Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Мельник Мар'яни Миколаївни

на здобуття ступеня вищої освіти Бакалавра

Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 301171.20.01.14 ПЗ

Виконала студентка 4 курсу група КБ-20-1 Мар'яна МЕЛЬНИК
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

12 06 2024 р.

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.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельник Мар'яні Миколаївні

1 Тема роботи комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету

Керівник роботи Чешун Віктор Миколайович

кандидат технічних наук, доцент

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 25.05.2024р

3 Вихідні дані до роботи Створити комплексну систему захисту інформації в в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету, розміщення системи – ауд 4-232

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Огляд існуючих рішень і нормативно-правового забезпечення захисту інформації. Проєктування та впровадження комплексної системи захисту інформації. Вимоги та рекомендації щодо експлуатації комплексної системи захисту інформації: впровадження та супровід системи, політики антивірусного захисту, політики (інструкції) адміністратора та користувачів. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Структура об'єкта захисту. Ситуаційний план. Генеральний план. План-схема політик безпеки

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	
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	
Розробка політик експлуатації і безпеки	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студентка Мар'яна МЕЛЬНИК

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Комплексна система захисту інформації в інформаційно-комунікаційній системі класу 1 Хмельницького національного університету.

Авторка роботи: Мельник Мар'яна Миколаївна.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 72 с., 11 додатків, 14 рис., 2 табл., 40 джерел.

Графічна частина: 3 плакати, 10 презентаційних слайдів.

ЗАХИСТ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНА СИСТЕМА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКИ БЕЗПЕКИ

Мета кваліфікаційної роботи: спроєктувати комплексну систему захисту інформації в автоматизованій системі класу «1», провести комплекс технічних, організаційних та організаційно-технічних заходів, відповідно до вимог законодавства. Спроєктувати документацію з технічного захисту інформації, проаналізувати можливі загрози та порушників, створити відповідну модель загроз та порушників. Спроєктувати план захисту інформації, технічне завдання.

Було 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. Налаштовано політики безпеки автоматизованої системи.

14.06.2024

ABSTRACT

Course project: Complex system of information protection in the information and communication system of class 1 of the Khmelnytskyi National University.

Author of the work: Melnyk Mariana Mykolaivna.

Supervisor: Cheshun Viktor Mykolayovych

Amount: 72 p., 11 appendix, 14 figures, 2 tables, 40 sources.

INFORMATION PROTECTION, AUTOMATED SYSTEM, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, SECURITY POLICIES.

The purpose of the qualification work: to create a complex information protection system in the automated system of class "1", to carry out a complex of technical, organizational and organizational-technical measures, in accordance with the requirements of the law. Develop documentation on technical information protection, analyze possible threats and violators, create an appropriate model of threats and violators. Design an information protection plan, technical task.

A study of the subject area was carried out, the legislative framework of the field of information protection was analyzed and an inspection of the object of information activity was carried out. The model of threats and the violator, the technical task, the form and the protection plan were also designed. Automated system security policies are configured.

14.06.2024

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КСЗІ – комплексна система захисту інформації;

ХНУ – Хмельницький національний університет;

КМУ – Кабінет Міністрів України;

НСД – несанкціонований доступ;

АС – автоматизована система;

СЗІ – служба захисту інформації

ІТС – інформаційно-комунікаційна система;

ПЗ – програмний забезпечення;

ОС – операційна система;

ТЗ – технічне завдання;

КЗЗ – комплекс засобів захисту;

ЦАЗІ – центр антивірусного захисту.

ВСТУП

В умовах постійного розвитку інформаційних технологій та зростаючої загрози кібератак створення, впровадження та ефективна експлуатація КСЗІ стає важливим завданням для організацій будь-якого масштабу. Інформаційні ресурси є ключовим активом бізнесу, державних установ та приватних осіб, тому забезпечення їхньої безпеки, а недопущення несанкціонованого доступу є пріоритетним завданням для інженерів, адміністраторів мереж та спеціалістів з інформаційної безпеки.

КСЗІ – це комплекс технологій, політик, процедур та контрольних механізмів, спрямованих на захист конфіденційності, цілісності та доступності інформації. Вони охоплюють усі аспекти інформаційної безпеки, від захисту від несанкціонованого доступу до забезпечення надійності даних у випадку аварійних ситуацій. КСЗІ використовуються у всіх сферах життя від великих корпорацій та урядових установ до малих бізнесів та приватних осіб.

Ця кваліфікаційна робота спрямована на проєктування процесів створення, впровадження та експлуатації КСЗІ з метою забезпечення високого рівня захисту інформаційних ресурсів. У світлі зростаючої складності та різноманітності загроз важливо розробляти та вдосконалювати методи та засоби захисту, які відповідають сучасним стандартам безпеки.

Робота охоплює аналіз та оцінку поточного стану систем захисту інформації, вибір та розробку відповідних заходів та стратегій захисту, а також практичні аспекти їх впровадження та подальшої експлуатації. Розгляд цих питань відкриває можливості для розробки ефективних заходів захисту, які враховують специфіку діяльності конкретної організації, а саме університету, та її потреби у забезпеченні конфіденційності, цілісності та доступності інформації.

Результати дослідження та практичні рекомендації, які будуть надані в цій роботі, мають на меті сприяти підвищенню ефективності захисту інформаційних ресурсів організацій та забезпеченню їхньої стійкості до сучасних кіберзагроз.

Актуальність роботи полягає в автоматизації процесів захисту інформації в установах та на підприємствах в реальному часі є полегшенням в роботі та пришвидшенні продуктивності виконання завдань. Проте, швидкий розвиток технологій рівнозначнй швидкому розвитку загроз, а методи, які використовують зловмисники вдосконалюються з кожним днем. Розробка КСЗІ є необхідною для запобігання несанкціонованого доступу. В умовах військового стану інформаційна війна є одним із методів, що використовують сторони. Витік важливої інформації має бути неможливим на усіх рівнях держави, приватних підприємств та установ, що безпосередньо готують спеціалістів, які можуть впливати на хід цієї війни.

Метою роботи є спроєктувати комплексну систему захисту інформації в ХНУ та, в результаті, отримати основні документи та забезпечити дієвість методів захисту інформації в університеті, створити службу захисту інформації, що регулюватиме стан захищеності інформації.

Основні завдання:

- проаналізувати закони України та вимоги до КСЗІ відповідно цих законів;
- провести аналіз захищеності інформації в університеті;
- розробити основні документи – накази, положення, акти;
- сформувати вимоги до системи;
- розробити моделі загроз та порушника відповідно до всіх вимог;
- розглянути план захисту ХНУ та політики безпеки.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ І НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Класифікація систем захисту інформації

Існує декілька можливих рішень в проєктуванні систем захисту. В комплексі вони виконують свої функції та запобігають несанкціонованого доступу порушниками.

Централізовані системи управління захистом, що надають єдину точку керування всіма аспектами захисту інформації, мають завдання забезпечувати централізоване керування політиками безпеки, моніторинг та аналіз подій. Також вони надають можливість оцінювати та відстежувати ризики.

Системи виявлення і запобігання вторгнень виявляють та реагують на аномалії або вторгнення в систему. Вони можуть виявляти вторгнення в реальному часі або на основі аналізу журналів.

Системи контролю доступу це системи, які визначають, хто має доступ до конкретних ресурсів чи об'єктів в системі, що дозволяє адміністраторам установлювати та контролювати права доступу.

Системи антивірусного захисту чи антивірусні програми призначені для виявлення та нейтралізації шкідливих програм та вірусів на комп'ютерах користувачів і забезпечують захист шляхом перевірки файлової системи та інших джерел на наявність потенційних загроз.

Шифрування даних забезпечує приватність та безпеку інформації, яка передається або зберігається. Цей метод забезпечує захист даних навіть у випадку їхнього непередбаченого перехоплення, забезпечуючи недоступність інформації для несанкціонованих осіб.

Системи ідентифікації та автентифікації гарантують захист від несанкціонованого доступу до системи і дозволяють відстежувати дії користувачів за часом користування ресурсами підзахистної системи та реалізовувати обмеження користувацьких прав доступу.

1.2 Аналіз законодавчої бази України в сфері захисту інформації

Інформація – це основа будь-якої держави, компанії, закладу, спілки, організації окремої людини або особи. Захист інформації є вимогою держави. Усі дії, що відбуваються під час створення КСЗІ, мають підпорядковуватись відповідним законам та нормативно-правовим актам.

Для того, щоб розібратись з інформацією, її видами та обов'язками сторін, базовим є закон України «Про інформацію».

Закон України «Про інформацію» встановлює основні правила одержання, поширення, зберігання та захисту інформації. Визначає інформаційні відносини та статус кожного, регулює доступ та допуск до інформації [1].

Якщо ви є власником компанії, у вас зберігаються данні працівників чи можливо дані, що належать державі, то ви є власником системи. Чи є ви володільцем системи допомагає розібратись закон України «Про захист інформації в інформаційно-комунікаційних системах». Цей закон регулює відносини у сфері захисту інформації [2]. Важливим пунктом закону є відповідальність.

Усі правила та відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречування, тощо, регламентує закон України «Про державну таємницю». У цьому законі можна знайти, що саме може відноситись до державної таємниці у різних сферах; як саме віднести ту чи іншу інформацію до державної; інформацію про звід відомостей та строки віднесення такої інформації; доступи та допуски з усіма аспектами взаємодії; детальний опис охорони державної таємниці; обов'язки сторін та обмеження. Особливо важливо розуміти відповідальність за порушення або розголос такої інформації, що також міститься у законні [3].

Права та свободи людини починаються з її особистої інформації. До персональних даних відноситься будь-яка важлива інформація про людину. Ім'я, телефон, пошта, банківський рахунок, та багато іншої інформації належить тільки

одній особі – фізичній чи юридичній особі та, головне, володільцю цієї інформації. Дані, що відносяться до персональних, використовуються майже в усіх сферах життя, проте поки ви керуєте цією інформацією, ви самі захищаєте свої дані. Ви влаштовуєтесь на роботу та надаєте свої персональні дані роботодавцю та, з того моменту, зберігати конфіденційність ваших даних зобов'язаний і роботодавець, конкретно на своїй території. Правові відносини, що пов'язані з персональними даними регулює закон України «Про захист персональних даних». Цим законом визначається й регулюється, що є даними, їх захист, обробка відповідно до прав та свобод людини.

Закони, що потрібно опрацювати та важливо знати для використання інформації і, головне, для створення КСЗІ вже є в переліку. Наступними, не менш важливими, є постанови КМУ.

У цій роботі зустрічатиметься дві постанови КМУ.

Постанова КМУ №373 містить правила захисту інформації в системах. Цими правилами визначено загальні вимоги та організаційні засади [5], інформацію, що за законом має охоронятись в різних системах: інформаційних, електронних комунікаційних та інформаційно-комунікаційних. Це один з важливих документів захисту інформації, оскільки тут ми можемо ознайомитись з термінами автентифікації та ідентифікації, криптографічного захисту, витоку технічними каналами та несанкціонованих дій з використанням комп'ютерних вірусів.

У цій постанові згадується про обов'язкову реєстрацію, що відповідає реєстрації усіх подій, які відбуваються в системі, включно зі спробами порушення правил користування політиками безпеки.

Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [6] – це інструкція, що регламентує вимоги до усіх дій з інформацією для службового користування. На що варто звернути увагу – це пункт «облік електронних носіїв». Флеш-носії, вінчестери, жорсткі та гнучкі диски, касети та усі електроні носії мають бути занесені до журналу обліку таких

носіїв. Лише занесені до журналу носії можуть використовуватись в автоматизованій системі, де зберігається інформація для службового користування та будь-яка інформація, що захищається законом.

Більш деталізовані технічні інструкції для створення, введення та успішної реалізації КСЗІ можна знайти в нормативно-правових актах галузі технічного захисту інформації.

НД ТЗІ 3.7-003-05 – це організаційний документ, що визначає порядок виконання робіт з технічного захисту інформації. Містить позначення та скорочення, що використовуються, виділяє основні етапи створення КСЗІ [7].

ДСТУ 3396.1-96 – це державний стандарт України в сфері технічного захисту інформації [8], що представляє собою вимоги до порядку проведення робіт. Цей документ допускає можливі варіанти захисту інформації з мінімальними затратами відповідно до інформації, що обробляється на АС.

НД ТЗІ 1.4-001-2000 – типове положення про службу захисту інформації в АС [9]. Це документ, що визначає вимоги до оформлення положення про службу захисту. Він містить інструкцію оформлення документу, що має бути в організації, підприємстві, закладі, тощо. Цей документ є так званою «рибою», а саме документом, що можуть використовувати заклади, доповнюючи його своїми даними, залишивши структуру документу, та основні, загальні положення, не дублюючи та додумуючи власними силами. Це досить корисний документ, що може полегшити роботу над організаційними документами організації чи підприємства.

НД ТЗІ 2.5-004-99 – цей документ містить критерії оцінки захищеності інформації [10]. З допомогою цього документу можна написати вдалий та точний профіль захищеності. Критерії поділяються на чотири пункти, а саме: конфіденційність, цілісність, доступність та критерій спостереженості. Ці чотири критерії мають послуги, які можна використати або якими можна знехтувати. Також документ містить детальне пояснення кожної послуги в додатку. Тому для

того, щоб правильно підібрати послуги, не потрібно звертатись до експерта з технічного захисту та простіше контролювати дії в розробці КСЗІ.

Визначити класифікацію, до якої відповідає система, можна з допомогою НД ТЗІ 2.5-005-99 [11]. Класів АС є три: перший, другий та третій. Залежить клас від самої АС: це однокористувачевий одномашинний комплекс чи глобальна мережа. Класифікаія системи є простою: один комп'ютер без доступу до мережі – це клас 1; декілька чи багато комп'ютерів, зв'язані кабелем, але без доступу до мережі – це клас 2; багато комп'ютерів зв'язані глобальною мережею – це клас 3. Відповідно до класу в кожної системи різний захист. Важко уявити, що на один відокремлений комп'ютер та на сотню комп'ютерів з доступом до мережі буде однаковий захист, оскільки загрози зовсім різні та можливості зловмисників, на жаль, теж.

Також важливою складовою документу є стандартні профілі захищеності. У попередньому документі ми вже зустрічали послуги, які у цьому документі зібрані в вже готові профілі, що можна використовувати. Перевага вже готового профілю в тому, що ви точно не помилитесь в його формуванні та такий профіль підтвердить Державна служба спеціального зв'язку. Мінус в тому, що не він може не містити усіх потрібних послуг, або навпаки містити ті, які реалізовувати не має потреби. Проте, в випадку, якщо ви вирішили сформувати профіль самі, його потрібно пояснити, деталізуючи для чого і з якою метою ви вибрали ту чи іншу функцію. Плюси власного профілю – це наявність усіх потрібних послуг, що реалізувати простіше. Вагомим мінусом є обов'язок пояснень, що не завжди супроводжується успіхом.

НД ТЗІ 3.7-001-99[12] – нормативний документ, що містить методичні вказівки з розробки технічного завдання. Почнемо з того, що технічне завдання один із засадних документів в комплексній системі захисту інформації. Саме з допомогою цього документу організація або отримує позитивний експертний висновок, або ж негативну відповідь. Тому дуже важливо сформувати цей

документ правильно. У нормативному документі зібрані вимоги до розділів, зміст технічного завдання, приклад побудови.

НД ТЗІ 1.6-005-2013 – положення про категоріювання об’єктів. Одним з організаційних етапів розробки КСЗІ є категоріювання об’єкту. Категорій є чотири та залежать вони від інформації, що обробляється на об’єкті, а саме ступенем доступу. Відповідно інформація, що не містить державної таємниці встановлюється четвертою категорію, а інформація з грифом «особливої важливості» отримає першу категорію. Категоріювання здійснюється комісією, що формується власником системи. Це можуть бути співробітники організації чи закладу, які не зацікавленні в компрометації результатів перевірки. В залежності від ситуації, категоріювання може бути первинним, черговим та позачерговим.[13] Чергове здійснюється не рідше ніж один раз на п’ять років. Позачергове у випадку зміни інформації.

1.3 Обстеження об’єкту інформаційної діяльності

ХНУ – це високорівневий навчальний та науковий заклад, що розташований у місті Хмельницькому.

Університет є навчально-науковою структурою з підрозділів, факультетів і кафедр, які пропонують широкий спектр навчальних програм у різних галузях, таких як гуманітарні науки, природничі науки, соціальні науки, технічні науки тощо. Ознайомитись з структурою (факультетами та кафедрами) університету можна за схемою на рисунку 1.1.

Університет складається з 5 корпусів та навчально виробничого корпусу, студмістечка та іншої інфраструктури, що забезпечує зручність студентам. Карта-схема Хмельницького національного університету розміщена на рисунку 1.2.

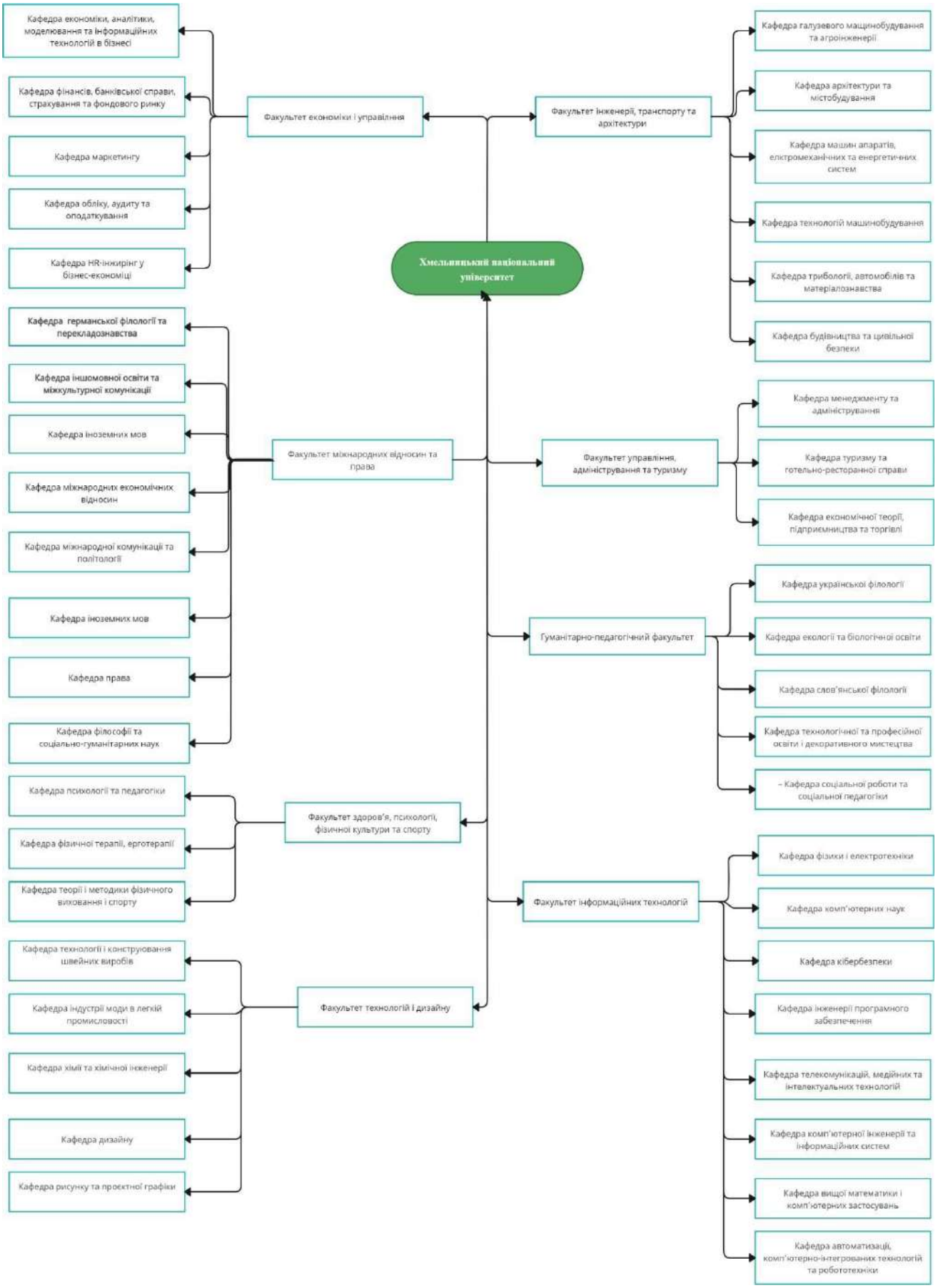


Рисунок 1.1 – Структурна схема Хмельницького національного університету

Рисунок 1.2 – Карта-схема Хмельницького національного університету[14]

Юридична адреса ХНУ: м. Хмельницький, вул. Інститутська, 11, 29016, Україна.

