Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Технологій захисту конфіденційної інформації державних підприємств "

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації »
(шифр і назва напряму підготовки, спеціальності)

Олекшій Зоряна Василівна
підпис (прізвище та ініціали)

Керівник Муж В.В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 «Кібербезпека та захист інформації »
(шифр і назва спеціальності)

Студенту Олекшій Зоряна Василівна
(прізвище, ім'я, по батькові)

1. Тема роботи Технології захисту конфіденційної інформації державних підприємств

Керівник роботи Муж Валерій Вікторович, кандидат юридичних наук, доцент КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «22» 11. 2024 року № 4/7-1120

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ, 1 Теоретико-правові засади захисту конфіденційної інформації; 1.1. Аналіз нормативно-правової бази у сфері захисту інформації,1.2. Еволюція систем захисту інформації в Україні, 1.3 Порівняльний аналіз систем захисту інформації: український та світовий досвід,1.4. Порівняльний аналіз КСЗІ та інших систем управління інформаційною безпекою.2 Аналіз Інормаційної безпеки підприємства; 2.1. Характеристика об'єкту захисту, 2.2. Аналіз загроз та вразливостей, 2.3. Обґрунтування необхідності створення КСЗІ. 3.Розробка елементів КСЗІ для підприємства.; 3.1. Організаційні заходи, 3.2. Технічні заходи, 3.3. Документальне забезпечення КСЗІ,3.4. Рекомендації щодо впровадження та атестації КСЗІ. 4.Охорона праці та безпека у надзвичайних ситуаціях. 4.1 Охорона праці при роботі на персональному комп'ютері, 4.2 Безпека під час роботи на персональному комп'ютері Висновки. Перелік використаних джерел. Додатки.

.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.Тема, автор науковий керівник квалафікаційної роботи. 2.Актуальність. 3.Мета,об'єкт,предмет дослідження. 4. Аналіз нормативно-правової бази України. 5.Еволюція систем захисту інформації.6. Порівняльний аналіз стандартів українських систем захисту інформації з міжнародними.7.Оцінка інформаційної бузпеки. 8. Необхідність створення Комплексної системи захисту інформації.9.Атестація КСЗІ.10.Висновок.

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., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Збір матеріалів і вивчення нормативно-правової бази	22.09 – 22.09	Виконано
3.	Аналіз літератури та наукових статей з тематики інформаційної безпеки	23.09 – 30.09	Виконано
4.	Формування структури роботи та затвердження з науковим керівником	01.10-03.10	Виконано
5.	Проведення порівняльного аналізу українського та світового досвіду	05.10 – 14.10	Виконано
6.	Розробка обґрунтування необхідності створення КСЗІ	15.10 –25.10	Виконано
7.	Розробка організаційних заходів для КСЗІ	26.11 – 03.11	Виконано
8.	Розробка технічних заходів для КСЗІ	04.11-18.11	Виконано
9.	Підготовка документального забезпечення КСЗІ	20.11-30.11	Виконано
10.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	01.12-09.12	Виконано
11.	Оформлення кваліфікаційної роботи	10.12-13.12	Виконано
12.	Нормоконтроль	14.12	Виконано
13.	Перевірка на плагіат	16.12	Виконано
14.	Попередній захист кваліфікаційної роботи		Виконано
15.	Захист кваліфікаційної роботи		

Студент _____ Олекшій З.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Муж В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Технологій захисту конфіденційної інформації державних підприємств // ОР «Магістр» // Олекшій Зоряна Василівна// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмд-61 // Тернопіль, 2024 // С.114 , рис. – - , табл. –13 , кресл. – - , додат. – 6.

Ключові слова:КСЗІ,ІТ,КІ.

У роботі досліджено теоретико-правові засади та практичні аспекти захисту конфіденційної інформації на підприємствах, зокрема державного сектору. Основну увагу приділено аналізу нормативно-правової бази України у сфері інформаційної безпеки, порівнянню українських систем захисту інформації зі світовим досвідом та вивченню особливостей створення комплексних систем захисту інформації (КСЗІ).

У першому розділі охарактеризовано правову основу захисту інформації, історичний розвиток систем безпеки в Україні та проведено порівняльний аналіз КСЗІ та інших систем управління інформаційною безпекою.

Другий розділ присвячений аналізу інформаційної безпеки підприємства, зокрема характеристиці об'єкта захисту, ідентифікації загроз і вразливостей та обґрунтуванню необхідності впровадження КСЗІ.

У третьому розділі запропоновано організаційні, технічні та документальні заходи для розробки КСЗІ.

Результати дослідження спрямовані на вдосконалення підходів до захисту інформації державних підприємств, адаптацію до сучасних технологій та підвищення рівня інформаційної безпеки в умовах зростання кіберзагроз.

ABSTRACT

Technologies for the Protection Confidential Information of State Enterprises // OR "Master" // Olekshii Zoriana // Ternopil National Technical University named after Ivan Puluy, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, SBmd-61 Group // Ternopil, 2024 // P.114, fig. – - , table. – 13, chair. – - , appendix. –6.

Keywords: CISS, IT, KI.

The paper examines the theoretical and legal foundations and practical aspects of the protection of confidential information at enterprises, in particular the public sector. The main attention is paid to the analysis of the regulatory framework of Ukraine in the field of information security, comparison of Ukrainian information security systems with world experience and study of the peculiarities of creating integrated information security systems (CIS).

The first section characterizes the legal basis for information protection, the historical development of security systems in Ukraine and conducts a comparative analysis of CISS and other information security management systems.

The second section is devoted to the analysis of the information security of the enterprise, in particular, the characteristics of the object of protection, the identification of threats and vulnerabilities and the justification of the need for the implementation of the CIS.

The third section proposes organizational, technical and documentary measures for the development of the CIS.

The results of the study are aimed at improving approaches to protecting information of state-owned enterprises, adapting to modern technologies and increasing the level of information security in the context of growing cyber threats.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ — Інформаційні технології

ЗІ — Захист інформації

КІ — Конфіденційна інформація

ЗІК — Захист інформаційних конфіденційних даних

ШІ — Шифрування інформації

VPN — Віртуальна приватна мережа

MPLS — Multiprotocol Label Switching (Мультипротокольна міткова комутація)

AES — Алгоритм симетричного шифрування (Advanced Encryption Standard)

RSA — Алгоритм асиметричного шифрування (публічний/приватний ключ)

TLS/SSL — Протоколи захисту передавання даних (Transport Layer Security/Secure Sockets Layer)

ПЗ — Програмне забезпечення

КРС — Контроль доступу до ресурсів

АУ — Аутентифікація

БІ — Біометрична ідентифікація

РП — Резервне копіювання

РК — Розподілені ключі

ППП — Політика безпеки підприємства

ДШ — Доступ до шифрованих даних

ДСК — Довірена сторона криптографії

ІКТ — Інформаційно-комунікаційні технології

МІС — Моделі інформаційних систем

IDS — Система виявлення вторгнень

IPS — Система запобігання вторгнень

Інфозахист — Інформаційна безпека

ЗШ — Захист шифрування

ІЗЗ — Ідентифікація та захист з’єднань

ФС — Фізична безпека (наприклад, захист серверних приміщень)

РМ — Ризик-менеджмент

ЧЗІ — Часова зона інтерфейсів

БЗ — Брандмауер (Firewall)

ЗМІСТ

ВСТУП

Захист конфіденційної інформації є однією з ключових складових інформаційної безпеки державних підприємств в умовах глобальної цифровізації та розвитку кіберпростору. Сучасні виклики, пов’язані з хакерськими атаками, витоком даних та інформаційним шпигунством, вимагають від державних структур розробки ефективних систем захисту конфіденційної інформації, які відповідають національним та міжнародним стандартам. Особливої актуальності питання захисту конфіденційної інформації набуває в умовах воєнного стану в Україні, де загрози для інформаційної безпеки суттєво зростають, оскільки держава є об’єктом кібернетичних атак з боку ворога.

