Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Центру перепідготовки та післядипломної освіти
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Проект комплексної системи захисту інформації автоматизованої системи класу «2» на базі підрозділу університету

Виконав: студент II курсу, групи СБд-2
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

		Петришин Ю.І.
	(підпис)	(прізвище та ініціали)
Керівник		*Марценюк В.П.*
	(підпис)	(прізвище та ініціали)
Нормоконтроль		*Лобур Т.Б.*
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		*Загородна Н.В.*
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет центру перепідготовки та післядипломної освіти
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Петришину Юрію Івановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Проект комплексної системи захисту інформації автоматизованої системи класу «2» на базі підрозділу університету

Керівник роботи Марценюк Василь Петрович, д.т.н., професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_25_» _листопада_ 2022 року № _4/7-966_

2. Термін подання студентом завершеної роботи 14 грудня 2022р.

3. Вихідні дані до роботи Наукові публікації системи менеджменту, модель iso 27001

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Аналіз нормативно-правової бази забезпечення комплексного захисту інформації в автоматизованих системах, 1.1 Загальні поняття та визначення в галузі проектування захищених автоматизованих систем, 1.2 Класифікація автоматизованих 1 систем, 1.3 Порядок створення комплексної системи захисту інформації, 1.4 Характеристика підприємства, цілі і завдання, структура кафедри, 1.5 Висновок до першого розділу, 2 Аудит інформаціної безпеки, 2.1 Аналіз інформації, що циркулює на кафедрі, 2.2 Категоріювання об'єкта, 2.3 Види загроз інформації, 2.4 Потенційні канали витоку інформації, 2.5 Ефективність існуючої системи безпеки кафедри, 2.6 Вискновок до другого розділу, 3 Визначення вимог до КСЗІ об'єкта, 3.1 Вимоги до АС, 3.2 Вимоги до КСЗІ в області виконання вимог, що регламентують обробку персональних данних, 3.3 Висновок до третього розділу, 4 Розробка КСЗІ та розробка заходів і методики по її впровадженню на об'єкт, що захищається, 4.1 Структурна і функціональна схеми КСЗІ об'єкта, 4.2 Організаційно-правові заходи, 4.3 Програмно-апаратні засоби захисту інформації 4.4 Інженерно-технічні заходи захисту, 4.5 Висновок до четвертого розділу, 5 Охорона праці та безпека в надзвичайних ситуаціях, 5.1 Охорона праці, 5.2 Безпека в надзвичайних ситуаціях, 5.3 Висновок до сьомого розділу, Висновки, Список літературних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Ситуаційний план будівлі, 2 Розміщення приміщень підрозділу, 3 Фізична схема мережі підрозділу, 4 Схема охоронно-пожежної сигналізації, 5 Схема відеоспостереження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., старший викладач		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.11.2022-15.11.2022	*Виконано*
2.	Підбір наукових джерел про хмарні платформи	16.11.2022-20.11.2022	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	дослідження методів захисту відомих хмарних		
	платформ	21.11.2022-23.11.2022	*Виконано*
4.	Виконання дослідження щодо аналіз інструментів для		
	організації інфраструктури та безпеки публічної		
	хмари	24.11.2022-27.11.2022	*Виконано*
5.	Оформлення розділу «Інструменти організації		
	безпеки хмарних серверів»	28.11.2022-30.11.2022	*Виконано*
6.	Оформлення розділу «Варіанти використання		
	моделей архітектури»	01.12.2022-04.12.2022	*Виконано*
7.	Оформлення розділу «Практична реалізація»	05.12.2022-07.12.2022	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2022-09.12.2022	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2022-11.12.2022	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2022-13.12.2022	*Виконано*
11.	Нормоконтроль	14.12.2022-15.12.2022	*Виконано*
12.	Перевірка на плагіат	9.12.2022	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2022	*Виконано*
14.	Захист кваліфікаційної роботи	.12.2022	

Студент _____ Петришин Ю.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценюк В.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Проект комплексної системи захисту інформації автоматизованої системи класу «2» на базі підрозділу університету // Кваліфікаційна робота освітнього рівня «Магістр» // Петришин Юрій Іванович // Тернопільський національний технічний університет імені Івана Пулюя, Центру перепідготовки та післядипломної освіти, кафедра кібербезпеки, група СБд-2 // Тернопіль, 2022 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: КСЗІ, АС, ISO 21700, ІНФОРМАЦІЙНА БЕЗПЕКА

Кваліфікаційній робота присвячена, розробці комплексної системи захисту інформації автоматизованої системи класу «2» підроьзділу університету. В ході виконання роботи був проведений аналіз інформаційної безпеки об'єкта, що захищається, в результаті якого виявлено склад джерел і носіїв інформації, проведено категоріювання інформації, виявлено можливі канали витоку інформації. В рамках аудиту інформаційної безпеки була проаналізована поточна діяльність підрозділу з питань захисту інформації, проведено оцінку інформаційної системи організації, в якій циркулює конфіденційна інформація; були виявлені недоліки системи захисту, способи, усунення яких представлені в роботі.

У першому розділі кваліфікаційної роботи представлена характеристика об'єкта.

У другому розділі кваліфікаційної роботи представлені результати аудиту інформаційної безпеки об'єкта, що захищається. В ході проведення аудиту інформаційної безпеки був виконаний аналіз інформації, що циркулює на об'єкті, що підлягає захисту, визначені її види; виявлені загрози, актуальні для даної інформації. Крім цього, були проаналізовані діючі засоби і методи захисту інформації та дано оцінку їх роботі. Також представлені вимоги, які слід

пред'явити до комплексної системи захисту інформації; описані вимоги до правової, організаційної, інженерно-технічної і програмно-апаратної складової системи захисту; визначено склад і характеристики відповідних підсистем і засобів захисту.

У третьому розділі кваліфікаційної роботи представлена розробка КЗСІ та розробка **заходів і методик по її впровадженню на об'єкт, що захищається; тобто** організаційно-правові заходи, програмно-апаратні засоби захисту інформації, інженерно-технічні заходи захисту інформації.

В результаті виконання дипломної роботи була розроблена комплексна система захисту об'єкта, був проведений підбір технічних і програмно-апаратних засобів, а так само розроблена документація, яка використовується при роботі з програмно-апаратними засобами захисту.

ANNOTATION

The project of the complex information protection system of the automated system of class "2" on the basis of the university division // Qualification work of the educational level "Master" // Petryshyn Yuriy // Ternopil Ivan Puluj National Technical University, Center of retraining and postgraduate education, Department of cyber security, sbd group -2 // ternopil, 2022 // s. , fig. - , tab. - , chair. - , add. – , bibliography -

Keywords: cips, as, iso 21700, information security

The qualification work is devoted to the development of a complex information protection system of the automated class "2" system of the university subdivision. In the course of the work, an analysis of the information security of the object being protected was carried out, as a result of which the composition of sources and carriers of information was identified, information was categorized, and possible channels of information leakage were identified. As part of the information security audit, the current activity of the information protection division was analyzed, an assessment of the organization's information system in which confidential information circulates was carried out; the shortcomings of the protection system were identified, the methods of elimination of which are presented in the work.

The first section of the qualification work presents the characteristics of the object.

The second section of the qualification work presents the results of the information security audit of the protected object. In the course of the information security audit, an analysis of the information circulating on the object subject to protection was performed, its types were determined; identified threats relevant to this information. In addition, current means and methods of information protection were analyzed and their work was evaluated. The requirements that should be presented to

the comprehensive information protection system; the requirements for the legal, organizational, engineering-technical and software-hardware components of the protection system are described; the composition and characteristics of relevant subsystems and means of protection are defined.

The third chapter of the qualification work presents the development of the kssi and the development of measures and methods for its implementation on the protected object; that is, organizational and legal measures, software and hardware means of information protection, engineering and technical measures of information protection.

As a result of the diploma work, a complex system of object protection was developed, technical and hardware and software tools were selected, and documentation was also developed, which is used when working with software and hardware protection tools.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизована система;

АСЕ – автоматизована система управління;

АСНД – автоматизована система наукових досліджень;

ДТЗС – додаткові технічні засоби та системи;

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України;

ЗОТ – засіб обчислювальної техніки;

ІзОД – інформація з обмеженим доступом;

ІСПДн – інформаційна система персональних даних;

КЗЗ – комплекс засобів захисту від несанкціонованого доступу;

КТ – контрольована територія;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОС – операційна система;

ОТЗС – основні технічні засоби та системи;

ПЗ – програмне забезпечення;

РСО – режимно-секретний орган;

САПР – системи автоматизованого проектування;

СУІБ – система управління інформаційною безпекою;

ТЗ – технічне завдання;

ФПЗ – функціональні послуги захисту.

ЗМІСТ

ВСТУП

Мета даної дипломної роботи полягає в розробці комплексної системи захисту інформації автоматизованої системи класу «2» пмідроздбілу університету.

Реалізація запропонованого проекту дозволить підвищити рівень захищеності інформації.

При розробці і побудові комплексної системи захисту інформації необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, виробництва, експлуатації. Системи захисту інформації відносяться до числа складних систем, і для їх побудови можуть використовуватися різні принципи побудови систем з урахуванням специфіки розв'язуваних ними завдань.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ – 2 %;
- укорінення вірусів – 3 %;
- технічні відмови апаратури мережі – 20 %;
- цілеспрямовані дії персоналу – 20 %;
- помилки персоналу (недостатній рівень кваліфікації) – 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

У першому розділі дипломної роботи представлена характеристика об'єкта.

У другому розділі дипломної роботи представлені результати аудиту

інформаційної безпеки об'єкта, що захищається. В ході проведення аудиту інформаційної безпеки був виконаний аналіз інформації, що циркулює на об'єкті, що підлягає захисту, визначені її види; виявлені загрози, актуальні для даної інформації. Крім цього, були проаналізовані діючі засоби і методи захисту інформації та дано оцінку їх роботі.

У третьому розділі дипломної роботи представлені вимоги, які слід пред'явити до комплексної системи захисту інформації; описані вимоги до правової, організаційної, інженерно-технічної і програмно-апаратної складової системи захисту; визначено склад і характеристики відповідних підсистем і засобів захисту.

У висновку дипломної роботи сформульовані загальні висновки щодо розробленої комплексної системи захисту.

РОЗДІЛ 1 АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

1.1 Загальні поняття та визначення в галузі проектування захищених автоматизованих систем

Існуюча нормативно-правова база в Україні ще не досягла необхідного розвитку в цій сфері. Наприклад, із величезного переліку стандартів і нормативних документів України можна виділити лише декілька, які можна використовувати при проектуванні захищеної АС.[2-5] Тому при виконанні даного виду робіт фахівці використовують також міжнародні (ISO) і міждержавні (ГОСТ, затверджений до 1992 року включно) стандарти.[6] Згідно з одним із цих стандартів [7], АС – це система, що складається з персоналу та комплексу засобів для автоматизації його діяльності та впровадження інформаційних технологій для виконання заданих функцій. Залежно від виду діяльності розрізняють такі види АС: автоматизовані системи управління (АСУ), автоматизовані системи проектування (САПР), автоматизовані науково-дослідні системи (АСНІ) та ін. Залежно від типу контрольованого об’єкта (процесу) АСУ поділяють на АСУ за технологічними процесами (АСУТП), АСУ підприємства (АСУП) тощо. У нашому випадку операційна система – це середовище обробки інформації, а також інформаційні ресурси в інформаційно-комунікаційній системі. Тому надалі ми будемо використовувати поняття автоматизованої інформаційної системи. Закон України «Про інформацію» [1] трактує термін «інформація» так: «Інформація — це документовані або публічно оголошені відомості про події та явища в суспільстві, державі та навколишньому середовищі». З іншого боку, захист інформації в АС є заходом, спрямованим на забезпечення безпеки інформації, що обробляється в АС, і АС в цілому, і дозволяє запобігти або

запобігти можливості виникнення загроз, а також підвищити величину потенційних ліміт збитків у результаті загроз. [2]

Таким чином, АІС є складною системою, яку необхідно розділити на окремі блоки (модулі) для подальшого проектування. В результаті кожен модуль незалежний від інших і утворює цілісну систему безпеки в комплексі.

Відображення окремих модулів АІС дозволяє службі захисту інформації:

• своєчасно та належним чином реагувати на певні види інформаційних загроз, характерних для конкретного модуля;

• швидко впровадити систему захисту інформації у щойно випущених модулях;

• Спрощення процедури контролю системи захисту інформації в цілому (під системою захисту ІТ-інфраструктури підприємства в цілому слід розуміти набір модулів систем захисту інформації).

Поступово збільшуючи кількість модулів, а також ускладнюючи захисну структуру, АІС набуває певної складності, що передбачає використання у всіх модулях не одного виду захисних функцій, а їхнього продукту. Таким чином, побудова ЦСЗІ стає невід'ємним фактором у розробці ефективної системи захисту від несанкціонованого доступу. Відповідно до [8] КСЗІ – це комплекс організаційно-технічних заходів, апаратно-програмних засобів, що забезпечують захист інформації в АС. Звідси видно, що, наприклад, при проектуванні КСЗІ не можна обійтися без простого екранування приміщення, оскільки цей спосіб забезпечує захист інформації лише від витоку по радіоканалу. У загальному вигляді термін «складність» означає розв’язання двох або більше багатоаспектних завдань у рамках однієї концепції (цільова складність), або використання багатоаспектних інструментальних засобів для вирішення одного завдання (інструментальна складність), або те й інше (загальна складність). Цільова комплексність означає, що система інформаційної безпеки повинна будуватися таким чином:

• Захист інформації, ресурсів та інформаційних систем людини,

суспільства та влади від зовнішніх та внутрішніх загроз;

• Захист особистості, суспільства і держави від негативного впливу інформації.

Інструментальна складність полягає в інтеграції всіх видів і напрямків ШІ для досягнення поставлених цілей. Сучасна система захисту інформації повинна враховувати структурну, функціональну та часову складність. Структурна складність полягає в забезпеченні необхідного рівня захисту всіх елементів системи обробки інформації. Функціональна складність означає, що процедури захисту повинні бути спрямовані на всі функції реалізованої системи обробки інформації. Часова складність передбачає безперервність заходів із захисту інформації, як у процесі їх безпосередньої обробки, так і на всіх етапах життєвого циклу суб’єкта обробки інформації.