Контактна інформація [14]:

– основний контактний номер телефону (приймальна ректора): (0382) 67-02-76;
– факс: (0382) 67-42-65
– електронна пошта: centr@khmnu.edu.ua
– веб-сайт: https://khmnu.edu.ua/

Університет – це місце, де отримують навички, які в майбутньому можуть забезпечити світ важливими професіями.

Аналіз факультетів та кафедр забезпечує розуміння напрямків та професійних здобутків університету, полегшує розуміння інформаційних ресурсів, що використовує університет, та обсяг можливостей студентів, а саме створення різних проєктів. Огляд схеми університету дає можливість ознайомитись з особливостями будівель, їх місцями розташування та сусідніми приміщеннями, схеми розміщення комунікацій та можливості входу в приміщення, де розташовується АС.

Аудиторії позначаються трьома інформативними цифровими десятковими значеннями, де перше значення – це номер корпусу, друге – поверху та третє значення позначає номер аудиторії. Як приклад, номер аудиторії 4-203 означає, що аудиторія знаходиться в четвертому корпусі, на другому поверсі, аудиторія – 03.

Кожна аудиторія має свій власний електричний щиток живлення приладів, що забезпечує захист університету від перебоїв напруги, можливого загоряння через проводку кафедри та університету.

Базою розміщення АС є кафедра кібербезпеки ХНУ.

Штат співробітників кафедри кібербезпеки складається з 13-ти людей. Проте, штат університету набагато більший, як і діючих викладачів. Окрім штатних співробітників кафедри, в університеті, згідно з даними, що опубліковані на сайті Хмельницького національного університету відповідно до даних 2023 та

2024 навчального року [14], загалом працюють 912 осіб. Контингент студентів складає 6683 особи.

До штату кафедри кібербезпеки відносяться завідувач кафедри Кльоц Юрій Павлович, що є відповідальною особою за захист інформації в університеті, та викладачі кафедри.

Кафедра кібербезпеки забезпечує напрямок, що навчає спеціалістів з захисту автоматизованого світу. Тому захист даних цієї кафедри є важливим аспектом у житті університету.

1.4 Постановка задачі

Університет здійснює вагомий вклад в розвиток держави, готуючи спеціалістів в різних напрямах, проводить різні дослідницькі роботи та дозволяє студентам ще за часів навчання отримати не тільки знання, а й досвід реальної праці. Інформація, що зберігається та обробляється в університеті поділяється на таку:

– інформація для службового користування, що належить до державних інформаційних ресурсів;

– відкрита інформація офіційного сайту університету, що має охоронятись;

– конфіденційна інформація, а саме персональні дані студентів, штатних працівників та запрошених, позаштатних викладачів та гостей університету, фінансова інформація;

– конфіденційна інформація (фінансова інформація).

Фінансова інформація університету включає:

– бюджетні звіти (доходи, витрати, активи та зобов’язання);

– фінансові звіти (звіт про прибуток і збитки, грошові потоки);

– бюджетні прогнози та плани;

– фінансові договори та угоди (фінансові договори та угоди з іншими організаціями, постачальниками, партнерами);

– фінансові дані студентів (стипендії, кредити, оплата навчання);

– фінансові дані персоналу (фінансові виплати, зарплати, податки, тощо).

Оскільки ці дані містять конфіденційну та чутливу інформацію, її захист від несанкціонованого доступу та зловживань є критично важливим завданням, що може бути вирішено за допомогою КСЗІ . Захист конфіденційної фінансової інформації відповідає не лише захисту приватності та дотриманню вимог законодавства про захист персональних даних, а й важливий для забезпечення фінансової стабільності та довіри до університету з боку студентів, персоналу, фінансових партнерів та громадськості. Доступ до цієї інформації має бути обмеженим та контрольованим, а також має бути забезпечено високий рівень її захисту від несанкціонованого доступу.

Інтелектуальна власність – це об’єкти, які створенні людським розумом та мають комерційну цінність. Захист інтелектуальної власності обов’язковий не тільки з точки зору захисту прав (порушення конфіденційності інформації), а й з точки зору комерції. В університеті такими об’єктами є:

– винаходи, відкриття та розробки, що розроблені в рамках дослідницької роботи університету, які в майбутньому можуть бути запатентовані;

– авторські права, роботи студентів та викладачів, які захищенні авторським правом;

– знаки, логотипи, найменування програм або проєктів, що захищенні як торгові марки;

– технології та знання, які виникають в результаті досліджень та відкриттів університету, що можуть бути визнані інтелектуальною власністю.

Відповідно до вимог законодавства про захист персональних даних, закону України «Про інформацію», «Про державну таємницю» та «Про захист інформації в інформаційно-комунікаційних системах», постанов Кабінету міністрів та інших нормативно правових актів, університет зобов’язаний створити та ввести в

експлуатацію комплексну систему захисту інформації для захисту даних, що існують на об’єкті. Проте, не тільки законодавство України є підставою, для введення КСЗІ. Важливо розуміти, що з прогресом цифрового світу, паралельно активно розвивався і світ кіберзлочинності. Кібератаки можуть погано вплинути на функціонування університету та конфіденційність, що в свою чергу впливає на репутацію університету. Порушення нормального режиму роботи – один з можливих аспектів порушень. Якщо наслідком атаки є витік персональних даних, можлива втрата довіри студенців, працівників, а також фінансових втрат серед вищеназваних суб’єктів. Створення КСЗІ є необхідним для забезпечення конфіденційності, цілісності, доступності інформації, дотримання вимог законодавства, захисту прав та інтересів як університету, так і осіб, що навчаються та працюють тут.

В ХНУ, згідно завдання кваліфікаційної роботи, створюється КСЗІ класу «1», що дає можливість обробляти інформацію для службового користування, має обмежений доступ, але не належить до інформації, що містить державну таємницю.

Потрібно розробити відповідні накази, акти та положення. Спроєктувати модель загроз та порушника, технічне завдання, формуляр, план захисту, генеральний та ситуаційний план.

2 ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Розробка документів технічного захисту першого етапу

Першими формуються такі документи:

– наказ про створення КСЗІ (додаток В);

– наказ про відповідальну особу (в випадку першого створення КСЗІ, якщо КСЗІ на об’єкті вже існує, то дублювати його не потрібно) (додаток А);

– положення, до наказу про відповідальну особу (положення містить правила та обов’язки відповідального, функції, тощо);

– наказ про створення служби захисту інформації (наказ назначає членів СЗІ, що підпорядковуються відповідальній особі) (додаток Б);

– положення СЗІ (функції, правила та обов’язки служби);

– перелік інформації, що підлягає обробленню в ІТС та потребує захисту.

Разом з вже відомою інформацію, можна починати оформлення перших документів, що формують вимоги до КСЗІ. Перший етап супроводжується створенням відповідних наказів, положень та актів. Як приклад, наказ про створення КСЗІ дозволяє почати роботу та визначає закони та акти, якими керується організація.

Насамперед, визначимо ролі. Щоб розуміти, як правильно сформувати вимоги та назначити відповідних людей, потрібно визначити хто є ким та яке завдання має кожен учасник системи.

Власником системи є ректор університету, він несе відповідальність за КСЗІ, призначає відповідальних та є головним в усіх справах, що стосується захисту інформації за законом. За порушення чи невідповідність вимог, неправильно наданої інформації експертній службі чи обробку інформації не за призначенням – відповідальність несе власник системи. Проте, йому не обов’язково керувати процесами захисту інформації – для цього призначають відповідальну особу, що розуміється в усіх процесах.

Система захисту має забезпечувати швидке вирішення можливих проблем та реагування на збої в системі. Головним завданням КСЗІ є безпечна обробка захищеної інформації, без можливості стороннього доступу до системи. Виконання функцій АС на усіх етапах життєвого циклу забезпечить продуктивність обробки інформації відповідно до вимог законодавства.

Відповідальна особа – це, як приклад, заступник директора (ректора), або, у випадку університету, проректор, можливо начальник інформаційного відділу або завідувач кафедри в сфері інформаційних технологій. Його обов'язки: контролювати та перевіряти роботу СЗІ, приймати звіти та звітувати керівництву. Така особа назначається один раз та на всі відділи об'єкту.

СЗІ має начальника служби захисту інформації та, відповідно, працівників, системного адміністратора та адміністратора безпеки, що можуть бути однією людиною. Проте, в залежності від класу АС, працівників може бути більше. Служба захисту визначається в кожному відділі окремо. Вони звітують про все відповідальній особі, створюючи ієрархію звіту.

СЗІ є важливою складовою КСЗІ і відповідає за реалізацію стратегій та політик безпеки в організації. Основні функції та завдання СЗІ включають:

- аналіз ризиків;
- політики безпеки;
- навчання та свідомість користувачів;
- моніторинг та виявлення вторгнень;
- реагування на інциденти;
- аудит та внутрішній контроль;
- звіт та відповідальність.

СЗІ проводить оцінку загроз та ризиків безпеки інформації для визначення потенційних слабких місць і розробки стратегій їх запобігання, розробляє та впроваджує політики та процедури збереження та захисту інформації, включаючи правила доступу, шифрування, автентифікації та інші. Надає або організовує навчання з іншими організаціями та підвищує свідомість персоналу щодо питань

кібербезпеки, включаючи навички виявлення помилок системи, захист від вірусів. СЗІ встановлює системи моніторингу та виявлення вторгнень для постійного контролю за активністю в мережі та системах, а також для виявлення аномальних патернів, що можуть вказувати на потенційні загрози, розробляє плани реагування на кіберінциденти та забезпечує швидке та ефективне припинення атак та відновлення нормальної роботи систем. Служба захисту виконує аудит безпеки для оцінки відповідності систем безпеці, встановленим стандартам та політикам, а також впроваджує внутрішній контроль для запобігання внутрішнім загрозам, формує звіти, для забезпечення аудиту подій системи, для вчасного реагування на інциденти та визначення відповідальних осіб.

Яка інформація зберігається та може зберігатись в університеті, було визначено в першому розділі. Проте, не уся перелічена інформація може оброблятись саме на конкретній АС. Для прикладу, фінансова звітність не обробляється на АС відділу кадрів бухгалтерією. Тобто, як і служба захисту, КСЗІ створюється на окремих АС в залежності від багатьох аспектів. Перелік інформації визначається з переліком детальних відомостей, що можуть оброблятись на окремій АС, та в залежності вже від цієї інформації визначається категорія об’єкту. Але цей перелік також встановлює обмеження. Обробляти інформацію на АС можна лише відповідно до створеного раніше переліку, додавати файли чи обробляти особисту інформацію – заборонено!

Після визначення переліку інформації визначається комісія з категоріювання та обстеження об’єкту. Комісією можуть бути штатні працівники, що не працюватимуть на АС, тобто не є користувачами. На цьому етапі формуються такі документи:

– наказ про призначення комісії з категоріювання та обстеження (в наказі додається перелік членів комісії) (додаток Г);

– акт категоріювання (формує комісія і визначає категорію об’єкту. ХНУ така комісія призначила категорію 4 – інформація, що не містить державної таємниці, службова та конфіденційна інформація) (додаток Д);

– акт обстеження (формує комісія після аналізу середовища об’єкту) (додаток Е);

– формуляр (додаток І).

Накази, що створюються під час роботи з КСЗІ, мають відповідати вимогам університету та спрямовуються на Міністерство освіти та науки України від іменні власника системи, тобто, ректора університету. Положення мають бути затверджені ректором, а також пройти усі етапи перевірки університетськими спілками та затверджуватись Вченою радою університету, у складі якої є студенти та особи, що не мають особистого інтересу. Окрім того, їх вивчає канцелярія на відповідність вимог та юристи університету на правомірність відносно сторін.

Після створення переліку інформації, що містить інформацію для службового користування, обов’язково університет створює наказ про інформацію, де вказуються відомості, що можуть містити службову інформацію. Та інформація, що міститься в переліку, не може оброблятись в незахищеній системі. Перелік обов’язково розміщують на офіційному сайті університету.

Обстеження середовища – це процес вивчення та аналізу існуючої інфраструктури, процесів та політик з метою виявлення потенційних слабкостей та ризиків в системі. Обстеження середовища включає етапи збору інформації, аналізу стану АС, розробки рекомендацій та слідкує за їх виконанням. Аналіз проводять за такими характеристиками:

– характеристика інфраструктури (сусідні кімнати або аудиторії, доступи, поверх розташування);

– приміщення (матеріал та товщина стін, покриття підлоги, кількість вікон, стеля, які саме двері);

– системи безпеки (пожежна та охоронна сигналізація та розміщення об’єктів сигналізації, опалення, кондиціонери, отвори в приміщенні, відеоспостереження, електроживлення, а саме: кількість розеток, вимикачів та їх розташування, світильники, заземлення).

В акті вказується вся інформація про АС, склад обчислювальної техніки (основна та допоміжна), середовище, в якому вона знаходиться, детальний опис кімнати, де розташована охорона, яке ПЗ використовується, повноваження користувачів і їх перелік. До цього додається ситуаційний та генеральний плани.

Також комісія проводить аналіз користувачів, визначає їх обов'язки та функції, повноваження та рівні можливостей, допуски користувачів до різної інформації.

Формуляр – це окремий документ, що складається з таблиць та має відомості про систему. Цей документ заповнюється на протязі усіх етапів створення КСЗІ та після закінчення робіт відправляється на перевірку в Службу спеціального зв'язку України. Вже за змістом та наповненням визначається, чи може заклад отримати атестат відповідності, що заповнюється такими відомостями:

– відомості про ІТС;

– склад техніки та програмного забезпечення;

– програми захисту від несанкціонованого доступу;

– відповідальні особи за захист та обслуговування системи;

– дати впровадження, випробовування та приймання в експлуатацію КСЗІ, результати цих етапів;

– реєстрація робіт, що проводились;

– перелік документів.

Техніка описується з серійними номерами, а склад системи включає материнську плату, оперативну пам'ять, жорсткий диск, процесор, тощо. Носії інформації мають окрему таблицю.

У формулярі також описуються встановлене ПЗ разом із експертними висновками, датами дійсності та інформацією про компанію, яка випустила ПЗ.

За зібраною інформацією розробляється план захисту інформації. План захисту інформації в КСЗІ є ключовим документом, який визначає стратегії, процедури та заходи, призначені для забезпечення безпеки інформації в організації.

План захисту включає такі аспекти:

– визначення мети та об'єктів захисту, що включає в себе чітке визначення цілей та об'єктів, які потрібно захищати, таких як конфіденційні дані, інтелектуальна власність, системи обробки даних тощо;

– аналіз ризиків, оцінка потенційних загроз, вразливості і ризиків для інформації та інформаційних ресурсів організації;

– розробка політик безпеки, встановлення правил, процедур і вимог щодо захисту інформації, включаючи контроль доступу, шифрування даних, резервне копіювання та відновлення, автентифікацію;

– визначення і впровадження технічних засобів захисту, таких як антивірусне програмне забезпечення, системи виявлення вторгнень, тощо;

– організаційні заходи захисту, розробка процедур та організаційних вимог для забезпечення безпеки інформації, включаючи навчання персоналу, розподіл обов'язків та відповідальності, моніторинг та аудит безпеки, тощо;

– реалізація плану захисту інформації та навчання персоналу щодо його виконання та відповідності дій правилам;

– постійний моніторинг ефективності заходів захисту інформації та проведення регулярних аудитів для виявлення можливих слабких місць та вразливості;

– розробка планів реагування на кіберінциденти та виконання необхідних заходів для припинення атак та відновлення нормальної роботи систем;

– постійне оновлення та підтримка плану захисту інформації відповідно до змін в загрозах, технологіях та вимогах організації.

Окрім аудиту в автоматизованій системі, служба захисту має вести фізичний журнал обліку носіїв інформації, в якому мають бути перелік носіїв та відстежуватись хто і коли використовував ту чи іншу «флешку».

2.2 Проєктування моделі загроз та технічного завдання

Результати акту обстеження середовища визначили усі слабкі та сильні сторони системи. Наступний етап – це аналіз потенційних загроз, які вже з відомою інформацією, потрібно передбачити. Насамперед, формуються документи «модель порушника» та «модель загроз» (додаток З).

Загрози, за походженням, виділяють випадковими та навмисними. Випадкові загрози – це ті загрози, що не супроводжуються метою. Тобто, загроза передбачає дії не для порушення роботи системи, а через необережність користувача. Наслідками такого порушення є відмова роботи системи; збій, або часткове порушення роботи; помилка системи або недосконала робота окремих функцій; вплив на систему . Навмисні загрози – це загрози спричинені людиною з метою викрадення інформації, пошкодження роботи системи або повної відмови виконання деяких функцій системою.

Джерелами загроз можна вважати системи, технічні засоби, середовище та людей.

Загрози також поділяють на внутрішні (ті, що потребують доступу до АС) та зовнішні (не вимагають доступу). Носії інформації за неправильного використання можуть стати загрозою. Наявність вікон в кімнаті додають загрозу конфіденційності зовнішнім спостережником за неправильного розташування АС відносно вікна. Загрозою інформації є людина, що має намір знищити якусь інформацію, порушити цілісність або навіть просто не має достатніх знань для роботи з системою.