Актуальність теми обумовлена необхідністю вдосконалення механізмів захисту інформації в державних підприємствах, що займаються стратегічними галузями, зокрема обороною, енергетикою, комунікаціями тощо. Сучасні засоби інформаційної безпеки дозволяють забезпечити збереження даних, однак їх постійна модернізація є необхідною для протистояння новим видам кіберзагроз. Тому дослідження та впровадження комплексної системи захисту інформації (КСЗІ) на державних підприємствах є важливим завданням для забезпечення стійкості та безпеки національної інформаційної інфраструктури.

Мета дослідження полягає у комплексному аналізі технологій захисту конфіденційної інформації на державних підприємствах України та розробці рекомендацій щодо впровадження КСЗІ на підприємстві.

Об’єкт дослідження – захист конфіденційної інформації в інформаційно-комунікаційних системах.

Предмет дослідження – технології захисту конфіденційної інформації державних підприємств.

Завдання дослідження:

1. Проаналізувати нормативно-правову базу сферою регулювання якої є захист інформації, зокрема законодавство, постанови КМУ, накази та

нормативні документи Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ), а також міжнародних стандартів.

2. Дослідити еволюцію систем захисту інформації в Україні та визначити перспективи їх розвитку.
3. Здійснити порівняльний аналіз українських систем захисту інформації з міжнародними аналогами, зокрема КСЗІ та ISO 27001.
4. Оцінити інформаційну безпеку обраного державного підприємства, проаналізувати загрози та вразливості.
5. Обґрунтувати необхідність створення КСЗІ на основі аналізу ризиків і критичних активів підприємства.
6. Розробити елементи КСЗІ для обраного підприємства, включаючи організаційні та технічні заходи.
7. Надати рекомендації щодо впровадження та атестації КСЗІ.

Для досягнення поставлених завдань та реалізації мети дослідження використовувалися різноманітні методи, що забезпечили комплексний підхід до аналізу технологій захисту конфіденційної інформації на державних підприємствах України. Основні методи, застосовані у даному дослідженні, включають:

1. Аналіз та синтез. Метод використовувався для дослідження нормативно-правової бази України у сфері захисту інформації, а також для оцінки еволюції систем захисту інформації. Аналіз дозволяє виявляти наявність сильних та слабких сторін існуючих систем, а за допомогою синтезу вбачається можливим формування нових рекомендацій, керуючись отриманими даними.
2. Застосування порівняльного аналізу мало місце для порівняння українських систем захисту інформації з міжнародними стандартами, зокрема КСЗІ та ISO 27001. Цей метод дав змогу виявити низку особливостей, переваг та недоліків різних підходів до захисту інформації, що є необхідним для вибору оптимальної системи для підприємства.

3. Метод оцінки ризиків був використаний для ідентифікації та оцінки загроз та вразливостей, з якими стикаються державні підприємства. Оцінка ризиків допомогла визначити активи, що потребують особливого захисту, а також підставила основу для обґрунтування необхідності створення КСЗІ.
4. Соціологічні методи потрібні для збору даних про інформаційну безпеку в підприємствах були використані анкетування та інтерв'ю з фахівцями в галузі інформаційної безпеки. Ці методи забезпечили отримання практичної інформації про наявні системи захисту, їх ефективність та недоліки.
5. Документальний метод базується на аналізі документів, таких як технічні завдання, політики безпеки, акти обстеження та інші регламентуючі документи, що стосуються захисту конфіденційної інформації на державних підприємствах. Це дозволяє об'єктивно оцінити існуючі практики та визначити напрямки для покращення.
6. Моделювання потрібне для розробки елементів КСЗІ було використано моделювання, яке дозволяє візуалізувати процеси захисту інформації, а також оцінити їх ефективність. Це дає можливість передбачити можливі наслідки від реалізації запропонованих рішень.

Таким чином, використані методи дозволяють глибоко проаналізувати технології захисту конфіденційної інформації на державних підприємствах, виявити проблеми та запропонувати ефективні рішення для підвищення інформаційної безпеки.

Наукова новизна полягає у комплексному підході до розробки та впровадження елементів КСЗІ для державних підприємств з урахуванням специфічних потреб в умовах воєнного стану. Особливістю даного дослідження є розробка рекомендацій, які базуються на сучасних міжнародних стандартах, таких як ISO 27001, а також адаптація цих стандартів до умов українських державних підприємств.

Практичне значення роботи полягає в тому, що результати дослідження можуть бути використані державними підприємствами для вдосконалення своїх систем захисту конфіденційної інформації. Рекомендації щодо створення КСЗІ та проведення атестації дозволять підприємствам підвищити рівень інформаційної безпеки, що сприятиме їх захищеності від зовнішніх та внутрішніх загроз.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічні конференції «Інформаційні моделі, системи та технології» (м.Тернопіль, Україна), 18-19.12.2024.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

1.1. Аналіз нормативно-правової бази у сфері захисту інформації

Захист конфіденційної інформації є елементом забезпечення національної, економічної та інформаційної безпеки держави. Нормативно-правова база, що регулює цей процес, складається з міжнародних стандартів, національного законодавства та підзаконних актів, які визначають основи захисту інформації, кола прав та обов’язків, якими наділені суб’єкти інформаційних відносин.

Головним нормативним актом у досліджуваній тематиці є Закон України "Про інформацію", який визначає поняття інформації, її види та правові засади її обробки та збереження. Особливе місце в ньому отримала інформація, що має обмеження у доступі, до якої доцільно віднести конфіденційну інформацію. Законом встановлено, що обмежити доступ до інформації можливо лише на підставах, передбачених законом, зокрема для захисту прав та інтересів особи, держави чи суспільства.

Іншим актом є Закон України "Про захист персональних даних", який регулює процес обробки, зберігання та передачі персональних даних фізичних осіб. Він визначає поняття "персональні дані", права суб’єктів цих даних та обов’язки розпорядників інформації, включаючи необхідність забезпечення їх конфіденційності. Закон також встановлює відповідальність за порушення правил роботи з персональними даними [8].

У контексті захисту державної таємниці слід відзначити Закон України "Про державну таємницю", який регулює порядок надання інформації статусу державної таємниці, організацію доступу до такої інформації, а також механізми її охорони. Цей акт закладає основи створення режимно-секретних органів та процедур доступу до секретної інформації.

Також не можна оминути Закон України "Про електронні довірчі послуги", який регламентує використання електронних підписів, сертифікатів ключів і

захищених носіїв інформації. У сучасних умовах цей закон відіграє роль у захисті електронної комунікації.

Варто враховувати й міжнародні стандарти, такі як ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, який пропонує комплексний підхід до забезпечення конфіденційності, цілісності та доступності інформації. Державна політика України у сфері захисту інформації поступово адаптується до цих стандартів, що сприяє інтеграції України до світового інформаційного простору [9].