1.2 Класифікація автоматизованих систем

Нормативним документом [4] передбачено класифікацію АС на 3 класи:

Клас 1 - це комплекс, що складається з машини та користувача, який обробляє інформацію, що належить до однієї або кількох категорій конфіденційності. Прикладом може служити автономний персональний комп'ютер, доступ до якого контролюється організаційними заходами.

Клас 2 – це локалізований комплекс із кількома машинами та кількома користувачами, який обробляє інформацію різних категорій конфіденційності. Прикладом може служити локальна комп'ютерна мережа.

Клас 3 — це розподілений комплекс із кількома машинами та кількома користувачами, який обробляє інформацію в різних категоріях конфіденційності. Прикладом може служити глобальна комп'ютерна мережа.

1.2.1 Особливості АС класу 1

Інформація з обмеженим доступом, а саме: конфіденційна інформація, що є власністю держави, та інформація, що становить державну таємницю, створюється, обробляється та зберігається в режимно-секретному органі (ОРС). Така інформація в більшості випадків обробляється за допомогою класу 1 АС, який має такі характеристики:

• одночасно з комплексом може працювати тільки один користувач, хоча загалом доступ до комплексу можуть мати кілька осіб, але всі повинні мати однакові дозволи (права) на доступ до інформації, що обробляється;

• Технічні засоби (носії інформації та засоби введення/виведення) з точки зору безпеки належать до однієї категорії і всі можуть використовуватися для зберігання та/або введення/виведення будь-якої інформації.

Для виконання робіт, пов'язаних з будівництвом КСЗІ РСО, спеціалісти організації-виконавця повинні мати дозвіл, який є державною таємницею. При створенні КСЗІ РСО використовуються лише такі технічні засоби захисту інформації, які мають експертний висновок або сертифікат відповідності Державної служби спеціального захисту зв’язку та інформації (ДСЗІ) України, інші технічні засоби захисту інформації заборонені.

Методика виконання робіт зі спорудження КСЗІ АС 1 класу базується на наступних попередніх даних:

• Запобіжний пристрій - робоче місце.

• Захист інформації від витоку технічними каналами здійснюється за допомогою захищеного робочого місця або спеціальних заходів.

• Захист від несанкціонованого доступу до інформації забезпечується спеціальним програмним або апаратно-програмним забезпеченням захисту від несанкціонованого доступу.

• Захист комп'ютера від вірусів, троянів і шпигунських програм - антивірусне програмне забезпечення.

1.2.2 Особливості АС класу 2 і 3

АС класів 2 і 3 в основному обробляють конфіденційну або публічну інформацію, що належить уряду та відповідає вимогам цілісності та доступності.

Характеристики АС 2 класу: Наявність користувачів з різними правами доступу та/або технічними засобами, які можуть обробляти інформацію різних категорій конфіденційності одночасно. Характеристики 3 класу AS: необхідність передачі інформації через незахищену мережу або, взагалі, наявність вузлів, які реалізують різні політики безпеки.

Клас АС 3 відрізняється від класу АС 2 наявністю каналу доступу в Інтернет. Як і при створенні КСЗІ РСО, при встановленні КСЗІ АС 2 та 3 класу організація-виконавець повинна мати ліцензію на виконання робіт у сфері технічного захисту інформації та застосовувати сертифіковані засоби технічного захисту інформації.

Робота над дизайном AS CSI Class 2(3) базується на наступних попередніх даних:

• Об’єкти захисту – це робочі місця, шляхи передачі даних, веб-сервери, периметри ІТ-систем тощо.

• Захист від несанкціонованого доступу реалізується за допомогою простих засобів операційної системи або за допомогою спеціальних програмних, апаратних і програмних засобів.

• Захист каналів передачі даних через незахищене середовище - апаратні, програмні, апаратно-програмні засоби шифрування інформації.

• Захист периметра – програмне забезпечення, апаратні брандмауери, системи виявлення вторгнень.

• Захист комп’ютера (мережі) від вірусів, троянів і шпигунського ПЗ – антивірусне програмне забезпечення.

• Захист електронного документообігу та електронної пошти - використання засобів електронного цифрового підпису.

Споживачами CSCI AS 2 та 3 класу є державні органи та компанії, діяльність яких пов’язана з обробкою конфіденційної інформації, що належить державі.

1.2.3 Системи інформаційної безпеки

Існує ще один вид АС [9] – системи захисту інформації (СЗІ).

SIB — це рішення, розроблене для забезпечення захисту критично важливої інформації організації від розголошення, втрати та несанкціонованого доступу. Подібно до КСЗІ, СІБ поєднує в собі комплекс організаційних заходів і технічних заходів захисту інформації. SIB в основному використовуються для захисту інформації в AS класів 2 і 3. Однак між KSZI і SIB є принципові відмінності. Перша відмінність полягає в тому, що при побудові СІБ немає необхідності дотримуватися вимог нормативних документів щодо захисту технічної інформації, оскільки основними одержувачами СІБ є комерційні організації, які не обробляють державну інформацію. Другою великою відмінністю є відсутність органу контролю, завдяки чому проектована СІБ не потребує державної експертизи. Ще однією відмінністю від КСЗІ є вільний вибір технічних засобів, можливість використання будь-яких апаратних і програмних засобів захисту інформації. SIB можна рекомендувати комерційним організаціям, які піклуються про збереження своєї комерційної (критично важливої) інформації або мають намір вжити заходів для забезпечення безпеки своїх інформаційних активів. Для того щоб визначити необхідність побудови системи інформаційної безпеки та напрямок роботи із захисту інформації, а також оцінити реальний рівень інформаційної безпеки в організації, необхідно провести аудит інформаційної безпеки. Для КСЗІ РСО та КСЗІ АС 2 і 3 класу впровадження такого аудиту також є першим кроком. Ця робота називається вивченням інформаційної інфраструктури організації.

Важливим моментом у роботі АС CSI Class 2 і Class 3 і SIB є те, що недостатньо просто побудувати та експлуатувати ці системи безпеки, необхідно постійно вдосконалювати їх, а також методи несанкціонованого доступу, злому. і Хакерські методи є розширеними атаками. Порівняльний аналіз усіх перелічених систем захисту інформації наведено в табл. 1.1. Як бачимо, до процесу будівництва CSZI та підрядника цієї роботи висуваються більш жорсткі вимоги порівняно з вимогами до будівництва SIB. Надалі ми будуватимемо проектування системи безпеки на АС 1 і 2 класів, оскільки саме ці системи обробки інформації найбільше цікавлять зловмисника з точки зору його крадіжки.

Таблиця 1.1 - Порівняльний аналіз систем захисту інформації

Особливості КСЗІ	РСО КСЗІ	АС класу 2 (3)	СІБ
1	2	3	4
споживачі послуг	Органи державної влади, комерційні організації	Органи державної влади, комерційні організації	комерційні організації
оброблювана інформація	Конфіденційна інформація, яка належить державі, або інформація, яка містить державну таємницю	Конфіденційна інформація, яка належить державі (фізичній особі), або відкрита інформація, яка належить державі	Критична інформація організації (персональна, фінансова, договірна інформація, інформація про замовників)
суб'єкти	Замовник виконавець Контролюючий орган	Замовник виконавець Контролюючий орган	Замовник виконавець
наявність ліцензії на проведення робіт з побудови	Ліцензія на проведення робіт з технічного захисту інформації	Ліцензія на проведення робіт з технічного захисту інформації	Не вимагається
проведення державної експертизи	обов'язково	обов'язково	Не вимагається
технічні засоби захисту інформації	Тільки сертифіковані засоби захисту інформації	Тільки сертифіковані засоби захисту інформації	Будь-які засоби захисту інформації
виконання вимог нормативної бази	обов'язково	обов'язково	Не вимагається

1.3 Порядок створення комплексної системи захисту інформації

Створення КСЗІ в ІТ здійснюється згідно з нормативним документом системи технічного захисту інформації [10] на основі технічного завдання (далі – ТЗ), розробленого відповідно до вимог нормативного документа технічної інформації. система захисту [5]. Крім того, при проектуванні КСЗІ можна керуватися стандартом [11]. ІЗО включає заходи та заходи щодо реалізації способів, способів і механізмів захисту інформації від:

• витік через технічні канали, у тому числі бічні канали електромагнітного випромінювання та провідності, електроакустикопроводи та інші;

• Несанкціоновані дії та доступ до інформації, отриманої шляхом підключення до пристроїв і ліній зв'язку, видавання себе за зареєстрованого користувача, обхід заходів безпеки для використання інформації або нав'язування неправдивої інформації, використання вбудованих пристроїв або програм, використання комп'ютерів, комп'ютерних вірусів тощо;

• специфічний вплив на інформацію, який може бути досягнутий шляхом створення полів і сигналів для порушення цілісності інформації або руйнування системи безпеки.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються характеристиками інформації, що обробляється, класом СА та умовами експлуатації. Загалом процес і зміст розробки дослідження CSZI можна розділити на 4 етапи. Незважаючи на простоту структури розробки КСЗІ, більшість організацій використовують цей алгоритм. Однак цей алгоритм є лише основою розробки. Кожен представлений етап відображає вимоги до його системи захисту на багатьох рівнях під час проектування залежно від структури АС. Розглянемо ці етапи докладніше.

1.3.1 Аналіз структури автоматизованої інформаційної системи

Цей етап розширення включає наступні роботи:

• попередній огляд проекту;

• Розробка аналітичного обґрунтування створення КСЗІ;

• Розробка технічного завдання на створення КСЗІ.

На цьому етапі проводиться аналіз ризиків. Щоб перевірити стійкість IT-системи проти несанкціонованого доступу та спроб впливу, іноді доцільно проводити тести на проникнення.

Існують різні типи досліджень [15]:

• Перед проектне діагностичне обстеження, що проводиться при модернізації або будівництві ГКВ;

• Аудит SHI на відповідність вимогам внутрішніх стандартів компанії або міжнародних/національних стандартів. Прикладом може бути сертифікаційний аудит системи менеджменту ІБ згідно з ISO 27001;

• спеціальні види розслідувань, наприклад, розслідування комп'ютерних інцидентів.

Світовий досвід створення систем захисту різних типів об’єктів дозволяє виділити три основні елементи, які присутні практично в кожному об’єкті та потребують забезпечення їх безпеки [16]:

• люди - працівники та гості об'єкта;

• основні засоби, основні засоби;

• критична інформація - інформація з різними секретними грифами.

Кожен із виділених елементів має свої особливості, які необхідно враховувати при визначенні можливих ризиків. Необхідність захисту випливає з результатів аналізу можливих загроз безпеці автономної системи. Повний захист від змінного струму складається з вимог захисту приватних компонентів шляхом поєднання функціонально однорідних вимог забезпечення захисту. За результатами цього етапу визначаються та формулюються вимоги до захисту.

Повний захист AS випливає з вимог захисту для приватних компонентів шляхом поєднання функціонально однорідних даних для забезпечення захисту. Ці дані включають інформацію, захищену на основі задокументованих списків захищеної інформації, загрози інформаційній безпеці та модель ймовірного порушника, склад використаних технічних заходів та зв'язки між ними, склад розробленої організаційної та адміністративної структури документації, клас безпеки АС у захищеній версії. На етапі проектування системи приймаються рішення про склад технічних засобів і систем, які будуть використовуватися в розробленій системі, а також про заходи щодо забезпечення конфіденційності інформації.

1.3.2 Визначення технічного рішення

Загалом процес проектування можна розділити на такі етапи [15,25]:

• Підготовка Конституційного Суду до створення системи захисту інформації;

• Створення моделі ГКВ;

• Розробка технічного та робочого проекту (ТРП) на створення ГКВ та архітектури ГКВ. ГТО для створення ГКВ включає такі документи:

1. Пояснення, що містить опис найважливіших технічних рішень щодо налагодження ГКВ та організаційних заходів щодо підготовки ГКВ до експлуатації;

2. Обґрунтування обраних елементів SHI та визначення місця розташування. опис розроблених профілів захисту;

3. Специфікація комплекту технічних засобів СУІБ;

4. Специфікація комплексу програмних засобів ІСУ;

5. Вкажіть налаштування та режим роботи компонентів SHI:

• Розробка організаційно-розпорядчих документів системи управління ІБ (політика інформаційної безпеки, процедури, положення тощо);

• Розробка робочого проекту (разом з документацією застосованих заходів безпеки та адміністративної процедури, плану запровадження SHI тощо), планування навчання користувачів та персоналу служби IT-системи;

• Впровадження системи дозвільних та організаційно-технічних заходів щодо захисту інформації в КСЗІ.

Проект повинен містити розділи, присвячені забезпеченню автоматизації діяльності співробітників організації, обміну інформацією за допомогою високошвидкісних каналів зв'язку, захисту інформації. При необхідності розробляються завдання і проекти на інші роботи, такі як будівельно-монтажні. На підставі цього документа буде складатися КІСІ, тому він повинен містити опис всіх використовуваних технічних засобів, їх налаштування, а також всі необхідні організаційні рішення. Розроблена організаційно-технічна та експлуатаційна документація включає технічний паспорт на КСЗІ, інструкції та методичні рекомендації для користувачів та адміністраторів системи щодо використання технічних засобів, нормативно-правові акти, нормативно-правові акти, пов’язані з проектуванням, впровадженням, випробуванням та введенням системи в експлуатацію. Технічне завдання на створення КСЗІ може бути розроблено як для новостворених ІТС, так і в рамках модернізації існуючих ІТС у вигляді окремого розділу ТЗ на створення ІТС, окремого (часткового) ТЗ або доповнення до ТЗ з метою створення ІТС. ТЗ визначає вимоги до функціонального складу та порядку розробки та впровадження технічних заходів із забезпечення безпеки інформації під час її обробки в IT-системі ІВС, а також вимоги до організаційних, фізичних та інших заходів безпеки. за межами IVS IT Systems, а також повну інформацію про програмне забезпечення та технічні заходи безпеки. Проект КСЗІ розроблено на основі та згідно технічного завдання. При розробці проекту КІСІ обґрунтовуються та приймаються проектні рішення, що дозволяють реалізувати вимоги КТ, забезпечують сумісність і взаємодію різних елементів КІСІ, а також різних засобів і методів захисту інформації. В результаті складається комплект експлуатаційної та експлуатаційної

документації, необхідної для забезпечення випробувань, налагодження, випробувань та управління КСЗІ. Під впровадженням системи авторизації доступу та організаційно-технічних заходів із захисту інформації розуміються такі види діяльності:

• визначення складу суб'єктів доступу до інформації, що захищається (працівників організації);

• ознайомити працівників із засадами обробки інформації, що захищається, та забезпечення інформаційної безпеки, покладання персональної відповідальності на всіх користувачів за розголошення довіреної їм інформації, що захищається, шляхом підписання відповідних документів;

• Розробка та затвердження переліку захищених інформаційних ресурсів, доступ працівників до захищених ресурсів;

• визначення складу захищених носіїв інформації та їх ідентифікація;

• Створення журналів паролів, журналів персональних ідентифікаторів, журналів захищених носіїв інформації.