Стихійне лихо має окреме місце в моделі загроз. Вказуються тільки дійсно можливі загрози, що можуть бути спричинені погодою чи стихією. Наприклад, якщо АС розташована на умовно 5-тому поверсі будинку, то повінь не може бути загрозою.

Конфіденційність порушується коли порушник отримав доступ, тобто, прочитав інформацію. Цілісність порушена якщо порушили структуру файлу,

модифікували його та/або замінили якісь дані. Доступність говорить сама за себе – це подія, коли порушник змінює доступи до файлу, видаляє користувачів та подібне. Спостережність – це властивість системи відстежувати події, порушення спостережності впливає не на саму інформацію, а більше на систему та її функціональні аспекти.

Класифікуються загрози за рівнем ризику (високий, низький, середній) та фактором на який впливає: конфіденційність, цілісність, доступність та спостережність. Модель загроз ХНУ зображена в таблиці 2.1.

Модель загроз в КСЗІ це уявлення про різноманітні загрози, які можуть виникати для інформації та інформаційних ресурсів організації. Така модель допомагає ідентифікувати, оцінювати та керувати потенційними загрозами щоб ефективно захистити інформацію. Ось деякі загальні складові моделі загроз в КСЗІ:

– кібератаки – включають в себе різноманітні форми кіберзлочинності, такі як віруси, черви, троянці, тощо;

– фізичні загрози – можуть бути такі фактори, як крадіжка або знищення обладнання, природні катастрофи, пожежі, повені;

– внутрішні загрози або спроби несанкціонованого доступу чи зловживання правами доступу з боку внутрішніх користувачів організації, включаючи неправомірний доступ до даних або витік конфіденційної інформації;

– загрози через соціальну складову – це атаки, які використовують маніпуляцію людьми для отримання несанкціонованого доступу до систем або інформації;

– технічні несправності та вразливості в апаратному й програмному забезпеченні використовують для атак або несанкціонованого доступу;

– загрози, що виникають внаслідок порушень правил та політик безпеки організації, таких як використання слабких паролів, недостатній контроль доступу тощо.

Таблиця 2.1 – Модель загроз ХНУ

№	Види загрози	Рівень ризику	К	Ц	Д	С
1.	Природні загрози					
1.1	Стихійні явища (пожежа, аварії)	Середній		×	×	×
2.	Зовнішні загрози					
2.1	Несанкціоноване підключення до технічних засобів	високий	×			
2.2	Читання даних та файлів, що роздруковуються, або залишених без догляду документів	низький	×			
2.3	Викрадення носіїв інформації	високий		×		×
3.	Порушення нормальних режимів роботи					
3.1	Зараження системи комп'ютерними вірусами	середній		×	×	×
3.2	Втрата (розголошення) засобів авторизації (паролів), магнітних носіїв інформації та резервних копій	високий	×	×	×	
3.3	Несанкціоноване внесення змін у технічні засоби, програмне забезпечення, компоненти інформаційного забезпечення, тощо	середній		×	×	×
3.4	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення	низький		×	×	×
3.5	Пошкодження носіїв інформації	середній			×	
3.6	Вхід у систему недопущених осіб (подолання систем захисту)	середній	×	×	×	
4.	Помилки персоналу					
4.1	Помилки адміністраторів (неправильне конфігурування та адміністрування систем захисту, операційної системи; неправомірне відключення засобів захисту)	середній	×	×	×	
4.2	Порушення технології обробки, введення та виведення інформації	середній	×	×	×	
4.3	Недбале зберігання та облік документів, носіїв інформації, баз даних	низький	×	×	×	
4.4	Отримання сторонньою особою інформації у персоналу ІКС	середній	×			

Модель загроз містить опис засобів здійснення загроз та складається з таких розділів: опис генерального та ситуаційного плану, перелік основних та допоміжних технічних засобів, загальна класифікація загроз;

Ситуаційний план – це план місцевості, на якому розташовані сусідні будівлі дорога, парки. Адреси та відстані виносяться в табличку, що додається до ситуаційного плану. Ситуаційний план ХНУ можна переглянути на рисунку 2.1.

Генеральний план – це план контрольованої зони (рисунок 2.2).

Контрольована зона – це захищена територія, яка контролюється організацією та має найменшу ймовірність вчинення злочину. Контрольована зона може поширюватись на поверх, кімнату, або повністю будівлю, в цій зоні встановленні охороні системи та доступ мають тільки особи, що визначенні політиками безпеки.

Генеральний план виділяє кімнату розташування АС, сусідні кімнати чи аудиторії, та як розташовані об’єкти контрольованої зони. Опис генерального плану містить дані з акту обстеження середовища: опис матеріалів, розташування вікон та дверей.

В ХНУ контрольованою зоною є аудиторія, де розміщується АС, а саме кабінет під номером 232. Складається аудиторія з двох кімнат. В першій вхідній кімнаті розташовані АС, що не обробляють інформацію, яка може охоронятись. На рисунку 2.2, де зображено, власне, контрольовану зону, видно, що можливість вчинення порушення ускладнено, оскільки прямого доступу до кімнати не має.

Основними технічними засобами є елементи АС: системний блок, дисплей, мишка, клавіатура. Допоміжними технічними засобами можуть бути телефон, принтер, кондиціонер.

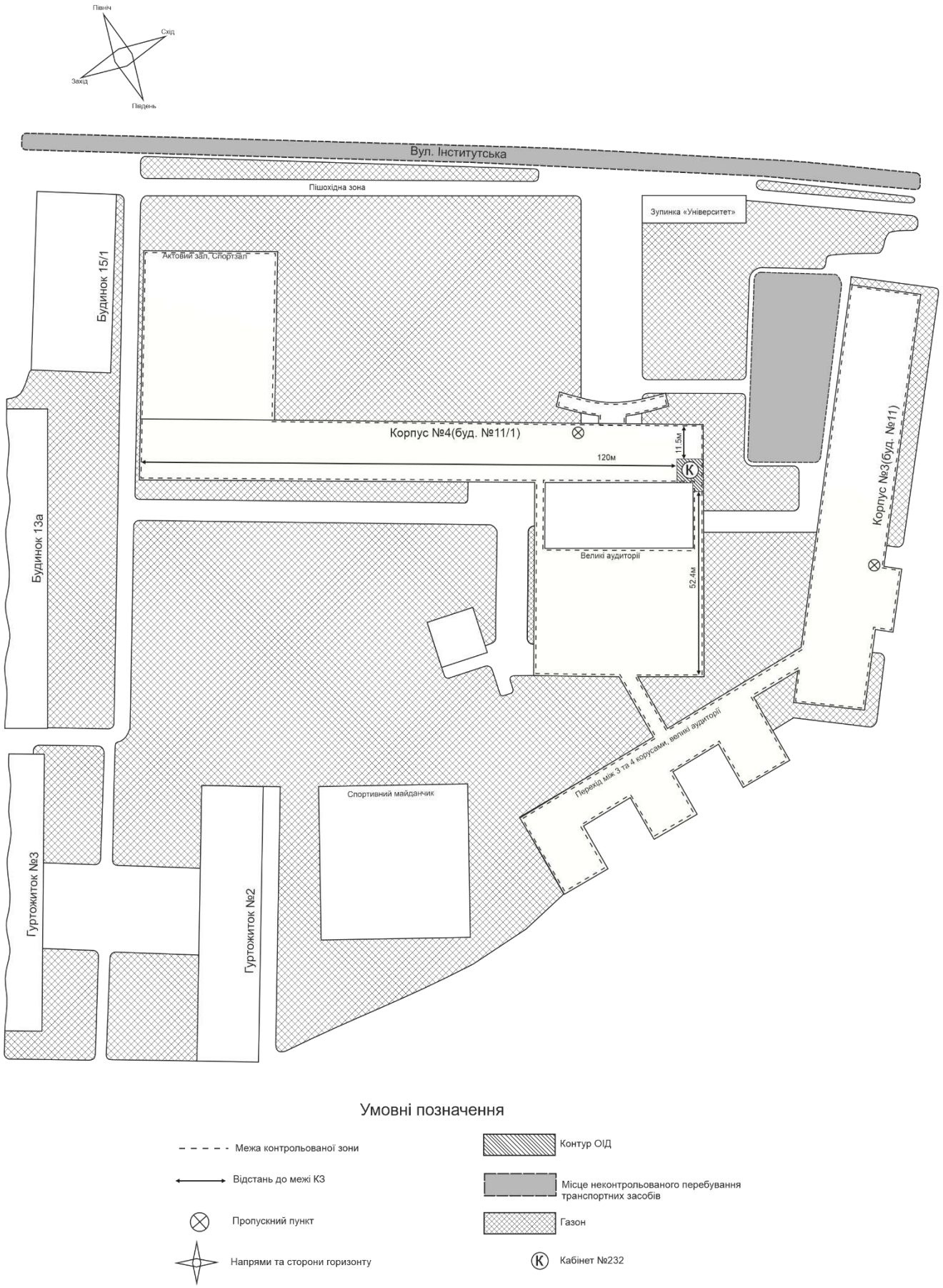


Рисунок 2.1 – Ситуаційний план ХНУ

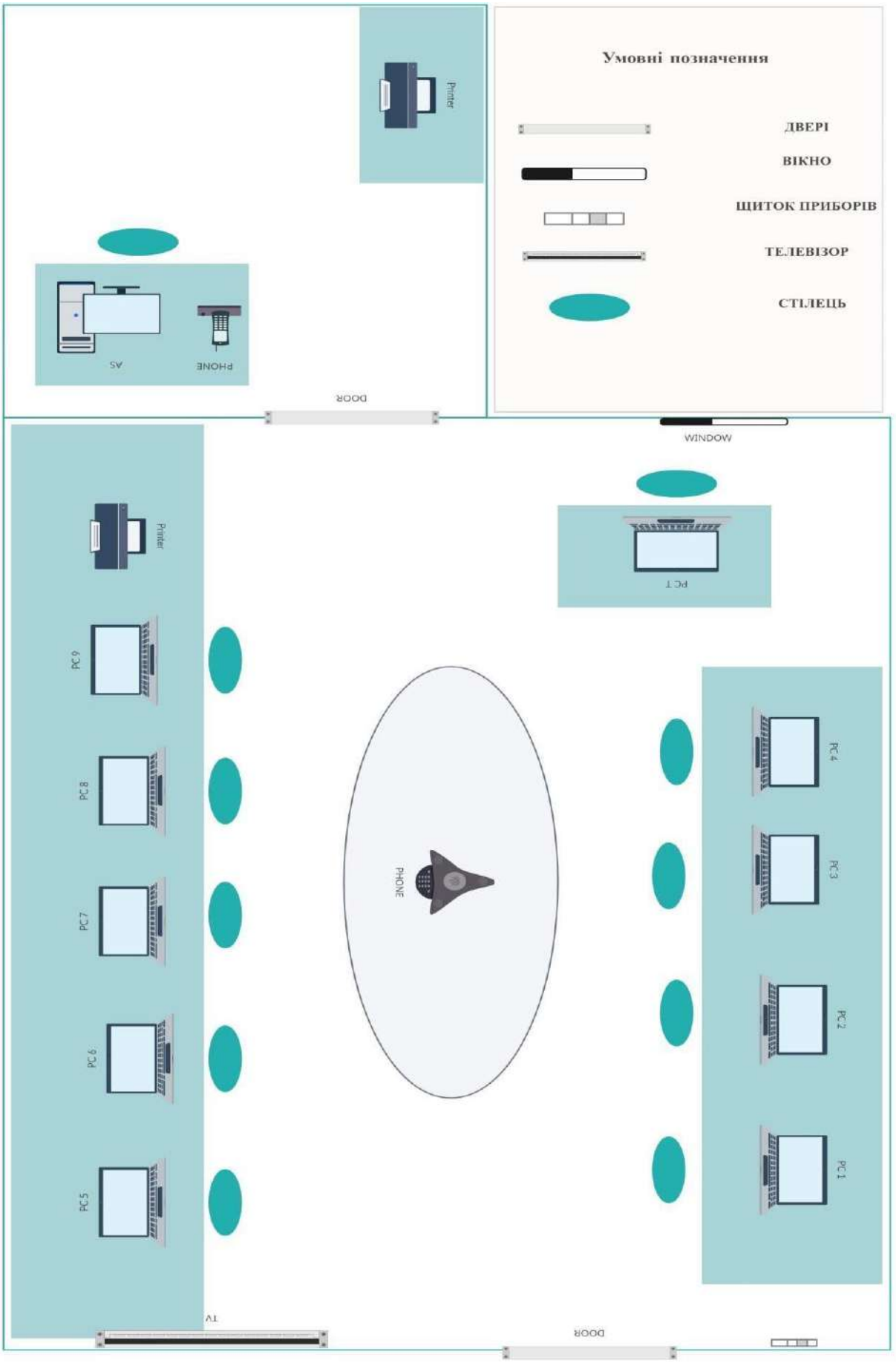


Рисунок 2.2 – Генеральний план

Фізичний захист системи здійснюється встановленням пропускних пунктів на кожному вході в будівлю. В ХНУ АС розташована в 4-му корпусі на другому поверсі будівлі. Потрапити в 4 корпус можливо з основного входу та за допомогою проходу з третього до четвертого корпусу. Охороні пункти повинні розташовуватись в обох корпусах, охорона при цьому не залишає пукти пропуску, тому можливість зовнішніх порушників потрапити в будівлю максимально обмежена. В ХНУ перепустками для студентів є студентський квиток, в викладачів та працівників університету окремі перепустки. Територія всього університету обмежена забором, на території паркінгу також влаштований охоронний пункт.

Модель порушника – це документ, що містить інформацію про потенційного порушника, де проводиться оцінка його можливостей та формується висновок про загрозу від окремих осіб; може створюватись як окремий документ або як розділ моделі загроз. Модель порушника – це умовна поведінкова модель, що формується за можливими доступом порушника до системи, що описує можливі дії порушника та відображає теоретичні можливості порушника за часом та місцем дії.

Модель порушника відображається системо таблиць та визначає такі дані:

– цілі порушника та ступінь небезпечності для інформації;

– можливі знання порушника та їх кваліфікаційний рівень;

– характеристики дій;

– категорії потенційних порушників;

– мета порушників.

Метою порушника може бути:

– отримання необхідної інформації в потрібному обсязі;

– вміти вносити зміни в інформаційні потоки відповідно до своїх намірів (інтересів, планів);

– заподіяння шкоди шляхом знищення матеріальних та інформаційних цінностей.

Порушників спочатку поділяють на дві основні групи [15]: зовнішні та внутрішні. Зовнішніх порушників можна розділити на групи порушників, що мають намір викрасти інформацію, та окремі особи.

Важливо враховувати усі аспекти, тому не потрібно забувати, що порушником може стати будь-яка особа.

Визначено такі особи, які можуть бути порушниками в університеті:

– запрошені гості університету (представники організацій);

– студенти;

– представники організацій, які взаємодіють з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);

– особи, які випадково або навмисно порушили пропускний режим;

– будь-які особи за межами контрольованої зони.

Потенційних внутрішніх порушників можна розділити на:

– обслуговуючий персонал закладу, допущений до закладу, але не допущений до життєво-важливого центру ІТС;

– основний персонал (найнебезпечніший вид порушників);

– співробітники служби безпеки, які часто формально не допускаються до життєво-важливого центру ІТС, але насправді мають достатньо широкі можливості.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

– користувачі системи (штатні співробітники);

– персонал, що обслуговує технічне обладнання (інженери, техніки);

– працівники відділів розробки та підтримки програмного забезпечення (прикладні та системні програмісти);

– технічний персонал, що обслуговує будівлю (прибиральники, електрики, сантехніки та інші працівники, які мають доступ до будівлі та приміщень, де розташовані ІТ-компоненти);

– працівники служби безпеки;

– керівники різних рівнів та посадових ієрархій.

Окрім професійного шпигунства можна виділити три основні мотиви порушення: безвідповідальність, самоствердження та особиста зацікавленість. Також оцінюється кваліфікація потенційного порушника.

Важливо не забувати і про людський фактор, особливо коли мова йде про університет. Вікова категорія студентів 1-4 курсів в середньому 17-23 роки. Навіть цікавість може стати на заваді якісному забезпеченню захисту інформації. В зв'язку з цим, важливо, щоб доступ до аудиторії мали тільки відповідні особи. Тому аудиторія, де знаходиться АС закривається на ключ, який знаходиться на кафедрі, і доступ до якого обмежено співробітниками кафедри.

За мотивом порушення категорії поділяються на [15]:

– безвідповідальність, несерйозне відношення до роботи та захисних функцій системи;

– самоствердження або цікавість;

– корисливий інтерес, спроби видалення або модернізації інформації зі змістом зацікавленої сторони;

– професійний обов'язок (найманці, що мають конкретну мету).

Критерії оцінки за знаннями поділяються на 4 категорії [15]:

– мінімальний рівень знань в системі, проте вміє працювати з технічними засобами;

– володіє середнім рівнем знань та частково володіє навичками роботи з технікою та інформаційними системами;

– має високий рівень знань та практичні навички роботи з технічними засобами та програмним забезпеченням;

– знає структуру захисних функцій, їх можливості та недоліки.

За доступом порушники поділяються на [15]:

– порушник, що може тільки підслуховувати інформацію, що озвучується;

– використовує технічні засоби перехвату;

– використовує недоліки системи для подолання засобів від несанкціонованого доступу;

– використовує технічні засоби, що можуть спричинити порушення роботи системи.

Порушення безпеки ІТС може бути спричинене особистим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту від несанкціонованого доступу до інформації в ІТ.

Наступним етапом є створення технічного завдання. «Технічне завдання» є ключовим документом технічного захисту правового та організаційного рівня – цей документ містить відомості про АС, доступи, роботи, що проводились на об’єкті та їх результати, характеристики складових ІТС, календарний план та профілі захищеності (додаток К). Основні елементи ТЗ можуть включати описи функціональності, тобто, які функції має виконувати система, які дії користувачів вона повинна підтримувати; вимоги до продуктивності – яку швидкість, ефективність і масштабованість повинна мати система; інтерфейси – опис інтерфейсів користувача, зовнішніх систем або пристроїв, з якими система повинна взаємодіяти; надійність і безпека – вимоги до стійкості системи до відмов, захисту від несанкціонованого доступу та інші аспекти безпеки; терміни – часові обмеження на розробку та впровадження проєкту; вимоги до документації – які документи мають бути створені під час розробки та після впровадження системи.

