інформаційно-комунікаційній системі» [17].

Загрози інформаційної безпеки можна визначити як джерела загрози. Джерелом загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Крім того, джерела загроз можуть бути внутрішніми для захищеної організації або зовнішніми для неї. Відмінність між суб'єктивними і об'єктивними джерелами обґрунтовується на основі потенціалу нанесення шкоди інформації. Крім того, відмінність між внутрішніми та зовнішніми джерелами виправдана, оскільки методи захисту цих джерел можуть відрізнятися.

Порушник (або Користувач Violator) - фізична особа, яка здійснює несанкціонований доступ до інформації. Враховуючи, що злочинець розуміється як особа, очевидно, що побудова формалізованої моделі, що представляє їх, є складним завданням [18]. Отже, можна лише обговорити неформальну або описову модель порушника. Злочинець - фізична особа, яка має можливість отримати доступ до ресурсів і можливостей, що входять до АС. Не виключено, що порушник може намагатися виконувати операції, які призвели або можуть призвести до порушення властивостей інформації, визначеної політикою безпеки, використовуючи різні можливості, методи і засоби, внаслідок незнання, цілеспрямовано, шляхом злого умислу або без нього [18].

Модель порушника – це стандартизований або неформальний абстрактний опис дій порушника, що відображає його практичні та теоретичні можливості,

попередні знання, час і місце дій тощо. З точки зору АС зловмисники можуть бути внутрішніми або зовнішніми [19].

Модель порушника повинна визначати [19]:

– можливу мету зловмисника та її градацію за ступенем небезпеки для відповідної системи;

– категорії осіб, з яких може виходити порушник;

– припущення про кваліфікацію порушника;

– припущення про характер дій порушника.

Метою порушника може бути [19]:

– отримання необхідної інформації в необхідному обсязі та обсязі;

– можливість модифікувати та змінювати інформацію;

– можливість модифікувати інформаційні потоки відповідно до своїх намірів;

– можливість отримати доступ до фізичних носіїв інформації;

– нанесення збитків шляхом знищення матеріальних та інформаційних ресурсів.

Для АРМК ПП «SBS» важливо враховувати мотив порушення, який може бути навмисним або випадковим. Випадковість означає, що обставини не залежать від мети виконання, тоді як навмисне вторгнення передбачає навмисні дії, спрямовані на пошкодження об'єкта або крадіжку інформації. Для захисту важливо проводити аудит усіх подій, що відбуваються в контрольованій зоні, щоб мінімізувати можливість порушення цілісності, конфіденційності та доступності інформації для зловмисників. Рівень обізнаності може бути різним, але важливо визначити, хто не знає про автоматизовану систему, а хто є довіреним користувачем. Доступність поділяється на тимчасову та користувацьку. Наприклад, випадкове вторгнення може статися під час прибирання, але коли система активно використовується, легше ідентифікувати порушника за допомогою персонального ідентифікатора. Після визначення критеріїв необхідно скласти список можливих порушників, записати його та проаналізувати, щоб

визначити, які з них потребують найбільшого контролю. Результати фіксуються у звіті для подальшого використання.

Модель загроз є одним з ключових документів на першому етапі створення глобальної системи інформаційної безпеки. Модель загроз містить загальний і ситуаційний план, а також описує область, що підлягає контролю. Малюнки планів повинні відповідати обстеженню об'єкта і все зображене має відповідати дійсності [19].

Важливою частиною моделі загроз є перелік засобів моніторингу та оцінки і засобів контролю та моніторингу. Абревіатурами позначені основні технічні засоби (ОТЗ) та допоміжні технічні засоби системи. До основних належать: монітор, клавіатура, центральний обчислювальний блок і миша. Допоміжними засобами є принтер, телефон і всі інші пристрої в приміщенні.

Варіанти моделі загроз визначають властивості безпеки інформаційних об'єктів, які можуть бути порушені – конфіденційність (К), цілісність (Ц), доступність (Д), а також якісну оцінку ймовірності загрози та рівня збитків для кожного типу загроз.

Метод створення такої моделі полягає у введенні переліку типів загроз в одну з колонок таблиці. Потім для кожної з потенційних загроз необхідно провести аналіз і визначити:

– ймовірність виникнення відповідної загрози;

– ймовірний розмір збитків;

– джерела загроз.

Модель загроз може бути як одним з підрозділів моделі загроз, так і окремим документом. Перелік потенційних загроз для АРМК зображено на рисунку 2.1.

Загрози	Джерело	Порушення властивостей		
		К	Ц	Д
Природні загрози				
Стихійні природні лиха, у результаті яких буде порушена робота систем електроживлення, цілісність приміщення	внутрішня		+	+
Ненавмисні (випадкові) загрози				
Ненавмисні дії, у результаті яких відбувається часткова чи повна відмова системи	внутрішня		+	+
Випадкове пошкодження каналів зв'язку	внутрішня		+	+
Ненавмисне виключення обладнання або зміна режимів роботи програм	внутрішня		+	+
Випадкова пошкодження носіїв інформації	внутрішня		+	+
Використання ПЗ, яке може нанести шкоду роботі системі	внутрішня		+	+
Випадковий запуск програм, які при некомпетентній роботі завдадуть шкоду роботі системі	внутрішня			+
Випадкове розголошення конфіденційної інформації 3-м лицям	внутрішня		+	+
Розголошення, передача, втрата атрибутів доступу до системи	внутрішня		+	+
Халатне ставлення співробітниками до правил при роботі з системою	внутрішня		+	+
Навмисні загрози	внутрішня			
Фізичне спотворення системи	внутрішня			+
Виключення чи припинення роботи систем функціонування	внутрішня			+
Вербування співробітників	зовнішня		+	+
Викрадення носіїв інформації	зовнішня	+	+	+
Несанкціоноване копіювання	зовнішня	+	+	
Несанкціоноване використання ПК співробітників	зовнішня	+	+	+
Незаконне отримання паролів, ключів або інших реквізитів доступу, для отримання доступу під іменем співробітника	зовнішня	+	+	+
Навмисне встановлення програмних закладок, вірусів, жучків	зовнішня	+	+	+
Незаконне підключення до ліній передачі даних	зовнішня	+	+	+

Рисунок 2.1 – Потенційні загрози для АРМК

Модель вторгнення також представлена у вигляді таблиці. Мета моделі вторгнення – оцінити та визначити місцезнаходження потенційного зловмисника на основі його рівня знань. Критеріями оцінки є: категорія порушника, мотив, рівень знань та доступність. Рівні поділяються на 4 бали, де 1 відповідає найменш потенційному порушнику, а 4 – найбільш потенційному порушнику [20].

Найбільш критичними і небезпечними загрозами для АРМК є:

– викрадення документів і носіїв інформації, що містять конфіденційну інформацію;

– відмова і відмова обладнання АРМК;

– пошкодження обладнання, спричинене стихійними лихами;

– загроза навмисної зміни або видалення співробітниками конфіденційної інформації;

– зловживання програмним і апаратним забезпеченням;

– загроза несанкціонованого доступу до програм АРМК і даних сторонніх осіб.

Рекомендується класифікувати порушників відповідно до ступеня можливостей [21]:

– перший рівень визначає найнижчий рівень діалогових опцій з АС – можливість виконання набору завдань (програм), що реалізують раніше надані функції обробки інформації;

– другий рівень залежить від можливості створення і запуску користувальницьких програм з новими функціями обробки інформації;

– третій рівень залежить від здатності контролювати роботу АС, тобто впливати на базове програмне забезпечення системи і склад і конфігурацію її апаратного забезпечення;

– четвертий рівень залежить від повного спектру навичок тих, хто займається розробкою, впровадженням, експлуатацією та обслуговуванням програмного та апаратного забезпечення АС, інтегрувати власні пристрої з новими функціями обробки інформації в АС.

Порушник – це людина, яка ненавмисно, через незнання, навмисно, зловмисно або іншим чином, використання різних можливостей, методів і засобів, спроб проведення операції, яка призвела або може призвести до порушення інформаційних характеристик, викладених у політиці безпеки [22]. Модель порушника відображає його поточні і потенційні здібності, апріорні знання, час і місце дії і т. д. Розроблена модель загроз представлена у Додатку І.

2.2 Розробка політики безпеки інформації в автоматизованій системі

Етап розробки політики безпеки інформації передбачає вивчення об’єкта, на якому буде розроблятися КСЗІ. При цьому необхідно уточнити модель загроз, модель потенційного порушника та аналіз ризиків, що виконується на основі попередніх етапів.

Політика безпеки для автоматизованого робочого місця керівника підприємства має свою специфіку у порівняні з іншими системами. АРМ має доступ до критично важливої інформації і розроблена політика безпеки повинна визначати правила та процедури, які спрямовані на захист інформації [23].

Під політикою інформаційної безпеки слід розуміти сукупність вимог, правил, обмежень, рекомендацій тощо, що регламентують порядок обробки інформації та спрямовані на захист інформації від певних загроз. Термін «політика безпеки» може застосовуватися до автоматизованої системи, її окремих компонентів, сервісу безпеки, що надається системою, тощо. Політика інформаційної безпеки в автоматизованій системі є частиною загальної політики безпеки організації і повинна приймати її основні принципи [24].

Отже, політика інформаційної безпеки АРМК є частиною загальної політики безпеки організації і може включати, зокрема, положення державної політики захисту інформації. Для кожного з них політика інформаційної безпеки може бути індивідуальною, залежно від використовуваних технологій обробки

інформації, характеристик операційної системи, фізичного середовища та багатьох інших факторів [24]. Розроблена політика безпеки представлена у Додатку К.