1.3.3 Реалізація та експлуатація КСЗІ

Робота над впровадженням системи включає наступні завдання:

• Придбання, встановлення та налагодження засобів захисту інформації в КСЗІ;

• Проведення приймально-здавальних випробувань;

• Сертифікат KSZI про відповідність вимогам політики інформаційної безпеки (добровільно);

• навчання користувачів;

• Запровадження ОМС.

Придбання, встановлення та налагодження (випробування) технічних засобів здійснюються відповідно до вимог, зазначених у проекті створення КСЗІ.

Випробування КСЗІ проводяться для перевірки його функціонування відповідно до встановлених вимог, а також для виявлення та усунення дефектів.

Проводиться за програмою, яка визначає умови та порядок роботи АС у захищеній версії, тривалість пробного запуску та порядок усунення виявлених помилок [17]. Для перевірки повноти і якості функціонування системи в різних експлуатаційних станах проводяться приймально-здавальні випробування. Вони проводяться за програмою, в якій зазначаються перелік об'єктів випробувань і вимоги до них, критерії приймання системи та її частин, умови і терміни випробувань, методика випробувань і обробки результатів [17].

Для приймальних випробувань:

• Розвиток технологій обробки інформації, поширення машинних носіїв, управління заходами безпеки, розмежування доступу користувачів до ІТ-ресурсів і автоматичний контроль за діяльністю користувачів;

• працівники служби захисту інформації та користувачі ІТС набувають практичних навичок поводження з технічними, програмно-технічними засобами захисту інформації, ознайомлюються з вимогами організаційно-розпорядчих документів, що стосуються питання обмеження доступу до технічних засобів та інформаційних ресурсів;

• Проведено доопрацювання програмного забезпечення, додаткове налагодження та налаштування комплексу засобів захисту інформації від несанкціонованого доступу (за потреби);

• Проводиться корекція оперативної та експлуатаційної документації (за необхідності).

За результатами вступних та випускних іспитів приймається рішення про придатність КСЗІ в ІТС до здачі державного іспиту. Сертифікація KISI є добровільною, якщо організація не зберігає та не обробляє інформацію, що належить державі. Сертифікація проводиться з метою перевірки відповідності системи захисту інформації вимогам, визначеним у нормативних документах Державної служби спеціального захисту зв'язку та інформації (ДСЗЗІ). Атестація КСЗІ проводиться за програмою та методикою сертифікаційних випробувань. За результатами випробувань робиться висновок і, у разі позитивного рішення

атестаційної комісії, видається сертифікат відповідності ІТ-системи вимогам безпеки інформації. Для узгодження створеної системи з робочим персоналом вживаються заходи щодо його навчання. Такі заходи, як правило, виключають неправильне використання встановлених системних компонентів (апаратних засобів, програмного забезпечення тощо), виникнення помилок та інші небезпеки для персоналу. Заключним етапом є постійний моніторинг стану КСЗІ та її функціонування відповідно до розроблених положень та вимог до її функціонування. Крім того, для підтримки якості роботи системи необхідно перевірити ефективність захисних заходів і методів.

1.4 Характеристика підприємства, цілі і завдання, структура підрозділу

Коротка характеристика Підрозділу Тернопільського Національного технічного університету імені І. Пулюя приведена в таблиці 1.2.

Таблиця 1.2 – Опис підприємства

Повне фірмове найменування українською мовою	Кафедра інформатики і математичного моделювання Тернопільського Національного технічного університету імені І. Пулюя
Скорочене найменування українською мовою	ТНТУ ім. І.Пулюя
Форма власності	Юридична особа публічного права
Види діяльності	Підготовка фахівців за освітніми рівнями:, бакалавр, магістр.
Керівник	Михайлишин М.С., к.ф.-м.н., доцент, професор, зав. кафедрою
Юридична адреса	м.Тернопіль, вул. Руська, 56, корпус № 2, к.62

Університет входить до складу факультету бізнес-інформатики та програмної інженерії.

Основною метою підрозділу є підготовка фахівців за рівнями освіти: бакалавр, магістр.

Виходячи з мети, компанія вирішує наступні завдання:

1. виховання учнів;

2. Забезпечення персоналу всім необхідним для виконання дорученої роботи;

3. Забезпечення інформаційної взаємодії між підрозділами.

Підрозділ входить до складу факультету інформаційних систем і програмного забезпечення, який очолює завідувач кафедри Михайлишин Михайло Стахович, кандидат фізико-математичних наук, професор. Організаційна структура відділу наведена на рисунку 1.1

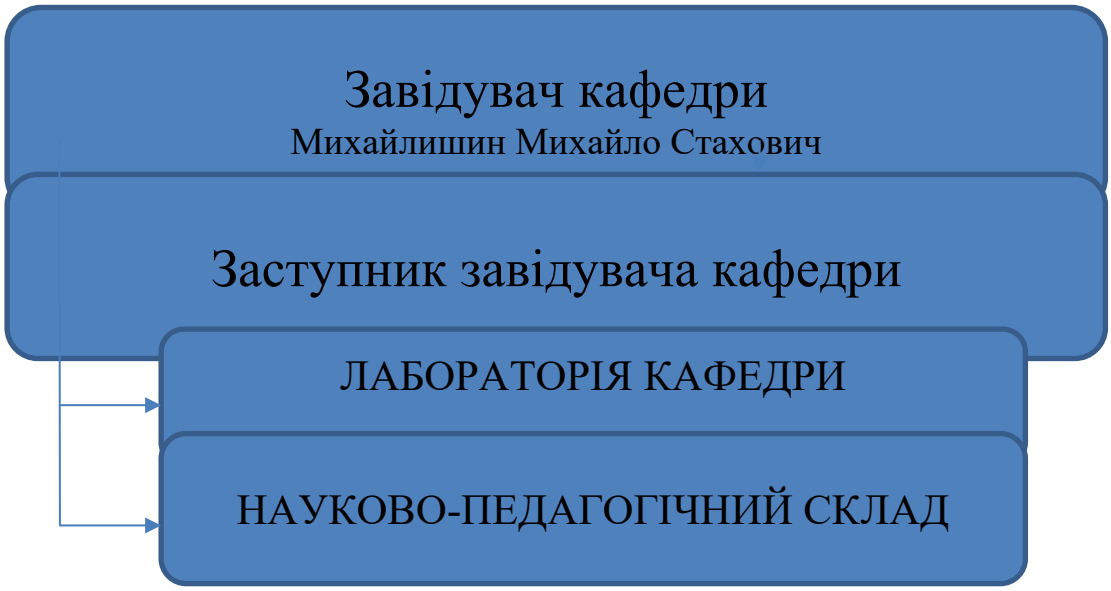

Рисунок. 1.1 – Організаційна структура кафедри

1.5 Висновок до першого розділу

Відповідно до стандарту ISO 27001 відділ повинен визначити обсяг і межі SMIB (організаційні, фізичні, комунікаційні межі та межі відповідальності), враховуючи характеристики бізнесу, організації, її розташування, активи та технології.

До складу СМІБ кафедри входять завідувач кафедри, його заступник та лабораторії кафедри, включаючи всіх співробітників. Просторовим каркасом СМІБ є функціональні межі приміщення, тобто всі навчальні приміщення факультету. Організаційні межі діяльності SMIB – усі відділи всередині департаменту зобов'язані виконувати вимоги SMIB у межах делегованих їм повноважень. До сфери діяльності СМІБ входять усі основні та допоміжні процеси діяльності відділу, його контроль, включаючи реєстрацію та координацію. Основним документом, який регулює діяльність ДУІБ та визначає відповідальність за порушення вимог, цілей та методів роботи ДУІБ, є «Політика інформаційної безпеки» департаменту.

РОЗДІЛ 2 АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Аналіз інформації, що циркулює в підроьзділі

Аналіз інформації, що циркулює у відділі, що підлягає захисту, дає змогу визначити, яку інформацію необхідно захищати та як цей захист можна побудувати. Основним завданням цього аналізу є виявлення повного переліку джерел і носіїв інформації та визначення структури конфіденційності інформації [1]. Інформація про охоронний об'єкт, яка могла б становити державну таємницю, відсутня. Інформація, яка циркулює в департаменті, є конфіденційною і узагальнена та представлена в таблиці 2.1.

Таблиця 2.1 – Елементи інформації, що підлягають захисту на об'єкті

№	Найменування елемента інформації	Конфіденційність інформації	Найменування джерела інформації	Місцезнаходження інформації
1.	Службові записки	К	Керівництво кафедри	Відділи, кабінети викладачів
2.	Доповідні	К	Керівництво кафедри	Відділи, кабінети викладачів
3.	Накази	К	Керівництво кафедри	Відділи, кабінети викладачів
4.	Розпорядження	К	Керівництво кафедри	Відділи, кабінети викладачів
5.	Звіти	К	Керівництво кафедри	Відділи, кабінети викладачів
6.	Відомості про працівників	К	Керівництво кафедри	Відділ кадрів
7	Відомості про студентів	К	Керівництво кафедри, студенти	Відділ кадрів

2.2 Категоріювання інформації

Проведено категоріювання інформації та оцінка вартості збитку в разі її розголошення. Результати категоріювання представлені в таблиці 2.2.

Таблиця 2.2 – Аналіз інформаційних активів на кафедрі

Найменування елемента інформації	Гриф	Ціна інформації (грн.)	Найменування джерела інформації	Місцезнаходження джерела інформації
Наказ про заходи захисту	К	20 000	Начальник служби безпеки	Служба безпеки
Наказ про введення в експлуатацію ПЕОМ	К	8 000	Ректор Університету	Служба безпеки
Посадові інструкції співробітників підприємства	К	5 000	Проректор з науково-педагогічної роботи	Відділ кадрів
Трудові договори співробітників, що працюють з конфіденційною інформацією	К	7 000	Зам. директора з кадрів і соц. питань	Відділ кадрів
Договори, укладені з студентами	К	300 000	Головний бухгалтер	Бухгалтерія
Акт здачі-приймання виконаних робіт	К	6 000	Головний бухгалтер	Бухгалтерія

З даної інформації наведеній у таблиці видно, що найбільш цінним елементом є договори укладені з студентами.

2.3 Види загроз інформації

Загроза інформаційній безпеці – можливість виникнення такого явища чи події, наслідком якої можуть бути небажані наслідки для інформації: порушення фізичної цілісності, логічної структури, несанкціонована зміна інформації, несанкціоноване отримання інформації, несанкціоноване тиражування інформації [3].].

Основними типами загроз інформаційній безпеці є наступні джерела загроз:

- стихійні лиха;

- збої та збої обладнання;
- помилки в експлуатації;
- умисних дій злочинців і зловмисників.

Перелік можливих загроз та методи боротьби з ними наведено в таблиці 2.3.

Таблиця 2.3 – Можливі загрози та засоби боротьби з ними

Можливі загрози	Засоби для зменшення кількості вразливостей і зниження ступеня шкоди від загроз
Основні ненавмисні штучні загрози	
ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (видалення, спотворення файлів з важливою інформацією або програм, в тому числі системних і т.п.); ненавмисна псування носіїв інформації	програма резервного копіювання Macrium Reflect
зараження комп'ютера вірусами;	Антивірус «Zillya», на сервері встановлений «Zillya для бізнесу»
необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;	Затвердження інструкцій по роботі з конфіденційною інформацією
ігнорування організаційних обмежень (установлених правил) при роботі в системі;	Контроль за дотриманням правил роботи і залучення до відповідальності за її порушення.
некомпетентне використання, настроювання або неправомірне відключення засобів захисту персоналом засобів захисту;	Затвердження Посадової інструкції системного адміністратора з інформаційних технологій (IT-фахівець). У ній перераховані обов'язки даного працівника по організації інформаційної системи і
Можливі загрози	Засоби для зменшення кількості вразливостей і зниження ступеня шкоди від загроз
7) ненавмисне пошкодження каналів зв'язку.	Лінії каналів зв'язку прокладені в коробах
Основні навмисні штучні загрози	
1) відключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);	Встановлено джерела безперебійного живлення. (Дозволяють зберегти дані і завершити роботу ПК.)
2) несанкціонований доступ в приміщення кафедри для скоєння крадіжки або інших дій в неробочий час;	В даному приміщенні Університету чергує охоронець. Рекомендується також встановлення охоронно-пожежної сигналізації, з покладанням

Продовження таблиці 2.3

	на охоронця обов'язків виклику міліції або пожежної служби при спрацюванні сигналізації.
Природні загрози	
1) пожежі;	Встановлено охоронно-пожежна сигналізація Інструкція з пожежної безпеки.
2) прорив труби, протікання в даху.	Інструкція з техніки безпеки. Ознайомлення персоналу з нею, і розподіл відповідальності при виникненні даної ситуації.

2.4 Потенційні канали витоку інформації

Класифікація потенційних каналів витоку інформації представлена в таблиці 2.4.