Опис функціональності в технічному завданні представлений профілем захищеності. Відповідно до НД ТЗІ 2.5-004-99, існує сім підкласів для трьох властивостей, за якими простіше читати та розуміти такий профіль. Такі дані має кожен продукт, що встановлюється в систему та регламентує функцію чи декілька функцій, які вони можуть виконувати. Як приклад, антивірус, який не тільки забезпечує захист від вірусів, а й налаштування якого дозволяють виділити адміністратора, політики безпеки Windows, що можуть виконувати декілька функцій з функціонального профілю.

ТЗ містить назву систему, що формує власник системи. Це може бути скорочена назва університету разом з кафедрою, як приклад, проте, саме за цією назвою систему реєструватимуть в реєстрі, тому важливо, щоб ця назва була

унікальна. В ХНУ такою назвою є: ХНУ ФІТ БЕМЗ – ХНУ факультет інформаційних технологій БЕМЗ.

Підкласи та позначення мають такий вигляд[10]:

– ХК – конфіденційність;
– ХЦ – цілісність;
– ХД – доступність;
– ХКЦ – конфіденційність та цілісність;
– ХКД – конфіденційність та доступність;
– ХЦД – цілісність та доступність;
– ХКЦД – конфіденційність, цілісність та доступність.

Функціональний профіль, що розроблений для ХНУ, виглядає так :

{КД-2, КО-1, ЦД-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1}

Критерії захищеності, вимоги до реалізації та спосіб реалізації можна переглянути в таблиці 2.2. Цифри, що розташовані після скорочень, визначають рівень захисту та важливість послуги.

Таблиця 2.2 – Критерії захищеності та їх реалізація.

Критерій захищеності	Вимоги	Спосіб реалізації
1	2	3
КД-2	Базова довірча конфіденційність	Розмежування прав доступу за допомогою Active Directory
КО-1	Повторне використання захищених об’єктів	Вбудовані засоби Windows
ЦД-1	Мінімальна довірча цілісність	Розмежування прав доступу за допомогою Active Directory
ДВ-1	Ручне відновлення	Вбудовані засоби Windows
НР-2	Захищений журнал	Вбудований журнал реєстрації Windows

Кінець таблиці 2.2

1	2	3
НИ-2	Одиночна ідентифікація та автентифікація	Вбудовані засоби Windows
НК-1	Одно направлений достовірний канал	Вбудовані засоби Windows
НО-1	Виділення адміністратора	Призначення адміністратора безпеки
НЦ-2	КЗЗ з контролером цілісності	Вбудовані засоби Windows

Технічне завдання містить інформацію про такі аспекти захисту як пар олі, доступи користувачів до окремої інформації та допуски усіх рівнів.

Забезпечення безпеки об'єктів захисту в ХНУ повинне здійснюватися шляхом комплексного використання організаційних (адміністративних) заходів, правови х і законодавчих норм, фізичних і технічних (програмних, апаратно-програмни х і апаратних) засобів захисту інформації.

Основні організаційні заходи повинні передбачати:

– призначення відповідальної за захист інформації особи, якій надаю ься повноваження щодо організації й впровадження технології захисту інформа ції, контролю стану захищеності інформації;

– створення служби захисту інформації;

– організацію проведення обстеження середовища функціонування;

– облік ресурсів системи, що захищаються (інформації, програм тощо), на основі використання відповідних формулярів;

– реалізацію положень політики безпеки інформації в ХНУ;

– реалізації плану захисту інформації та надання в установленому поря дку адміністраторам безпеки пропозицій щодо внесення у нього змін;

– надання адміністратору безпеки інформації для реєстрації нових (блокування/видалення існуючих) облікових записів користувачів;

– порядок проведення відновлювальних робіт і забезпечення безперервного функціонування системи;

– порядок проведення модернізації КСЗІ.

На правовому рівні для забезпечення безпеки інформації повинні бути розроблені рішення відносно:

– системи нормативно-правового забезпечення робіт із захисту інформації в університеті;

– процедур доведення до персоналу й користувачів основних положень політики безпеки інформації, їхнього навчання й підвищення кваліфікації з питань безпеки інформації;

– системи контролювання своєчасності, ефективності й повноти реалізації рішень із захисту інформації, дотримання персоналом і користувачами положень політики безпеки.

Враховуючи реалізовані у ХНУ технології обробки інформації, для КСЗІ висуваються такі загальні вимоги (цілі безпеки) комплексу засобів захисту. КЗЗ має забезпечити:

– реєстрацію подій, що мають відношення до безпеки;

– захист від несанкціонованого отримання або викривлення даних початкової ідентифікації та автентифікації користувача;

– можливість здійснити відновлення компонентів, що були виведенні з ладу у наслідок реалізації атаки чи випадкового збою;

– доступ на читання інформації об’єктів захисту тільки для авторизованих користувачів;

– доступ на модифікацію інформації об’єктів захисту тільки для авторизованих користувачів;

– можливість заміни окремих компонентів з мінімально можливим впливом на ефективність роботи користувачів;

– захист своїх компонентів від атак спрямованих на вивід їх з ладу;

– реалізувати політику згідно з якою функції адміністраторів та користувачів відокремлені, а права користувачів надаються у мінімальному обсязі, що дозволяє виконувати посадові обов'язки;

– реалізувати політику ідентифікації та автентифікації, що є захищеною від атак зловмисника типу маскарад.

Найкращий захист – це унеможливити доступ. Для цього потрібно правильно підібрати та вчасно замінювати пароль. Стандартні вимоги до паролів звучать так: мінімальна кількість символів 8, пароль має містити букви верхнього та нижнього регістру (тобто великі та малі літери), мати один спеціальний символ (такий як зірочка, решітка, знак оклику, тощо) та цифри.

Як часто змінювати пароль визначає власник системи. В ХНУ визначено, що заміна паролю користувачами має відбуватись не рідше ніж раз на рік. Паролі не мають повторюватись, тобто придумати два паролі і по черзі їх замінювати не вийде, оскільки такі дії порушать політику безпеки. За допомогою налаштувань політики АС адміністратор виявить такі дії дуже швидко.

2.3 Налаштування локальних політик безпеки Windows 10

Технічним аспектом розробки та введення безпеки є налаштування політики АС. Це може бути додатково встановлене ПЗ, таке як ЛОЗА™-1, Гриф версії 3, Рубіж-. Також політику можна налаштувати за допомогою функцій Windows 10.

КЗЗ складається з комплексу технічних засобів (КТЗ) та програмного забезпечення та складаються з програмного засобу MS Windows та ПК антивірусного захисту. Розглянемо захист пристрою за допомогою служб Windows 10 та захист від вірусів за допомогою доступних функцій.

Для початку потрібно відкрити вікно «Безпека у Windows». Шукаємо службу таким шляхом: Налаштування – Оновлення та захист – Безпека у Windows,

або через Пошук. Після цього кроку відкриється вікно, що зображено на рисунку 2.4

Зокрема, тут можна настроїти і протестувати опції:

– захист від вірусів і загроз, швидка перевірка поточних загроз, налаштування захисту в реальному часі, перевірка і оновлення тощо;

– безпека облікового запису, зокрема, можемо налаштувати, як буде захищено обліковий запис при вході до системи. Наприклад, можемо використовувати паролі, фізичні ключі безпеки або інші;

– щоб захист від несанкціонованого доступу працював, повинен бути включений брандмауер;

– керування додатками та браузерами. Тут можна настроїти параметри для захисту пристрою від шкідливих і потенційно небажаних додатків, файлів і веб-сайтів;

– можемо переглянути інформацію про ємність пам'яті, час роботи акумулятора, додатки, тощо.

Налаштування групових політик здійснюється із дотриманням рекомендацій щодо конфігурування за наступними розділами параметрів безпеки ОС:

– політика облікових записів;

– параметри локальної політики;

– журнал подій;

– системні служби;

– налаштування реєстру;

– файлова система;

– адміністративні шаблони ОС Windows;

– політика обмеженого використання програм.

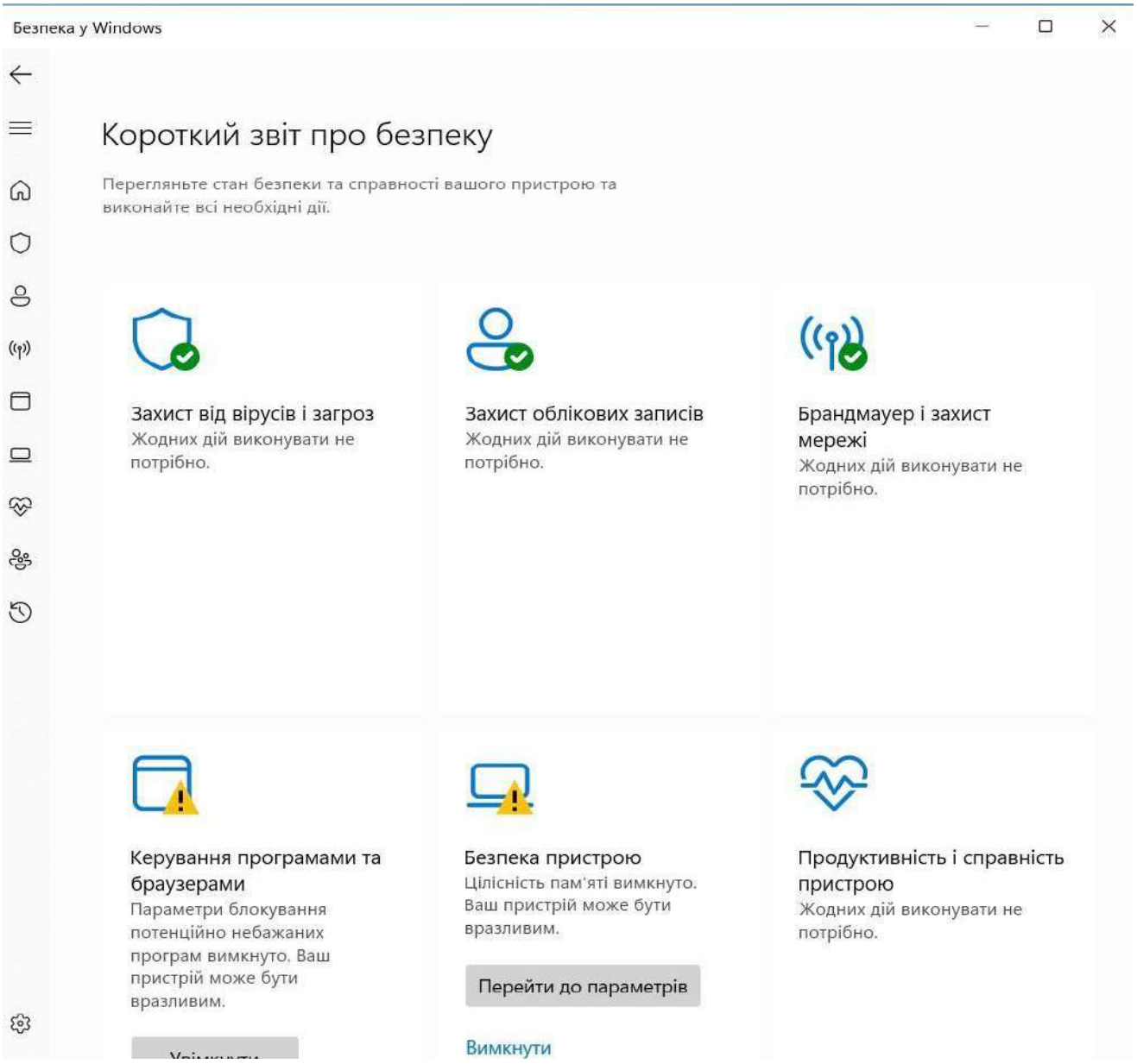


Рисунок 2.4 – Початковий екран «безпека у Windows»

Налаштування параметрів виконується шляхом редагування об’єктів групових політик за допомогою відповідних засобів ОС Windows[16], в тому числі:

– редактора «Локальна політика безпеки» – для редагування локального об’єкта групової політики Windows;

– редактора групової політики – для редагування групових політик в централізованій базі даних Active Directory домену Windows [17].

Шлях Пуск–Пошук–Local Security Policy, дозволяє нам отримати доступ до налаштувань системи. Відкриється вікно, що зображено на рисунку 2.5

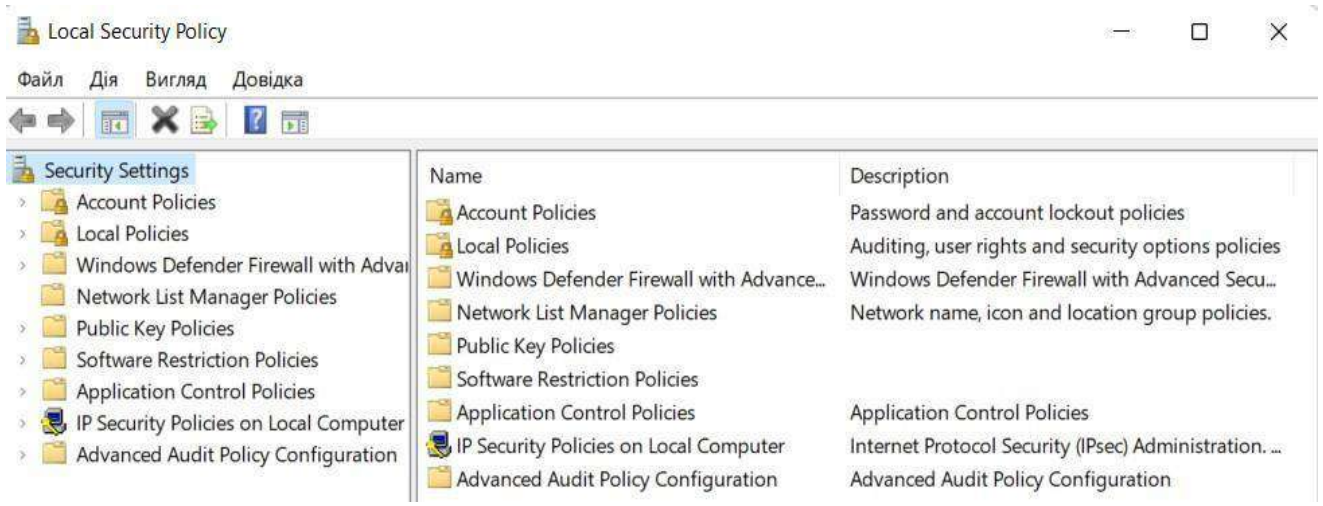


Рисунок 2.5 – Налаштування безпеки

Локальні політики в ОС Windows дозволяють адміністраторам налаштовувати різноманітні параметри безпеки, доступу і конфігурації для користувачів і комп'ютерів у мережі [18]. Ці політики дозволяють контролювати різні аспекти системи, такі як обмеження доступу до певних функцій, встановлення паролів, налаштування аудиту та багато іншого.

Інструмент для управління локальними політиками "Локальні групові політики" доступний на комп'ютерах з ОС Windows (рисунок 2.6). Зазвичай він використовується адміністраторами для налаштування безпеки і доступу до різних ресурсів системи [19].

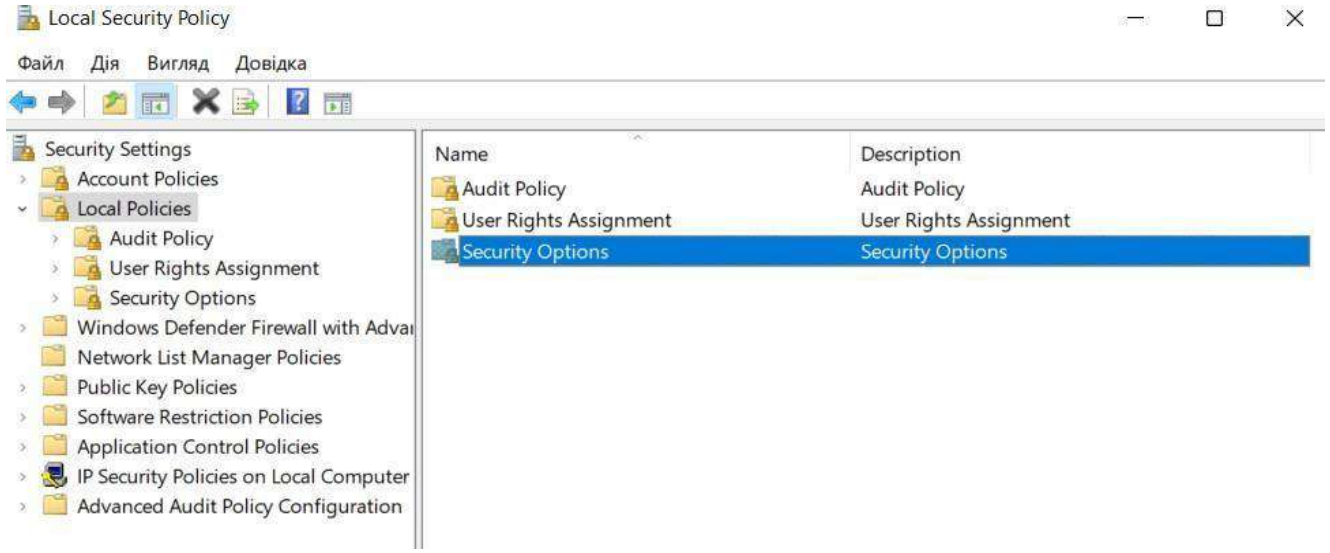


Рисунок 2.6 – Локальні політики безпеки

На рисунку 2.7 можна звернути увагу, що система не налаштована, оскільки навпроти кожної політики ми бачимо відповідь системи No auditing. До переліку аудиту системи відносяться такі функції:

– аудит подій входу в обліковий запис;
– аудит менеджменту системи;
– аудит каталогів системи;
– аудит подій входу;
– аудит доступу до об’єктів, тощо.

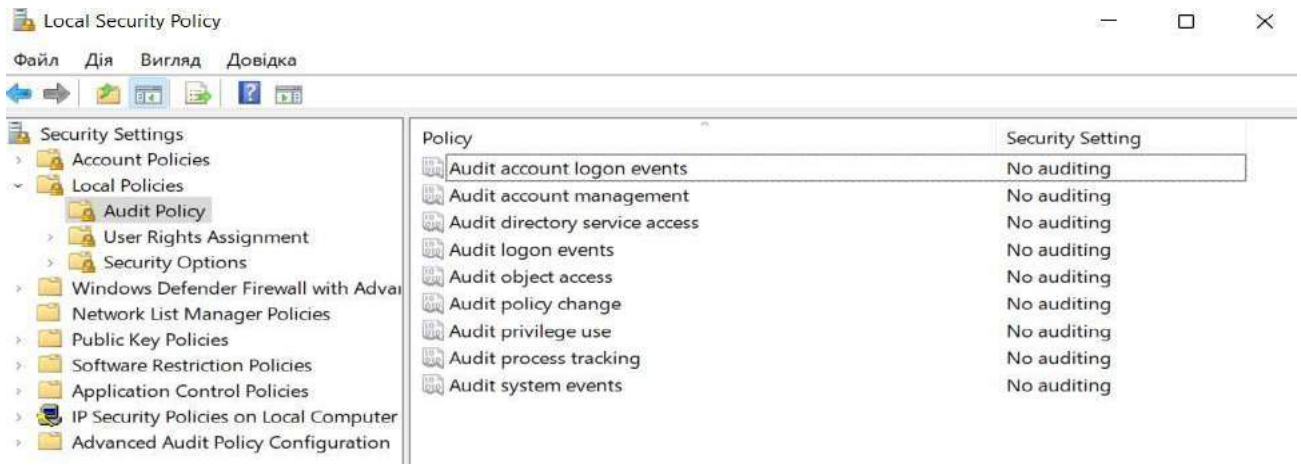


Рисунок 2.7 – Політики аудиту системи

На рисунку 2.8 зображено, як виглядає система з активованою політикою аудиту подій входу в обліковий запис.