Крім того, слід звернути увагу на підзаконні акти, які конкретизують положення вищезазначених законів. Наприклад, постанови Кабінету Міністрів України та накази Держспецзв'язку, що визначають технічні аспекти захисту інформації, процедури сертифікації засобів захисту, вимоги до криптографічного захисту тощо.

Таким чином, нормативно-правова база у сфері захисту інформації включає багаторівневу систему актів, яка забезпечує регулювання цієї сфери на різних рівнях – від загальних принципів до технічних деталей. Її подальший розвиток і гармонізація з міжнародними стандартами є необхідною умовою для забезпечення ефективного захисту інформації в Україні.

Сучасний розвиток корпоративних і локальних мереж зумовлює постійне вдосконалення способів і засобів комплексного захисту інформації. Це передбачає підвищення ефективності організації захисту інформаційних ресурсів за допомогою новітніх програмних і технічних рішень.

Комплексна система захисту інформації (КСЗІ) охоплює заходи та засоби, які спрямовані на попередження наступних загроз [9]:

- Витік інформації через технічні канали, такі як побічні електромагнітні випромінювання чи акустичні впливи.
- Несанкціоновані дії та доступ до інформації, зокрема через неавторизоване підключення, маскування під легального користувача чи використання шкідливих програм.

- Цілеспрямовані впливи на інформацію, наприклад, створення електромагнітних або інших полів, що порушують її цілісність.

Захист інформації в сучасних ІКСМ має враховувати особливості оброблюваних даних, клас автоматизованої системи та умови її експлуатації. Основною метою таких заходів є забезпечення безпеки інформації на всіх етапах життєвого циклу системи.

Інформація в інтегрованих комплексних системах управління (ІКСМ) постійно піддається впливу внутрішніх і зовнішніх загроз. Серед внутрішніх загроз можна виділити ненавмисні помилки персоналу, недостатню кваліфікацію співробітників або навіть навмисні дії, наприклад, крадіжку даних чи саботаж. Зовнішніми факторами ризику є кібератаки, шкідливі програми, несанкціонований доступ сторонніх осіб, а також стихійні лиха чи технічні збої в обладнанні.

Такі загрози можуть призводити до порушення основних характеристик інформації, зокрема її точності, доступності та конфіденційності. Цілісність інформації страждає внаслідок її спотворення чи втрати, доступність — у разі неможливості отримати до неї доступ у потрібний момент, а конфіденційність — через несанкціоноване розкриття чи використання даних [8].

З метою зменшення впливу цих ризиків використовуються спеціалізовані заходи, спрямовані на захист інформації на всіх етапах її обробки, передачі та зберігання.

Нормативно-правове забезпечення відіграє ключову роль у захисті інформації, оскільки воно регламентує правила та стандарти захисту інформаційних ресурсів. Під ним розуміють систему правових норм, що визначають [6]:

- Порядок створення та використання захищених ІКСМ.
- Регламентацію отримання, обробки та збереження інформації.
- Вимоги до побудови КСЗІ та захисту базових властивостей інформації, таких як конфіденційність, цілісність і доступність.

– Права та обов’язки персоналу, який працює з інформаційною системою.

Нормативно-правове забезпечення також передбачає впровадження заходів щодо виявлення та усунення загроз, визначення статусу інформаційної системи з точки зору безпеки, а також етапів створення та експлуатації КСЗІ.

Захист інформації в сучасних умовах вимагає комплексного підходу, який поєднує технічні, організаційні та правові заходи. Нормативно-правове забезпечення є базовою складовою, яка дозволяє забезпечити ефективний і надійний захист інформаційних ресурсів, враховуючи сучасні виклики та ризики інформаційної безпеки [5].

Для створення комплексної системи захисту інформації (КСЗІ) в інформаційно-комунікаційних системах і мережах необхідно враховувати вимоги низки нормативно-правових актів, які визначають основи організації захисту інформаційних ресурсів на всіх етапах їх життєвого циклу. Ключовими документами є Закони України "Про інформацію" та "Про захист інформації в автоматизованих системах". Окрім того, велике значення мають галузеві нормативні документи, зокрема НД ТЗІ, які регламентують положення щодо захисту інформації від несанкціонованого доступу, термінологію в цій галузі, класифікацію автоматизованих систем і функціональні профілі їх захищеності.

Визначення стандартних функціональних профілів захищеності є етап побудови КСЗІ. Такі профілі включають перелік мінімально необхідних послуг і механізмів, які система захисту має реалізовувати. Їхнє формування базується на аналізі потенційних загроз і вимог до захищеності інформації, таких як забезпечення її цілісності та доступності [5].

Функціональні профілі дозволяють протидіяти загрозам, таким як несанкціонована модифікація або передача даних, випадкові чи навмисні помилки користувачів. Серед основних механізмів, які застосовуються, є процедури ідентифікації, аутентифікації та виявлення порушень цілісності інформації. Це сприяє забезпеченню захисту як окремих повідомлень, так і потоків даних в цілому.

Отже, побудова захищених інформаційно-комунікаційних систем базується на дотриманні нормативно-правових вимог і впровадженні методологічної бази для ефективної протидії загрозам інформаційній безпеці. Основна мета цих заходів полягає у забезпеченні цілісності, доступності та конфіденційності інформації, яка обробляється, зберігається і передається в системі.

1.2. Еволюція систем захисту інформації в Україні

Еволюція систем захисту інформації в Україні відображає розвиток інформаційних технологій та відповідь на зростаючі загрози в інформаційній сфері. З моменту здобуття незалежності країна почала активно розвивати законодавчу базу та впроваджувати технічні рішення для захисту даних, що стало необхідним у контексті інтеграції до глобального інформаційного простору [1].

Перші кроки у створенні систем захисту інформації в Україні були зосереджені на адаптації радянського досвіду до нових умов незалежної держави. На початку 1990-х років було розроблено основи національного законодавства, що регламентує питання захисту інформації, зокрема прийняття законів "Про інформацію" та "Про захист інформації в автоматизованих системах".

На наступному етапі, в 2000-х роках, було створено нормативно-правові акти та стандарти, які визначили технічні та організаційні аспекти захисту даних. Впровадження стандартів НД ТЗІ дозволило класифікувати інформаційні системи за рівнем захищеності та визначити механізми захисту, що відповідають сучасним вимогам.

З розвитком інформаційних технологій у 2010-х роках акцент змістився на протидію кіберзагрозам та забезпечення кібербезпеки на національному рівні. Це включало створення Державної служби спеціального зв’язку та захисту

інформації України, а також ухвалення законодавства, спрямованого на забезпечення кіберзахисту важливих об’єктів інфраструктури [29].

Сучасний етап характеризується посиленням міжнародної співпраці, гармонізацією національних стандартів із міжнародними, а також інтеграцією новітніх технологій, таких як блокчейн, шифрування даних та системи штучного інтелекту для моніторингу та виявлення загроз.

Розвиток систем захисту інформації в Україні демонструє поступову еволюцію від базових технічних заходів до комплексних стратегій кіберзахисту, що враховують сучасні виклики. Законодавча база та технічні рішення постійно вдосконалюються, забезпечуючи належний рівень захисту інформаційних ресурсів, що є необхідним для національної безпеки в умовах зростання цифрових загроз.