Таблиця 2.4 – Потенційні канали витоку інформації на об'єкті

№ елемента інформації	Джерело сигналу	Шлях витоку інформації	Вид каналу	Оцінки реальності каналу,%
1-7	Персонал	ініціативне співробітництво	МВ, АК	10 (малоймовірно)
		схиляння до співпраці	МВ, АК	5 (малоймовірно)
		підслуховування	АК	45 (ймовірно)
		спостереження	ВО	45 (ймовірно)
		розкрадання	МВ	5 (малоймовірно)
		модифікація	МВ	35 (ймовірно)
		знищення	МВ	5 (малоймовірно)
		негласне ознайомлення	ВО	80 (високій ймовірності)
		несвідоме розголошення	МВ, АК	80 (високій ймовірності)
1-7	Документи, паперові носії	спостереження	ВО	80 (високій ймовірності)
		розкрадання	МВ	10 (малоймовірно)
		копіювання	МВ	10 (малоймовірно)
		модифікація	МВ	35 (ймовірно)
		знищення	МВ	10 (малоймовірно)
		перехоплення	МВ	10 (малоймовірно)
		негласне ознайомлення	ВО	35 (ймовірно)
		фотографування	ВО	10 (малоймовірно)
		збір і аналітична обробка	МВ	45 (ймовірно)

Продовження таблиці 2.4

1-7	Технічні засоби обробки інформації	спостереження	ВО	40 (ймовірно)
		розкрадання	МВ, ЕМ	5 (малоймовірно)
		копіювання	МВ, ЕМ	10 (малоймовірно)
		модифікація	МВ, ЕМ	5 (малоймовірно)
		знищення	МВ, ЕМ	5 (малоймовірно)
		незаконне підключення	МВ, ЕМ	10 (малоймовірно)
		перехоплення	МВ, ЕМ	5 (малоймовірно)
1-7	Відходи	розкрадання	МВ	25 (ймовірно)
		збір і аналітична обробка	МВ	25 (ймовірно)
7	Електронні носії інформації	розкрадання	МВ	25 (ймовірно)
		копіювання	МВ	35 (ймовірно)
		модифікація	МВ	20 (малоймовірно)
		знищення	МВ	10 (малоймовірно)
		спотворення	МВ	20 (малоймовірно)
		збір і аналітична обробка	МВ	45 (ймовірно)

З даної таблиці можна зробити висновок, що найбільшу загрозу може завдати персонал кафедри, умисно чи ні.

2.5 Ефективність існуючої системи безпеки кафедри

За результатами аудиту інформаційної безпеки існуючої системи безпеки кафе встановлено:

Існуюча система захисту недостатньо надійна.

Відкриті канали вивезення майна в обхід КПП з використанням неоднакового периметра охорони території університету. Крадіжка перспективних рішень підриває здатність відділу до інновацій. Існуючі недоліки розглядаються в наступних категоріях.

2.5.1 Організаційно-правовий напрямок захисту

Аудит інформаційної безпеки об’єкта, що охороняється, виявив, що у філії циркулює велика кількість цінної інформації.

Відповідальність за знищення, фальсифікацію чи втрату інформації у відомчих положеннях та робочих інструкціях для працівників не передбачена, про безпеку інформації не йдеться. Жодних інструкцій чи правил інформаційної безпеки.

Окремо виділяють встановлені організаційні заходи щодо технічних заходів:

• На вході встановлено контрольно-пропускний пункт для запобігання неконтрольованим пересуванням у будівлі.

• Конфіденційні документи зберігаються в сейфах.

Додаткових заходів щодо забезпечення інформаційної безпеки IT-фахівцями, які працюють у відділі, не визначено. З метою покращення безпечного документообігу доповнено наступні нормативні документи, що діють на даному підприємстві:

• Інструкція з ведення секретного діловодства;

• політика конфіденційності відділу;

• Обов'язок працівника зберігати комерційну таємницю.

2.5.2 Програмно-апаратні напрямки захисту

Апаратно-програмні засоби, які використовуються на факультеті:

1. Використання систем контролю доступу (захист від несанкціонованого скачування даних з ПК, обмеження доступу до внутрішніх ресурсів).

2. Використання антивірусних засобів.

Програмно-технічні заходи знижують ризик таких загроз, як порушення доступності інформації, ймовірність помилок, вразливостей, збоїв і поломок.

Використання неавторизованих USB-пристроїв ставить вашу корпоративну мережу та дані під загрозу. Крім доступу до USB-портів, існує ряд потенційно небезпечних пристроїв: дисководи, CD-ROM, а також FireWire, порти

2.5.3 Інженерно-технічні напрямки захисту

Приміщення кафедри розташована в 2 корпусі на обгородженій території Університету. Приміщення кафедри обладнані сучасними засобами пожежної безпеки.

Всі точки входу / виходу та в'їзду / виїзду контролюються за допомогою контрольно-пропускних пунктів, оснащених постами охорони, турнікетами, системами оповіщення і відеомоніторингу. Територія обгороджена парканом і охороняється силами охорони. Всі приміщення обладнані взломостійкими сейфами в міру необхідності. Налагоджена чітка система пожежної та аварійної безпеки. З вищевказаної інформації випливає, що в даний момент на кафедрі відсутня комплексна система захисту інформації. Заходи, що вживаються для захисту інформації, є недостатніми. Інформація на кафедрі недостатньо захищена від загроз втрати, перекручування та знищення.

2.6 Вимоги до АС

Для визначення вимог до ШІ використовуємо посібник: «Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем та вимоги до захисту інформації. Відповідно до нормативного документу та наведених даних ІТ-система факультету відноситься до 2 групи класифікаторів АС. АС клас - 2-й. До другої групи відноситься безліч користувачів операційних систем, в яких одночасно обробляється і (або) зберігається інформація різного ступеня конфіденційності. Не всі користувачі мають право доступу до всієї інформації про операційну систему. Група включає п'ять класів - 1Д, 1Г, 1Б, 1Б і 1А.

Вимоги до класу безпеки 1D.

• Для підсистеми контролю доступу: ідентифікація та дійсність екземплярів доступу при вході в систему за умовним постійним паролем, що складається не менше ніж з шести літер і цифр (реалізується через операційну

систему).

• Підсистема реєстрації та обліку: забезпечення реєстрації входів (виходів) екземплярів доступу до системи або реєстрації завантаження та ініціалізації операційної системи та її програмного завершення. Вимкнення системи або реєстрація завершення роботи не відбувається, коли апаратне забезпечення змінного струму вимкнено.

У параметрах реєстру (виконується з операційною системою):

• дата та час входу (виходу) суб'єкта, який здійснює доступ (із системи) або завантажує (зупиняє) систему;

• Результат спроби входу: успішний або невдалий - неавторизований;

• Ідентифікатор (код або назва) суб'єкта, наданий під час відбору доступ;

• Облік усіх захищених носіїв інформації шляхом ідентифікації та запису даних журналу обліку (облікової картки) (реалізовано організаційно);

• Облік захищених носіїв у журналі (картці) з реєстрацією їх звільнення (надходження) (організаційно реалізовано).

Підсистема цілісності:

• Забезпечення цілісності програмних засобів ГКВ з НСД, оброблюваної інформації та незмінності програмного середовища (виконується засобами ОС);

• Впровадження фізичного захисту СВТ (обладнання та носіїв), що полягає в контролі доступу сторонніх осіб до приміщень АС, наявності надійних бар’єрів, що перешкоджають проникненню сторонніх осіб у приміщення АС та зберігання носіїв інформації, особливо в позаробочий час (реалізується організаційно-технічні заходи);

• Періодична перевірка функціонування ГКВ НРД при зміні програмного середовища та персоналу АС тестовими програмами для імітації спроб несанкціонованого доступу (здійснюється організаційно);

• Наявність інструментарію для відновлення СІЗ НРД, що полягає у підтримці двох копій програмних засобів СІЗ НРД та регулярному їх оновленні

та контролі за їх роботою (здійснюється організаційно та з використанням систем резервного копіювання).

2.7 Вимоги до КСЗІ в області виконання вимог, що регламентують обробку персональних даних

- Для ІТ-систем 2-го класу з багатокористувацьким режимом обробки персональних даних і різними правами доступу користувачів до них використовуються наступні основні способи та способи захисту інформації:
- Визначення, документування та погодження керівником відділу цілей обробки персональних даних.
- Визначення необхідності повідомлення органу, до компетенції якого входить захист прав фізичних осіб, персональні дані яких стосуються обробки персональних даних.
- Для кожної мети обробки персональних даних визначення, документування та затвердження керівником відділу:
- обсяг і зміст персональних даних;
- умови обробки, включаючи умови зберігання персональних даних;
- про необхідність отримання згоди суб’єктів даних.
- Класифікація персональних даних за ступенем тяжкості наслідків втрати персональних даних Охоронні властивості для суб'єкта персональних даних.
- Розголошення відділом персональних даних третім особам за згодою суб’єкта персональних даних. Якщо управління залучає третю особу для обробки персональних даних, важливою умовою для укладення такого договору є зобов’язання третьої особи забезпечувати конфіденційність персональних даних та безпеку персональних даних під час їх обробки.
- Припинення обробки персональних даних та знищення зібраних персональних даних, якщо інше не передбачено законом, у випадках та на

умовах, встановлених законом:

- після досягнення цілей обробки або коли потреба в їх досягненні більше не актуальна;
- за зверненням суб'єкта персональних даних або уповноваженого органу з питань захисту прав суб'єктів персональних даних;
- якщо персональні дані є неповними, застарілими, недостовірними, отриманими незаконним шляхом або не є необхідними для досягнення заявленої мети обробки;
- якщо суб’єкт даних відкликає згоду на обробку своїх персональних даних, якщо така згода вимагається законом;
- якщо порушення оператором неможливо усунути при обробці персональних даних.

Визначення та документальне оформлення порядку знищення персональних даних (у тому числі матеріальних носіїв персональних даних). Встановлення та документування порядку розгляду звернень суб’єктів (або їх законних представників) щодо обробки їх персональних даних.ьВизначення та документування процедури відповіді на запити Уповноваженого органу з питань захисту прав суб’єктів даних або інших контролюючих органів, які здійснюють контроль та нагляд у сфері персональних даних. Визначення та запис документації для кожної організації ISPDn:

• мета обробки персональних даних;

• Обсяг і зміст оброблених персональних даних;

• перелік дій, що стосуються персональних даних, і способів їх обробки.

Обсяг і зміст персональних даних та перелік видів діяльності та методів обробки персональних даних відповідно до цілей обробки. При обробці різних категорій персональних даних рекомендується використовувати окремий матеріальний носій для кожної категорії персональних даних. Створення та документальне оформлення списку (переліку) працівників, які обробляють персональні дані в ІСПД або мають доступ до персональних даних. Наявність

списку (списку) в електронному вигляді можлива за умови надання працівникам прав доступу до ІСПД тільки на підставі розпорядчого документа в порядку, задокументованому в організації. Доступ співробітників організації до персональних даних і обробка персональних даних співробітниками організації здійснюється виключно з метою виконання службових обов'язків. Співробітники організації, що здійснюють обробку персональних даних в ІСПД, поінформовані про те, що вони обробляють персональні дані, категорії персональних даних, що обробляються, і ознайомлені з усім комплексом вимог, що стосуються безпеки та обробки персональних даних у частині, що відноситься до їх посадових обов'язків. Визначення та документальне оформлення порядку доступу працівників організації та інших осіб до приміщень, в яких обробляються персональні дані.

Визначення та документальне оформлення порядку зберігання матеріальних носіїв персональних даних, який визначається:

• місця зберігання матеріальних носіїв персональних даних;

• вимоги щодо забезпечення безпеки персональних даних при зберіганні їх носіїв;

• працівники, відповідальні за виконання вимог щодо забезпечення безпеки персональних даних;

• спосіб контролю за дотриманням вимог щодо забезпечення безпеки персональних даних під час зберігання матеріальних носіїв персональних даних.

При обробці персональних даних на паперових носіях, зокрема при використанні типових форм документів, характер інформації, в якій вона міститься, або включення до неї персональних даних. Виконання вимог «Положення про особливості обробки персональних даних, що здійснюється без використання засобів автоматизації»

2.8. Висновок до другого розділу

Після описаної вище оцінки ризиків, експерти з ІБ склали приватну модель загроз включаючи як загрози державну таємницю, так і загрози персональних даних. Після складання приватної моделі загроз робляться організаційні і технічні заходи з протидії загрозам ІБ. На кафедрі такі заходи описуються в приватних політиках безпеки, вимогах до процедур ІБ, посадових інструкціях і записах по ІБ. Також був проведений аналіз роботи АС класу «2», моделі загроз даної системи, наявних засобів захисту інформації. План захисту було складено на підставі зіставлення аналізу моделі загроз і наявних в організації засобів захисту. Був зроблений висновок, що є істотні недоліки в системі захисту, які можуть привести до істотних збитків в разі їх виявлення. На підставі цих даних в План захисту поставлені ті організаційні заходи, які необхідно виконати в першу чергу для безпечного функціонування АС класу «2».

РОЗДІЛ 3 РОЗРОБКА КСЗІ ТА РОЗРОБКА ЗАХОДІВ І МЕТОДИКИ ПО ЇЇ ВПРОВАДЖЕННЮ НА ОБ'ЄКТ, ЩО ЗАХИЩАЄТЬСЯ

3.1 Структурна і функціональна схеми КСЗІ об'єкта

Для розробки КСЗІ об'єкта і дотримання комплексності була складена структурна схема порядку створення КСЗІ, представлена на рисунку 3.1.

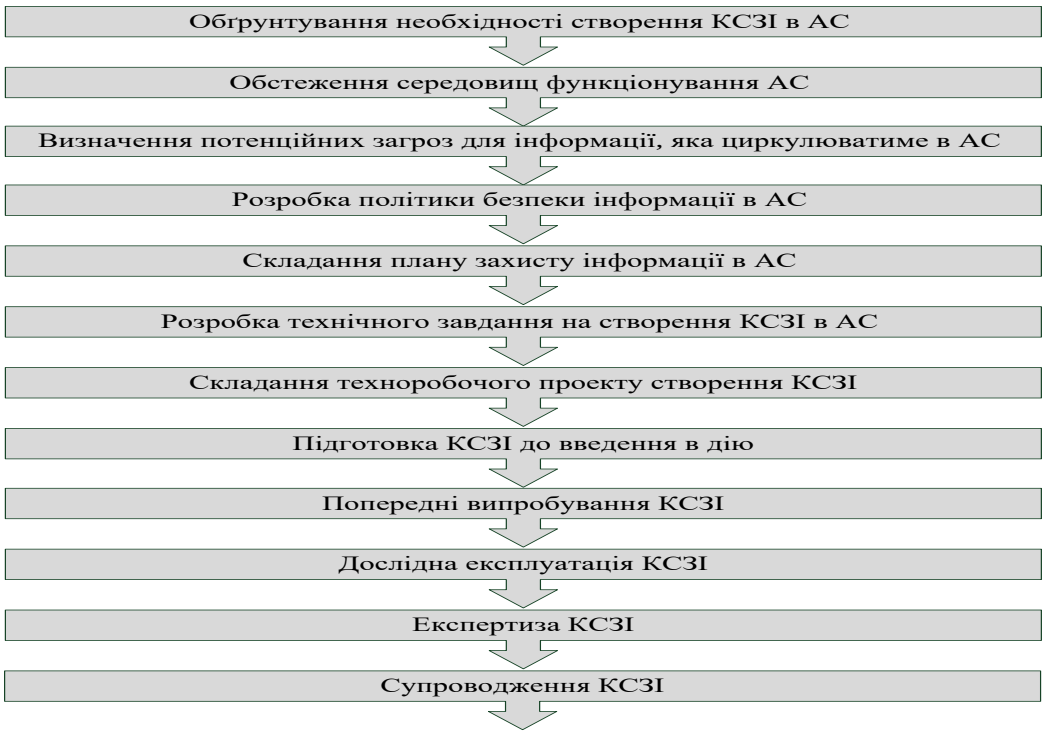

Рисунок 3.1– Структурна схема порядку створення КСЗІ.