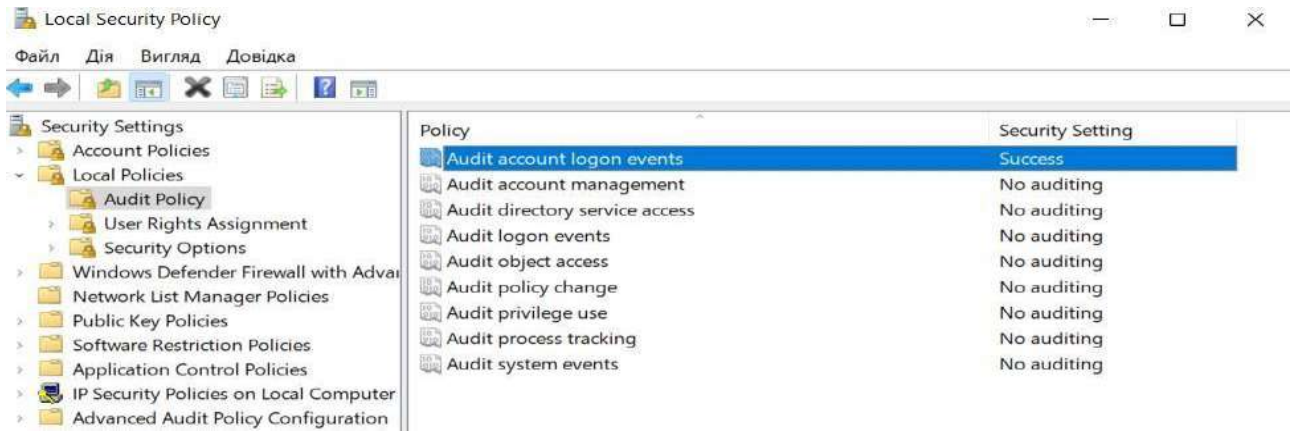


Рисунок 2.8 – Приклад активованої політики безпеки

На рисунку 2.9 розміщено доступи юзерів та на рисунку 2.10 налаштування паролів. Деякі звичайні аспекти, які можна налаштовувати за допомогою локальних політик, включаючи:

– вимоги до паролів;

– правила блокування облікових записів після некоректних спроб входу;

– налаштування аудиту подій;

– обмеження доступу до певних програм або функцій;

– налаштування політик безпеки для файлів і каталогів;

– керування автоматичними оновленнями.

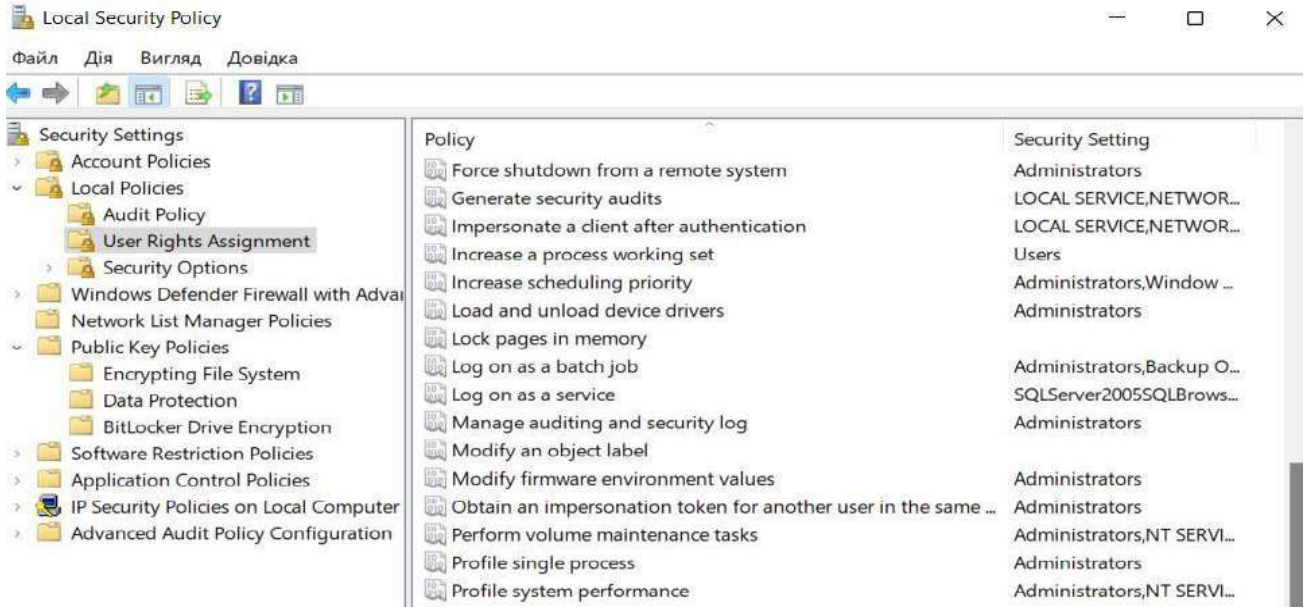


Рисунок 2.9 – Доступи юзерів системи

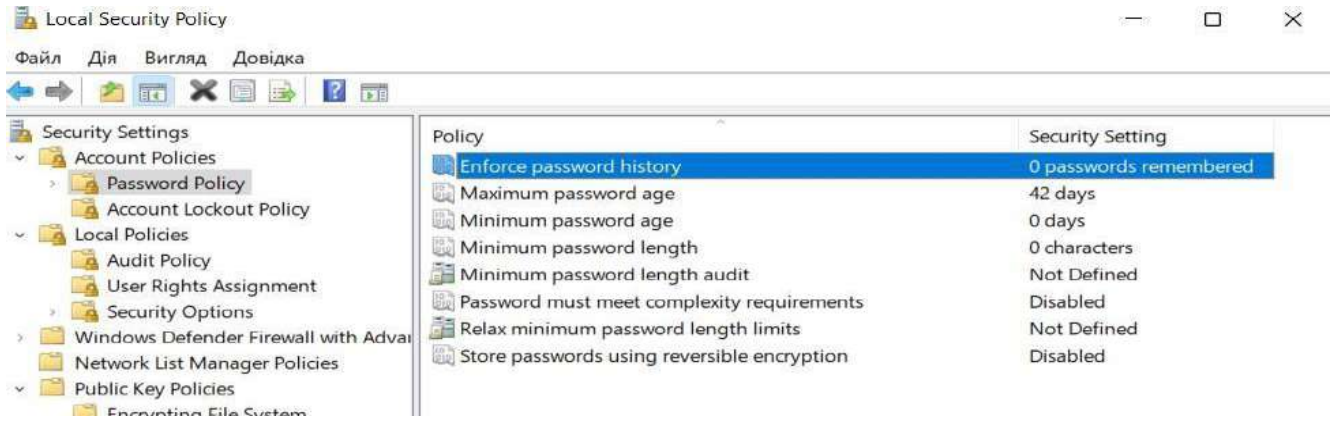


Рисунок 2.10 – Налаштування паролів системи

Ці політики можуть бути налаштовані як для локального комп'ютера, так і для комп'ютерів у мережі, які керуються контролером домену. Вони дозволяють створювати і реалізувати різні стратегії безпеки в залежності від потреб організації або конкретного випадку використання [20].

2.4 Впровадження КСЗІ

Коли усі документи, проєкт та підготовка теоретичної частини роботи закінченні, наступає етап робіт з системою. Перший крок – це введення КСЗІ в дію. На цьому етапі проводяться навчання персоналу, роботи з системою, введення політик безпеки та ознайомлення користувачами з правилами експлуатації системи [21,22].

Робота з системою на цьому етапі розуміється як правильне розміщення АС відповідно до вимог, налаштування Windows та антивірусу.

Навчання персоналу проводиться для усіх рівнів осіб, що працюють в університеті, або всіх хто має допуск до кімнати з КСЗІ. До списку таких осіб відносяться: власник системи, користувачі, прибиральники, техніки, охорона. В кожного свій рівень допуску і навчання проводиться відповідно до повноважень відносно системи.

Обслуговуючий персонал навчають правильного поводження з окремими елементами системи. Для прикладу, прибиральниці демонструють допуск до яких елементів вона може отримати, охороні – де знаходяться системи сигналізації й пожежної безпеки та пояснюють, як діяти в окремих ситуаціях. Також навчають базових знань в сфері захисту для розуміння серйозності їх обов’язків та функцій.

Користувачам демонструють систему та пояснюють поведінку в системі. Демонструють систему входу та виходу, збереження даних, кожному з користувачів окремо їх дозволи. В залежності від рівня пізнання, але обов’язково, проводяться лекції з безпеки, щоб рівень розуміння важливості захисту не

змінювався. Також важливо звернути увагу на розпізнавання вразливості та реагування на загрозу – користувачі мають вчасно реагувати на інциденти та знати, що робити в непередбачуваних ситуаціях, знати базові терміни та заповнювати звіти. Навчання користувачів проводиться і після введення користувачів, для оновлення інформації, щоб забезпечити безпеку у реагуванні навіть на нові технології кіберзлочинного світу.

Окрім технічного навчання усіх працівників ознайомлюють з документацією, а саме з планом захисту та політиками безпеки, інформацією про доступи кожного особисто.

Етап введення КСЗІ в дію також супроводжується і роботами в системі. Відповідно до плану захисту інформації встановлюється та інсталюються усі програмні засоби, що мають експертний висновок, проводиться перевірка працездатності комплексу. Мають бути встановленні всі механізми захисту інформації згідно плану. Реєструють користувачів, встановлюються їх доступи, для кожного окремі, вводять в базу їх паролі (кожен свій особистий) та інформацію, що не захищається законом, допоки АС не отримає атестат відповідності. Доступи користувачів будуть різними – хтось матиме можливість тільки читати інформацію, хтось редагувати та вносити правки. Проте додавати та видаляти інформацію дозволено тільки адміністратору системи.

Коли система повністю готова для роботи, починається етап попередніх випробувань та дослідної експлуатації. Випробування проводяться розробником КСЗІ. Перевірка визначає готовність та працездатність системи до експлуатації. Перевіряється захист системи усіма можливими засобами.

Після тестувань, за потреби, додаються програмні засоби, яких не вистачає, замінюються апаратні складові, що не відповідають вимогам, проводяться додаткові налаштування системи. Якщо виявлено, що окреме ПЗ не має експертного висновку, його необхідно замінити.

Останнім етапом є державна експертиза, що проводиться Державною службою спеціального зв’язку. Існує положення про державну експертизу, що

регламентує правила та поводження під час експертизи. За результатом випробувань та відповідності системи технічному завданню система отримує атестат відповідності.

Після отриманого атестату наказом ректора або керівника установи, згідно з отриманим атестатом відповідності, можна починати експлуатувати систему. В силу вступають план захисту та політики безпеки. Служба захисту інформації повинна зауважувати усі аспекти користування, пропонувати засоби та заходи модернізації системи, вчасно проходити атестації та відповідати вимогам.

2.5 Висновок

В розділі було спроєктовано накази та положення, акт обстеження та категоріювання об’єкту. Розроблено модель загроз та порушника за критеріями оцінки порушника, генеральний та ситуаційний плани. Спроєктовано технічне завдання, формуляр та план захисту. Налаштовано політики безпеки в АС за допомогою політик безпеки Windows.

3 ВИМОГИ ТА РЕКОМЕНДАЦІЇ ЩОДО ЕКСПЛУАТАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Супровід системи під час та після впровадження

Автоматизація усіх інформаційних просторів дозволяє розширити межі обробки, зберігання та передачі інформації. Кожна ланка суспільства, так чи інакше, стикається з автоматизованим світом, що неабияк полегшує роботу. Розвиток технологій змінює світ, а розвиток кіберзлочиного світу змінює кібербезпеку та методи захисту. Найкращим варіантом для установ, організацій та підприємств є комплексний підхід до захисту, що унеможливлює атаки у різних варіантах їх реалізації.

КСЗІ – це комплекс організаційних та технічних засобів щодо захисту інформації в автоматизованій системі, спрямовані на унеможливлення несанкціонованих дій в системі, витоку інформації, її крадіжці, модифікації чи видалення без дозволу.

Типова схема системи захисту інформації зображена на рисунку 3.1 та складається з трьох основних складових: нормативно-правова система захисту (включає як нормативну базу відповідно до законів, так і документи, що розробляються в системі), організаційна система (система заходів безпеки на фізичному рівні); інженерно-технічна (налаштування системи та організація фізичних засобів, тобто пожежна сигналізація та подібне).

Усі складові захисту переплітаються між собою. Деякі завдання, що виконуються під час проєктування КСЗІ, можуть відноситись до інших етапів створення. Як приклад, організаційні заходи захисту переплітаються з інженерно-технічними заходами. Один виходить з іншого. Фізичні засоби захисту переплітається з організацією пропускного режиму.

Нормативно-правова система захисту враховує документи, що створюються в системі для університету. Проте, світ кіберзлочиності розвивається з швидкістю хорошого автомобіля, що не дозволяє відставати кібербезпеці, що впливає на

зміни в законодавчій базі України. Тому під час створення і введення КСЗІ нормативні акти та закони потрібно перечитувати на кожному етапі, адже зміни можуть вноситись «вже вчора». І для економії фінансів, часу, нервових клітин та основне для швидкого введення КСЗІ краще перевіряти закони частіше.

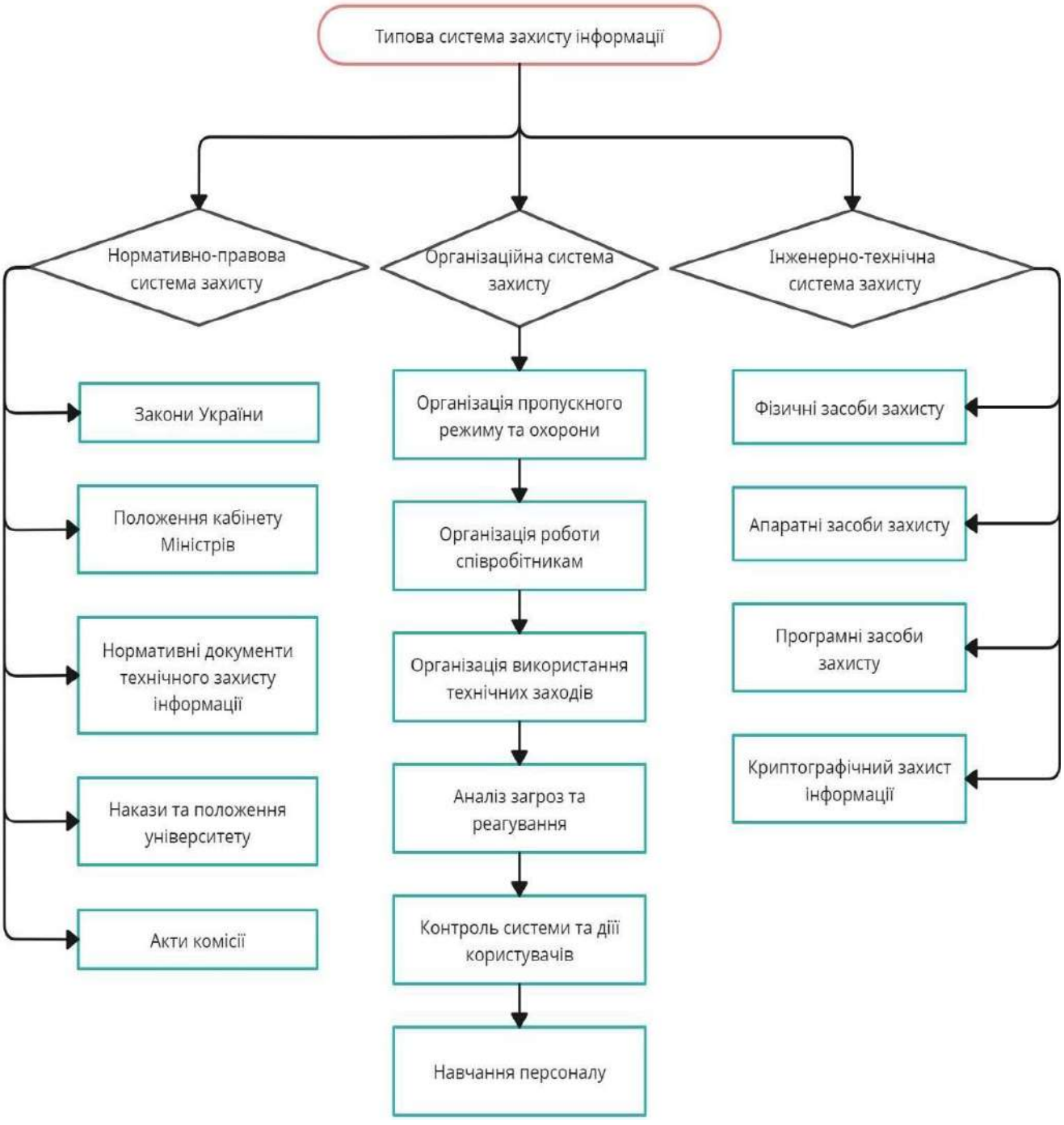


Рисунок 3.1 – Типова схема захисту інформації

Організаційні заходи КСЗІ спрямовані на забезпечення безпеки та конфіденційності інформації у всіх аспектах її життєвого циклу. Можливими організаційними заходами, які можуть бути введені в рамках КСЗІ, є:

– розробка політик і процедур безпеки, розроблення та впровадження політик, стандартів, процедур та правил, що стосуються збереження, обробки, передачі та знищення інформації;

– навчання та свідомість користувачів, проведення навчань, тренінгів та інформаційних кампаній для персоналу щодо правил безпеки, обережного використання інформаційних ресурсів та реагування на загрози;

– управління доступом, встановлення процедур управління доступом до інформації на основі принципу "необхідності доступу", реалізація систем автентифікації та ідентифікації;

– моніторинг та аудит безпеки, проведення регулярного моніторингу та аудиту системи захисту інформації для виявлення вразливостей та вчасного реагування на можливі загрози;

– контроль фізичної безпеки, забезпечення фізичної безпеки приміщень, де зберігається чи оброблюється важлива інформація, через контроль доступу, використання систем відеоспостереження тощо;

– реагування на інциденти безпеки, визначення процедур реагування на інциденти безпеки, в тому числі виявлення, аналіз та виправлення порушень безпеки;

– стандартизація та сертифікація, впровадження стандартів безпеки, сертифікація систем захисту інформації відповідно до вимог міжнародних та національних стандартів.