1.3 Порівняльний аналіз систем захисту інформації: український та світовий досвід

Порівняльний аналіз систем захисту інформації між українським і світовим досвідом є кроком для розуміння ефективності існуючих моделей захисту даних, а також для виявлення можливостей для їх вдосконалення. З цього боку доцільно зфокусувати акцент на ключові аспекти, такі як законодавче регулювання, технологічні рішення, підходи до управління ризиками та організаційні структури.

В Україні основою для захисту інформації є кілька законів, зокрема Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закон України «Про захист персональних даних». Ці закони формують правову базу для захисту даних, але потребують подальшої адаптації до сучасних викликів, зокрема в контексті кібератак та захисту персональної інформації.

У світовій практиці, зокрема в Європейському Союзі, вбачається існування Загального регламенту щодо захисту даних (GDPR), яким встановлюється високий рівень стандартів для обробки персональних даних. GDPR зобов'язує

організації забезпечувати конфіденційність та безпеку даних, передбачаючи серйозні штрафи за порушення. Порівнюючи з українським законодавством, можна зазначити, що українські норми часто є менш жорсткими, що може мати наслідком знижений рівень захищеності інформації.

На рівні технологій в Україні спостерігається впровадження різних систем, покликаних захищати інформацію, зокрема систем криптографічного захисту, систем управління доступом і моніторингу безпеки. Однак, через обмежені фінансові ресурси та недостатню підтримку з боку держави, не всі підприємства можуть реалізувати сучасні технології на належному рівні.

У світі, особливо в країнах з розвиненою економікою, технології захисту інформації постійно вдосконалюються. Наприклад, компанії в США та Західній Європі активно впроваджують рішення на основі штучного інтелекту для виявлення та реагування на загрози в режимі онлайн. В Україні ще не всі організації можуть дозволити собі таке впровадження через високі витрати на новітні технології [8].

В Україні питання управління ризиками в інформаційній безпеці не завжди розглядається системно. Багато підприємств не мають чітких стратегій управління ризиками, що призводить до вразливості перед новими загрозами. Законодавство лише починає вводити вимоги щодо регулярної оцінки ризиків, але їх реалізація залишається на низькому рівні.

Водночас, у світовій практиці управління ризиками в інформаційній безпеці є невід’ємною частиною корпоративного управління. Організації у США та Європі використовують розроблені стандарти, такі як ISO 31000, для оцінки та управління ризиками в інформаційній сфері. Ці підходи дозволяють знижувати ймовірність інцидентів та забезпечувати надійний захист даних.

В Україні організаційні структури, що відповідають за інформаційну безпеку, часто є недостатньо розвиненими. Багато підприємств покладаються на старші підходи без чіткої інтеграції між різними підрозділами. Це може призводити до неефективності в управлінні інформаційною безпекою.

У світовій практиці, зокрема в міжнародних корпораціях, інформаційна безпека інтегрована в загальну структуру управління підприємством. Системи управління інформаційною безпекою (СУІБ) мають чітку організаційну структуру, що включає окремі підрозділи, відповідальні за різні аспекти безпеки. Це дозволяє забезпечувати існування комплексного підходу до захисту інформації.

Порівняльний аналіз систем захисту інформації в Україні та у світі виявляє як досягнення, так і недоліки. Україні необхідно покращити законодавче регулювання, впровадити новітні технології, системно підходити до управління ризиками та створити ефективні організаційні структури для забезпечення належного рівня захисту інформації. Вивчення світового досвіду може стати основою для реформ у цій = сфері, що в свою чергу сприятиме зміцненню національної безпеки.

1.4 Порівняльний аналіз КСЗІ та інших систем управління інформаційною безпекою

За допомогою Порівняльного аналізу Комплексної системи захисту інформації (КСЗІ), міжнародного стандарту ISO 27001 та системи управління інформаційною безпекою (СУІБ) дозволяє виявити ключові особливості кожної з них, а також їх переваги та недоліки. Цей аналіз є необхідним для вибору оптимальної системи захисту інформації, відповідно до специфіки діяльності організації.

КСЗІ в Україні є основним механізмом, покликаним забезпечити інформаційну безпеку на установах та підприємствах державної форми власності. Вона включає в себе заходи, технології та організаційні структури, які призначені забезпечувати захист інформації від несанкціонованого доступу, зміни або знищення [10].

КСЗІ забезпечує комплексний підхід, інтегруючи технологічні та організаційні рішення для захисту інформації. КСЗІ відповідає вимогам

українського законодавства, що робить її незамінною для державних установ. Систему можна адаптувати відповідно до специфіки підприємства або установи.

В Україні технології, що використовуються в КСЗІ, можуть бути застарілими, що знижує ефективність захисту. КСЗІ не завжди відповідає міжнародним практикам, що може ускладнити інтеграцію з іноземними партнерами.

ISO 27001 є міжнародним стандартом, що встановлює вимоги до систем управління інформаційною безпекою (СУІБ). Стандарт надає організаціям структуру для забезпечення безпеки інформації через оцінку ризиків і впровадження відповідних контролів.

ISO 27001 є визнаним стандартом у всьому світі, що підвищує довіру клієнтів і партнерів. Стандарт акцентує увагу на ідентифікації та оцінці ризиків, що дозволяє організаціям своєчасно реагувати на загрози. Стандарт може бути адаптований до потреб будь-якої організації, незалежно від її розміру чи сфери діяльності [11].

Впровадження стандарту може вимагати значних ресурсів і часу, що може бути проблематичним для малих підприємств. Процес сертифікації може бути дорогим, що може стати перешкодою для деяких організацій.

Система управління інформаційною безпекою (СУІБ) є більш широким поняттям, яке охоплює всі аспекти управління інформаційною безпекою в організації, включаючи політики, процедури та контрольні механізми. СУІБ забезпечує інтеграцію всіх аспектів інформаційної безпеки, від технологій до організаційних процедур. Система дозволяє організаціям відповідати вимогам як національного, так і міжнародного законодавства. СУІБ дозволяє постійно оцінювати ефективність заходів безпеки та вносити корективи.

СУІБ вимагає постійного оновлення політик та процедур відповідно до змін у технологіях та загрозах. Управління СУІБ може бути складним завданням, особливо в великих організаціях з різноманітними бізнес-процесами.

Проведений аналіз КСЗІ, ISO 27001 та СУІБ свідчить про те, що кожна з систем має свої унікальні переваги та недоліки. КСЗІ є ефективною для

забезпечення відповідності національному законодавству, але має обмежену технологічну базу. ISO 27001 пропонує міжнародні стандарти, але може бути дорогим та складним у впровадженні. СУІБ є комплексним підходом, але вимагає постійного вдосконалення [11].

Вибір між цими системами залежить від специфіки організації, її розміру, ресурсів та стратегічних цілей у сфері інформаційної безпеки. З огляду на світові тенденції та виклики, Україні необхідно інтегрувати елементи міжнародних стандартів у національні системи, щоб забезпечити належний рівень захисту інформації в умовах швидко змінюваного інформаційного середовища.

РОЗДІЛ 2. АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Характеристика об'єкту захисту

Об'єктом захисту в рамках аналізу інформаційної безпеки підприємства є його інформаційні ресурси, що включають дані, програмне забезпечення, обладнання та мережеву інфраструктуру. Ці ресурси використовуються для забезпечення основної діяльності підприємства, прийняття управлінських рішень і підтримання взаємодії з партнерами, клієнтами та постачальниками.