У політиці безпеки слід вказати ресурси АС, що підлягають захисту, і, зокрема, категорії інформації, що обробляється в АС. Слід сформулювати основні загрози для операційної системи, персоналу та інформації різних категорій та вимоги щодо захисту від цих загроз. У рамках глобальної політики інформаційної безпеки АС повинні існувати керівні принципи для забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Відповідальність співробітників за виконання положень плану безпеки повинна бути персоналізованою.

Технологія обробки інформації, моделі вторгнень і загроз, характеристики операційної системи, фізичне середовище та інші фактори повинні бути враховані при розробці політики безпеки. В автоматизованих системах може бути реалізовано багато різних політик безпеки, які суттєво різняться між собою.

Політика, спрямована на забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, повинна бути невід'ємною частиною загальної політики безпеки автоматизованих систем [25].

Політика безпеки повинна охоплювати: інформацію (рівень критичності ресурсів автоматизованої системи), взаємодію об'єктів (правила, гарантії, відповідальність за захист інформації) та сферу застосування (які компоненти автоматизованої системи підпадають під дію політики безпеки, а які ні).

Політика безпеки повинна бути написана таким чином, щоб не вимагати частих змін (потреба в частих змінах є ознакою надмірної деталізації, наприклад, не завжди доречно вказувати назву або конкретну версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, таких як правові, морально-етичні норми, організаційні (адміністративні), фізичні та технічні (апаратні та програмні) заходи, а також

визначати правила та порядок використання кожного з цих видів заходів в автоматизованій системі [26].

Політика безпеки має бути розроблена таким чином, щоб її не потрібно було часто змінювати (необхідність частих змін свідчить про надмірну конкретизацію; наприклад, не завжди доцільно вказувати конкретне ім'я або версію програмного продукту).

Концепція безпеки має передбачати використання всіх можливих заходів щодо захисту інформації, наприклад, правових, моральних та етичних норм, організаційних (адміністративних), фізичних і технічних (апаратних і програмних) заходів, а також заходів безпеки.

Основними принципами на яких базується політика безпеки є [21]:

– системності;

– комплексності;

– неперервності захисту;

– достатності механізмів і заходів захисту та їхньої адекватності загрозам;

– гнучкості керування системою захисту, простоти і зручності її використання;

– відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою низки методів, засобів і прийомів, які в сукупності складають метод. Метод передбачає певну послідовність дій, що ґрунтується на конкретному плані. Методи можуть значно відрізнятися і залежать від типу діяльності, в якій вони використовуються, та сфери їх застосування.

Опис і класифікація методів важливі для аналізу стану інформаційної безпеки. Для ефективного захисту системи управління необхідно спочатку описати, а потім класифікувати різні типи загроз і небезпек, ризиків і викликів, і відповідно сформулювати систему заходів щодо управління ними.

Серед найпоширеніших методів аналізу стану інформаційної безпеки є методи причинно-наслідкового аналізу. Ці методи виявляють причинно-наслідкові зв'язки між загрозами, ризиками, викликами та небезпеками, шукають причини, що стали джерелом та реалізацією певних небезпек, і розробляють заходи щодо протидії їм. До методів дослідження причинно-наслідкових зв'язків належать: метод подібності, метод відмінностей, комбінація методів подібності та відмінностей, метод супутніх змін та залишковий метод [26].

Вибір методів аналізу стану інформаційної безпеки залежить від конкретного рівня та сфери діяльності організації захисту. Залежно від загрози можна виділити різні рівні загрози та рівні захисту. У галузі інформаційної безпеки, як правило є такі рівні: фізичний, програмно-апаратний, управління, технологічний, користувацький, мережевий та процесний.

При оцінці здатності комп'ютерної системи захищати оброблювану інформацію від несанкціонованого доступу враховуються два типи вимог:

– вимоги до функцій захисту (послуг безпеки);

– вимоги до засобів захисту.

Для цілей цих критеріїв в комп’ютерній системі розглядається як набір функціональних сервісів. Кожен сервіс – це набір функцій, які дозволяють протистояти певній кількості загроз. Кожна послуга може включати декілька рівнів. Чим вищий рівень сервісу, тим повніший захист від певного типу загроз. Рівні послуг є ієрархічними з точки зору повноти захисту, але не обов'язково є точною підмножиною один одного. Рівні починаються з першого і збільшуються до n, де n є унікальним для кожного типу послуг [27].

Функціональні критерії поділені на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів [27].

Перша група описує конфіденційність. Загрози, що виникають внаслідок несанкціонованого доступу до інформації, є загрозами конфіденційності. Якщо вам потрібно обмежити можливість вивчення інформації сторонніми, зверніться

до розділу «Критерії конфіденційності», щоб знайти відповідні сервіси. У цьому розділі описані такі послуги: конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність обміну [28].

Друга група описує цілісність. Загрози, пов'язані з несанкціонованою модифікацією інформації, є загрозами цілісності. Якщо необхідно обмежити можливість модифікації інформації, слід звернутися до відповідних послуг у розділі, присвяченому критеріям цілісності. У цьому розділі описані такі сервіси: довірена цілісність, адміністративна цілісність, зворотний обмін та обмінна цілісність[28].

Третя група описує доступність. Загрози, пов'язані з перериванням можливості використання IT-систем або інформації, що обробляється, становлять загрози доступності. Якщо існує потреба у захисті від відмови в доступі або помилок, слід проконсультуватися з відповідними службами в розділі "Критерії доступності". У цьому розділі описані наступні послуги: використання ресурсів, відмовостійкість, гаряча заміна та аварійне відновлення [28].

Четверта група описує спостережність. Ідентифікація та контроль дій користувачів і працездатності комп'ютерної системи охоплюються послугами спостережуваності та працездатності. Якщо є потреба у перевірці дій користувача або законності доступу та здатності системи безпеки виконувати свої функції, відповідні сервіси слід шукати в розділі "Критерії спостережуваності". У цьому розділі описані такі сервіси: реєстрація, ідентифікація та автентифікація, довірений канал, розподіл обов'язків, цілісність комплексу безпеки, самотестування, автентифікація обміну, автентифікація (неспростування) відправника, автентифікація (неспростування) одержувача [28].

Загроза несанкціонованого проникнення в систему включає всі види несанкціонованого доступу, такі як підробка для доступу, зловживання паролями, спроби працювати від імені іншої особи, несанкціоноване використання носіїв інформації, перехоплення повідомлень в каналах зв'язку, вірусні атаки тощо. Існує

ризик ненавмисних змін через помилки програмного забезпечення, апаратні збої, помилки персоналу та користувачів тощо. Затримка або погіршення якості обслуговування може призвести до втрати коштів через штрафні санкції і, перш за все, до втрати довіри, наприклад, довіри до банківської системи.

2.3 Розробка плану захисту інформації в автоматизованій системі

Служба захисту інформації – це підрозділ організації, метою якого є забезпечення захисту інформації шляхом керування комплексною системою захисту. Проте, для розроблюваної КСЗІ не передбачено створення окремого підрозділу СЗІ, а призначено відповідальних осіб за реалізацію ключових організаційних та організаційно-технічних заходів з утворення та забезпечення роботи КСЗІ. Здійснюють свою роботу відповідальні особи у відповідності з планами робіт, а підставою для розробки даних планів є План захисту інформації в автоматизованій системі [29].

Для забезпечення ефективного захисту АС розробляють план захисту інформації для організації – набір документів, згідно до яких здійснюється організація захисту інформації на всіх етапах життєвого циклу автоматизованої системи, а саме [29]:

- класифікація інформації автоматизованої системи;
- загальний опис компонентів автоматизованої системи;
- технології розробки інформації в автоматизованої системи;
- модель загроз автоматизованої системи.

План захисту інформаційної безпеки автоматизованої системи – це сукупність документів, які організовують захист інформації на всіх етапах життєвого циклу автоматизованої системи. В окремих випадках план забезпечення інформаційної безпеки автоматизованої системи може бути створений в одному документі [30]. Розроблений План захисту інформації представлений у Додатку Б.

План захисту інформаційної безпеки автоматизованої системи готується на основі аналізу технології обробки інформації, аналізу ризиків та сформульованої політики інформаційної безпеки. План захисту визначає та документально оформлює мету захисту інформації в автоматизованій системі, найважливіші завдання захисту, загальні правила обробки інформації в автоматизованій системі, призначення структури та функціонування КСЗІ та заходи щодо захисту інформації. У плані захисту повинен бути визначений склад автоматизованої системи, перелік оброблюваних даних, технологія обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації тощо на певний момент часу.

План захисту повинен регулярно переглядатися і в разі необхідності до нього вносяться зміни.

Зміни до плану захисту повинні бути затверджені на тому ж рівні і в тому ж порядку, що і основний документ [30].

План захисту є обов'язковим документом для автоматизованих систем, в яких обробляється інформація, що становить державну або іншу передбачену законом таємницю, таємна інформація, інформація, що належить до державних інформаційних ресурсів, або інформація, необхідність захисту якої передбачена законом.

Склад і зміст плану захисту для цих автоматизованих систем встановлюються правилами забезпечення режиму секретності при обробці інформації, що становить державну таємницю, в автоматизованих системах та правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

У планах також необхідно передбачити наступні заходи [30]:

– разові – заходи, які виконуються лише раз і у разі необхідності їх повторення повинно бути прийнятне відповідне рішення;

– постійно виконувані – заходи, які необхідно виконувати неперервно або дискретно у випадковий чи заданий час;

– періодично виконувані – заходи, які виконуються у відповідно заданий час;

– виконувані за необхідності – заходи, які виконуються у разі здійснення або появи змін в АС чи у зовнішньому середовищі.