Технічні заходи захисту інформації включають в себе використання спеціалізованих технологій, програмного забезпечення та апаратного забезпечення для захисту інформації від несанкціонованого доступу, зміни, втрати або пошкодження:

– системи автентифікації та ідентифікації. Ідентифікація – це логін (ім’я), автентифікація – пароль, з відповідними вимогами. Використання систем автентифікації, таких як паролі, біометричні дані або двохфакторна автентифікація, потрібне для перевірки ідентичності користувачів. Після автентифікації системи також мають механізми ідентифікації, які визначають права доступу користувачів до різних ресурсів.;

– використання шифрування для захисту конфіденційної інформації від несанкціонованого доступу під час зберігання або передачі. Шифрування може застосовуватися як до цілих дисків, так і до окремих файлів або комунікаційних каналів;

– антивірусне програмного забезпечення для виявлення, блокування та видалення шкідливого програмного забезпечення, включаючи віруси, черви, троянські коні та інші загрози;

– резервне копіювання та відновлення даних (регулярне створення резервних копій даних і розробка планів відновлення даних у випадку їх втрати або пошкодження в результаті аварій, кібератак або інших подій;

– використання фізичних засобів захисту, таких як захищені USB-накопичувачі, апаратні модулі безпеки та інші, для збереження інформації та забезпечення безпеки систем.

Усі перераховані технічні заходи спільно з організаційними та фізичними заходами допомагають створити КСЗІ, яка забезпечує безпеку і цілісність інформації. Основне завдання – це правильний підхід до роботи, та визначення усіх категорій та їх етапів. Організаційні заходи повинні забезпечити непрохідну фізичну систему, що забезпечить безпеку фізичної складової. За допомогою таких правил нелегітимний доступ до системи стане неможливий. Технічна складова захисту забезпечить нормальну роботу працівникам, що мають допуск до системи, та зменшить бажання порушити режими роботи через неможливість таких дій.

До основних етапів захисту інформації можна віднести:

– аналіз ризиків і визначення потенційних загроз. Цей етап передбачає

оцінку ризиків для інформаційної системи, виявлення потенційних загроз і вразливостей, які можуть призвести до порушення конфіденційності, цілісності або доступності даних;

– розробка політики безпеки. На цьому етапі встановлюються правила, процедури, стандарти та рекомендації, що стосуються захисту інформації, включаючи визначення допустимих методів роботи, вимог до паролів, контроль доступу тощо;

– впровадження технічних та організаційних заходів. На цьому етапі здійснюється впровадження технічних засобів захисту, таких як антивірусне ПЗ, системи шифрування, а також впровадження організаційних заходів, таких як навчання персоналу, проведення аудиту безпеки;

– використання КСЗІ. Після впровадження заходів захисту інформації важливо проводити моніторинг та аналіз стану безпеки, виявлення і аналіз потенційних загроз, а також реагувати на інциденти безпеки;

– постійне вдосконалення системи захисту. На цьому етапі вносяться зміни та вдосконалення в КСЗІ відповідно до змін в загрозах, технологіях та потребах організації.

Такий порядок заходів забезпечить створення безпечної та нормально сформованої комплексної системи, дозволить на кожному етапі зменшити можливість неправильних дій та збереже нерви працівників служби захисту інформації на процесі розробки та введення.

Проблеми та основні функції захисту інформації в будь-якій системі, яка обробляє інформацію та може містити дані, що не підлягають поширенню, допомагають провести аналіз та виділити основні напрямки та принципи заходів, що забезпечують захист:

– організація зовнішнього захисту, таких як аудит подій, охорона, правила доступу;

– організація внутрішнього захисту, встановлення антивірусів, забезпечення правил реєстрації, аудит подій та доступу в відповідних журналах;

– забезпечити швидке реагування на події, що можуть нашкодити системі, назначити відповідальних та осіб, що стежитимуть за подіями в АС;

– попереджувальні дії та можливі наслідки, потрібно бути готовими до можливих спроб знищення систем. До таких дій можна віднести навчання персоналу, вчасні перевірки доступу.

Етап виявлення або зовнішній захист – це найперший етап, що більше відноситься до організаційних питань та правил. Основне та принципове правило – це організація пропускного режиму з охороною. Найкраще, коли доступ до відповідної кімнати з АС мають тільки штатні працівники або ті, хто має доступ відповідно до політик безпеки. Важливим аспектом є відеоспостереження та сигналізація. Ці фактори зменшують ризик фізичної атаки на АС та інформацію і обмежують можливості порушника безпеки.

Етап зупинення або внутрішній захист є не менш важливим у випадку, якщо попередні дії та захист все ж не зупинили порушника. Наступне, з чим доведеться зіштовхнутися, ПЗ. Усі дії порушника мають бути заблоковані: спроби НСД до інформації, ураження системи вірусами. Для забезпечення захисту встановлюються відповідні програми та налаштовуються політики безпеки. Обов’язкова ідентифікація та автентифікація є ще однією проблемою для можливого порушника, але важливо, щоб етапи авторизації проходили відповідно до правил, що встановленні законами України.

Аудит подій в АС має записувати кожен крок будь-якого користувача, що дозволяє відстежити дії. Це не забезпечує захисту, проте дані, які там зберігаються, дозволяють відновити інформацію, якщо є така потреба, та встановити порушника або данні людини, що могла посприяти створенню такого порушення.

Важливо пам’ятати, що витік важливої інформації, може призвести до відповідальності, такої як кримінальна, адміністративна та дисциплінарна.

Етап нейтралізації або реагування на події – це етап, на якому ми вже знаємо усі наслідки, тому тут важлива правильна реакція. Насамперед, потрібно зафіксувати порушення та ліквідувати потенційні загрози. Важливо

проаналізувати, як порушення могло відбутись і що робити, щоб більше такого не повторилось. Саме цей етап говорить про покарання. Якщо ж порушення трапилось, потрібно оцінити, отримати відповіді що хотів отримати порушник, випадковість це чи поганий намір, скільки часу потрібно на відновлення?

Не завжди порушення може бути навмисним. Уявимо ситуацію, коли прибиральниця, яка не має доступу до АС, проте прибирається в сусідній кімнаті під наглядом охорони, випадково вимикає електроенергію, коли працівник працює за АС. З однієї сторони, прибиральниця не може знати, чи там хтось працює, адже інформація таємна, з іншої, якщо політики безпеки налаштовані не правильно, ця ситуація могла мати погані наслідки. Для попередження таких ситуації політики налаштовують з відновленням системи, інформації, дисків, збереженням режиму роботи, тощо.

Етап попередження – це знову ж таки аудит подій в АС. Саме аудит загроз відомих та цілком можливих загроз. Попередження загроз визначається одним з першим та проводиться на кожному етапі, від написання наказів до оформлення кімнати. Вибір, якою стороною поставити комп'ютер до дверей, може здатись очевидним, але якщо в кімнаті є вікно навпроти дверей, чи буде настільки ж очевидним цей вибір?

Ситуація з прибиральницею, про яку ми говорили раніше, не відбудеться у випадку грамотного навчання персоналу (не тільки працівників, що мають доступ до АС, але всіх задіяних відносно захисту). У кожного працівника є власні доступи та допуски, але навчання має проводитись з швидкістю поширення технологій. Тобто, дуже часто – в часи стрімкого розвитку кіберзлочинності, захист інформації аж ніяк не може пасти задніх.

Психологічна сторона захисту – це один з аспектів, що впливає на якість створення КСЗІ, розуміння відповідальності та своїх обов'язків. Підкуп за інформацію цілком можливе явище. Тому правильне пояснення обов'язків та відповідальності позитивно вплине на роботу в системі та в установі загалом.

Що не менш важливо, на високому рівні має бути фізичний захист АС. Тобто, пожежі, цунамі та землетрус, перебої енергії та подібне не повинно шкодити системі. Протипожежна сигналізація, заземлення і схожі системи стають другом для збереження цілісності інформації не тільки на фізичному, але й на організаційному рівні.

3.2 Політики встановлення антивірусного захисту

Правильно підібраний антивірус – перший крок до захищеної системи. Антивірус має бути куплений, а власник системи або відповідальна особа повинна бути зареєстрована на офіційному сайті центру антивірусного захисту інформації (ЦАЗІ) [24]. Вимогою законодавчої бази України є встановлення антивірусу, що має експертний висновок та атестат відповідності дійсний на момент його покупки [25].

Реєстрація закладу здійснюється після купівлі антивірусу за допомогою реєстраційної карти, що відправляється на пошту. Перелік засобів з експертним висновком є на сайті, в розділі «перелік програмних засобів» [26]. Реєстраційна інформація містить дані про власника системи (відповідальної особи), назву антивірусу, що підключений до системи та IP-адресу домену. Після перевірки на достовірність ЦАЗІ дозволяє зайти в особистий кабінет, щоб мати можливість встановити оновлення, які публікуються кожного дня. Встановлювати оновлення потрібно обов’язково [27] (додаток Ж).

В АС класу 1 у ХНУ встановлений антивірус ESET [23], що відповідає цим правилам.

Процедура оновлень в АС класу 1 відбувається з допомогою іншої АС, оскільки, як нам вже відомо, АС класу 1 не має доступу до мережі. Відповідно, адміністратор системи викачує оновлення на захищеному комп’ютері на USB-носій, що зареєстрований в системі та в журналі аудиту, і тільки потім встановлює їх на потрібну АС.

3.3 Інструкції адміністратора та користувачів

Політики безпеки розробляються як окремі інструкції адміністраторам та користувачам. Порушувати ці правила заборонено. Вони включають як загальні принципи безпеки, так і окремі індивідуальні компоненти, що розробляються для окремих осіб. Права та обов'язки користувачів системи різняться, тому існують загальні правила, такі як правила авторизації, а існують окремі, що зобов'язують, як приклад, адміністратора до якихось дій.

Детальна схема розробки політик безпеки для університету зображена на рисунку 3.2.

Схема розробки політик безпеки говорить, що політики безпеки виділяють три напрямки інформаційної безпеки, а саме: програмна, системно-орієнтована, проблемно-орієнтована політика безпеки. Різниця полягає в способах реалізації. Програмна відповідає за ПЗ та рішення програмних комплексів, про які ми говорили в попередньому підрозділі. Проблемно орієнтовна – окремі випадки або політики непередбачуваних обставин, реагування на окрему проблему, що непередбачуваною [28]. Системно-орієнтована політика – правильна робота системи захисту, адміністрування систем, охоронна система, функції та процеси, яких потрібно дотримуватись.

Поговоримо про системно-орієнтовні політики, а саме політики-інструкції для основних осіб, що взаємодіють з системою: функції адміністратора, обов'язки користувачів, стандарти власника системи.

Політики безпеки розробляються для всіх учасників та користувачів КСЗІ, включаючи адміністраторів систем, інженерів з безпеки, користувачів та всіх інших осіб, які мають доступ до інформації та ресурсів системи. Ці політики визначають правила, процедури та вимоги щодо захисту інформації, встановлюють відповідальність за дотримання цих правил та визначають наслідки порушення правил безпеки [29].

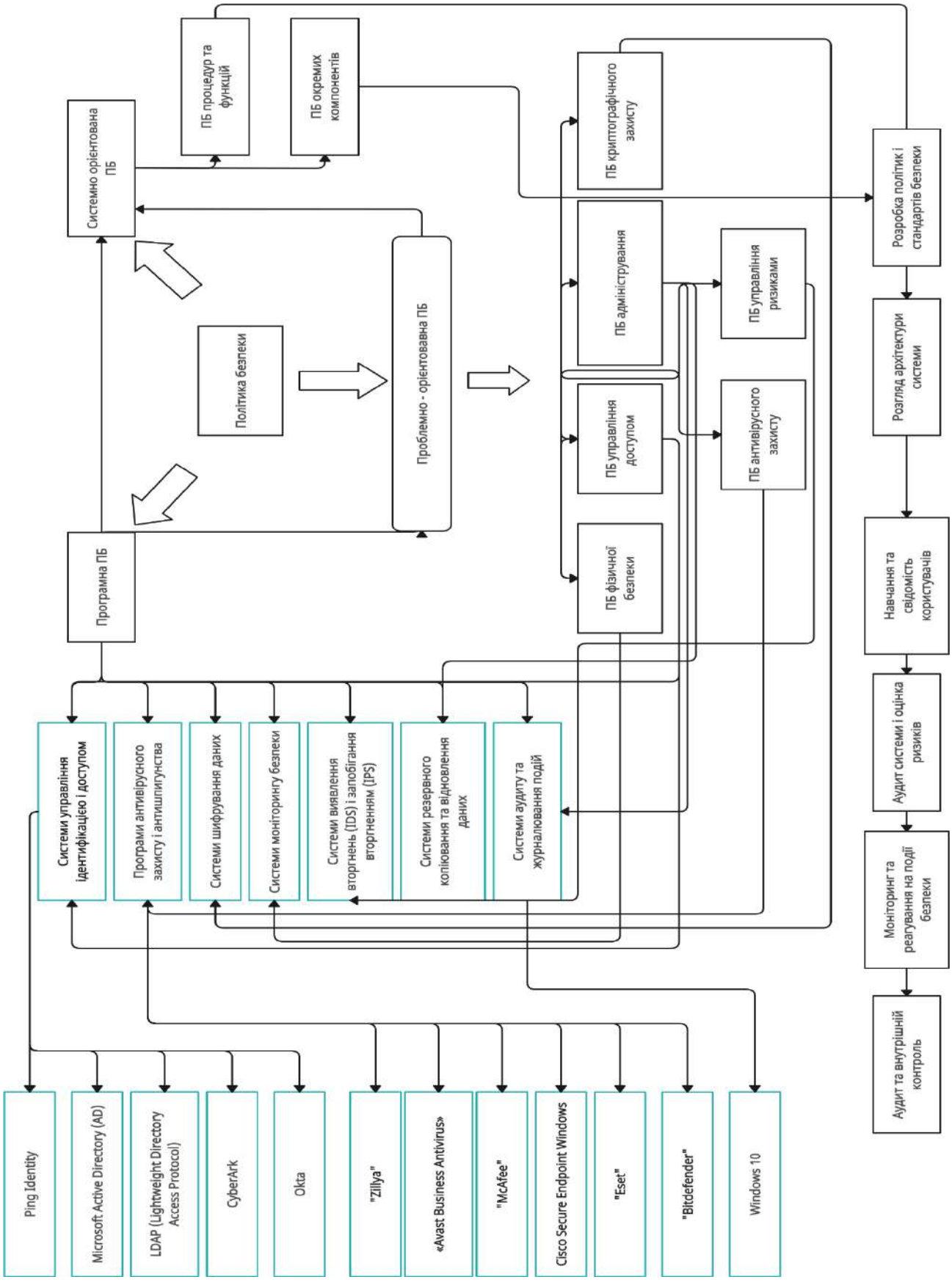


Рисунок 3.2 – Схема розробки політик безпеки

В ХНУ адміністратор системи має найбільше обов’язків, оскільки система контролюється повністю адміністратором. Надання доступу до окремих файлів визначає власник системи, але реалізація наданих доступів в автоматизованій системі – це обов’язки адміністратора.

Системний адміністратор та адміністратор безпеки мають різні політики безпеки, в різних ситуаціях це є одна людина. У випадку якщо об’єкт інформаційної діяльності проєктує КСЗІ категорії 3 адміністраторів обов’язково має бути 2, оскільки обов’язків буде набагато більше.

Політика безпеки адміністратора – це набір правил, процедур і рекомендацій, які адміністратор системи повинен дотримуватися для забезпечення безпеки та захисту інформації та інфраструктури. Основні складові політики безпеки адміністратора:

– визначення процедур контролю доступу до систем, даних та інших ресурсів, забезпечення відповідності рівнів доступу до потреб користувачів;

– керування автентифікацією та ідентифікацією, встановлення правил і вимог для безпечної авторизації користувачів і надання їм відповідних дозволів для доступу до ресурсів;

– реалізація систем моніторингу та аудиту, які виявляють аномальну або підозрілу активність, а також зберігають журнали подій для подальшого аналізу;

– забезпечення конфіденційності, цілісності та доступності даних шляхом застосування шифрування, засобів резервного копіювання та інших заходів захисту;

– використання заходів, таких як системи виявлення вторгнень і антивірусне ПЗ, для запобігання та виявлення атак;

– регулярне оновлення програмного забезпечення для усунення відомої вразливості і забезпечення безпеки систем;

– надання навчання та інформаційних матеріалів користувачам щодо правил безпеки, створення свідомої культури безпеки.

Для користувача політики безпеки включають вимоги:

– використовувати сильні паролі і виконувати процедури автентифікації, такі як двохфакторна автентифікація, для захисту своїх облікових записів;

– дотримуватися правил і обмежень доступу до ресурсів інформаційної системи відповідно до їх ролі в організації;

– бути свідомими щодо заходів захисту інформації, таких як шифрування даних, застосування паролів до файлів тощо;

– дотримуватися правил щодо використання особистих і робочих пристроїв, таких як комп'ютери, смартфони та планшети, і вживати заходів для їх захисту;

– бути обережними щодо запитів на введення особистої інформації або фінансових даних, а також вміти впізнавати шахрайські атаки;

– організації повинні надавати користувачам навчання щодо правил безпеки, регулярно інформувати їх про потенційні загрози та віруси, навчати користувачів реагувати на них.

Політика безпеки користувача є важливим елементом управління безпекою і допомагає забезпечити захист інформації та інфраструктури від внутрішніх загроз та обґрунтовує вимоги поведінки користувача в системі [30].

Користувачі мають найменше повноважень, проте саме від них залежить безпека, адже користувач використовує систему.

Політика безпеки власника системи – це набір стандартів, які встановлюються власником системи для забезпечення безпеки інформації та захисту активів системи і включають такі моменти:

– визначення стратегічних цілей та пріоритетів щодо захисту інформації – власник системи встановлює політики, які відповідають цим цілям;

– власник системи визначає ризики безпеки, оцінює їх потенційні наслідки та приймає заходи для зниження ризиків до прийнятного рівня;

– власник встановлює правила та процедури для керування доступом до ресурсів системи, забезпечуючи необхідний рівень конфіденційності та захисту даних;

– власник приймає заходи для захисту конфіденційної інформації та забезпечує її цілісність та доступність за допомогою шифрування, захисту від втрати даних та інших технічних та організаційних заходів;

– власник встановлює правила для управління пристроями та мережами, забезпечуючи їх безпеку та захист від несанкціонованого доступу;

– власник забезпечує моніторинг і аудит безпеки системи для виявлення потенційних загроз та виявлення некоректної діяльності [31];

– розробляє плани відновлення та надійності, щоб забезпечити швидке відновлення діяльності в разі інцидентів безпеки або відмов системи;

– забезпечує навчання та свідомість користувачів щодо правил та процедур безпеки, а також надає їм необхідні засоби для виконання цих правил.