Структурно КСЗІ поділяється на три основні напрями: організаційно-правовий, інженерно-технологічний та програмно-технічний. Організаційно-правове керівництво включає роботу з розробки нових і перегляду діючих організаційно-розпорядчих документів, що обертаються на підприємстві. Інженерно-технічний курс стосується забезпечення інформаційної безпеки за допомогою охоронної сигналізації та систем відеоспостереження. Узгодження програмно-технічного забезпечення включає комплекс заходів, спрямованих на

захист інформаційних процесів на робочому місці персоналу за допомогою програмного захисту.

На основі схеми структури розроблено функціональну схему, яка відображає процес забезпечення інформаційної безпеки. Процесний підхід показано на рисунку 3.2.

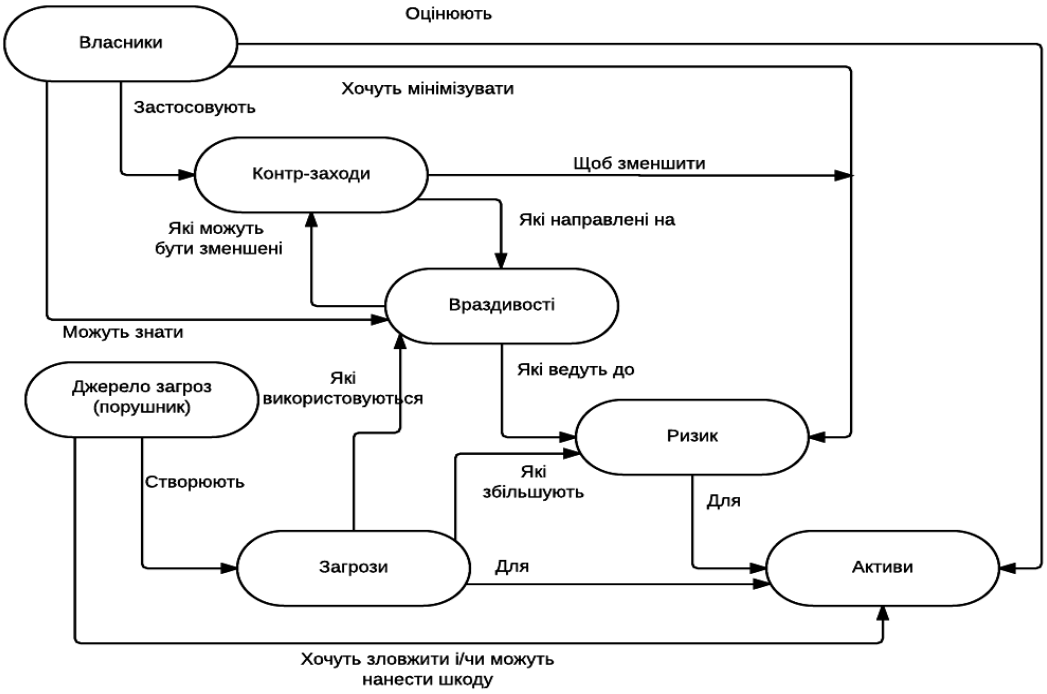

Рисунок 3.2 – Процесний підхід КСЗІ об'єкту

Функціональна схема відображає етапи забезпечення безпеки у виробничому процесі. До реалізації цього процесу залучаються різні підрозділи служби безпеки та весь особовий склад відділу. Кожен етап захисту інформації відділу супроводжується організаційно-розпорядчою документацією, яка регламентує діяльність служби безпеки та персоналу в рамках конкретного процесу захисту.

Результатом такого підходу має бути безпечне адміністрування кафедри факультету.

3.2 Організаційно-правові заходи

На основі переліку загроз, виявлених у відомстві, були обрані заходи щодо зменшення кількості вразливостей та зменшення масштабів збитку від загроз. Внесено зміни в систему документообігу, необхідні для повної відповідності документації та фізико-технічного оснащення. Основним джерелом витоку інформації є співробітники відомства. Тому розглядалися додаткові заходи безпеки. Навчання персоналу після всіх інших заходів безпеки. Обов'язкове навчання співробітників після встановлення нового апаратного або програмного забезпечення, щоб уникнути помилок при експлуатації. Навчання всіх працівників щодо поведінки у разі виникнення різних видів небезпек. Роз’яснення працівникам, які не мають права працювати з охоронюваними документами, що робити у разі виявлення такого документа. Для цього розробляється «Інструкція щодо забезпечення безпеки відомостей, що становлять комерційну таємницю». Постійне навчання працівників шляхом направлення їх на курси підвищення кваліфікації. До працюючих на підприємстві айтішників вжито додаткових заходів. До основних завдань IT-фахівця належать: впровадження передових інформаційних технологій для автоматизації управління бізнесом; Використання мінімуму IT-інструментів для досягнення цілей автоматизації; Формування корпоративної культури роботи користувачів. Ця посада має дві основні складові – технологічний і соціальний менеджмент. З одного боку, в компанії необхідно впровадити IT-систему, яка б максимально відповідала потребам користувачів, з іншого боку, пояснити її структуру та функції, навчити правилам використання, розподілити завдання. та сфери відповідальності персоналу за підтримку його ефективності. Доповнення до статуту відділу: «Відділ має право самостійно визначати обсяг відомостей, що становлять охоронювану законом комерційну та іншу таємницю, та спосіб їх захисту». Це розширить можливості для організації заходів. З метою підвищення безпеки документообігу в даній компанії були доповнені існуючі нормативно-

правові документи:

• Інструкція щодо ведення конфіденційного діловодства;

• Політика конфіденційності відділу;

• Обов'язок працівника зберігати комерційну таємницю.

3.3 Програмно-апаратні засоби захисту інформації

Щоб захистити цінну інформацію на персональних комп’ютерах, всюди на всіх робочих станціях, залучених до процесу обміну інформацією, було розкрито важливість планових оновлень програмного забезпечення. Потреба в цьому на окремих робочих станціях обмежена допоміжним використанням обчислювальних засобів. Комп’ютер підключений до локальної мережі та містить конфіденційну інформацію. Він піддається досить великій кількості різноманітних загроз, масштаби яких можна зменшити за допомогою програмно-апаратних засобів безпеки. Апаратне та програмне забезпечення, впроваджене в компанії:

1. Використання систем контролю доступу (захист від несанкціонованого скачування даних з ПК, обмеження доступу до внутрішніх ресурсів).

2. Реєстрація, зберігання та обробка даних про події, що стосуються безпеки системи.

3. Використання антивірусних засобів.

Програмно-технічні заходи знижують ризик таких загроз, як порушення доступності інформації, ймовірність помилок, вразливостей, збоїв і поломок.

Були визначені наступні заходи захисту:

Щоб обмежити доступ до апаратного забезпечення та USB-портів, використовуйте DeviceLock, спосіб керування доступом до знімних носіїв і пристроїв у системах Windows NT/2000/XP і Windows Server 2008. За допомогою DeviceLock ви можете призначати права доступу користувачам і групам користувачів, контролювати доступ до жорстких дисків, приводів CD-ROM,

портів принтера та модему та всіх інших пристроїв. При цьому підтримуються всі типи файлових систем - FAT, NTFS (версії 4+), CDFS та інші. Вбудовані засоби віддаленого керування, які дозволяють контролювати доступ до пристроїв на будь-якому комп’ютері в локальній мережі. Використання неавторизованих USB-пристроїв ставить під загрозу корпоративні мережі та дані. Все це робить вбудований механізм аутентифікації USB-пристроїв DeviceLock незамінним, а часом і безальтернативним рішенням проблем корпоративної безпеки. Окрім доступу до USB-портів, DeviceLock дозволяє контролювати цілий ряд потенційно небезпечних пристроїв: приводи, CD-ROM, а також FireWire, інфрачервоний порт, порти принтера (LPT) і модему (COM), адаптери WiFi і Bluetooth. Антивірусна система Zillya призначена для захисту від шкідливих кодів і програм - це потужний антивірус з дуже частим оновленням антивірусних баз. Під час спалаху вірусу ви отримуватимете оновлення кілька разів на годину, за допомогою яких ви зможете ефективно захистити свій комп’ютер від зовнішніх загроз.Zillya визначає:

1. поштові черв'яки;
2. мережеві черв'яки;
3. файлові віруси;
4. троянські програми;
5. стелс-віруси;
6. поліморфні віруси;
7. безтілесні віруси;
8. макро-віруси;
9. віруси, що вражають документи MS Office;
10. скрипт-віруси;
11. шпигунське ПЗ (Spyware);
12. програми-викрадачі паролів;
13. клавіатурні шпигуни;
14. програми-дозвонщики;

15. рекламне ПО (Adware);

16. потенційно небезпечне ПО;

17. хакерські утиліти;

18. програми-люки;

19. програми-жарти;

20. шкідливі скрипти;

21. інші небажані коди;

Ключові функції:

1. Zillya Scanner - якісне виявлення та знешкодження вірусів і шкідливих об'єктів на жорстких дисках, знімних носіях і в оперативній пам'яті;

2. Захист від вірусів за допомогою технології руткіт;

3. Виявлення та знешкодження вірусів, які знаходяться в оперативній пам'яті і ніколи не відображаються окремими файлами (безтілесні хробаки);

4. Визначення вірусів в архівах будь-якої вкладеності та в упакованих елементах;

5. Перевірка файлів, стиснутих пакувальниками, в тому числі невідомих;

6. Перевірка вхідної та вихідної кореспонденції на наявність вірусів за протоколами SMTP/POP3/NNTP/IMAP;

7. Захист від масової розсилки повідомлень з комп'ютера поштовими хробаками;

8. Захист від несанкціонованого зовнішнього доступу, запобігання витоку важливих даних через мережу, блокування підозрілих підключень на рівні пакетів і додатків;

9. Сканування на вимогу та індивідуальні графіки перевірки комп'ютерів;

10. Автоматично отримувати оновлення вірусної бази Zillya з будь-якою періодичністю;

11. автоматичне сповіщення про виявлені інфіковані, невиліковні або підозрілі об'єкти;

12. Нагадування про оновлення вірусної бази;

13. Централізоване управління всіма налаштуваннями компонентів;

14. Прозорість роботи – детальні звіти про роботу кожного модуля.

3.4 Інженерно-технічні заходи захисту інформації

Способи і засоби технічного захисту інформації застосовуються для створення навколо об'єкта захисту перешкоди, що перешкоджає реалізації загроз безпеці інформації.

3.4.1 Встановлення і розміщення охоронної сигналізації

Для захисту інформаційних ресурсів у закладі обрано охоронні сповіщувачі, які реагують на відкриття дверей та вікон, а також розбиття скла.

Як сповіщувач відкривання дверей обрано магнітний охоронний сповіщувач ІС-102-6 (СМК-6), який призначений для прихованої установки в металеві двері. Зовнішній вигляд детектора показано на рисунку 3.1. Властивості наведені в таблиці 3.1.

Рисунок 3.3 – Сповіщувач ІС-102-6 (СМК-6)

Таблиця 3.1 – Характеристики сповіщувача ІС-102-6 (СМК-6)

Відстань між герконом і магнітом, мм: для замикання контактів (для розмикання контактів)	6,25
Діапазон робочих температур, С	-50 ... + 50
Вартість, грн.	39.36

Сповіщувачем, що реагує на розбиття скла, обрано акустичний (акустичний) охоронний сповіщувач GBD-2.

Вимоги до розміщення сповіщувача

• Відстань від сповіщувача до найдальшої точки скляної поверхні, що захищається, не повинна перевищувати 10 м;

• При установці сповіщувача рекомендується, щоб всі зони захищеного склом об'єкта знаходилися в його прямому полі зору, не рекомендується закривати сповіщувач декоративними шторами або жалюзі, які можуть знизити чутливість сповіщувача;

• Сповіщувач не можна використовувати в приміщенні, де рівень шуму перевищує 70 дБ;

• Двері, кабіни, вентилятори, динаміки трансмісії та інші джерела шумових перешкод у приміщенні на період охорони повинні бути вимкнені.

Зовнішній вигляд детектора показано на рисунку 3.4. Властивості наведено в таблиці 3.3.

Порівняльні характеристики детекторів розбиття скла наведені в таблиці 3.2.

Таблиця 3.2 – Порівняльні характеристики звукових сповіщувачів

Характеристика Найменування	Тип	Дальність виявлення, м	Кут виявлення по горизонталі
1	2	3	4
Скло-3 (ІС-329-4)	сповіщувач охоронний звуковий (акустичний)	6	360◦
Скло-4	сповіщувач охоронний звуковий (акустичний)	6	360◦
Арфа (ІС-329-3)	сповіщувач охоронний звуковий (акустичний)	6	120◦
Арфа-2 (ІС 329-12)	сповіщувач охоронний звуковий (акустичний)	6	120◦
Астра-531СМ	сповіщувач комбінований (ІК + АК)	6	120◦
Сова-2Б (ІС 315-2)	сповіщувач комбінований (ІК + АК)	6	120◦
Сова-3Б (ІС 315-3)	сповіщувач комбінований (ІК + АК)	6	120◦
Орлан-Ш (ІС 315-1)	сповіщувач комбінований (ІК + АК)	6	180◦
Дзвін-1 (ІО329-8)	сповіщувач охоронний поверхневий звуковий	4	-
GBD-2	сповіщувач охоронний звуковий (акустичний)	10	360◦

Оскільки дальність виявлення всіх сповіщувачів достатня для обраного об'єкта, вибір сповіщувача GBD-2 є оптимальним рішенням. Зовнішній вигляд детектора показано на рисунку 3.4. Властивості наведені в таблиці 3.3.