Основними видами планів робіт можна виділити наступні [30]:

– календарний план – план щодо реалізації заходів з проектування, впровадження, оцінки, впровадження, супроводу, експлуатації КСЗІ та інші питання;

– план заходів оперативного реагування на інциденти та непередбачувані ситуації та поновлення роботи АС;

– поточний план робіт – план робіт на місяць, квартал та рік;

– перспективний план розвитку та удосконалення питань захисту інформації до 5 років;

– план заходів забезпечення безпеки інформації під час виконання важливих робіт, при нарадах, укладеннях договорів, угод і т.д.;

– бізнес-план створення та функціонування КСЗІ.

Плани робіт мають складатися відповідальною особою після дискусійного обговорення з усіма причетними до діяльності КСЗІ стосовно організаційно-технічних питань, а також мають затверджуватися відповідною особою Це або керівник організації, або ж відповідальний за впровадження комплексної системи захисту інформації.

План захисту повинен містити такі розділи, як:

– завдання захисту інформації в АС;

– класифікація інформації, що обробляється в АС;

– опис компонентів АС та технології обробки інформації;

– загрози для інформації в АС;

– політика безпеки інформації в АС;

– система документів з забезпечення захисту інформації в АС.

На основі Плану захисту необхідно також розробити календарний план робіт з захисту інформації в АРМК.

2.4 Розробка технічного завдання на створення комплексної системи захисту інформації

Технічне завдання на КСЗІ є основним організаційно-технічним документом для проведення робіт із забезпечення безпеки інформації в системі [31]. Даний документ містить в собі усі вихідні дані з усіх документів. Зокрема даний документ місить мету, призначення, завдання комплексної системи захисту інформації, а також назву автоматизованої системи.

Технічне завдання на КСЗІ складається відповідно до вимог до функціонального складу та порядку розроблення і впровадження технічних засобів, призначених для забезпечення безпеки інформації під час її обробки в автоматизованій системі. Також зазначаються вимоги до організаційних, фізичних та інших заходів захисту.

Вихідними даними для розробки технічного завдання на КСЗІ є функціональний профіль захищеності АС від порушників та вимоги до захисту інформації від витоку технічними каналами [32].

Функціональний профіль захищеності інформації в конкретній допоміжній системі може бути визначений в результаті аналізу загроз та оцінки ризиків або обраний виходячи з класу автоматизованої системи згідно з НД ТЗІ 2.5-005-99 [32].

Вимоги до захисту інформації від технічного витоку встановлюються на підставі нормативних документів з технічного захисту інформації, які визначають стандарти захисту інформації від технічного витоку та порядок проведення відповідних робіт. Вибір функціонального профілю захищеності та вимоги до показників захищеності інформації від технічного витоку обґрунтовуються в технічному завданні [32].

Технічне завдання є обов'язковим документом для проведення експертизи відповідності автоматизованої системи встановленим вимогам. Робота з погодження проєкту технічного завдання на КСЗІ в автоматизованій системі

здійснюється спільно розробником технічного завдання та замовником. Розроблене технічне завдання представлене у Додатку В.

Технічне завдання повинно оформлюватися відповідно до ДСТУ та містити такі основні підрозділи [32]:

– загальні відомості;
– мета і призначення КСЗІ;
– загальна характеристика АС та умов її функціонування;
– вимоги до КСЗІ;
– вимоги до складу проєктної та експлуатаційної документації;
– етапи виконання робіт;
– порядок внесення змін і доповнень до ТЗ;
– порядок проведення випробувань КСЗІ.

Загальні відомості – це основна інформація про автоматизовану систему, яка містить: повну назву та умовне позначення КСЗІ, шифр, реквізити, замовника та виконавця, перелік документів на основі яких створюється КСЗІ, терміни роботи, угоди про фінансування робіт, про оформлення та подання результатів. У приватного підприємства «SBS» фінансування проєктування КСЗІ здійснюватиметься за власні кошти.

Мета та призначення КСЗІ – вказується мета створення КСЗІ в АС, її функціональне призначення та особливості застосування. Необхідно вказати, на основі яких нормативно-правових актів та інших нормативних документів регламентується порядок захисту інформації в АС [32].

Загальна характеристика АС та умов її функціонування – підрозділ, який визначає моменти, що безпосередньо впливають на безпеку інформації в той час, коли вона обробляється в АС, а також загальні вимоги які необхідно дотримуватися під час реалізації захисту інформації. У даному розділі важливо вказати клас автоматизованої системи, в даному випадку це АС класу «1» – одномашинний однокористувачевий комплекс, тобто одна машина для однієї людини. Загальна характеристика АС визначає перелік і склад обладнання,

технічне та програмне забезпечення, технічні характеристика каналів зв’язку, категорію інформації, гриф секретності, характеристику персоналу, опис фізичного середовища, фізичні параметри компонентів АС, загальну технічну характеристику автоматизованої системи, особливості функціонування, тобто, режим роботи без відключення живлення, надання машинного часу, режимні заходи у приміщенні, потенційні загрози інформації [32].

Вимоги до комплексної системи захисту інформації – підрозділ у якому описуються вимоги до КСЗІ в різних частинах захисту, зокрема таких, як захист від несанкціонованого доступу та від витоку технічними каналами. Вимоги до комплексної системи захисту інформації автоматизованої системи в частині захисту від нерозголошення інформації визначаються відповідно до НД ТЗІ 2.5-004-99. Відповідно до цього документу, при оцінці захищеності КС необхідно враховувати два типи вимог: вимоги, що стосуються засобів (послуг) захисту, та вимоги, що стосуються рівня гарантій. Таким чином, ТЗ на КСЗІ повинне включати ці два типи вимог. Що ж стосується технічних каналів, то необхідно сформулювати загальні вимоги до об'єктів захисту (компонентів автоматизованої системи) та визначити засоби захисту і способи їх використання (наприклад, вимоги щодо захисту повинні реалізовуватися без екранування приміщень, активні засоби повинні використовуватися тільки для захисту інформації на головному сервері автоматизованої системи тощо). Також потрібно навести перелік нормативно-методичних документів, на основі яких необхідно проводити роботи із захисту інформації від витоку технічними засобами [32].

Вимоги до КЗСІ є одним з найважливіших пунктів розробки технічного завдання. Найважливішою інформацією даного розділу є функціональний профіль захищеності. Профіль може бути обраний з профілів, описаних у НД ТЗІ 2.5-005-99, або визначений як упорядкований набір рівнів обслуговування відповідно до вимог цього документа. Для автоматизованої системи відповідно до вимог було обрано перелік функціональних профілів захищеності, що зображено у таблиці 2.1.

Таблиця 2.1. – Перелік функціональних профілів захищеності

Позначення	Вимоги	Пояснення
КД-2	Конфіденційність даних 2-го рівня	Забезпечує захист від несанкціонованого доступу до даних
КО-1	Контроль обчислювальних ресурсів 1-го рівня	Забезпечує захист від несанкціонованого використання обчислювальних ресурсів
ЦД-1	Цілісність даних 1-го рівня	Забезпечує захист від несанкціонованого змінення даних
ДВ-1	Доступність даних 1-го рівня	Забезпечує захист від несанкціонованого блокування доступу до даних
НР-2	Незаперечність 2-го рівня	Забезпечує можливість довести факт виконання дії
НИ-2	Нерозголошення 2-го рівня	Забезпечує захист інформації від розголошення
НК-1	Контроль несанкціонованих копіювань 1-го рівня	Забезпечує захист від несанкціонованого копіювання даних
НО-1	Необхідність знання 1-го рівня	Забезпечує захист інформації, що вимагає знання певної інформації для доступу
НЦ-1	Контроль цілісності програмного забезпечення 1-го рівня	Забезпечує захист від несанкціонованого змінення програмного забезпечення

Профілі безпеки визначають дозволи, доступ і користувачів, доданих системним адміністратором. Працювати з системою може лише один користувач.

Антивірусна програма, встановлена в автоматизованій системі, повинна бути налаштована на перевірку цілісності інформації на наявність вірусів. Кожен користувач матиме різний доступ, наприклад, тільки системний адміністратор або керівник відділу інформаційної безпеки може змінювати та видаляти інформацію. Всі користувачі, авторизовані відповідно до політики безпеки, матимуть доступ на читання, але не до всіх файлів. Повторне використання об'єктів дозволяє користувачеві відкрити потрібний йому об'єкт у первісному вигляді, навіть якщо інший користувач змінив його відповідно до своїх потреб.

Вимоги до складу проєктної та експлуатаційної документації – у цьому розділі наведено перелік проєктної та експлуатаційної документації, що підлягає розробці в процесі створення КСЗІ в АС. Склад обов'язкової проєктної та експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких здійснюється розробка (зокрема, вимогами критеріїв відповідного рівня гарантій). Повний перелік обов'язкової документації визначається розробником КСЗІ та узгоджується із замовником.

Визначимо етапи виконання робіт. Процес створення комплексної системи захисту інформації (КСЗІ) поділяється на три етапи: підготовка, проєктування та розробка, тестування та введення в експлуатацію. Кожна фаза складається з підфаз. На етапі підготовки виконуються роботи, описані раніше. Етап проєктування та розробки включає вибір та модернізацію засобів захисту, розробку архітектури захищеної обробки інформації та стандартних інтерфейсів. Етап тестування і передачі включає організацію тестів і можливу розробку спеціального обладнання, програмного забезпечення та документації. Кожна фаза має свій власний графік з кінцевими термінами виконання робіт та звітування перед замовником [32].