Інформаційні ресурси підприємства умовно поділяються на дві основні категорії: дані, без яких діяльність підприємства неможлива, та допоміжна інформація, яка підтримує роботу системи, але не є життєво необхідною. До критичних даних належать комерційні та фінансові звіти, конфіденційна інформація клієнтів, технічна документація та інші стратегічні матеріали.

Об'єктами захисту також є програмно-апаратні комплекси, зокрема сервери, робочі станції, бази даних та мережеве обладнання, які забезпечують зберігання та обробку даних. Інфраструктура, що підтримує інформаційні потоки, включає внутрішні локальні мережі, доступ до Інтернету та віддалені точки підключення [12].

Особливу увагу слід приділити обліковим записам користувачів і системам управління доступом, адже їх несанкціоноване використання становить суттєву загрозу для безпеки підприємства. Усі об'єкти захисту характеризуються залежністю від ефективної реалізації політики безпеки, що включає ідентифікацію, аутентифікацію, моніторинг та реагування на інциденти.

Таким чином, характеристика об'єкта захисту дозволяє визначити слабкі місця, оцінити ступінь ризику для інформаційної безпеки та сформувати необхідні заходи для мінімізації загроз.

Організаційна структура підприємства є складовою для забезпечення ефективного функціонування та управління інформаційною безпекою. Вона

визначає ролі, відповідальність та взаємодію між різними підрозділами, що впливають на захист інформації та управління ризиками.

Зазвичай, організаційна структура підприємства включає кілька основних рівнів управління інформаційною безпекою. На верхньому рівні знаходиться керівництво підприємства, яке відповідає за загальну політику безпеки та прийняття стратегічних рішень щодо захисту інформаційних ресурсів. Воно затверджує основні принципи безпеки, визначає пріоритети і забезпечує фінансування заходів з інформаційної безпеки [12].

Нижче керівництва може бути створена спеціалізована служба або відділ з інформаційної безпеки, який здійснює безпосередній контроль за впровадженням політики безпеки на практиці. Цей підрозділ розробляє та реалізує заходи щодо захисту інформаційних ресурсів, таких як захист від несанкціонованого доступу, забезпечення резервного копіювання, управління доступом, захист від вірусів та інших шкідливих програм, а також реагування на інциденти.

Також в організаційній структурі підприємства можуть бути окремі підрозділи або спеціалісти з безпеки інформаційних систем, мереж, програмного забезпечення, а також фахівці, які займаються навчанням співробітників щодо вимог інформаційної безпеки та правильного поводження з даними.

У деяких підприємствах може існувати також роль координатора з безпеки, який взаємодіє з іншими відділами та служить зв'язком між технічними фахівцями і керівництвом. Ця структура забезпечує своєчасне реагування на загрози та інциденти, а також постійну підтримку та оновлення політик безпеки.

Таким чином, організаційна структура підприємства повинна бути чітко визначена і узгоджена з усіма рівнями управління, щоб забезпечити ефективне управління інформаційною безпекою та захист інформаційних ресурсів від внутрішніх і зовнішніх загроз [11].

Інформаційні потоки на підприємстві відображають рух даних і інформації між різними підрозділами та користувачами, як всередині організації, так і поза її межами. Вони охоплюють передачу даних між різними інформаційними

системами, внутрішніми та зовнішніми користувачами. Ще одною складовою є те, як саме відбувається передача інформації між різними рівнями: від працівників до відділів, відділів до керівництва або між підприємством і зовнішніми партнерами.

Ключовим є те, що кожен з таких потоків несе ризики щодо порушення цілісності, конфіденційності та доступності інформації. Зовнішні потоки включають дані, які передаються підприємством партнерам, постачальникам або клієнтам через інтернет чи інші канали комунікації, тоді як внутрішні потоки — це інформація, що передається між працівниками або підрозділами в межах організації.

Для забезпечення належної безпеки інформаційних потоків варто використовувати спеціалізовані системи захисту, які відповідають за запобігання витоку даних та їх пошкодження. Це включає впровадження систем шифрування, які забезпечують конфіденційність переданих даних, а також заходи з моніторингу і контролю доступу до інформації. Ще одною частиною є використання фаєрволів та антивірусних програм, які допомагають захистити від зловмисних вторгнень [11].

Додатково, для ефективного контролю інформаційних потоків підприємство може впровадити системи виявлення аномалій та потенційно небезпечних операцій. Це дозволяє своєчасно виявляти підозрілі дії, що можуть загрожувати цілісності або доступності інформації. Всі ці заходи сприяють збереженню належного рівня безпеки інформаційних потоків і забезпечують захист підприємства від різноманітних загроз.

2.2. Аналіз загроз та вразливостей

Аналіз загроз та вразливостей є певним етапом у забезпеченні інформаційної безпеки підприємства, оскільки допомагає ідентифікувати потенційні ризики, які можуть вплинути на цілісність, доступність і конфіденційність інформації. Процес аналізу загроз передбачає оцінку факторів,

які можуть призвести до негативних наслідків, а також визначення слабких місць у системах захисту, які ці загрози можуть експлуатувати.

Що стосується вразливостей, то вони виникають через слабкі місця в системах безпеки, програмному забезпеченні або процесах управління інформацією.

Загалом, регулярний аналіз загроз і вразливостей дозволяє своєчасно виявляти і нейтралізувати потенційні ризики, що сприяє підтримці високого рівня інформаційної безпеки підприємства [12].

Класифікація загроз інформаційної безпеки підприємства є необхідним етапом для формулювання стратегії захисту інформації та визначення пріоритетів у розробці заходів захисту. Загрози можна класифікувати за кількома ознаками, враховуючи різноманітні аспекти, такі як джерело загрози, мета нападу, а також наслідки для інформаційних ресурсів.

Загрози можуть виникати як з боку внутрішніх учасників, так і з боку зовнішніх. Внутрішні загрози можуть походити від співробітників або підрядників підприємства, які мають доступ до інформаційних систем. До таких загроз належать умисні або ненавмисні дії співробітників, що призводять до розголошення або зміни конфіденційної інформації, або ж інші порушення політик безпеки. Водночас зовнішні загрози виникають від сторонніх осіб або організацій, таких як хакери, кіберзлочинці або конкуренти, які намагаються отримати несанкціонований доступ до інформаційних ресурсів.

Загрози можуть бути класифіковані залежно від того, які саме аспекти інформації порушуються. Існує три основні категорії, які визначають основні вимоги до захищеності інформації [12]:

- Загрози цілісності інформації спричиняють порушення правильності та точності даних. Це може бути результатом модифікацій даних без дозволу, зловмисних змін або випадкових помилок, що призводять до корупції або втрати інформації.
- Загрози доступності пов’язані з ускладненням доступу до інформаційних ресурсів або сервісів. Вони можуть призвести до зниження

працездатності системи або навіть до повної відмови в доступі до необхідних даних, що може мати серйозні наслідки для бізнесу.

– Загрози конфіденційності виникають тоді, коли інформація потрапляє до несанкціонованих осіб. Це може стосуватися як розголошення особистих даних, так і комерційно інформації, що завдає шкоди репутації або конкурентоспроможності підприємства.