Рисунок – 3.4 Сповіщувач GBD-2

Таблиця 3.3 – Характеристики сповіщувача GBD-2

Максимальна дальність дії АК каналу	10м
Кут огляду АК каналу в горизонтальній площині	360 °
Максимальна площа об'єкту, що охороняється скляного листа	100 м2
Мінімальна площа об'єкту, що охороняється скляного листа	0,05 м2
Напруга живлення	10В – 16В
Струм споживання	Не більше 22мА
Канали	двоканальний (ВЧ + НЧ)
Висота установки	2м -5м.
Діапазон робочих температур	-20 ° С ... + 50 ° С
Габаритні розміри	140х65х20мм

Вибір та порядок монтажу охоронних сповіщувачів проводився згідно РД 78.145-93, п. 3.1. [16]

При виборі типу охоронних сповіщувачів враховуються такі фактори, як уразливість об’єкта до несанкціонованого проникнення, модель зловмисника (захист забезпечується в основному від зловмисників, які мають намір проникнути на об’єкт вночі без фізичної охорони шляхом злому дверей, злому або відкриття). вікна та пробивання стелі з підвалу або з другого поверху) та дотримання нормативних документів (забезпечення надійної роботи).

3.4.2 Вибір засобів відеоконтролю для об'єкта захисту

У цьому розділі розглядається система телевізійного спостереження з відеозаписом об'єкта охорони ООПТ з обґрунтуванням вибору.

Категорія предметного значення

Як рекомендовано, усі об’єкти розділені на різні категорії залежно від їх важливості. Наше охоронне майно віднесено до категорії Б. До цієї категорії належать об’єкти, «несанкціонований доступ до яких може завдати значної шкоди майну та матеріальним цінностям, створити загрозу здоров’ю та життю людей, які знаходяться на об’єкті».

Таблиця 3.4 – Категоріювання значущості об'єкта

Клас системи	Категорія значущості об'єкта	Характеристика значущості об'єкта	Виробниче або інше призначення об'єкта
1	2	3	4
Вищий	А	Об'єкти, зони об'єктів (будівлі, приміщення, території), несанкціоноване проникнення на які може принести особливо великий або непоправної матеріальний і фінансовий збиток, створити загрозу здоров'ю і життю великої кількості людей, які перебувають на об'єкті та поза ним, привести до інших тяжких втрат	Сховища і депозитарії банків, місця зберігання шкідливих і радіоактивних речовин і відходів, місця зберігання зброї, боєприпасів, наркотичних речовин і інше
середній	Б	Об'єкти, зони об'єктів, несанкціоноване проникнення на які може принести значні матеріальні та фінансові збитки, створити загрозу здоров'ю і життю людей, що знаходяться на об'єкті	Касові зали банків, під'їзди інкасаторських машин, шляхи перенесення грошей, автостоянки, склади і приміщення з цінними матеріалами, оргтехнікою та ін.
загального застосуван-ня	В	Інші об'єкти	Торгові зали магазинів, службові приміщення установ і інше

Режим роботи системи

У зв'язку зі специфікою даного об'єкта необхідне цілодобове

відеоспостереження. Це дозволяє при необхідності вчасно виявити причину і винуватців тієї чи іншої події в охоронному пристрої.

Перша оцінка складу системи

Перш за все, слід зазначити, що в охоронному об'єкті є приміщення різної категорії важливості, тому відеоспостереження кожного об'єкта має ряд особливостей і необхідно враховувати наступні умови:

• Необхідно контролювати пересування всіх людей на другому поверсі.

• Необхідно контролювати вхід до приміщення майстерні, дидактики, АКПП.

Тому на першому поверсі, навпроти сходових клітин та парадного входу, евакуаційного виходу, необхідно встановити 5 камер спостереження.

Виходячи з цих умов ми підбираємо камери для відеоспостереження.

Вибір телекамери

Правильний вибір телевізійних камер, як правило, є найважливішим моментом у проектуванні системи, оскільки саме характеристики камер в кінцевому рахунку визначають характеристики решти системи. При виборі телекамери і місця її установки враховується:

1. Категорія зонної важливості.

2. Геометричні розміри зони.

3. Необхідність ідентифікації спостережуваного об'єкта.

4. Освітленість об'єкта спостереження.

5. Умови використання.

6. Вид спостереження - негласне чи гласне.

Оскільки об'єкт віднесений до категорії «В», використання камер середнього класу абсолютно виправдано. Для контролю коридорів і проходів до житла необхідний кут огляду 40º з довжиною контрольованої зони 10 м. Контроль під'їздів та сходових клітин. У коридорах поверху навпроти сходових клітин встановити відеоспостереження. Довжина зони моніторингу становить 8 м, для моніторингу цієї зони необхідний кут огляду 60º. За технічними

характеристиками підійде мініатюрна чорно-біла камера KT & C KPC-190SP4.

Її основні характеристики: ПЗС матриця 1/3 ", 420 ТБ ліній, 0.05 Lx, f = 4.3 мм,, рівень сигнал / шум – 50 дБ, напруга 12 В, розміри 19× 42 мм.

Ідентифікація об'єкта, що спостерігається

Ідентифікації об'єкта, що спостерігається визначається мінімальним розміром об'єкта, помітний відеокамерою за формулою 4.1:

$$S = \frac{150 \cdot L \cdot tg(\frac{\alpha}{2})}{R} \qquad (4.1)$$

де L – відстань від камери до об’єкта спостереження, м;

R - мінімальний розмір об'єкта, що розрізняється, мм;

tg - роздільна здатність камери, ТБ рядків.

Формула визначає мінімальний розмір об'єкта, який буде розрізняти відеокамера:

Для 60º: S = 150 * 6 * tg (60/2) / 420 = 1,23 м;

Для 40º: S = 150 * 10 * tg (40/2) / 420 = 1,29 м;

Розрахунки показали, що камери з такими характеристиками достатньо для чіткого визначення слідів можливого зловмисника. SP4 використовується для ретельного огляду, який не потребує підвищеної чутливості та роздільної здатності. Завдяки невеликим розмірам їх можна використовувати всередині будівель як для відкритого, так і для прихованого спостереження. Разом з лінзою це полегшує їх вибір, оскільки їх характеристики незмінні і визначаються виробником. Наявність кріплення дозволяє прикріпити камеру до будь-якої поверхні і відрегулювати її в потрібному напрямку.

Зовнішній вигляд камери KT&C KPC-190SP4 наведено на рисунку 4.5. Технічні характеристики представлені в таблиці 4.5.

Рисунок 3.5 – Мініатюрна відеокамера KT & C KPC-190SP4 чорно-біла

Таблиця 3.5 – Технічні характеристики відеокамери KT & C KPC 190SP4

Автоматичний електронний затвор AES	1 / 50-1 / 100 000 сек.
Вбудований об'єктив:	так
Габарити:	Ø19 × 42 мм мм
Гамма корекція:	0,45
Діапазон робочих температур:	-10 ... + 50 ° C
Кліматичне виконання:	внутрішнє
об'єктив:	є
Виробник ПЗС матриці:	LG
Розмір ПЗС матриці:	1,0 "
Дозвіл:	500 × 582
Система АРУ:	Є
Стандарт сигналу:	чорно-білий (CCIR)
Тип відеовиходу:	композитний, BNC
Тип корпусу:	мініатюрний
Тип розгорнення:	надшвидка
Тип різьби кріплення об'єктива:	M12× 0,5
Тип синхронізації:	внутрішня
Мінімальна освітленість на об'єкті:	0,050 Лк
напруга:	12 В
Відносний отвір об'єктива F:	2,0
Відношення сигнал шум s / n:	50 дБ
Споживана потужність:	0,001 кВт
Дозвіл по горизонталі:	420 ТВЛ
Фокусна відстань вбудованого об'єктиву:	4 мм

Розташування відеокамер у каналі перегляду та передачі відеосигналу

• Кількість відеокамер - 5 шт.

• Висота установки відеокамери - 2,7 метра;

• Канал передачі - коаксіальний кабель РК-75-4 (опір 75 Ом).

3.4.3 Вибір системи прийому та обробки відео

Розглянемо кілька варіантів пристрою для прийому і обробки відеозображення і виберемо оптимальний. Порівняльні дані представлені в таблиці 3.6.

Таблиця 3.6 – Порівняльна характеристика пристроїв прийому та обробки відеосигналу

Назва	Кількість відеовходів	Роздільна здатність, пікс.	Загальна швидкість запису, к / с
1	2	3	4
AVC-777	16	720 × 576	18
Ai-D163	16	704 × 576	200
1	2	3	4
BestDVR -1600	16	720 × 576	100
EDSR -1600	16	720 × 576	50
PVDR-1654	16	720 × 576	400
TX168-16	16	720 × 576	100

Оскільки на об'єкті поряд з відеоспостереженням буде вестися відеозапис, найкращими характеристиками володіє цифровий відеореєстратор на 16 каналів PVDR-1654 виробництва фірми Polyvision.

Зовнішній вигляд відеореєстратора представлений на рисунку 3.6. Технічні характеристики відеореєстратора наведені в таблиці 3.7

Рисунок 3.6 – Відеореєстратор PVDR-1654

Таблиця 3.7 – Характеристики відеореєстратора PVDR-1654

Відео	входи	16 (BNC)
	наскрізні виходи	немає
	виходи на монітор	1 – BNC, 1 – VGA
	відображення	400 fps – загальна, 25 fps – на канал
Аудіо	входи	16 (RCA)
	наскрізні виходи	немає
	виходи на монітор	1 (RCA)
Тривожні	входи	16
	виходи	4
Операційна система	RTOS	Спеціалізована Real Time Operating System
Меню	русифіковане	
Запис	компресія	H-264 (потоковий алгоритм стиснення MPEG-4 Part10)
	Дозвіл	180x144, 360x288, 528x384, 720x288
	Загальна швидкість запису	400 fps при будь-якому дозволі
	Швидкість запису на кожен канал	1-25 fps за вибором індивідуально для кожної камери
	Активація запису	Постійна, по детектору, по датчику, за розкладом, по команді оператора
Пошук в архіві	багатоваріантний	За часом, за подією, «до першого запису», «до останнього запису»
Багатоза-дачність	Запис, перегляд архіву і робота по мережі одночасно	
Управління		З передньої панелі, ІЧ – пульт (в комплекті), по мережі
Порти		1 – RS-485 (для управління поворотними камерами), 1 – USB (Підключення CD-RW і HDD), 1 line in (мікрофонний – для голосового спілкування з мережевим клієнтом)
Робота по мережі TCP / IP	підключення	ADSL, LAN / Dynamic IP supported
	функції	Моніторинг, перегляд архіву, настройка, архівація, управління PTZ-камерами, upgrade, запис архіву на мережевий диск, голосове спілкування з оператором DVR
	швидкість моніторингу	До 25 fps на канал
HDD	доступний обсяг	4000 Gb
	диски	8 дисків SATA до 500Gb (можливо читання на ПК)
	рекомендовані диски	Maxtor 80-300 Gb WD 40-300 Gb
Резервне копіювання	За мережі TCP / IP	Кадри та відеофрагменти

Продовження таблиці 3.7

	через CompactFlash	Кадри та відеофрагменти
	через USB	на USB-Flash, USB-HDD, USB – CD-RW, USB – DVD-RW
Розміри і вага	розміри пристрою	450x450x95
	вага пристрою	9 кг
	Вага в упаковці	11 кг

Працездатність відеореєстратора.

1. Мережа TCP/IP, дистанційне керування мережею.

2. 4 варіанти якості зображення, регульована швидкість запису та перегляду відео.

3. Параметри для кожного каналу: Контраст, Яскравість, Відтінок і Насиченість.

4. Можливість збереження подій і відеозаписів, зображень в певний час на FLASH носій через USB.

5. Кілька режимів відеозапису: ручний відеозапис, дротовий відеозапис, вбудований датчик руху, відеозапис датчика тривоги.

6. 3 види пошуку: пошук за часом, подіями та розділами.

7. Автоматичне перемикання каналів, водяний знак, стоп-кадр та інші функції.

8. Триплекс (одночасний перегляд в режимі реального часу, запис відео, перегляд архіву).

9. Інтерфейс жорсткого диска ATA-100, підтримка 2 жорстких дисків розміром понад 200 ГБ.

10. Можливість встановлення пристрою для запису CD-RW або знімного жорсткого диска.

Відеозображення виводиться на 2 монітори: Загальний і Тривожний. На загальний монітор виводиться квадратне зображення з усіх камер, а на сигнальний монітор – зображення з камери, яка зафіксувала присутність зловмисника. В якості монітора спостереження обрано монітор Ai-ML247N 20

TFT-LCD, зовнішній вигляд якого показано на рисунку 3.7. Технічні характеристики наведені в таблиці 3.8.

Рисунок 3.7 – Монітор Ai-ML247N

Таблиця 3.8 – Технічні характеристики монітора Ai-ML247N

Тип 20 "TFT LCD	Дозвіл 800 x 600
Видима частина, мм. 408 x 306	Співвідношення 4: 3
Кількість квітів, млн. 16.7	Яскравість, кд / м2. 450
Контрастність 500: 1	Кут огляду (вертикальний / горизонтальний) 60/80
Час відгуку, мс. 16	Вхідні сигнали Відео: 2 CH Composite video. 1.0Vp-pt 75Ом. S-Video: Y: 1.0Vp-p w / Neg. SYNC. C: 0.285Vp-p. Аналогові: RGB. Аудіо: стерео, 50 ~ 100mVp-p.
Вхідна / Вихідна опір, Ом. 75	Тип відеосигналу NTSC / PAL / SVGA / VGA
Сигнальні роз'єми Відео: 2CH BNC входу / виходу. Аудіо: 2CH RCA RL вхід / вихід. 15 Pin D-Sub роз'єм. S-Video: 4-pin Min-DIN.	Живлення 90 ~ 260VAC 60Hz / 50Hz / DC12V
Струм 3.5A / 42W	Розміри, мм. (ШхВхГ) 491x400x80
Вага, кг. 7	Кріплення на стіну VESA 100
Робоча температура, С. -10 ~ 50	

Функції монітора.