Порядок внесення змін і доповнень до ТЗ – у даному підрозділі потрібно описати зміни до затвердженого технічного завдання на створення КСЗІ в АС, необхідність яких виявлена під час виконання робіт. Оформлюються окремим додатком, який погоджується та затверджується в тому ж порядку та на тому ж

рівні, що й основний документ. Додаток до ТЗ на створення КСЗІ в автоматизованій системі складається зі вступної частини та змінених підрозділів. У вступній частині зазначається причина видання доповнення. У змінених підрозділах зазначаються номери та зміст змінених пунктів, а також нові або вилучені пункти [32].

Порядок проведення випробувань КСЗІ – підрозділ описує процес тестування комплексної системи захисту інформації (підсистеми, компонента). Для кожного виду випробувань розробляється «Програма та методика випробувань», яка затверджується в установленому порядку. Замовник призначає комісію з проведення випробувань, умови та обладнання якої зазначаються в документі. Після завершення випробувань складається перелік документів, що підтверджують результати [32].

Субпідрядник за погодженням із замовником надсилає проект технічного завдання на КСЗІ в автоматизованій системі до Адміністрації Держспецзв'язку для погодження. У разі необхідності на період перевірки адміністрація Держспецзв’язку може запросити додаткові документи, які їм будуть необхідні, наприклад план захисту інформації.

2.5 Висновки

У даному розділі було розроблено основну документацію до комплексної системи захисту інформації для автоматизовано робочого місця керівника приватного підприємства «SBS».

В першому підрозділі було визначено перелік потенційних загроз та найбільш критичних для АРМК, одними з таких загроз є: викрадення документів і носіїв інформації, відмова в обслуговуванні чи пошкодження обладнання АРМК, халатне ставлення чи вербування співробітників і т.д. В результаті даного підрозділу було розроблено модель загроз.

Ще одним важливим документом який було розроблено це політика безпеки інформації в АС. В другому підрозділі було визначено основні принципи, на яких повинна базуватися політика безпеки.

Для забезпечення ефективної роботи над створення КСЗІ визначено і розроблено план захисту інформації в якому описується класифікація інформації в АС, описуються компоненти АС та визначається перелік загроз для інформації.

І основний документ який було розроблено це технічне завдання на створення КСЗІ. Даний документ містить в собі усі вихідні дані з усіх необхідних документів, зокрема такий пункт, як вимоги до КСЗІ, де було визначено функціональний профіль захищеності інформації. Повний зміст розроблених документів наведено у додатках. В наступному розділі буде здійснюватися введення в дію системи, що розробляється.

3 ВВЕДЕННЯ В ДІЮ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Розробка техноробочого проєкту створення комплексної системи захисту інформації

Техноробочий проєкт КСЗІ в АС розробляється на підставі та у відповідності до ТЗ на створення КСЗІ в АС. На цьому етапі розробляється перелік документів, в якому описується як саме створюється система, її експлуатація, а також модернізація КСЗІ в АС.

Техноробочий проект включає такі етапи, як розробка технічного проекту і розробка робочого проекту [33].

Розробка робочого проекту здійснюється відповідно до стандарту ДСТУ 34.601-90. Згідно з цим документом допускається об'єднання стадій «Розробка технічного проекту» і «Розробка робочого проекту» в одну стадію «Технологічний і робочий проект».

Основні положення до робочого проєктування [34]:

– підготовка робочого проєкту або робочих креслень повинна здійснюватися відповідно до умов навколишнього середовища, в якому знаходиться будівля;

– метою робочого проєкту є визначення основної конструктивної схеми системи;

– основним принципом складання робочого проєкту є його максимальна відповідність нормативним документам, які повинні бути враховані при розробці КСЗІ, та технічному завданню на проєктування цієї КСЗІ;

– при проєктуванні установок, побудованих за типовими або багаторазово використовуваними моделями, проєктування може здійснюватися в одну стадію – це робоче проектування;

– після затвердження технічного завдання на проектування проектна організація, якщо можливі різні проектні рішення, встановлює основні положення робочого проекту, обсяг якого залежить від складності запропонованої системи.

Ключові положення узгоджуються із замовником та постачальником і лягають в основу робочого проекту.

Розробка проектних рішень системи здійснюється для реалізації функціональних можливостей робочих станцій та організації навчального процесу за цим напрямом на робочих станціях АС встановлена операційна система Windows 10.

Ця операційна система була обрана, виходячи з апаратно-програмного забезпечення та специфіки організації навчальної діяльності.

Основними функціями операційної системи в організації є:

– ідентифікація користувачів;

– розмежування прав доступу відповідно до навичок та обов'язків користувачів;

– апаратна підтримка локальної мережі;

– взаємодія між кінцевими робочими станціями;

– моніторинг та аудит активності користувачів та мережі на конкретній робочій станції;

– організація доступу до навчального обладнання та прикладних програм.

Доступ до локальної мережі в аудиторії є незалежним, оскільки забезпечується комутатором, розташованим у сусідній аудиторії.

Безпека даних на робочих станціях забезпечується антивірусним захистом у вигляді програмного забезпечення ESET Protect Essential.

Розробка документації на АС КСЗІ проектується згідно з визначеним в пункті 4 технічним завданням та відповідно до переліку нормативних документів, які враховуються при створенні КСЗІ [34].

На етапі розробки технічного проекту необхідно розробити загальні проекті рішення для реалізації вимог ТЗ на КСЗІ, рішення щодо структури КСЗІ, її

алгоритмів функціонування та умов використання засобів захисту, рішень щодо архітектури КЗЗ та механізмів реалізації, визначення профілем послуг безпеки інформації [34].

Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до рівня гарантій реалізації послуг безпеки.

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

Розроблений техноробочий проєкт містить такі розділи, як:

1. Відомості щодо проєктної документації для техноробочого проєкту КСЗІ. У вигляді таблиці описується яка документація необхідна для техноробочого проєкту. Розроблена таблиця зображена на рисунку 3.1.

№	Найменування	К-сть арк.
1	Перелік відомостей, що відносяться до конфіденційної інформації ПП «SBS» та якій надається гриф обмеження доступу	
2	Акт визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на ОІД	
3	Акт обстеження середовищ функціонування АРМК на ОІД ПП «SBS»	
4	Модель загроз для інформації, яка планується до циркуляції в АРМК на ОІД ПП «SBS»	
5	Політика безпеки інформації, яка циркулює в АРМК на ОІД ПП «SBS»	
6	План захисту інформації	
7	АРМК ПП «SBS». Комплексна СЗІ. ТЗ	

Рисунок 3.1 – Відомість проєктної документації

2. Відомість щодо експлуатаційної документації для техноробочого проєкту КСЗІ. У даному пункті необхідно зазначити наявність паспорта формуляра, представлено на рисунку 3.2.

№	Найменування	К-сть арк.
1	Паспорт-формуляр на АРМК ПП «SBS»	

Рисунок 3.2 – Відомість експлуатаційної документації

3. Пояснювальна записка для техноробочого проєкту КСЗІ. У даному розділі необхідно зазначити такі відомості, як: загальні відомості, основні технічні рішення та заходи, що використовуються при створення КСЗІ, показники захищеності, порядок проведення тестування, порядок адаптації, схеми розміщення АС, заходи, які проводяться перед введенням у дію КСЗІ та порядок проведення експертизи КСЗІ.

На етапі створення робочого проекту виконується опис порядку функціонування АС та настанови щодо забезпечення цього порядку обслуговуючим персонал і користувачами, порядку супроводження КСЗІ впродовж життєвого АС.

Робоча документація містить детальні рішення щодо реалізації технічного проекту КСЗІ для забезпечення управління КСЗІ та її компонентів, а також документацію, необхідну для проведення випробувань, введення в експлуатацію та верифікації КСЗІ [36].

Здійснюється розроблення засобів захисту інформації, що визначається розробленням документації на створення засобів захисту інформації та/або технічних вимог (технічного завдання) на їх розроблення або адаптацією кінцевих продуктів до умов функціонування КСЗІ. Розроблення засобів захисту інформації від НСД здійснюється відповідно до НД ТЗІ 3.6-001.

Робоча документація систем технічного захисту інформації від витоку технічними каналами повинна містити схеми розташування ІКС, кабельних

систем, мереж електроживлення та систем заземлення, які виконуються відповідно до вимог нормативних документів ТР ЕОТ-95, ТР ТЗІ-ПЕМВН-95, П-2, П-3, НД ТЗІ-3.3-001, НД ТЗІ-2.4-007, СВТР-78 [36].

При цьому повинні враховуватися умови їх розміщення та мінімально допустимі відстані між цими пристроями і ТЗ (пристрої зв'язку, системи і пристрої кондиціонування повітря, сигналізації, електроосвітлення, радіомовлення, хронометражу тощо, розташовані в приміщеннях, де встановлено обладнання ІКС, і в суміжних з ними приміщеннях). Зазначені умови розміщення та мінімально допустимі відстані можна знайти в експлуатаційній документації, що додається до сертифікованих ТЗІ.

Якщо засоби ІКС, що використовуються в межах ІКС, не мають атестатів відповідності технічним вимогам із захисту інформації, мінімально допустимі відстані та інші умови розміщення цих засобів визначаються на підставі результатів їх спеціальних досліджень.