Політика безпеки власника системи визначає рамки і стандарти безпеки для всієї організації та забезпечує ефективний захист інформації.

Власник системи має найбільше вимог та правил, адже саме він має найбільше повноважень в установі. Обов’язки власника системи включають аспекти не тільки рівня безпеки, але й організаційного [34].

Отже, політики безпеки визначають правила та обов’язки на різних рівнях використання системи. Обов’язки адміністратору, правила користувачам, вимоги власнику – така ієрархія визначень в політиках безпеки.

Кожен етап формує окремі дії та документи, які все ж пов’язані та можуть містити подібну або навіть таку ж інформацію.

Для полегшення роботи розроблено схему, на основі якої простіше в майбутньому отримати документи, які ми обговорювали в попередніх розділах.

На рисунку 3.3 зображена детальна схема основних документів та їх змісту. Основними виділяємо три документи, два з яких розробляються для університету та один для перевірки Державною службою спеціального зв’язку, а саме – проєкт, технічне завдання та план захисту [35].

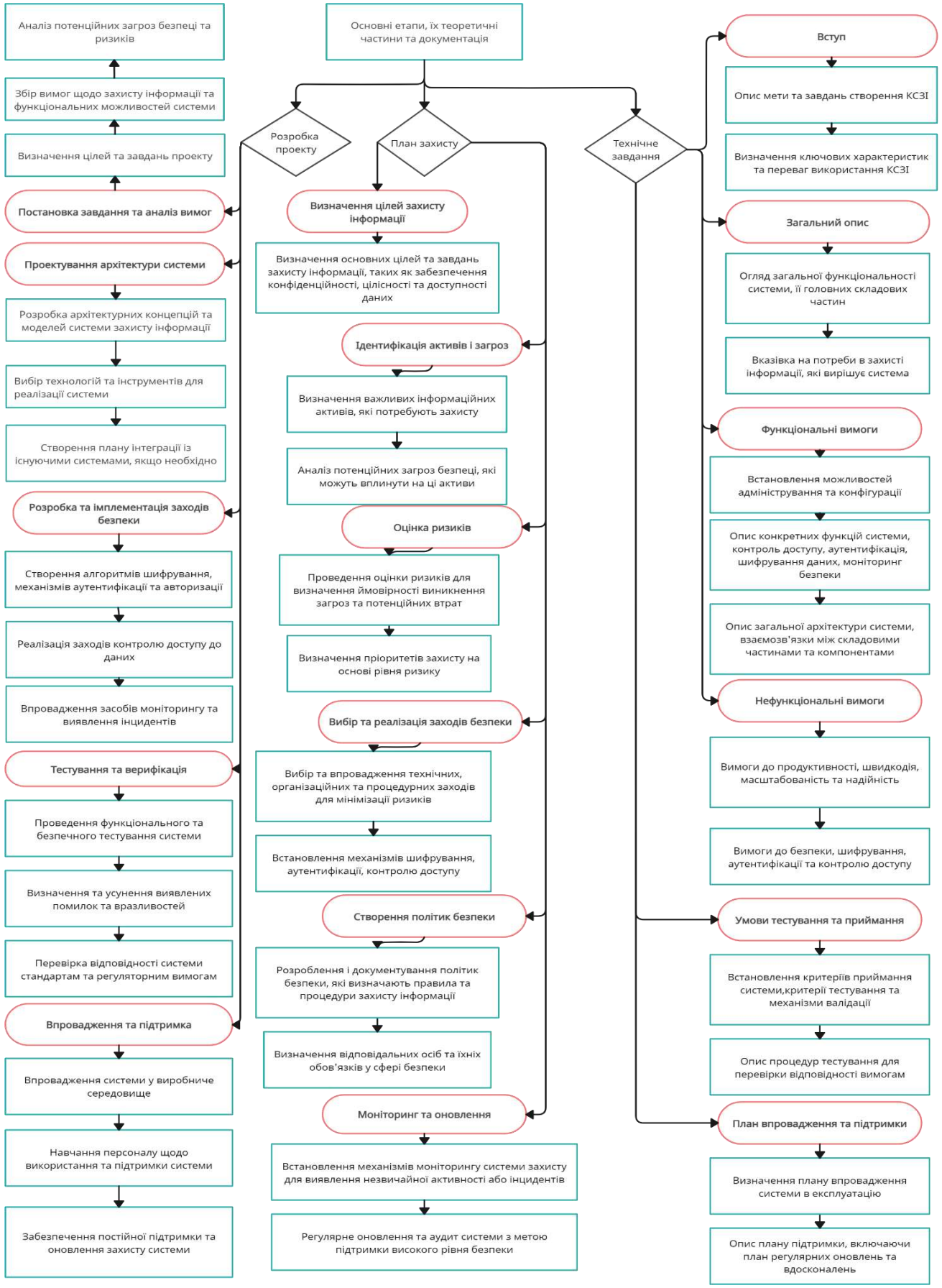


Рисунок 3.3 – Основні етапи та їх характеристики

План захисту формує точну постановку задачі та описує дії, що розробляються та формуються в технічному завдані (додаток Л).

3.4 Висновки

В розділі розглянуто супровід КСЗІ, а саме типову систему захисту інформації, описано організаційні, нормативно-правові та інженерно-технічні заходи, щодо впровадження та експлуатації. Розглянуто етапи підготовки та заключні етапи встановлення КСЗІ. Спроєктовано вимоги до політик встановлення антивірусного ПЗ, було ознайомлено з Центром антивірусного захисту та політиками безпеки суб’єктів.

ВИСНОВКИ

У даній кваліфікаційній роботі спроєктовано КСЗІ класу «1» категорії 4 в ХНУ, зокрема, визначено принципи, методи та технології захисту інформації в сучасному інформаційному середовищі. Результатом аналізу стало розуміння того, що захист інформації стає все більш актуальним та критичним у цифровому світі, де зростає кількість загроз та потенційних атак.

Основною метою проєкту було визначення важливості комплексного підходу до захисту інформації та особливості їх створення та введення. Виявлено, що комплексні системи захисту інформації є ефективним інструментом для забезпечення безпеки даних та мереж у різних сферах діяльності, навіть на рівні університету. Зокрема, проєктування архітектури та розробка КСЗІ, було враховано не лише технічні аспекти, але й вимоги до безпеки та функціональності. Також важливим етапом було тестування та оцінка ефективності спроєктованої системи, що дозволило визначити її придатність для захисту інформації в реальних умовах експлуатації.

У рамках кваліфікаційної роботи також було спроєктовано впровадження КСЗІ в університетському середовищі. Особлива увага була приділена специфіці університетських потреб та вимог до захисту інформації, а також аналізу існуючих підходів та методів впровадження КСЗІ в освітніх установах.

Виявлено, що університети мають великий обсяг конфіденційної інформації, такої як персональні дані студентів і співробітників, дослідницькі матеріали, бюджетні та фінансові документи тощо, тому впровадження ефективної системи захисту інформації є надзвичайно важливим завданням для забезпечення безпеки цих даних.

На основі даної роботи було визначено, що впровадження КСЗІ в університетському середовищі дозволяє забезпечити: конфіденційність даних, такі як, захист особистих даних студентів, викладачів та інших працівників від несанкціонованого доступу; цілісність інформації, а саме забезпечення цілісності

дослідницьких матеріалів, аудиторських звітів та інших документів, що містять критичну інформацію; доступність даних, тобто забезпечення надійного доступу до навчальних та адміністративних ресурсів для студентів, викладачів та адміністраторів.

Отже, впровадження КСЗІ в університеті сприяє забезпеченню безпеки даних, збільшенню довіри користувачів та підвищенню загального рівня інформаційної безпеки університетського середовища.

У цій роботі були опрацьовані закони, нормативні документи сфери захисту інформації та положення відповідно до яких забезпечити захист інформації на рівні законодавства України простіше [37]. Також представлено етапи створення та введення в експлуатацію КСЗІ для АС класу 1 четвертої категорії. Було розроблено документи першого етапу створення КСЗІ відповідно до вимог. Включно з усіма елементами було розроблено: накази та положення; акти; модель загроз та порушника; технічне завдання; формуляр тощо.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 р. № 2657-XII. Редакція від 27.07.2023. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 21.04.2024).

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Редакція від 04.04.2024. – Режим доступу: https://ips.ligazakon.net/document/Z008000?an=4816 (дата звернення 21.04.2024).

3. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII Редакція від 01.01.2024. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 21.04.2024).

4. Про захист персональних даних : Закон України від 20.11.2012 № 2297-VI. Редакція від 27.04.2024. – Режим доступу : https://ips.ligazakon.net/document/T102297?an=371 (дата звернення 21.04.2024).

5. Про затвердження Правил забезпечення захисту інформації інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : Постанова від 29.03.2006 № 373-2006-п. Редакція від 21.10.2022. – Режим доступу : https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення 21.04.2024).

6. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова від 19.10.2016 р. № 736-2016-п. Редакція від 25.08.2023. – Режим доступу : https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text (дата звернення 21.04.2024).

7. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі : Нормативний документ технічного захисту

інформації від 28.12.2012 № z0910-19. Редакція від 25.04.2023. – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення 21.04.2024).

8. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf (дата звернення: 21.04.2024).

9. Типове положення про службу захисту інформації в автоматизованій системі : Нормативний документ технічного захисту інформації від 04.12.2000 № 53. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення 21.04.2024).

10. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : Нормативний документ технічного захисту інформації від 28.04.1999 № 22. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення 21.04.2024).

11. Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Нормативний документтехнічного захисту інформації від 28.04.1999 № 22 URL: https://tzi.ua/assets/files/%D0%9D%D0%94%D0%A2%D0%97%D0%86-2.5-005--99.pdf (дата звернення 21.04.2024).

12. Методичні вказівки щодо розробки технічного завдання на створення КСЗІ в автоматизованій системі : Нормативний документ технічного захисту інформації від 28.06.2002 №22 URL: https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення 22.04.2024).

13. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці : Нормативний документ технічного захисту інформації від 15.04.2013 № 215 URL: https://tzi.com.ua/downloads/1.6-005-2013.pdf (дата звернення 22.04.2024).

14. ЄКТС. Інформаційний пакет (каталог курсу). Загальна інформація. 2023–2024 навчальний рік / упоряд.: А. В. Козак, Л. С. Любохинець. Хмельницький : ХНУ, 2023. 30 с. URL : https://isu1.khmnu.edu.ua/isu/pub/ECTS_paket_ukr/01_zagalna_info.pdf (дата звернення 22.04.2024).

15. Гребеніков В. В. Комплексні системи захисту інформації. проєктування, впровадження, супровід. 2013. 161 с. URL : https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070 (дата звернення 22.04.2024).

16. Танцюра Д. М. Автоматичне налаштування і перевірка налаштувань служб операційної системи при використанні комплексних засобів захисту інформації в А Сах. Київ: НТУУ «КПІ», 2015. 20 с.

17. Бондарчук Ю. В., Марущак А.І. Безпека бізнесу: організаційно-правові основи : науково-практичний посібник. Київ: Видавничий дім «Скіф», 2008. 369 с.

18. Гринь А. К. Управління та організація служби захисту інформації : навчальний посібник. Київ: НА СБ України, 2010. 75 с.

19. Технічний захист інформації. Теоретичні основи та організаційно-технічне забезпечення / В. М Богуш., В. Д. Бровко, О. С. Кобус, В. Д. Козюра Київ: Ліра-К, 2023. 484 с.

20. Основи кіберпростору, кібербезпеки та кіберзахисту / В. М. Богуш, В. Д. Бровко, В. П. Настрадін Київ: Ліра-К, 2021. 554 с.

21. Організаційно-правові основи забезпечення кібербезпеки. / А. І. Марущак та ін. Київ: Ліра-К, 2023. 320 с.

22. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика./ С. В. Пєтков та ін. Київ: ЦУЛ, 2022. 460 с.

23. ECET. Експертні висновки URL: https://www.eset.com/ua/about/why-eset/experts/ (дата звернення: 17.02.2024).

24. Офіційний сайт ЦАЗІ. URL: https://cazi.gov.ua/uk (дата звернення: 17.05.2024).

25. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації» від 26.03.2007 № 45. URL: https://zakon.rada.gov.ua/laws/show/z0320-07#Text (дата звернення: 18.05.2024).

26. Перелік антивірусних засобів в ЦАЗІ. URL: https://cazi.gov.ua/uk/verified-releases (дата звернення: 19.05.2024).

27. Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 19.05.2024).

28. Основи інформаційних технологій і систем. / В. А. Павлиш, Л. К. Гліненко, Н. Б. Шаховська. Львів: Львівська політехніка, 2018. 620 с.

29. Технології захисту інформації. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король, м. Львів: Новий світ-2000, 2022. 678 с.

30. Мирошниченко В. О. Використання сучасних інформаційних технологій: формування мультимедійної компетентності. Київ: Центр учбової літератури, 2023. 296 с.

31. Пухова Г. Є. Системи, технології, інформаційні послуги. Львів: Новий світ-2000, 2007. 90 с.

32. Необхідність створення КСЗІ. URL: https://tzi.com.ua/neobxdnst-stvorennya-kompleksno-sistemi-zaxistu-nformacz-ksz.html (дата звернення: 12.05.2024).

33. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв'язку. URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku (дата звернення: 19.05.2024).

34. Визначення коефіцієнта важливості для експертного оцінювання в галузі інформаційної безпеки. / Д. А. Горніцька, В. В. Волянська, А. О. Корченко Київ: Ліра-К, 2012. 340 с.

35. Віткуп М. О., Петренко В. В. Microsoft Office в прикладах і завданнях з методикою їх розв'язання. Харків: 4-е, 2007. 352 с.

36. Майк Ксі, Сяодун Хуан Evolutionary Topology Optimization of Continuum Structures: Methods and Applications. Видавництво: Wiley. John Wiley & Sons, LTD, 2010. 240 с.

37. Офіційний сайт Адміністрації Держспецзв’язку. URL: https://www.cip.gov.ua/ua/news/ekspertiza (дата звернення: 17.05.2024).

38. Мельник А. О. Архітектура комп'ютера. Луцьк: Волинська обласна друкарня, 2008. 470 с.

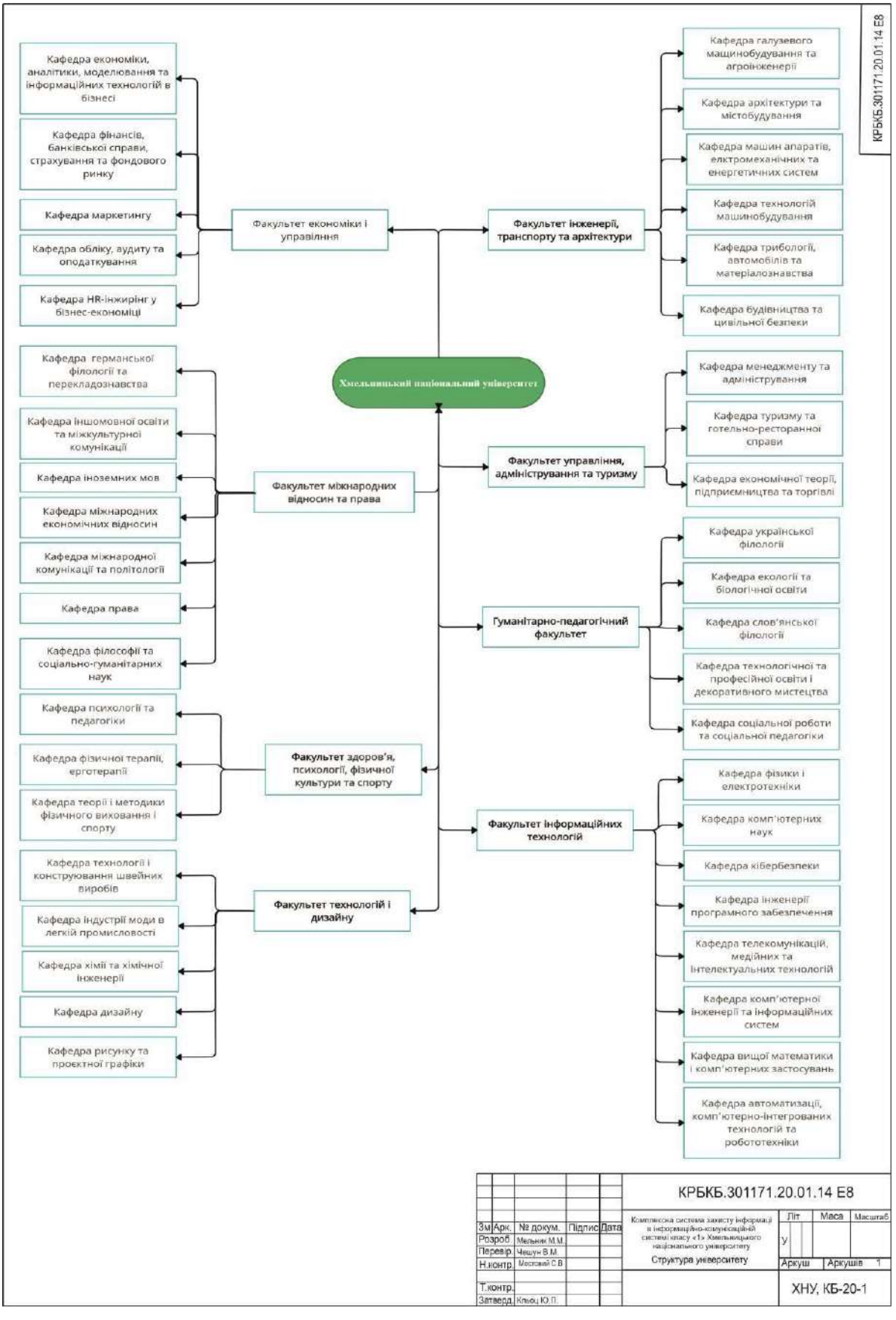
39. З чого почати побудову КСЗІ? URL: https://www.ukrinform.ua/rubric-technology/2446109-z-cogo-pocati-pobudovu-kompleksnoi-sistemi-zahistu-informacii.html (дата звернення: 16.05.2024).