• Повна підтримка NTSC/PAL/SECAM;

• Адаптивний 2/4 сітчастий фільтр для яскравості та кольороподілу;

• Збільшення зображення подвоєння пікселів і CTI;

• Автоматичне налаштування зображення;

• Легке регулювання контрастності/яскравості/кольору/спотворення;

• Пульт;

• 2 композитних входу/виходу, 1 S-video вхід/вихід;

3.5 Висновок до третього розділу

Підводячи підсумок, можна сказати, що для побудови якісного КІСІ, який відповідає всім нормативно-правовим актам України, необхідно використовувати тільки сертифіковані засоби захисту даних. Також необхідний детальний аналіз засобів інформаційної безпеки, щоб визначити всі чутливі зони відділу.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

4.1.1 Характеристика умов праці при роботі з ЕОМ

Людство сьогодні практично не мислить свою діяльність у вирішенні актуальних завдань без обчислювальної техніки та інформаційних технологій. Впровадження ПЕОМ забезпечує більш високу ефективність виробництва за рахунок удосконалення технологічного процесу і підвищення продуктивності праці. Очевидність необхідності сучасних інформаційних технологій, побудованих на базі комп'ютерів, незаперечна.

Однак, разом з позитивною стороною, людство при використанні комп'ютерних технологій піддається цілого ряду негативних факторів, які істотно позначаються на його життєздатності.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням користувача, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ПЕОМ. Велике значення має раціональна конструкція і розташування елементів робочого місця, що важливо для підтримки оптимальної робочої пози людини користувача ПЕОМ.

Умови праці працюючих з ПЕОМ характеризуються можливістю впливу на них наступних виробничих факторів: шуму, тепловиділень, шкідливих речовин, статичної електрики, іонізуючих та неіонізуючих випромінювань, недостатнього освітлення, параметрів технологічного обладнання та робочого місця. У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці та відпочинку. В іншому випадку у персоналу наголошуються значна напруга зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в попереку, в області шиї і руках.

4.1.2 Режим праці

Як вже було зазначено, при роботі з персональним комп'ютером дуже важливу роль грає дотримання правильного режиму праці і відпочинку. В іншому випадку у персоналу наголошуються значна напруга зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в попереку, в області шиї і руках.

У таблиці 4.1 представлені відомості про регламентовані перерви, які необхідно робити при роботі на комп'ютері, в залежності від тривалості робочої зміни, видів і категорій трудової діяльності з ВДТ (відеодисплейний термінал) і ПЕОМ

Таблиця 4.1 – Час регламентованих перерв при роботі на комп'ютері

Категорія роботи з ВДТ або ПЕОМ	Рівень навантаження за робочу зміну при видах роботи з ВДТ			Сумарний час регламентованих перерв, хв	
	Група А, кількість знаків	Група Б, кількість знаків	Група В, годин	При 8-годинній зміні	При 12-годинній зміні
I	до 20000	до 15000	до 2,0	30	70
II	до 40000	до 30000	до 4,0	50	90
III	до 60000	до 40000	до 6,0	70	120

Всі види трудової діяльності, пов'язані з використанням комп'ютера, розділяються на три групи:

- група А: робота з зчитування інформації з екрану ВДТ або ПЕОМ з попереднім запитом;
- група Б: робота з введення інформації;
- група В: творча робота в режимі діалогу з ЕОМ.

Час безперервної роботи для I кат. – 2 години; для II і III категорії 1,5-2 години.

Режим праці і відпочинку операторів, що працюють з ЕОМ, повинен бути

наступним: через кожну годину інтенсивної роботи необхідно влаштовувати 15-хвилинну перерву, при менш інтенсивної через кожні 2 години.

Ефективність перерв підвищується при поєднанні з виробничою гімнастикою або організації спеціального приміщення для відпочинку персоналу із зручними м'якими меблями, акваріумом, зеленою зоною і т.п.

4.1.3 Вимоги до мікроклімату

Параметри мікроклімату можуть змінюватися в широких межах, в той час як необхідною умовою життєдіяльності людини є підтримка постійності температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла в навколишнє середовище. Принцип нормування мікроклімату – створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Обчислювальна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості в приміщенні. Ці приміщення повинні бути обладнані пристроями кондиціонування повітря для дотримання нормативних параметрів мікроклімату.

Мікрокліматичні умови на робочих місцях в приміщеннях з обчислювальною технікою повинні відповідати вимогам, зазначеним в таблиці 4.2.

Таблиця 4.2 – Мікроклімат виробничих приміщень

Період року	Температура повітря, °С	Швидкість руху повітря, м / с	Відносна вологість повітря, %
холодний	22-24	до 0,1	40-60
теплий	23-25	0,1-0,2	40-60

Повітря, що надходить в робочі приміщення операторів ЕОМ, повинен

бути очищений від забруднень, в тому числі від пилу і мікроорганізмів.

Норми подачі свіжого повітря в приміщення, де розташовані комп'ютери, з урахуванням, що категорія виконуваних робіт «I_a», наведені в таблиці 4.3.

Таблиця 4.3 – Норми подачі свіжого повітря в приміщення, де розташовані комп'ютери

Характеристика приміщення	Об'ємна витрата подаваного в приміщення свіжого повітря, $м^3$ / на одну людину в годину
Обсяг до 20$м^3$ на людину	Не менш 30
20 ... 40$м^3$ на людину	Не менш 20
Більш 40$м^3$ на людину	Природна вентиляція

Кондиціювання повітря має забезпечувати підтримку параметрів мікроклімату в необхідних межах протягом усіх сезонів року, очищення повітря від пилу і шкідливих речовин, створення необхідного надлишкового тиску в чистих приміщеннях для виключення надходження неочищеного повітря. Температура повітря, що подається повинна бути не нижче 19°С.

Температуру в приміщенні слід регулювати з урахуванням теплових потоків від обладнання. Перевага повинна віддаватися обладнання з малою електричною потужністю. Устаткування треба встановлювати так, щоб теплові потоки від нього не були спрямовані на операторів. Слід також обмежувати кількість обчислювальної техніки в приміщенні і уникати підлогових опалювальних систем.

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціонування повітря, опалювальна система).

4.1.4 Вимоги до рівнів шуму та вібрації

Шум погіршує умови праці, роблячи шкідливий вплив на організм людини. Працюючі в умовах тривалої шумової дії випробовують дратівливість, головні болі, запаморочення, зниження пам'яті, підвищену стомлюваність, зниження апетиту, біль у вухах і т. Д. Такі порушення в роботі ряду органів і систем організму людини можуть викликати негативні зміни в емоційному стані людини аж до стресових. Під впливом шуму знижується концентрація уваги, порушуються фізіологічні функції, з'являється втома у зв'язку з підвищеними енергетичними витратами і нервово-психічним напруженням, погіршується мовна комутація. Все це знижує працездатність людини і його продуктивність, якість і безпеку праці.

Основними джерелами шуму в приміщеннях, обладнаних обчислювальною технікою, є принтери, плоттери, розмножувальна техніка та обладнання для кондиціювання повітря, вентилятори систем охолодження, трансформатори.

Рівень шуму на робочих місцях не повинен перевищувати 50 дБА. Нормовані рівні шуму забезпечуються шляхом використання малошумного обладнання, застосуванням звукопоглинальних матеріалів (спеціальні перфоровані плити, панелі, мінераловатні плити).

Крім того, необхідно використовувати підвісні акустичні стелі.

4.1.5 Вимоги до освітлення на робочих місцях

Важливе місце в комплексі заходів по створенню умов праці, які працюють з ПЕОМ, займає створення оптимальної світловий середовища, тобто раціональна організація природного та штучного освітлення приміщення і робочих місць.

Правильно спроектоване і виконане виробниче освітлення покращує умови зорової роботи, знижує стомлюваність, сприяє підвищенню продуктивності праці, благотворно впливає на виробниче середовище, надаючи

позитивну психологічну дію на працюючого, підвищує безпеку праці і знижує травматизм.

Недостатність освітлення призводить до напруги зору, послаблює увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає осліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань, тому настільки важливий правильний розрахунок освітленості.

Існує три види освітлення – природне, штучне і поєднане (природне і штучне разом).

Природне освітлення – освітлення приміщень денним світлом, що потрапляє через світлові прорізи в зовнішніх огороджувальних конструкціях приміщень.

Штучне освітлення застосовується при роботі в темний час доби і вдень, коли не вдається забезпечити нормовані значення коефіцієнта природного освітлення (похмура погода, короткий світловий день). Освітлення, при якому недостатнє за нормами природне освітлення доповнюється штучним, називається змішаним освітленням.

Штучне освітлення підрозділяється на робоче, аварійне, евакуаційне, охоронне. Робоче освітлення, у свою чергу, може бути загальним або комбінованим. Загальне – освітлення, при якому світильники розміщуються у верхній зоні приміщення рівномірно або стосовно до розташування обладнання. Комбіноване – освітлення, при якому до загального додається місцеве освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об'єкта розрізнення 0,3 ... 0,5 мм) величина коефіцієнта природного освітлення (КПО) повинна бути не нижче 1,5%, а при зоровій роботі середньої точності (найменший розмір об'єкта розрізнення 0, 5 ... 1,0 мм) КЕО повинен

бути не нижче 1,0%. Як джерела штучного освітлення звичайно використовуються люмінесцентні лампи типу ЛБ, або ДРЛ, які попарно об'єднуються в світильники, які повинні розташовуватися рівномірно над робочими поверхнями.

Штучне освітлення в приміщеннях і на робочих місцях повинні створювати хорошу видимість інформації на екрані ЕОМ. При цьому в полі зору працюючих повинні бути забезпечені оптимальні співвідношення яскравості робочих і оточуючих поверхонь. Найбільш оптимальною для роботи з екраном є освітленість 200 лк, при роботі з екраном в поєднанні з роботою над документами – 400 лк.

Для освітлення робочих місць застосовується комбіноване освітлення (загальне плюс місцеве), хоча більш переважно загальне освітлення через більшого перепаду яркостей на робочому місці при використанні світильників місцевого освітлення.

Для загального освітлення використовуються в основному стельові або вбудовані світильники з люмінесцентними лампами. Яскравість повинна бути не більше 200 кд / м^2. Джерела світла краще використовувати нейтрально-білого або "теплого" білого кольору з індексом передачі кольору не менше 70. Для виключення засвічення екранів прямими світловими потоками світильники загального освітлення мають в своєму розпорядженні збоку від робочого місця, паралельно лінії зору оператора.

Найбільш придатними світильниками є світильники типу ЛПО 36, ЛБ, ЛПО 36 з ВуПР і інші аналогічні. При використанні світильників з люмінесцентними лампами необхідно вживати заходів щодо обмеження пульсації освітленості в межах до 5%.

Місцеве освітлення на робочих місцях забезпечується світильниками, що встановлюються безпосередньо на робочому столі або на вертикальних панелях спеціального обладнання. Вони повинні мати відбивач і розташовуватися нижче або на рівні лінії зору операторів, щоб не викликати засліплення.

4.1.6 Електромагнітне і іонізуюче випромінювання

Більшість вчених вважають, що як короткочасне, так і тривалий вплив усіх видів випромінювання від екрану монітора не небезпечно для здоров'я користувача, що працює з цими комп'ютерами. Проте вичерпних даних щодо небезпеки дії випромінювання від моніторів на працюючих з комп'ютерами не існує і дослідження в цьому напрямку тривають.

Максимальний рівень рентгенівського випромінювання на робочому місці користувача ПЕОМ зазвичай не перевищує 10мкбер / ч, а інтенсивність ультрафіолетового і інфрачервоного випромінювань від екрану монітора лежить в межах 10 ... 100МВт / м^2. Допустимі значення параметрів неіонізуючих електромагнітних випромінювань представлені в таблиці 7.4.

Таблиця 5.4 Допустимі значення параметрів неіонізуючих електромагнітних випромінювань.

Найменування параметру	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	10В / м
Напруженість магнітної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	0,3А / м
Напруженість електростатичного поля не повинна перевищувати для дорослих користувачів	20кВ / м

Для зниження впливу цих видів випромінювання рекомендується застосовувати монітори із зниженим рівнем випромінювання, встановлювати захисні екрани, а також рекомендується обмежувати тривалість роботи з екраном ВДТ, не розміщувати їх концентровано в робочій зоні і вимикати їх, якщо на них не працюють.

Поряд з цим потрібно встановлювати в приміщенні з ВДТ іонізатори повітря, частіше провітрювати приміщення і хоча б один раз протягом робочої зміни очищати екран від пилу.

4.1.7 Загальні вимоги до організації робочих місць користувачів ПЕОМ

Проектування робочих місць, забезпечених ЕОМ, відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки.

Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця співробітника повинні бути дотримані наступні основні умови:

- оптимальне розміщення устаткування, що входить до складу робочого місця
- достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення.

Ергономічними аспектами проектування комп'ютеризованих робочих місць, зокрема, є: висота робочої поверхні, розміри простору для ніг, вимоги до розташування документів на робочому місці, характеристики робочого крісла, вимоги до поверхні робочого столу, можливість регулювання елементів робочого місця.

Головними елементами робочого місця співробітника банку є стіл і крісло.

Робоча поза сидячи викликає мінімальне стомлення. Раціональне планування робочого місця передбачає чіткий порядок і сталість розміщення предметів, засобів праці і документації. Те, що потрібно для виконання робіт частіше, розташоване в зоні легкої досяжності робочого простору.

Для комфортної роботи стіл повинен задовольняти наступним умовам

- висота столу повинна бути вибрана з урахуванням можливості сидіти вільно, в зручній позі, при необхідності спираючись на підлокітники;
- нижня частина столу повинна бути сконструйована так, щоб працівник міг зручно сидіти, ні змушений підбирати ноги;

- поверхню столу повинна мати властивості, що виключають появу відблисків;
- конструкція столу повинна передбачати наявність висувних ящиків (не менше 3 для зберігання документації, лістингів, канцелярського приладдя).
- висота робочої поверхні рекомендується в межах 680-760 мм. Висота поверхні, на яку встановлюється клавіатура, повинна бути близько 650 мм.

Велике значення надається характеристикам робочого крісла. Так, рекомендована висота сидіння над рівнем підлоги знаходиться в межах 420-550 мм. Поверхня сидіння м'яка, передній край закруглений, а кут нахилу спинки – регульований.