Робоча документація КСЗІ повинна містити опис процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформаційних та матеріальних ресурсів КСЗІ, моніторингу дій користувачів, створення та оновлення баз даних захисту, перевірки цілісності програмного забезпечення та баз даних захисту.

Документація робочого проекту повинна включати вихідні дані для доступу до баз даних безпеки.

Експлуатаційна документація повинна включати опис порядку функціонування КСЗІ та інструкції, що дозволяють обслуговуючому персоналу та користувачам дотримуватися цього порядку, а також порядок обслуговування КСЗІ протягом життєвого циклу АС.

Розроблений технороботчий проєкт представлений у додатку Г.

3.2 Підготовка комплексної системи захисту інформації до введення в дію

Проводиться робота з підготовки організаційної структури та розпорядчих документів, що регламентують діяльність із забезпечення інформаційної безпеки в автоматизованій системі. Створюється КСЗІ, якщо це не було зроблено на попередніх етапах. Зазвичай цю роботу необхідно завершити та затвердити документи, що містяться в плані захисту [38].

Проєкт КСЗІ розробляється на основі та відповідно до технічного завдання на розробку ТЗІ. Під час розроблення проекту КСЗІ обґрунтовуються та приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечують сумісність та взаємодію між різними складовими КСЗІ та різними заходами і методами захисту інформації. Проектування КСЗІ здійснюється на наступних етапах розробки ІТС: ескізний проект, технічний проект та робочий проект [38].

Для всіх стадій розробки проекту КСЗІ склад документації визначається технічним завданням на КСЗІ, види та зміст – ДСТУ 34.201, НД ТЗІ 2.5-004. Якщо проект КСЗІ розробляється відповідно до Закону «Про безпеку та охорону навколишнього середовища», то документація повинна бути підготовлена відповідно до Закону «Про охорону праці». Програмні засоби документуються відповідно до всіх стандартів, в той час як апаратні засоби документуються відповідно до всіх стандартів.

Формуляр є документом технічного захисту інформації, одним з документів, які створюються та надсилаються до Держспецзв'язку на перевірку. На початку формуляру зазначаємо, що відповідальним за ведення паспорту є керівник ПП «SBS», тобто той для кого розробляється КСЗІ. Наступним кроком зазначаємо загальні відомості про об’єкт інформаційної діяльності, а саме що собою являє ОІД, у даному випадку це приміщення керівника ПП «SBS», організація має власну будівлю недалеко від метро з площею 329 кв.м. Також варто зазначити характеристику приміщення: які стіни, їх товщина, матеріал, підлога, стеля, вікна,

двері і т.п. Зазначити і допоміжні технічні засоби, такі як: міський телефон, пожежна сигналізація, заземлення, електропостачання, охоронна сигналізація, опалення тощо та описати як розташовані лінії перед даних засобів відносно об’єкту інформаційної діяльності. Важливо у паспорті зазначити мету створення КСЗІ а АС: дотримання політики інформаційної безпеки, блокування дій пов’язаних з несанкціонованим доступом, підтримка цілісності та доступності важливих даних АРМК, захист інформації від витоку технічними каналами і т.п. Також формуляр повинен містити таблиці про автоматизовану систему та інформацію про раніше створені документи. Структура таблиць включатиме наступну інформацію [39]:

- склад технічних засобів автоматизованої системи;
- склад програмного комплексу ;
- відомості про програмно-технічний комплекс захисту інформації;
- відомості про впровадження, випробування та експлуатацію системи;
- посадові особи, відповідальні за технічне обслуговування;
- посадових осіб, відповідальних за захист;
- акт виконаних робіт;
- атестаційні знаки АС класу 1 ;
- перелік документів з технічного захисту;

Приклад такої таблиці зображений на рисунку 3.3.

Таблиця 7 – Реєстрація проведених робіт

Дата проведення робіт	Найменування технічного засобу та вид проведених робіт	Підстава для проведення робіт	Прізвище та ініціали особи, яка виконувала роботи	Підпис

Рисунок 3.3 – Приклад таблиці з формуляру

Особливу увагу слід приділити забезпеченості програмно-технічними засобами захисту інформації, включно з інформацією про антивірусне програмне забезпечення. В якості антивірусного програмного забезпечення для системи, що розробляється було обрано ESET Protect Essential. Дане антивірусне програмне забезпечення має ряд переваг, серед яких: комплексний захист від вірусів на основі евристичного аналізу, наявність персонального брандмауера, антиспам, антифішинг, низький вплив на продуктивність системи і т.п. Найважливішою перевагою є те, що дане ПЗ має експертний висновок, тобто є сертифіковане Державною службою спеціального зв'язку та захисту інформації України, а це означає, що використання такого продукту відповідає всім нормативним документам, які визначають вимоги щодо засобів технічного захисту інформації. Ліцензія на дане програмне забезпечення зображено на рисунку 3.4.

ЕКСПЕРТНИЙ ВИСНОВОК

Програмний продукт антивірусного захисту інформації ESET Endpoint Protection Standart розроблений компанією «ESET»

За результатами експертизи встановлено, що програмний продукт антивірусного захисту інформації ESET Endpoint Protection Standart, у складі: ESET Endpoint Antivirus для Windows версії 6.X з системою централізованого керування антивірусним захистом корпоративних мереж ESET Remote Administrator версії 6.X, ESET File Security для Microsoft Windows Server версії 6.X, ESET File Security для Linux/BSD/Solaris версії 4.X, ESET Endpoint Security для Android версії 3.X,

який наданий на експертизу ADEON SK s.r.o.,

Špitálska ulica číslo 55, 811 01, Bratislava, Slovenská republika

відповідає

Директор
ТОВ «ЕФІТ ТЕХНОЛОДЖІС»

Однак, важливо не пропустити жодного кроку в період підготовки до придбання антивірусної програми. Для того, щоб отримувати щоденні антивірусні оновлення (обов'язкова умова комплексної системи захисту інформації), необхідно зареєструватися в Центрі антивірусного захисту інформації. Для реєстрації необхідно заповнити документ, який називається «реєстраційна картка», що містить інформацію про власника системи або особу, відповідальну за технічний захист, IP-адресу, адресу електронної пошти та номер телефону. Оновлення антивірусного програмного забезпечення публікуються на офіційному вебсайті ЦАЗІ і їх необхідно завантажувати та встановлювати щодня. Форма заповнюється на кожному етапі проектування, впровадження та тестування комплексної системи захисту інформації, і ця інформація додається протягом усього процесу.

Форма є своєрідним додатком до технічного завдання і містить таблиці для заповнення відсутньої інформації: номери замовлень, серійні номери об'єктів захисту, перелік компонентів, що входять до складу об'єктів, тощо.

Розроблений формуляр представлений у Додатку Д.

3.3 Попередні випробування комплексної системи захисту інформації в автоматизованій системі

Метою попередніх випробувань є перевірка працездатності комплексної системи захисту інформації та визначення можливості його допуску до дослідної експлуатації. Під час випробувань перевіряється працездатність КСЗІ та його відповідність вимогам технічної специфікації [40].

Попередні випробування проводяться відповідно до програми та методики випробувань. Програма та методика випробувань розробляються розробником в ЕА та затверджуються замовником. Програма випробувань, методика випробувань та протоколи випробувань розробляються та оформлюються відповідно до вимог РД 50-34.698.

Попередні випробування організовуються замовником та проводяться розробником КСЗІ в АС спільно із замовником. Замовник призначає комісію для проведення попередніх випробувань. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються протоколом та актом, який містить висновок щодо можливості допуску КСЗІ до випробувань в АС з метою тестування.

У протоколі попередніх випробувань варто зазначити наступні пункти:

1. Відповідальні особи за здійснення попереднього випробування КСЗІ. Для розробленої системи такими людьми виступали заступник керівника ПП «SBS» Кимчук В.К та безпосередньо керівник ПП «SBS» Верещук А.С.

2. Вихідні дані, тобто навести перелік усіх документів які є важливими для проведення випробувань, тобто усі розроблені в процесі документи.

3. Методика проведення випробувань, тобто необхідно зазначити відповідно до якого документу здійснюватиметься програма та методи випробувань.

4. Результати попередніх випробувань, тобто має бути детально описано про перевірку середовища функціонування АС, перевірку експлуатаційної документації, перевірку заходів із захисту інформації з обмеженим доступом від витоку технічними каналами, перевірку щодо блокування усіх можливих шляхів несанкціонованого доступу до елементів АС та до ІзОД та перевірку щодо реалізації заходів щодо перешкоджання загроз ІзОД в АС.

5. Висновок відповідальних осіб про готовність КСЗІ.

Програма та методика випробувань КСЗІ в АС на етапі дослідної експлуатації має на меті визначити технічні дані, що підлягають перевірці під час випробувань компонентів АС, а також процедуру випробувань та методи контролю.

Програма та методика випробувань КСЗІ в АС на етапі дослідної експлуатації призначена для визначення даних, які забезпечать отримання та перевірку проектних рішень, виявлення причин відмов, визначення якості робіт,

визначення якості функціонування системи (підсистеми), перевірку відповідності системи вимогам безпеки, а також визначення тривалості та методики випробувань.

Перелік перевірок, які повинні бути включені в програму тестування, включає в себе [40]:

– відповідність системи вимогам ТЗ;

– повнота системи;

– повнота та якість документації;

– повнота, відповідний склад та якість програмного забезпечення та програмної документації;

– кількість та кваліфікація обслуговуючого персоналу;

– ступінь відповідності вимогам, що стосуються функціонального призначення системи;

– можливість проведення аудиту системи;

– відповідність вимогам техніки безпеки, пожежної безпеки, виробничої санітарії та ергономіки;

– функціонування системи за допомогою програмного забезпечення.