Фізичні загрози пов’язані з можливими пошкодженнями обладнання чи інфраструктури. Це можуть бути природні катастрофи (повінь, землетрус), несанкціонований доступ до серверів або даних, крадіжка обладнання або ж фізичне знищення інформаційних ресурсів. Кіберзагрози виникають, коли зловмисники використовують інформаційні технології для проникнення в комп’ютерні системи. До таких загроз відносяться різноманітні вірусні атаки, хакерські зломи, фішинг, або інші методи злому паролів і кодів. Загрози соціальної інженерії виникають тоді, коли зловмисники маніпулюють людьми для того, щоб отримати доступ до систем або конфіденційної інформації. Це можуть бути телефонні дзвінки, фальшиві електронні листи або інші способи обману [13].

За рівнем впливу на діяльність організації є загрози – це загрози, які можуть призвести до серйозних наслідків для діяльності підприємства, таких як значні фінансові збитки, репутаційні втрати або порушення законодавчих вимог. До загроз відносяться зломи, крадіжка конфіденційної інформації, а також катастрофи, що можуть призвести до зупинки діяльності компанії.

Помірковані загрози – це загрози, які можуть вплинути на роботу підприємства, але їхні наслідки менш серйозні і можуть бути швидко усунені без значних втрат для організації. Це можуть бути незначні порушення доступності інформаційних систем, проблеми з програмним забезпеченням або незначні порушення цілісності даних. Незначні загрози – це мінімальні загрози, що, як правило, не спричиняють серйозних наслідків для підприємства. Вони можуть бути пов’язані з помилками в роботі програмного забезпечення або дрібними збої в системах, які легко усуваються.

Загрози можуть виникати як з природних, так і техногенних чинників. Природні загрози включають стихійні лиха, такі як повені, пожежі, землетруси або інші природні катастрофи, які можуть пошкодити інфраструктуру підприємства або призвести до втрати даних. Техногенні загрози пов’язані з людським фактором: помилки персоналу, збої в апаратному забезпеченні, неполадки у програмному забезпеченні або в системах управління інформацією [16].

Тимчасові загрози можуть впливати на інформаційну безпеку лише впродовж обмеженого періоду. Наприклад, вірусні атаки або короткочасні відмови в доступі до системи. Постійні загрози мають тривалий або постійний характер, як-от безперервні спроби злому або постійні інсайдерські загрози.

Загалом, класифікація загроз дозволяє організаціям краще зрозуміти ризики, з якими вони можуть зіткнутися, та розробити відповідні стратегії для їх мінімізації. Детальний аналіз загроз допомагає визначити пріоритети в захисті інформаційних ресурсів і вчасно приймати необхідні контрзаходи.

Процес оцінки ризиків дозволяє визначити потенційні загрози та вразливості, що можуть вплинути на цілісність, доступність та конфіденційність інформації. Це дозволяє підприємствам ефективно управляти ресурсами, виявляти слабкі місця в системах безпеки та впроваджувати відповідні заходи для зниження рівня ризику.

Оцінка ризиків включає в себе кілька етапів, серед яких є ідентифікація загроз, аналіз вразливостей, оцінка ймовірності виникнення загроз, а також визначення можливих наслідків цих загроз. Після проведення оцінки ризиків підприємство отримує уявлення про напрямки в інформаційній безпеці, що дозволяє оптимізувати інвестиції в заходи захисту та забезпечити відповідність стандартам безпеки.

Таблиця 2.1 – Оцінка ризиків інформаційної безпеки підприємства

Загроза	Вразливість	Ймовірність (оцінка)	Вплив (оцінка)	Ризик (ймовірність × вплив)	Заходи для зниження ризику
Хакерський злам серверів	Недостатній захист паролів та доступу	8	9	72	Впровадження двофакторної аутентифікації, оновлення програмного забезпечення
Втрата даних через техногенну аварію	Відсутність резервного копіювання	7	10	70	Регулярне створення резервних копій, використання засобів аварійного відновлення
Викрадення даних через фішинг	Відсутність навчання персоналу	6	8	48	Проведення тренінгів для співробітників, впровадження фільтрів для пошти
Недотримання політики конфіденційності	Слабка організація доступу до конфіденційної інформації	7	8	56	Впровадження чіткої політики доступу, контроль за доступом до даних
Втрата даних через збій обладнання	Відсутність моніторингу та обслуговування обладнання	5	6	30	Регулярне технічне обслуговування, моніторинг роботи обладнання

Оцінка ризиків спрямована на виявлення ймовірних загроз для інформаційної безпеки підприємства, а також на визначення рівня їхнього

впливу на діяльність організації. Для цього використовуються різні методи, включаючи кількісну та якісну оцінку ризиків, що дозволяє точно визначити, які заходи варто впровадити для зменшення потенційних загроз.

Ризик оцінюється на основі ймовірності виникнення загрози та можливого впливу на систему. Оцінка проводиться за шкалою від 1 до 10, де 1 — мінімальна ймовірність або вплив, а 10 — максимальна. Ризик обчислюється як добуток ймовірності та впливу, що дає змогу визначити пріоритетність заходів захисту.

Загрози, що мають високий рівень ризику, вимагають негайного реагування, а для загроз із поміркованим рівнем ризику можна розробити стратегічні заходи для зниження ймовірності їхнього виникнення.

Оцінка ризиків допомагає не лише виявити потенційні загрози, а й приймати рішення щодо того, як краще розподілити ресурси для забезпечення безпеки. У процесі оцінки ризиків варто враховувати всі можливі аспекти, від технічних до людських факторів, оскільки людина може бути як джерелом загрози, так і її засобом зниження. Ще одним етапом є також впровадження заходів для зниження ризиків, таких як підвищення рівня безпеки доступу, навчання персоналу, регулярне оновлення програмного забезпечення, а також використання сучасних технологій для резервного зберігання даних та відновлення після аварій [18].

Загалом, ефективна оцінка ризиків є запорукою створення надійної системи інформаційної безпеки, здатної протистояти сучасним загрозам.

Критичні активи підприємства — це ресурси, які є потрібними для забезпечення безперервної діяльності організації та її здатності виконувати основні функції. Вони можуть бути як фізичними, так і інформаційними, і їхнє збереження, а також захист від можливих загроз має вирішальне значення для функціонування підприємства. До активів відносяться не лише основні матеріальні засоби, але й інформаційні ресурси, технології, а також дані, що мають стратегічне значення для організації.

Процес визначення активів дозволяє встановити, які саме елементи системи потребують найбільш ретельного контролю та захисту. Це дозволяє

сформулювати стратегії управління ризиками та запровадити необхідні заходи для збереження їх цілісності, доступності та конфіденційності. Ключовим етапом є класифікація активів за рівнем значення, що дає змогу правильно розподілити ресурси для забезпечення найвищого рівня безпеки.