Необхідно передбачати при проектуванні можливість різного розміщення документів: збоку від комп'ютера між монітором і клавіатурою і т.п. Крім того, у випадках, коли комп'ютер має низьку якість зображення, наприклад помітні мелькання, відстань від очей до екрана роблять більше (близько 700 мм), ніж відстань від ока до документа (300-450 мм). Взагалі при високій якості зображення на комп'ютері відстань від очей користувача до екрану, документа і клавіатури може бути рівним.

Положення екрану визначається:

- відстанню зчитування (0,6 ... 0,7 м);
- кутом зчитування, напрямком погляду на 20° нижче горизонталі до центру екрану, причому екран перпендикулярний цьому напряму.

Повинна також передбачатися можливість регулювання екрану:

- по висоті +3 см;
- по нахилу від -10° до +20° щодо вертикалі;
- в лівому і правому напрямках.

Велике значення також надається правильній робочій позі користувача.

При незручній робочій позі можуть з'явитися болі в м'язах, суглобах і сухожиллях. Вимоги до робочої пози користувача ПЕОМ наступні:

- голова не повинна бути нахилена більш ніж на 20°,
- плечі повинні бути розслаблені,
- лікті – під кутом 80°... 100°,
- передпліччя і кисті рук – в горизонтальному положенні.

Причина неправильної пози користувачів обумовлена наступними факторами:

- немає хорошої підставки для документів;
- клавіатура знаходиться дуже високо, а документи – низько;
- нікуди покласти руки і кисті;
- недостатньо простір для ніг.

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць має велике значення, як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці.

4.2 Безпека в надзвичайних ситуаціях

Аналіз умов експлуатації комп'ютерної техніки свідчить, що однією із основних причин виникнення надзвичайної ситуації може бути пожежа. Детальний аналіз стану пожежної безпеки в установі, де проводилась робота, свідчить про її належний рівень, оскільки за десятилітній період не зареєстровано жодного випадку виникнення пожежі.

Пожежі являють собою неконтрольоване горіння поза спеціальним вогнищем, яке наносить матеріальні збитки. Джерелом запалювання можуть бути електронні схеми, прилади для технічного обслуговування, пристрої для електроживлення кондиціонера тощо. Адже кисень як джерело процесу горіння є в будь-якій точці на робочому місці. Пожежна безпека – це такий стан об'єкта, при якому з регламентованою ймовірністю виключається можливість

виникнення і розвитку пожежі, а також впливу на людей її небезпечних чинників й забезпечується захист матеріальних цінностей.

У даному разі у приміщенні із комп'ютерною технікою осередком загоряння може стати будь-яке обладнання, що живиться від електромережі, а причиною пожежі може бути:

- халатне поводження з електроприладами (паління, залишення без нагляду нагрівальних приладів);
- коротке замикання;
- перевантаження мережі;
- іскріння від пошкодження ізоляції;
- неякісні контакти в місцях з'єднання проводів (скрутки).

Система запобігання пожежі регламентується комплексом організаційних заходів і технічних засобів, направлених на виключення умов виникнення пожежі, а система протипожежного захисту – комплексом організаційних заходів і технічних засобів, спрямованих на запобігання впливу на людей небезпечних чинників (токсичних продуктів) і обмеження матеріального збитку від нього.

Пожежа може виникнути в результаті короткого замикання. Причинами виникнення пожежі можуть бути:

- порушення режимних вимог;
- несправність і неправильна експлуатація ЕОМ і пристроїв місцевого освітлення.

Пожежні сигналізація, оповіщення та зв’язок. Швидке виявлення і сигналізація про виникнення пожежі, своєчасний виклик пожежних підрозділів та оповіщення про пожежу людей, що перебувають у зоні можливої небезпеки, дозволяє швидко локалізувати осередки пожежі, провести евакуацію і необхідні заходи щодо гасіння пожежі. Тому організації, установи тощо необхідно забезпечувати засобами зв’язку і системами пожежної сигналізації та оповіщення.

Виконання всіх робіт за персональним комп'ютером повинне обов’язково супроводжуватися дотриманням всіх вимог пожежної безпеки, обумовлених Законом України “Про пожежну безпеку”, прийнятим 17 грудня 1993 року.

У розрізі дотримання цих вимог передбачаємо розробку комплексних заходів щодо забезпечення пожежної безпеки:

- розробку і затвердження нормативних актів і інструкцій в межах підприємства, організації, установи;
- здійснення постійного контролю за їх дотриманням;
- забезпечення додержання протипожежних вимог стандартів, норм, правил;
- забезпечення виконання вимог приписів і постанов органів державного пожежного нагляду;
- утримування в справному стані засобів протипожежного захисту і зв’язку, пожежної техніки, обладнання та інвентарю, недопускання їх використання не за призначенням;
- здійснення заходів щодо впровадження автоматичних засобів виявлення та гасіння пожеж;
- своєчасне інформування пожежної охорони про несправність пожежної техніки, системи протипожежного захисту, водопостачання тощо.

Експлуатація персональних електронно-обчислювальних машин повинна супроводжуватися виконанням:

- технічних заходів;
- експлуатаційних заходів;
- організаційних заходів;
- протипожежних заходів режимного характеру.

До технічних заходів відносяться заходи по дотриманню протипожежних правил, норм особливо при:

- монтуванні електрообладнання;

- обслуговуванні електрообладнання;
- монтуванні опалення;
- монтуванні освітлення;
- правильному розміщенні електрообладнання.

До експлуатаційних протипожежних заходів відносяться своєчасні профілактичні огляди, ремонти та випробування обладнання.

Організаційні заходи передбачають:

- правильну експлуатацію обладнання;
- протипожежний інструктаж робітників;
- підготовку та видання наказів з питань посилення пожежної безпеки.

Заходи режимного характеру – це заборона куріння в невстановлених місцях.

Найбільш швидким та надійним засобом виявлення та сповіщення про пожежу вважається автоматична установка пожежної сигналізації, яка повинна працювати цілодобово. Основні елементи системи електричної пожежної сигналізації:

- сповіщувачі (давачі), котрі монтуються в приміщеннях або по території об’єкта і призначені для повідомлення про пожежу;
- приймальні апарати (станції), котрі забезпечують прийом сигналів від сповіщувачів;
- лінійні мережі чи кабелі, що з’єднують сповіщувачі з приймальними апаратами;
- джерела електроживлення.

Залежно від схеми з’єднання існують променеві (радіальні) та шлейфові (кільцеві) автоматичні установки пожежної сигналізації. При променевій схемі приймальна станція і кожен сповіщувач з’єднує окрема лінія (промінь складається із двох окремих проводів: прямого і зворотного). У кожний промінь може бути включено паралельно до 3-4 сповіщувачів. Променеву систему

застосовують при невеликій протяжності ліній пожежної сигналізації. Шлейфова (кільцева) система електричної пожежної сигналізації відрізняється тим, що сповіщувачі ввімкнені послідовно у однопровідну лінію (шлейф), початок і кінець якої з'єднані з приймальною станцією. У один шлейф включають до 50 сповіщувачів. Дія шлейфової системи основана на принципі передачі від сповіщувача на приймальну станцію певного числа імпульсів. Приймальна станція виявляє номери сповіщувачів, які спрацювали, за допомогою спеціальних пристроїв, котрі являють собою шукачі чи багатократні перемикачі і записуючі пристрої.

Пожежні сповіщувачі перетворюють неелектричні фізичні величини (випромінювання теплової і світлової енергії, рух частинок диму) в електричні, які у вигляді сигналів певної форми надходять по проводах на приймальну станцію. За способом перетворення пожежні сповіщувачі поділяються на параметричні, котрі перетворюють неелектричні величини у електричні за допомогою допоміжного джерела струму, і генераторні, в яких зміна неелектричної величини призводить до появи власної ЕРС. Пожежні сповіщувачі можуть бути ручної дії, призначені для видачі дискретного сигналу при натискуванні відповідної пускової кнопки, і автоматичної дії для видачі дискретного сигналу при досягненні заданого значення фізичного параметра (температури, спектра світлового випромінювання тощо).

Ручні сповіщувачі встановлюються всередині приміщення (в коридорах та на сходових площадках) як додатковий технічний засіб до автоматичної установки пожежної сигналізації. Передбачаємо використання автоматичних засобів виявлення пожежі – світлових сповіщувачів. Світлові сповіщувачі побудовані на принципі дії ультрафіолетового випромінювання вогню. У них в якості чутливого елемента застосовані лічильники фотонів, які володіють високою чутливістю і здатні виявляти навіть невеликі осередки вогню (наприклад, горіння сірника) практично миттєво. Незважаючи на високу чутливість, світлові сповіщувачі не спрацьовують як від денного світла, котре

надходить у приміщення через вікна, так і від електричного освітлення, тому що ультрафіолетові промені поглинаються склом вікон і ламп. Світлові сповіщувачі застосовуються у закритих приміщеннях, в яких відсутні джерела ультрафіолетових променів, відкритого вогню тощо.

4.3 Висновок до четвертого розділу

До інструкції з охорони праці при роботі за комп’ютером можна добавити наступні загальні вимоги безпеки:

- до самостійної роботи допускаються особи віком після 18 років, які ознайомлені з інструкціями по експлуатації обладнання і інструкціями по охороні праці (під розпис), правилами надання першої медичної допомоги, пройшли навчання безпечним методам праці і мають необхідну кваліфікацію та практичні навики роботи;
- на території кафедри і необхідно бути уважним, дотримуватись вимог Правил внутрішнього розпорядку і виробничої санітарії;
- кількість символів при обробці текстового та цифрового матеріалу не повинно перевищувати 30 тисяч символів за 4 години роботи;
- необхідно уникати попадання вологи всередину принтера, блоку живлення та ЕОМ ПК;
- помітивши неполадки, що не забезпечують вимоги охорони праці, до роботи не приступати до їх усунення;
- при виникненні нещасного випадку з працюючим на ЕОМ ПК, потерпілий або свідок нещасного випадку повинен негайно повідомити начальника підрозділу для проведення розслідування і усунення причин нещасного випадку, надати першу допомогу;
- порушення вимог даної інструкції тягне за собою відповідальність порушника згідно з чинним законодавством.

При проектуванні комп'ютерної техніки необхідно враховувати умови її

експлуатації з тим, щоб при дії на неї: вологи, сонячної радіації, механічних коливань, високих та низьких тисків і температур, агресивних речовин – вона починає працювати неправильно.

Конструкції елементів комп'ютерної техніки повинна забезпечувати захист людини від ураження електричним струмом, а також запобігати накопиченню зарядів статичної електрики в небезпечних кількостях. Елементи комп'ютерної техніки повинні бути оснащеними засобами сигналізації про порушення нормального режиму роботи, а в необхідних випадках (аваріях, небезпечних пошкодженнях, режимах, близьких до небезпечних) – засобами автоматичної зупинки та відімкнення від джерел енергії[14].

ВИСНОВКИ

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

Отже, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

За результатами роботи можна зробити висновки про ефективність розробленої системи за трьома критеріями:

- сумарний річний збиток, розрахований методом еквівалентного шкоди, на порядок перевищує номінальну вартість запропонованої системи захисту і її обслуговування в однорічному періоді;
- величина сумарного річного збитку неприйнятна для кафедри таких розмірів, тим самим введення в експлуатацію КСЗІ є невідкладні заходом щодо забезпечення стабільності діяльності підприємства;
- витрати на введення в дію та експлуатацію складають п'яту частину кошторису кафедри, що вважається прийнятним.

За результатом роботи, з урахуванням висновків про ефективність системи, можна рекомендувати КСЗІ на впровадження з приватними доробками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про інформацію” [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12 [Дата доступу] 10.01.2018р.;
2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” ” [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12 [Дата доступу] 09.01.2018р.;
3. Закон України "Про телекомунікації" [Електронний ресурс] // 12. – 2003. – Режим доступу до ресурсу: http://zakon.rada.gov.ua/go/1280-15. - Ст. 155 [Дата доступу] 10.01.2018р.;.
4. Закон України "Про науково-технічну інформацію" від 25 червня 1993 року № 3322-XII // Відомості Верховної Ради. - 1993. - № 33. - Ст. 345.
5. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / Р.А. Калюжний - К., 2002. - 296 с.
6. Інформаційна безпека України. Проблеми та шляхи їх вирішення. Заочний круглий стіл // Національна безпека та оборона. - 2001. - № 1. - с. 60 - 70.
7. Інформаційний простір України // Національна безпека і оборона. - 2001. - № 1 (13) - с. 3 - 16.
8. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23 лютого 2002 р. № 9.
9. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації" 30 листопада 1999 р. № 53.

10. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах" від 24 грудня 2001 № 76.

11. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про Положення про державну експертизу в сфері технічного захисту інформації" від 29 грудня 1999 р. № 62.

12. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про Положення про контроль за функціонуванням системи технічного захисту інформації" від 22 грудня 1999 р. № 61.

13. Указ Президента України "Про заходи щодо захисту інформаційних ресурсів держави" від 10 квітня 2000 р. № 582/2000.

14. Указ Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 31 липня 2000 р. № 928/2000.

15. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації;

16. ДБН А.2.2-3-97 Проектування. Склад, порядок розробки, узгодження і затвердження проектної документації для будівництва;

17. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;

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

19. НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

20. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної

діяльності. Створення комплексу технічного захисту інформації. Основні положення;

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

22. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

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

24. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи;

25. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;

26. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

27. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

28. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

29. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено постановою КМУ від 16.02.98 № 180;

30. Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Держспецзв'язку України від 16.05.07 № 93,

зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087;

31. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України;

32. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ 29.03.06 № 373;

33. РД 50-34.698-90. Автоматизированные системы. Требования к созданию документов.

34. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок;

35. Мотузко Ф.Я. Охрана праці. – К.: Вища школа, 1989. – 336с.

36. Белова Н.А. Безпека життєдіяльності. - М.: Знание, 2000 - 364с.

37. Самгин Е.Б. Освітлення робочих місць. – К.: МИРЭА, 1989. – 186с.

38. Боротьба з шумом на виробництві: Довідник / Е.Я. Юдін, Л.А. Борисов; Під ред. Е.Я. Юдіна – К.: КПІ, 1985. – 400с.

39. Зінченко В.П. Основі ергономіки. – М.: МГУ, 1979. – 179с.

40. Тарасова В.В. Навчальний посібник. - К.: Ніка-Центр, 2007. – 276 с.