Метою попереднього тестування є перевірка працездатності КСЗІ та визначення можливості її випуску в дослідну експлуатацію.

Попередні випробування КСЗІ в АС проводяться відповідно до нормативних документів, які були враховані при створенні КСЗІ в АС.

Попередні випробування проводяться у випробувальному приміщенні – керівника приватного підприємства «SBS». Тривалість випробувань визначається замовником і не може бути меншою за час, необхідний для проведення повного тестування КСЗІ.

Організація, що проводить випробування, визначається замовником.

Попередні випробування включають детальне тестування апаратних і програмних засобів для перевірки відповідності заздалегідь визначеному технічному завданню.

Програмні та апаратні компоненти КСЗІ в складі операційної системи повинні забезпечувати захист інформації відповідно до всіх критеріїв, визначених у функціональному профілі захищеності: { КД-2, КО-1, ЦД-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1}.

Етапи тестування полягають у перевірці здатності апаратних і програмних компонентів працювати в нештатних (екстремальних) ситуаціях шляхом піддавання їх високим навантаженням протягом тривалого періоду часу з метою перевірки їх стійкості. Особливу увагу слід приділити тестуванню локальної мережі для перевірки її здатності підтримувати робочий стан у періоди високої мережевої активності, а також засобам інформаційної безпеки, зокрема, антивірусному захисту та Системі захисту базової та оборонної інформації. Остання повинна бути протестована на стійкість до численних атак як зсередини, так і ззовні системи [40].

Умови проведення випробувань визначаються замовником і повинні включати присутність затверджених експертів організації на всіх етапах випробувань.

Вимоги до технічного обслуговування ООВ повинні бути визначені як необхідні та достатні для забезпечення повної функціональності системи.

Попередні випробування проводяться тільки відповідно до програми та методики, розробленої для проведення попередніх випробувань КСЗІ в АС.

До участі у випробуваннях повинні залучатися тільки висококваліфіковані фахівці з відповідним обладнанням та навичками.

На всіх етапах проведення випробувань обов'язковою є перевірка організації випробувань затвердженими експертами організації-замовника.

Методи випробувань визначаються замовником, виходячи з технічних можливостей постачальника.

Акт приймання КСЗІ засвідчує, що розроблена система пройшла усі випробування і дотримана усіх прописаних вимог відповідно до технічного завдання. Розроблений акт приймання КСЗІ для АРМК ПП «SBS» представлений на рисунку 3.5.

«**ЗАТВЕРДЖУЮ**»
Керівник приватного
підприємства «SBS»
_____ Верещук А.С.
«16» травня 2024 р.

АКТ
приймання КСЗІ АРМК ПП «SBS»

Комісія у складі:
голови: керівник підприємства «SBS» Верещук А.С.;
члена: заступник керівника ПП «SBS» Кимчук В.К.

Було проведено приймання у дослідну експлуатацію КСЗІ яка створена в АРМК класу 1 ПП «SBS».

Під час роботи комісії встановлено:

1. КСЗІ в АРМК створена відповідно вимог документу «АРМК керівника ПП «SBS». КСЗІ. Технічне завдання», а саме:

вимог до захисту інформації від витоку технічними каналами;

вимог до захисту інформації від НСД до інформації в АРМК, компонентів АРМК та на об'єкт інформаційної діяльності в цілому;

вимог щодо унеможливлення загроз інформації, які можуть виникати під час циркуляції в АРМК.

2. КСЗІ в АРМК пройшла попередні випробування та здійснює захист інформації в АРМК

3. Комплект експлуатаційних документів КСЗІ в АРМК є достатнім щодо можливості прийняття КСЗІ у дослідну експлуатацію.

Висновок:

Враховуючи вище зазначену інформацію доцільно провести дослідну експлуатацію КСЗІ в АРМК.

Голова комісії:
Керівник ПП «SBS» Верещук А.С.

Члени комісії:
Заступник керівника ПП «SBS» Кимчук В.К.

Рисунок 3.5 – Акт приймання КСЗІ

Вимоги до випробувань визначаються функціональним профілем безпеки, який включає ряд критеріїв, спрямованих на забезпечення інформаційної безпеки в ОС, а саме {КД-2, КО-1, ЦД-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1}.

В результаті проведення усіх вище описаних етапів в результаті визначено, що КСЗІ може бути застосована для проведення дослідної експлуатації, тому що виконує наступні вимоги:

– відбувається впровадження визначеної політики безпеки інформації в АС;

– забезпечується захист ІзОД від витоку технічними каналами;

– запобігають загрозам інформації з обмеженим доступом, що обробляється в автоматизованій системі;

– забезпечується дотримання конфіденційності під час роботи;

– забезпечується цілісність критичних ресурсів АРМК;

– здійснюється керування та контроль за засобами захисту КСЗІ;

– здійснюється блокування несанкціонованого доступу, як і до компонентів АРМК, так і до інформації, яка циркулює.

За результатами випробувань складається звіт про попередні випробування КСЗІ в автоматизованій системі, який включає інформацію про всі етапи випробувань із зазначенням використаних методів випробувань, вимог, результатів та висновків щодо стану КСЗІ та продовження випробувань і експлуатації [40].

3.4 Висновки

У даному розділі описувалась підготовка до введення в дію комплексної системи захисту інформації і в результаті розроблено відповідну документацію. Першим документом є технороботчий проєкт, який складався на підставі та у відповідності до вже розробленого у другому розділі технічного завдання. У даному документі було описано як саме створювалась система, як відбувалась її експлуатація, а також модернізація. Для введення в дію КСЗІ було розроблено

формуляр – документ, який містить таблиці про АС та інформацію про раніше створені документи. Даний документ надсилається для адміністрації Держспецзв’язку на перевірку. І останнім етапом було здійснено попередні випробування КСЗІ в автоматизованому робочому місці керівника підприємства та визначено дієвість розробленої системи.

ВИСНОВКИ

В рамках підготовки до кваліфікаційної роботи були виконані наступні завдання:

– обстеження об'єктів для підготовки до розробки КСЗІ;

– розробка політик, планів та специфікацій для аудиторії АС;

– підготовка до введення в експлуатацію КСЗІ.

В результаті виконання кваліфікаційної роботи було розроблено КСЗІ для ПП «SBS». Було проаналізовано стан захищеності інформації, визначено потенційні загрози для інформації та розроблено перелік заходів для забезпечення захисту інформації та як результат розроблено супровідну документацію до КСЗІ. Серед таких документів є:

– план захисту інформації:

– технічне завдання;

– технороботчий проєкт;

– формуляр;

– наказ про затвердження переліку відомостей;

– акт визначення ступеня обмеження інформації;

– акт обстеження об’єкту інформаційної діяльності;

– модель загроз;

– політика безпеки;

– генеральний план;

– ситуаційний план.

І як результат було впроваджено КСЗІ для АРМК ПП «SBS» в дію.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Автоматизоване робоче місце фахівця, основні функції та компоненти. URL: https://pidru4niki.com/1374121047746/informatika/avtomatizovane_roboche_mistse_fahivtsya_osnovni_funktsiyi_komponenti (дата звернення: 20.02.2024)

2. Що таке комплексна система захисту інформації (КСЗІ). URL: https://zahyst-ua.com/korisna-informaciya/shho-take-kompleksna-sistema-zahistu-informacii-kszi/ (дата звернення: 20.04.2024)

3. Закон України "Про інформацію". URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 25.02.2024)

4. Закон України "Про захист інформації в інформаційно-комунікаційних системах". URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (Дата зверення:25.02.2024)

5. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі». URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 26.02.2024)

6. НД ТЗІ 3.7-001-99: «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». URL:https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення: 26.02.2024)

7. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». URL:https://www.tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf (дата звернення: 27.02.2024)

8. Автоматизоване робоче місце. URL: https://www.pharmencyclopedia.com.ua/article/8892/avtomatizovane-roboche-misce (дата звернення: 27.02.2024)

9. Комплексна система захисту інформації (КСЗІ). URL: http://surl.li/ukrth (дата звернення: 28.02.2024)

10. Типове робоче місце користувача інформаційно-телекомунікаційної системи Єдиного державного реєстру транспортних засобів. URL: https://www.mezhova.otg.dp.gov.ua/storage/app/uploads/public/616/686/693/61668669312aa648013395.pdf (дата звернення: 28.02.2024)

11. Комплексна система захисту інформації. URL: https://uh.ua/ua/solutions-services/kszi.html (дата звернення: 28.02.2024)

12. Тимчасове положення про категоріювання об’єктів. URL:https://zakon.rada.gov.ua/rada/show/v0035267-95#Text (дата звернення: 10.03.2024)

13. 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". URL:https://tzi.com.ua/downloads/1.6-005-2013.pdf (дата звернення: 11.03.2024)

14. Закон України "Про державну таємницю". URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 11.03.2024)

15. Категоріювання об’єктів інформаційно-телекомунікаційної системи. URL: https://duikt.edu.ua/ua/news-1-569-9828-kategoriyuvannya-obektiv-informaciyno-telekomunikaciynoi-sistemi_kafedra-cistem-tehnichnogo-zahistu-informacii?lang=ua&act=view&page=1&category=569&id=9828&sys_link=kategoriyuvannya-obektiv-informaciyno-telekomunikaciynoi-sistemi_kafedra-cistem-tehnichnogo-zahistu-informacii. (дата звернення: 15.03.2024)

16. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. URL:https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 17.03.2024)

17. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. URL:https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 18.03.2024)

18. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. URL:https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 18.03.2024)

19. Етапи побудови КСЗІ. URL: https://zahyst-ua.com/korisna-informaciya/etapi-pobudovi-kszi/ (дата звернення: 27.03.2024)

20. Розділ. Моделі загроз та моделі порушника. URL: https://e-tk.lntu.edu.ua/pluginfile.php/25376/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2017.pdf (дата звернення: 27.03.2024)

21. Розробка моделі загроз інформації та вибір методі в засобів технічного захисту інформації для об'єкта інформаційної діяльності. URL: https://openarchive.nure.ua/server/api/core/bitstreams/6acd9a3b-b043-49cf-b841-baf79234019c/content (дата звернення: 28.03.2024)

22. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. URL:https://tzi.com.ua/downloads/1.1-005-07.pdf (дата звернення: 29.03.2024)

23. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / Володимир Михайлович Богуш, Володимир Володимирович Богуш, Володимир Дмитрович Бровко, Володимир Петрович Настрадін ; під ред. Володимир Михайлович Богуш. – Київ : Ліра-К, 2020. – 553 с. : табл.