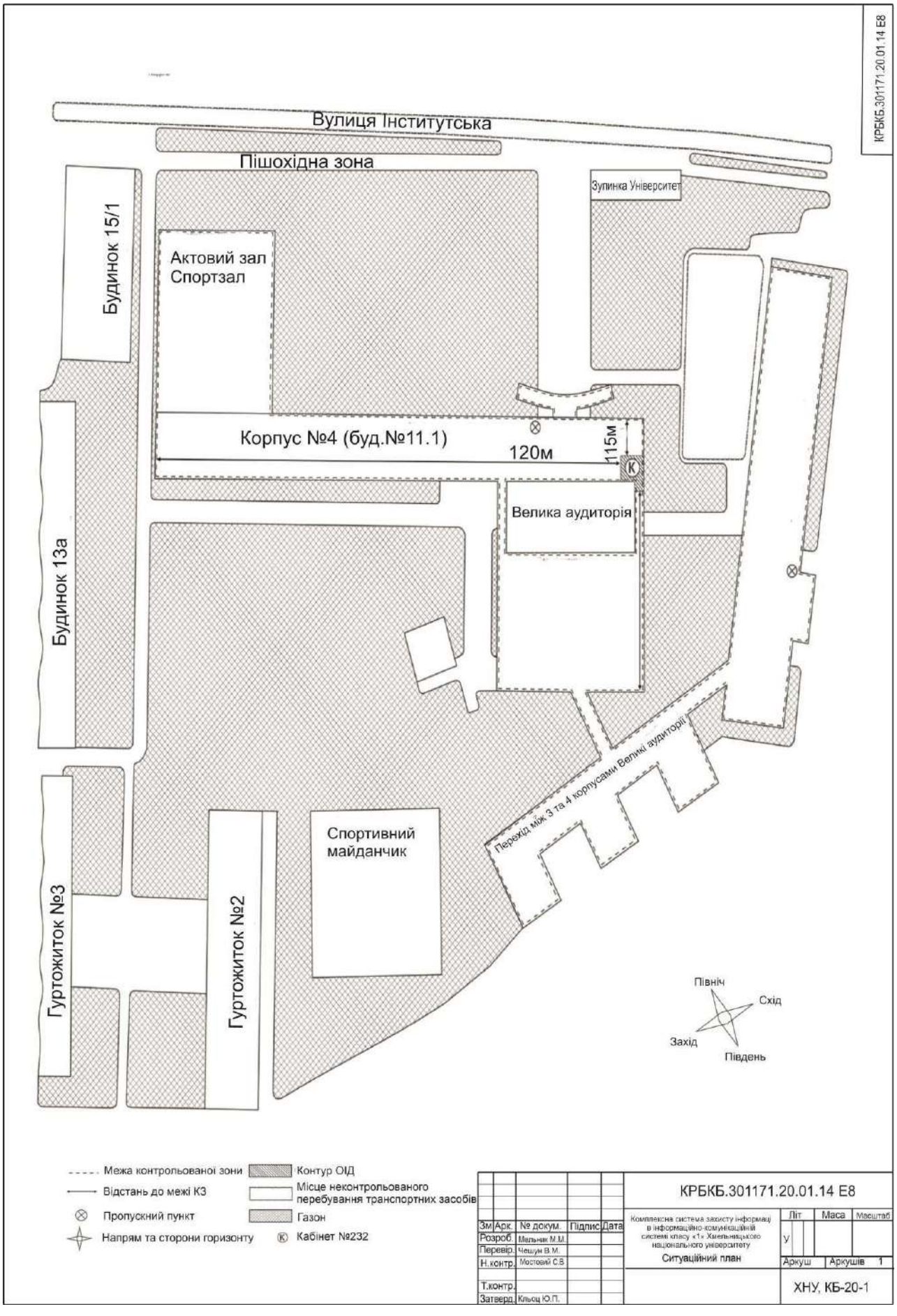
40. КСЗІ – наступний рівень безпеки. URL: https://www.ukrinform.ua/rubric-technology/2803498-kompleksna-sistema-zahistu-informacii-nastupnij-riven-bezpeki.html (дата звернення: 16.05.2024).

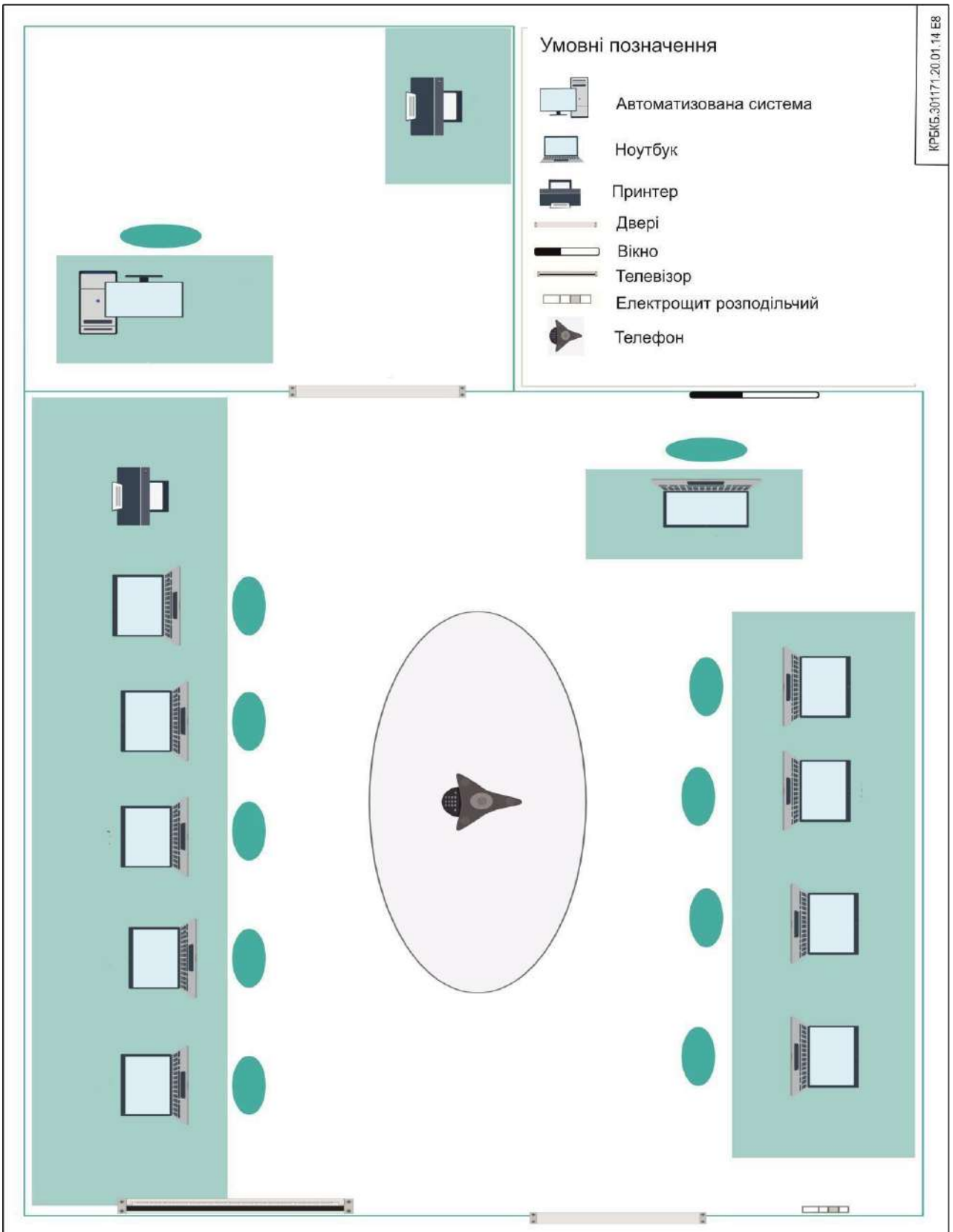
ДОДАТОК А

(обов'язковий)

Копії графічної частини

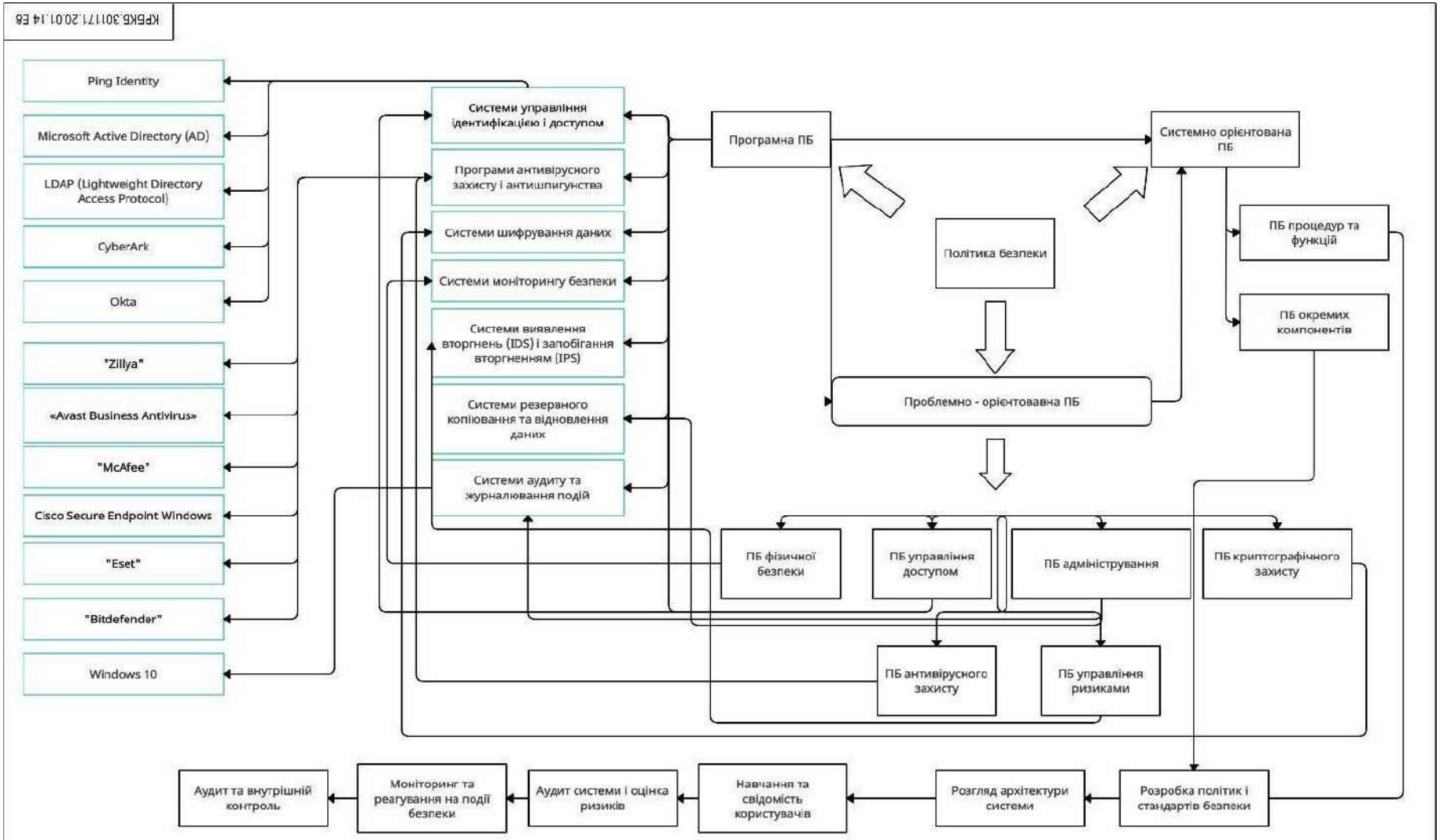



КРБКБ.301171.20.01.14 Е8
Вулиця Інститутська
Пішохідна зона
Зупинка Університет
Будинок 15/1
Актовий зал
Спортзал
Корпус №4 (буд.№11.1)
120м
115м
К
Велика аудиторія
Будинок 13а
Перехід між 3 та 4 корпусами Великої аудиторії
Спортивний майданчик
Гуртожиток №3
Гуртожиток №2
Північ
Схід
Захід
Південь
Межа контрольованої зони
Відстань до межі КЗ
Пропускний пункт
Напрям та сторони горизонту
Контур ОІД
Місце неконтрольованого перебування транспортних засобів
Газон
К Кабінет №232
КРБКБ.301171.20.01.14 Е8
Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету
Ситуаційний план
Літ
Маса
Масштаб
У
Аркуш
Аркушів 1
ХНУ, КБ-20-1
Зм Арк. № докум. Підпис Дата
Розроб. Мельник М.М.
Перевір. Чешум В.М.
Н.контр. Мостовий С.В.
Т.контр.
Затверд. Кльоц Ю.П.


Умовні позначення
Автоматизована система
Ноутбук
Принтер
Двері
Вікно
Телевізор
Електрощит розподільчий
Телефон
КРБКБ.301171.20.01.14 Е8
КРБКБ.301171.20.01.14 Е8
Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету
Генеральний план
Літ
Маса
Масштаб
Аркуш
Аркушів 1
ХНУ, КБ-20-1
Зм. Арк. № докум. Підпис Дата
Розроб. Мельник М.М.
Перевір. Чешун В.М.
Н.контр. Мостовий С.В
Т.контр.
Затверд. Кльоц Ю.Л.


КРБКБ.301171.20.01.14 Е8
Основні етапи, їх теоретичні частини та документація
Розробка проекту
План захисту
Технічне завдання
Аналіз потенційних загроз безпеці та ризиків
Збір вимог щодо захисту інформації та функціональних можливостей системи
Визначення цілей та завдань проекту
Постановка завдання та аналіз вимог
Проектування архітектури системи
Розробка архітектурних концепцій та моделей системи захисту інформації
Вибір технологій та інструментів для реалізації системи
Створення плану інтеграції із існуючими системами, якщо необхідно
Розробка та імплементація заходів безпеки
Створення алгоритмів шифрування, механізмів аутентифікації та авторизації
Реалізація заходів контролю доступу до даних
Впровадження засобів моніторингу та виявлення інцидентів
Тестування та верифікація
Проведення функціонального та безпечного тестування системи
Визначення та усунення виявлених помилок та вразливостей
Перевірка відповідності системи стандартам та регуляторним вимогам
Впровадження та підтримка
Впровадження системи у виробниче середовище
Навчання персоналу щодо використання та підтримки системи
Забезпечення постійної підтримки та оновлення захисту системи
Визначення цілей захисту інформації
Визначення основних цілей та завдань захисту інформації, таких як забезпечення конфіденційності, цілісності та доступності даних
Ідентифікація активів і загроз
Визначення важливих інформаційних активів, які потребують захисту
Аналіз потенційних загроз безпеці, які можуть вплинути на ці активи
Оцінка ризиків
Проведення оцінки ризиків для визначення ймовірності виникнення загроз та потенційних втрат
Визначення пріоритетів захисту на основі рівня ризику
Вибір та реалізація заходів безпеки
Вибір та впровадження технічних, організаційних та процедурних заходів для мінімізації ризиків
Встановлення механізмів шифрування, аутентифікації, контролю доступу
Створення політик безпеки
Розроблення і документування політик безпеки, які визначають правила та процедури захисту інформації
Визначення відповідальних осіб та їхніх обов'язків у сфері безпеки
Моніторинг та оновлення
Встановлення механізмів моніторингу системи захисту для виявлення незвичайної активності або інцидентів
Регулярне оновлення та аудит системи з метою підтримки високого рівня безпеки
Вступ
Опис мети та завдань створення КСЗІ
Визначення ключових характеристик та переваг використання КСЗІ
Загальний опис
Огляд загальної функціональності системи, її головних складових частин
Вказівка на потреби в захисті інформації, які вирішує система
Функціональні вимоги
Встановлення можливостей адміністрування та конфігурації
Опис конкретних функцій системи, контроль доступу, аутентифікація, шифрування даних, моніторинг безпеки
Опис загальної архітектури системи, взаємозв'язки між складовими частинами та компонентами
Нефункціональні вимоги
Вимоги до продуктивності, швидкодія, масштабованість та надійність
Вимоги до безпеки, шифрування, аутентифікації та контролю доступу
Умови тестування та приймання
Встановлення критеріїв приймання системи,критерії тестування та механізми валідації
Опис процедур тестування для перевірки відповідності вимогам
План впровадження та підтримки
Визначення плану впровадження системи в експлуатацію
Опис плану підтримки, включаючи план регулярних оновлень та вдосконалень
КРБКБ.301171.20.01.14 Е8
Зм Арк. № докум. Підпис Дата
Розроб. Мельник М.М.
Перевір. Чешун В.М.
Н.контр. Мостовий С.В.
Т.контр.
Затверд. Кльоц Ю.П.
Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету
Алгоритм впровадження КСЗІ
Літ
Маса
Масштаб
У
Аркуш
Аркушів 1
ХНУ, КБ-20-1

КРБКБ.301171.20.01.14 Е8



				КРБКБ.301171.20.01.14 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	
Розроб.		Мельник М.М.			Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «І» Хмельницького національного університету
Перевір.		Чешун В.М.			Політики безпеки
Н.контр.		Мотовні С.В.			
Т.контр.					
Затверд.		Кльоц Ю.П.			

Літ	Маса	Масштаб
У		
Аркуш	Аркушів 1	
ХНУ, КБ-20-1		

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Мельник Мар'яни Миколаївни
ПІБ здобувача вищої освіти
Студентки 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, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена 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.

08.06.2024
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016347109

Дата перевірки:
11.06.2024 20:44:13 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 22:35:02 EEST

ID користувача:
100008300

Назва документа: Мельник_Дипломна (на плагіат)

Кількість сторінок: 65 Кількість слів: 10838 Кількість символів: 88934 Розмір файлу: 1.27 MB ID файлу: 1016148835

4.57%
Схожість

Найбільша схожість: 1.87% з Інтернет-джерелом (http://www.sai.gov.ua/uploads/filemanager/file/tz_zovn_korist.pdf)

4.38% Джерела з Інтернету	444	Сторінка	67
0.83% Джерела з Бібліотеки	35	Сторінка	69

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 129633 Назва: Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету Додано в БД: 2024-06-11 Автора: Мельник М.М. Керівники: Чешун В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	72019	1116	950 (1%)	17 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

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 в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету

Автор: Мельник Мар'яна Миколаївна

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий 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 95,43%, 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»

Студентка Мельник Мар'яна Миколаївна

Тема Комплексна система захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 5; кількість сторінок записки 72.

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. Налаштовано політики безпеки автоматизованої системи. У підсумку розроблено технчну документацію і необхідні проєктні рішення комплексної системи захисту інформації в інформаційно-комунікаційній системі класу «1» Хмельницького національного університету.

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 роглянуті 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, вимоги та рекомендації щодо експлуатації комплексної системи захисту інформації, політики безпеки встановлення антивірусного захисту, інструкції користувачам та адміністратору

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 в інформаційно-комунікаційній системі Хмельницького національного університету

5. Негативні сторони роботи В роботі недостатньо 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

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 «відмінно»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Бойко Юлій Миколайович
професор кафедри ТМІТ, доктор технічних наук, професор

« 11 » 06 2024. (підпис)