Таблиця 2.2 - Визначення активів підприємства

Категорія активу	Опис активу	Значення для підприємства	Потенційні загрози	Заходи для захисту
Інформаційні системи	Комп'ютерні системи, сервери, програмне забезпечення	Висока	Кіберзагрози, несанкціонований доступ	Шифрування, антивірусне ПЗ, контроль доступу
Технологічні процеси	Процеси виробництва або надання послуг	Висока	Аварії, технічні збої, втрати даних	Підтримка резервних копій, аварійне відновлення
Персонал	Працівники, їхні навички та знання	Висока	Втрата кваліфікації, звільнення співробітників	Програми навчання, мотивація персоналу
Фінансові активи	Грошові кошти, рахунки, фінансові документи	Середня	Викрадення, шахрайство, несанкціоновані транзакції	Контроль за фінансовими операціями, захист від шахрайства
Операційна інфраструктура	Будівлі, транспортні засоби, офісне обладнання	Середня	Пожежі, стихійні лиха, пошкодження інфраструктури	Охорона, технічне обслуговування, перевірки безпеки
Дані клієнтів та партнери	Особисті дані, договори, угоди, маркетингові дослідження	Висока	Викрадення даних, витік конфіденційної інформації	Шифрування, політика конфіденційності, доступ за дозволами

Визначення активів полягає в оцінці ресурсів, без яких функціонування підприємства буде неможливим або серйозно порушеним. Це вимагає комплексного підходу до кожного типу активів, адже деякі з них можуть бути менш очевидними, але не менш необхідними. Наприклад, знання та досвід персоналу також можна віднести до активів, оскільки їх відсутність або зниження кваліфікації можуть призвести до серйозних втрат для організації.

Загрози для активів можуть бути різноманітними: від фізичних пошкоджень до кіберзагроз або втрат даних. Оцінка потенційних загроз для кожного типу активів дозволяє вибрати правильні методи захисту, що допоможуть мінімізувати негативні наслідки.

Завдяки цьому підходу можна також правильно організувати пріоритети для інвестування в безпеку та технічні засоби захисту. Для кожного активу обираються відповідні заходи, наприклад, для захисту інформаційних систем це можуть бути антивірусні програми та системи шифрування, а для персоналу — регулярне навчання та вдосконалення навичок.

Визначення активів є важливим в управлінні інформаційною безпекою підприємства. Чітке розуміння, які активи є найбільш необхідними для безперебійної роботи організації, дозволяє ефективно планувати заходи щодо їх захисту. Враховуючи постійно змінювану ситуацію з новими загрозами, необхідно регулярно переглядати і актуалізувати список активів та методи їх захисту. Це допомагає знизити ризики, зберігаючи ресурси в безпеці та забезпечуючи стійкість підприємства до можливих інцидентів у сфері інформаційної безпеки [19].

2.3. Обґрунтування необхідності створення КСЗІ

КСЗІ (Комплексна система захисту інформації) є інструментом для забезпечення безпеки інформаційних ресурсів підприємства. У сучасному цифровому середовищі загрози безпеці інформації стають усе більш складними та різноманітними. Відсутність ефективної системи захисту може призвести до

серйозних наслідків: від втрати даних до фінансових та репутаційних втрат. Тому створення КСЗІ є кроком для забезпечення належного рівня безпеки та стійкості організації до можливих кіберзагроз.

Різноманітність загроз та вразливостей інформаційних систем, що зростають, вимагає комплексного підходу до захисту. Це означає, що для успішного забезпечення захисту інформації повинна бути створена спеціалізована система, яка інтегрує різні методи і технології захисту: від захисту на рівні мережі до шифрування даних і контролю доступу. КСЗІ є необхідним елементом у створенні стратегії безпеки, яка дозволяє своєчасно реагувати на загрози, оцінювати рівень вразливості і адаптувати захисні заходи під нові виклики.

У сучасному світі багато підприємств мають інформаційні системи, які зберігають інформацію і використовуються для виконання основних бізнес-процесів. Однак більшість з цих систем не завжди оснащені достатньо надійними механізмами захисту. Відсутність централізованого підходу до забезпечення безпеки інформації часто призводить до численних проблем: від несанкціонованого доступу до даних до їх знищення в результаті атак ззовні чи зсередини. Системи, що використовуються в організаціях, можуть мати різні вразливості, які не завжди помітні на перший погляд [20].

Оцінка поточного стану захищеності підприємства показує, що наявні методи захисту, хоч і є ефективними для деяких типів загроз, не можуть гарантувати всебічний захист від сучасних кіберзагроз. Багато організацій застосовують фрагментарні заходи безпеки, наприклад, антивірусні програми чи фаєрволи, але ці інструменти не завжди можуть захистити від більш складних атак, таких як фішинг, шкідливі програми, зловмисний внутрішній доступ або навіть атаки на рівні фізичної інфраструктури.

Іншою проблемою є недостатня інтеграція різних систем безпеки. Це може призводити до "дір" у захисті, коли окремі заходи не враховуються в загальній стратегії. Така ситуація вимагає впровадження комплексного підходу до захисту

інформації, який дозволяє враховувати всі можливі загрози та ефективно протидіяти їм.

Аналіз поточного стану захищеності показує необхідність створення КСЗІ для підприємства. Без централізованого, багаторівневого захисту інформації організація може стати вразливою до численних сучасних загроз. Варто створити систему, яка інтегрує різні методи захисту та забезпечує ефективне управління безпекою, враховуючи всі аспекти інформаційної безпеки: від кіберзагроз до фізичного доступу до даних. КСЗІ дозволить підприємству не лише забезпечити захист даних, але й знизити ймовірність кіберінцидентів, зберегти конфіденційність, цілісність та доступність інформації.

Комплексна система захисту інформації (КСЗІ) є ключовим елементом стратегічної політики безпеки на підприємстві. Її основне завдання полягає в забезпеченні цілісності, конфіденційності та доступності інформаційних ресурсів підприємства, захисті від несанкціонованого доступу, витоку даних та кіберзагроз. Оскільки КСЗІ має бути здатною ефективно працювати в умовах різноманітних загроз, до її створення висуваються специфічні вимоги. Визначення цих вимог є основою для формування стратегії та розробки заходів для забезпечення належного рівня захисту інформаційних активів [20].

Основними вимогами до КСЗІ є надійність, гнучкість, масштабованість і можливість інтеграції з іншими системами безпеки, що існують в організації. Крім того, варто враховувати специфіку діяльності підприємства, типи інформаційних активів, що потребують захисту, а також можливі загрози, які можуть виникнути внаслідок зовнішніх чи внутрішніх впливів. Розробка вимог до КСЗІ базується на таких аспектах, як рівень безпеки, технології захисту даних, управління доступом, моніторинг та аналіз інцидентів.

Для забезпечення комплексного підходу до безпеки необхідно встановити чіткі вимоги до архітектури системи, визначити роль кожного елементу в процесі захисту, а також організувати механізми реагування на інциденти безпеки.