24. Політика інформаційної безпеки. URL: https://kitsoft.ua/ua/politika-informacijnoyi-bezpeki (дата звернення: 01.04.2024)

25. Методи забезпечення інформаційної безпеки URL: https://pidru4niki.com/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki (дата звернення: 01.04.2024)

26. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 04.04.2024)

27. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL:https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 06.04.2024)

28. Метод ідентифікації функціонального профілю захисту. URL: https://www.researchgate.net/publication/370830014_Metod_identifikacii_funkcionalnogo_profilu_zahistu. (дата звернення: 06.04.2024)

29. НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL:https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 13.04.2024)

30. Рекомендації щодо структури та змісту Плану захисту інформації в автоматизованій системі. URL: https://wiki.tntu.edu.ua/Рекомендації_щодо_структури_та_змісту_Плану_захисту_інформації_в_автоматизованій_системі (дата звернення: 13.04.2024)

31. Впровадження КСЗІ. URL: https://www.h-x.technology/ua/services/kszi-implementation-ua (дата звернення: 17.04.2024)

32. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. URL:https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 17.04.2024)

33. Порядок побудови комплексної системи захисту інформації (КСЗІ). URL: https://zahyst-ua.com/poriadok-pobudovy-kompleksnoi-systemy-zakhystu-informatsii-kszi/ (дата звернення: 20.04.2024)

34. Технічний захист інформації. URL: https://infotech.gov.ua/services/technical-protection-of-information (дата звернення: 22.04.2024)

35. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с.

36. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів безпеки від несанкціонованого доступу. URL:https://tzi.com.ua/downloads/3.6-001-2000.pdf (дата звернення: 29.04.2024)

37. Комплексна система захисту інформації. URL: https://uh.ua/ua/solutions-services/kszi.html (дата звернення: 29.04.2024)

38. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL:https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf (дата звернення: 02.05.2024)

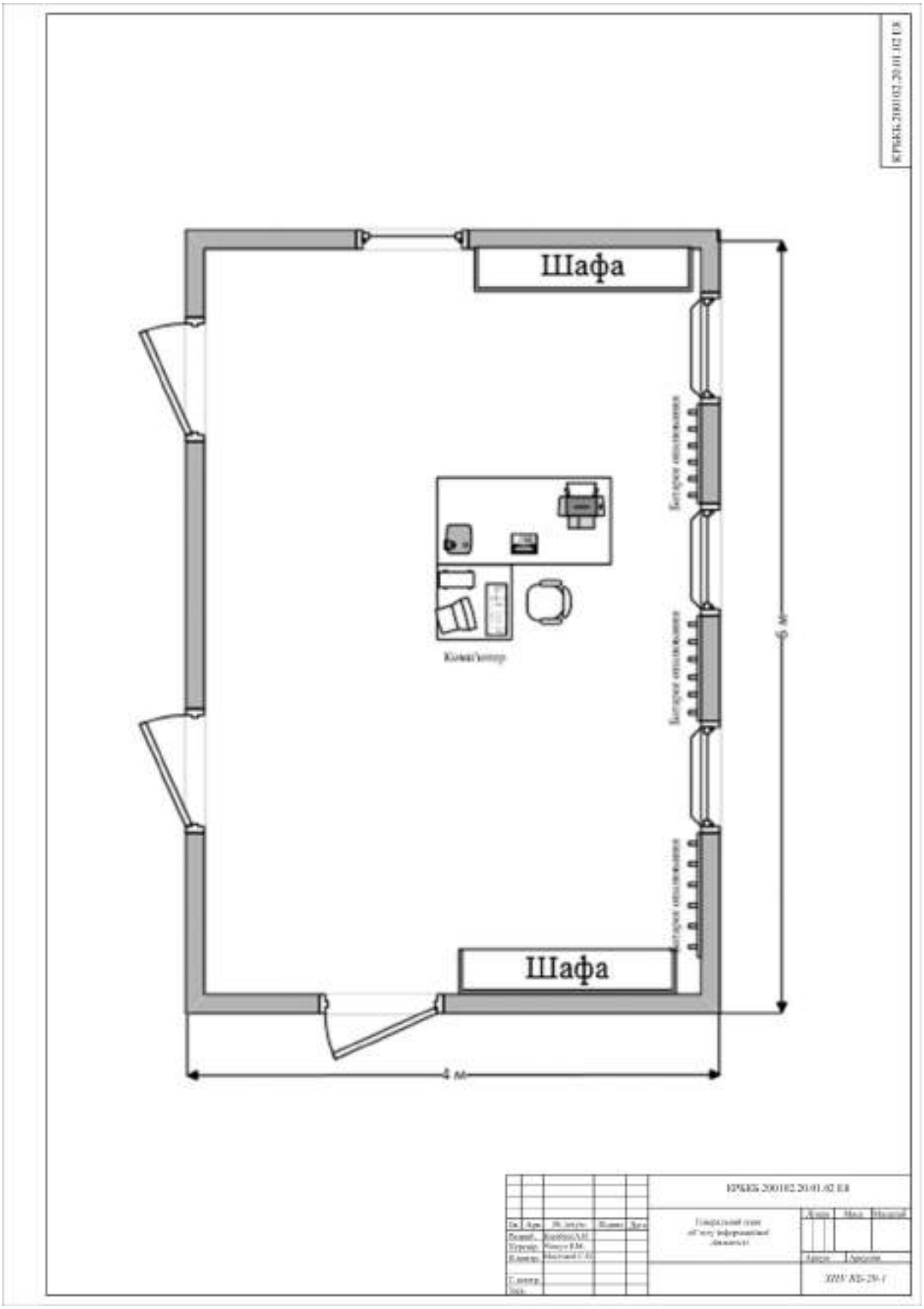
39. Комплексні системи захисту інформації. Методичні вказівки до виконання курсового проєкту / Укладачі: Ткач Ю.М., Семендяй С.М. – Чернігів: Національний університет «Чернігівська політехніка», 2021. –-132 с.

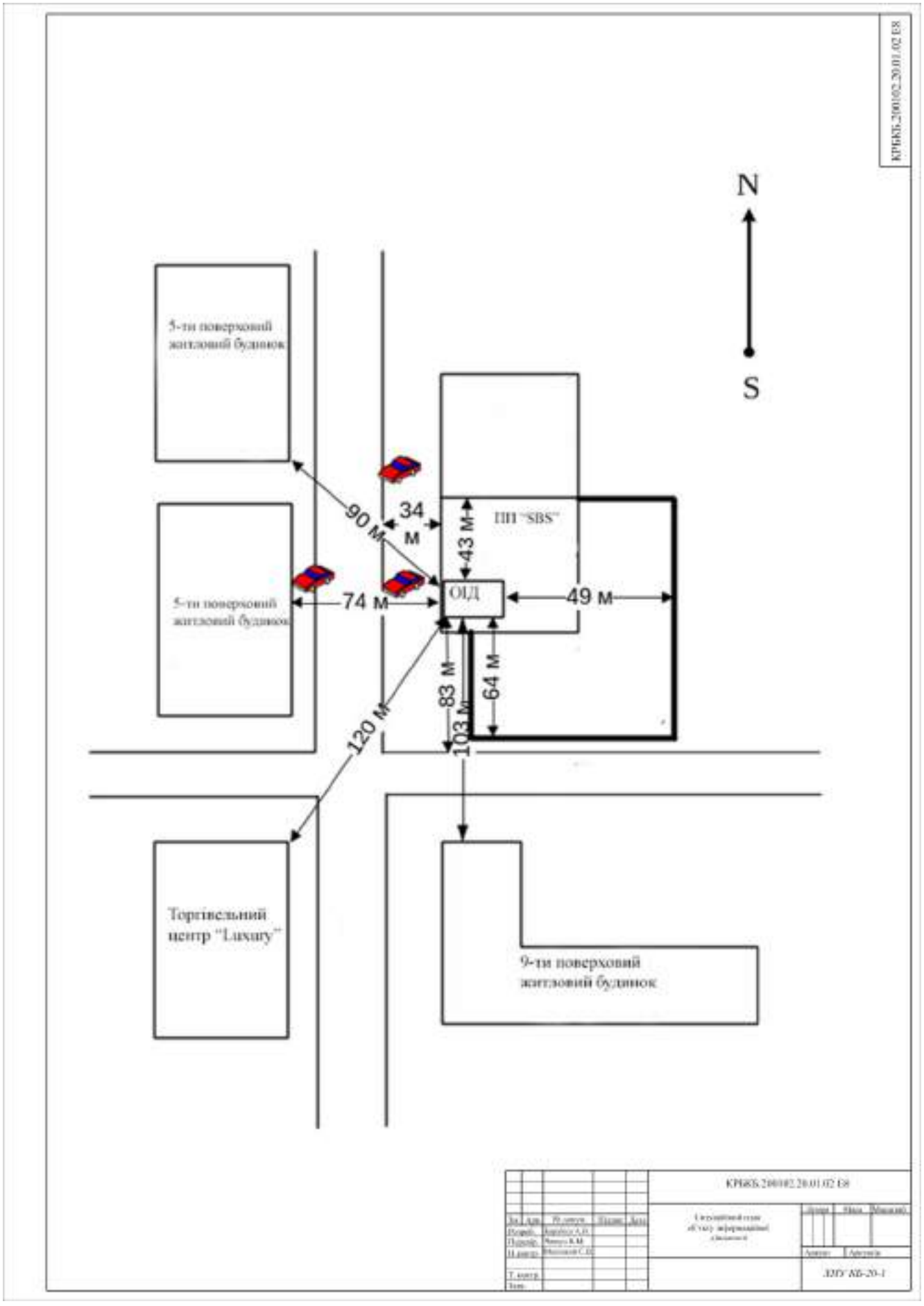
40. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. URL: https://openarchive.nure.ua/server/api/core/bitstreams/23a61da8-bbc5-4d38-a379-393838b41d98/content (дата звернення: 10.05.2024)

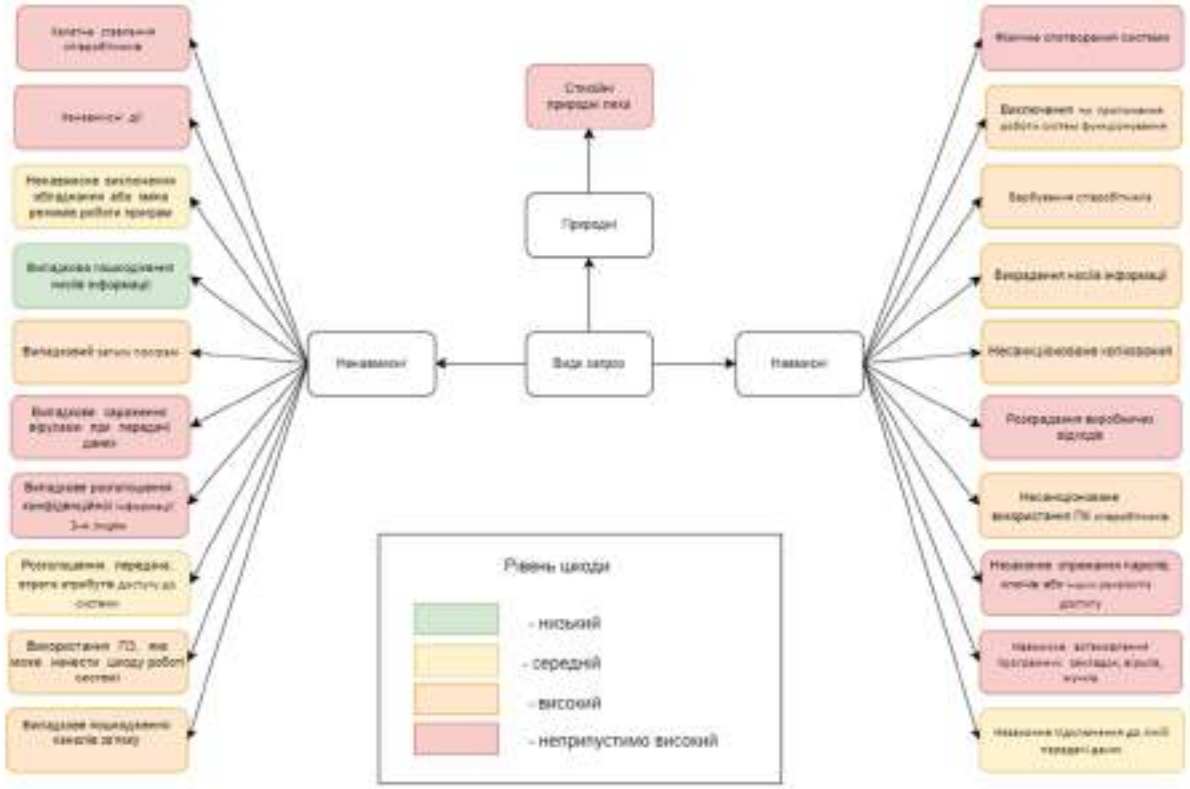
ДОДАТОК А

(обов’язковий)

Копії графічної частини




КРБКБ.280102.20.01.02 Е8
N
S
5-ти поверховий житловий будинок
5-ти поверховий житловий будинок
ТЦ "SBS"
ОЦД
90 м
34 м
74 м
43 м
49 м
83 м
103 м
64 м
120 м
Торгівельний центр "Luxury"
9-ти поверховий житловий будинок
КРБКБ.280102.20.01.02 Е8
Розроб.
Перевір.
Н.контр.
Т.контр.
Затв.
Літера
Маса
Масштаб
Аркуш
Аркушів
ЛПУ КБ-20-1



					КРБКБ200102.20.01.02 ЕЗ	
Зм.	Арк.	№ докум.	Підпис	Дата	Модель загроз	Літера / Маса / Масштаб
Розроб.		Коляда Н.В.				
Перевір.		Ягуда О.М.				Аркуш / Аркушів
Н.контр.		Мостовий С.В.				
Т.контр.						ХНУ КБ-20-1
Затв.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Барабаша Артема Вадимовича
ПІБ здобувача вищої освіти
Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

20.06.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

	Документ		Сумарний збіг по Базі Даних	
ID: 131639 Назва: Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства Додано в БД: 2024-06-19 Автора: Барабаш А.В. Керівники: Чешун В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	70690	1062	2473 (3%)	42 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016376587

Дата перевірки:
19.06.2024 22:14:11 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
19.06.2024 22:57:39 EEST

ID користувача:
100008300

Назва документа: **Барабаш_Диплом_плагіат**

Кількість сторінок: 59 **Кількість слів:** 10283 **Кількість символів:** 82925 **Розмір файлу:** 837.62 KB **ID файлу:** 1016184692

12.7%
Схожість

Найбільша схожість: 3.69% з Інтернет-джерелом (https://er.nau.edu.ua/bitstream/NAU/46565/1/%d0%a4%d0%9a%d0%...

12.5% Джерела з Інтернету | 805 ..... Сторінка 61

2.66% Джерела з Бібліотеки | 55 ..... Сторінка 69

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 1

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства

Автор: Барабаш Артем Вадимович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Керівник: Чешун Віктор Миколайович, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 87,3%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v 15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Барабаш Артем Вадимович

Тема Комплексна система захисту інформації автоматизованого робочого місця керівника підприємства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3 ; кількість сторінок записки 68

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі, відповідно до поставленого завдання, проведене дослідження предметної області, проаналізовано законодавчу базу сфери захисту інформації та проведено обстеження об'єкта інформаційної діяльності. Також спроєктовано модель загроз та порушника, технічне завдання, формуляр та план захисту. Описано політики безпеки автоматизованого робочого місця. У підсумку розроблено технічну документацію і необхідні проєктні рішення комплексної системи захисту інформації автоматизованого робочого місця керівника підприємства

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі повністю виконано поставлене завдання як у теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У розділі 1 розглянуті існуючі рішення в побудові КСЗІ, вимоги нормативно-правового забезпечення захисту інформації (проаналізовані закони та положення). Описано загальні відомості про досліджуваний об'єкт, а саме університет. У розділі 2 розроблені розпорядчі накази, акти та положення. Спроєктовано формуляр, модель загроз та порушника, технічне завдання. Розроблено план захисту інформації. Налаштовано політики безпеки в автоматизованій системі. У розділі 3 розглянуто основні етапи введення КСЗІ в експлуатацію, здійснено розробку техноробочого проєкту комплексної системи захисту інформації. Описано підготовку комплексної системи захисту інформації до введення в дію, попередні випробування комплексної системи захисту інформації в автоматизованій системі.

4. Позитивні сторони роботи Робота базується на детальному аналізі вимог нормативних документів та законів України, що регулюють питання проєктування, впровадження і супроводу комплексних систем захисту інформації. Кваліфікаційна робота має практичну цінність і орієнтована на вдосконалення захисту інформації на рівні автоматизованого робочого місця керівника підприємства

5. Негативні сторони роботи В роботі не надано опис настроювань політики безпеки автоматизованого робочого місця керівника підприємства на рівні операційної систми та спеціалізованого програмного забезпечення остатньо уваги приділено аналізу технічних характеристик автоматизованої системи класу 1, що підлягає захисту, та деталізації прийнятих проєктних рішень

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень у проєктуванні та супроводі розробленої комплексної системи захисту інформації.

8. Інші зауваження В роботі окремі таблиці представлено як рисунки без обгрунтування доцільності і причин застосування такого способу подання матеріалу

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є «добре»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мішан Віктор Володимирович
доцент кафедри ТМІТ, кандидат технічних наук

« 18 » 06 2024. (підпис)