Таблиця 2.3 - Вимоги до КСЗІ

Категорія	Вимоги
Надійність	Система повинна забезпечувати безперервну роботу без збоїв, а також стійкість до відмов компонентів та атак, включаючи відмови в мережевих з'єднаннях, захист від вірусів, а також відновлення після можливих атак.
Конфіденційність	Інформація має бути захищена від несанкціонованого доступу. Необхідно впровадити шифрування даних, використання криптографічних технологій для захисту інформації під час передачі і зберігання. Обмеження доступу до інформації повинно здійснюватися на основі принципу мінімальних прав.
Цілісність	Система повинна гарантувати збереження цілісності інформації, тобто захистити дані від їх несанкціонованих змін або знищення. Це передбачає використання механізмів перевірки цілісності даних та контроль доступу до систем.
Доступність	Інформація повинна бути доступною для авторизованих користувачів в будь-який час. Включає в себе розробку заходів для запобігання відмовам у роботі системи, атак типу DDoS та забезпечення аварійного відновлення після інцидентів.
Масштабованість	Система повинна бути здатна до розширення для охоплення зростаючих потреб підприємства без значних втрат у функціональності або безпеці. Варто передбачити можливість інтеграції з іншими інформаційними системами та платформами, що використовуються на підприємстві.
Інтеграція	КСЗІ повинна бути інтегрована з іншими існуючими системами безпеки (антивірусами, фаєрволами, системами управління інцидентами та моніторингу). Це дозволить створити єдину екосистему для управління інформаційною безпекою на підприємстві.
Аудит і моніторинг	Необхідно організувати механізм постійного моніторингу і аудиту роботи системи для виявлення потенційних загроз. Система повинна реєструвати всі дії, що можуть мати вплив на інформаційну безпеку, і бути здатною до проведення аналізу виявлених інцидентів.
Управління доступом	Для запобігання несанкціонованому доступу, необхідно впровадити систему управління доступом (автентифікація, авторизація, обмеження прав доступу, багатофакторна автентифікація). Необхідно, щоб доступ до інформації отримували тільки уповноважені користувачі.

Продовження таблиці 2.3

Інцидент-менеджмент	Система повинна мати чітко визначену стратегію для реагування на інциденти безпеки, включаючи ідентифікацію, аналіз та ліквідацію загроз, а також відновлення роботи системи після інциденту.
Навчання та підвищення обізнаності	Необхідно постійно проводити навчання для персоналу щодо основних аспектів інформаційної безпеки. Всі користувачі повинні бути обізнані щодо політик доступу, правила поведінки в разі підозри на інцидент або атаки, а також щодо використання системи захисту.

Розробка вимог до КСЗІ є невід'ємною частиною процесу забезпечення інформаційної безпеки підприємства. Визначення чітких і обґрунтованих вимог дозволяє створити систему, яка відповідатиме потребам підприємства, ефективно захищатиме інформацію та буде гнучкою для адаптації до нових загроз. Ключовими вимогами є забезпечення надійності, конфіденційності, цілісності та доступності даних, а також інтеграція з іншими системами безпеки, що сприяє підвищенню рівня захисту від потенційних загроз.

Клас АС визначає рівень вимог до захисту інформації, технічних характеристик та організаційних аспектів її функціонування. Вибір правильного класу є важливим для забезпечення належної захищеності системи, її відповідності вимогам підприємства та здатності адекватно реагувати на існуючі загрози [21].

При виборі класу автоматизованої системи необхідно враховувати різноманітні фактори, зокрема специфіку діяльності підприємства, рівень загроз, вимоги до обробки та зберігання даних, а також можливості системи щодо забезпечення безпеки в режимі реального часу. Врахування цих факторів дозволяє сформулювати чіткі вимоги до КСЗІ, яка буде впроваджена на підприємстві.

Таблиця 2.4 - Вибір класу автоматизованої системи

Клас АС	Опис
Клас 1	Цей клас підходить для автоматизованих систем з низькими вимогами до рівня захисту інформації. АС класу 1 часто використовуються для обробки незначної інформації або в умовах, де загрози досягнення значного шкоди від витоку чи знищення даних є мінімальними. Необхідно мінімальне застосування засобів криптографії та автентифікації.
Клас 2	Клас 2 передбачає середній рівень захисту. АС цього класу використовуються для обробки більш чутливої інформації, де можливі наслідки загрози можуть бути суттєвими, але не катастрофічними. У системах класу 2 повинні бути впроваджені базові методи захисту, такі як шифрування даних та автентифікація користувачів.
Клас 3	АС класу 3 є найбільш підходящими для обробки даних або для виконання функцій, де порушення безпеки може призвести до значних втрат для підприємства чи організації. Ці системи потребують високого рівня захисту, включаючи багатофакторну автентифікацію, криптографію високого рівня та регулярний моніторинг безпеки.
Клас 4	АС класу 4 застосовуються в умовах максимально високих вимог до безпеки, зокрема для обробки найчутливішої інформації або для систем, де потенційні загрози можуть завдати незворотних або катастрофічних наслідків для підприємства. Це можуть бути системи для оборонної промисловості, фінансових установ або інфраструктур.

Визначення класу повинно базуватись на рівні чутливості оброблюваної інформації, потенційних загрозах та вимогах до захисту. Клас АС визначає необхідний рівень криптографії, автентифікації та інших технічних заходів безпеки, що дозволяють забезпечити належний захист від можливих атак і зловживань.

РОЗДІЛ 3. РОЗРОБКА ЕЛЕМЕНТІВ КСЗІ ДЛЯ ПІДПРИЄМСТВА

3.1. Організаційні заходи

Політика інформаційної безпеки (ПІБ) є стратегічним документом, що визначає основні принципи, вимоги та підходи до забезпечення безпеки інформації на підприємстві. Вона є ключовим елементом системи управління інформаційною безпекою (СУІБ) та визначає рамки для захисту конфіденційної, цілісної та доступної інформації в організації. Розробка ПІБ повинна враховувати специфіку діяльності підприємства, характер оброблюваної інформації, рівень потенційних загроз, а також нормативні вимоги та міжнародні стандарти з інформаційної безпеки [22].

Основною метою політики інформаційної безпеки є створення такого середовища, яке забезпечить належний рівень захисту інформаційних активів підприємства, мінімізуючи ризики від внутрішніх та зовнішніх загроз. Розробка ПІБ включає аналіз поточного стану безпеки, визначення вимог до захисту інформації, а також формулювання конкретних заходів щодо її забезпечення.

Таблиця 3.1 - Основні складові політики інформаційної безпеки

Складова	Опис
Цілі та завдання ПІБ	Визначаються основні цілі політики, що включають захист інформаційних активів підприємства, забезпечення безпеки даних, гарантування доступності, конфіденційності та цілісності інформації.
Оцінка загроз	Аналізуються потенційні загрози для інформаційної безпеки, як з боку внутрішніх, так і зовнішніх факторів. Визначаються найбільші загрози та відповідні заходи їх мінімізації.
Правила доступу	Визначаються правила доступу до інформаційних систем та ресурсів. Це включає впровадження багатофакторної автентифікації, обмеження прав доступу залежно від ролей користувачів та впровадження політики мінімальних привілеїв.

Продовження таблиці 3.1

Захист даних	Описуються заходи щодо захисту інформації, зокрема використання криптографії, шифрування даних, а також методи захисту при передачі інформації через мережі (VPN, SSL/TLS тощо).
Аудит і моніторинг	Визначається порядок проведення аудиту та моніторингу інформаційних систем для виявлення можливих порушень політики та вчасного реагування на інциденти безпеки. Це також включає звітність про інциденти та їх аналіз.
Навчання та підвищення кваліфікації	Описуються програми навчання для співробітників з питань інформаційної безпеки, щоб забезпечити їх обізнаність з основними загрозами та правильним використанням інформаційних ресурсів.
Відповідальність і санкції	Визначаються відповідальність за порушення політики інформаційної безпеки, а також санкції для порушників. Це може включати дисциплінарні заходи або юридичні наслідки у разі серйозних порушень.

Розробка політики інформаційної безпеки має на меті забезпечення надійного та ефективного захисту інформаційних активів підприємства. ПІБ повинна охоплювати всі аспекти, що стосуються безпеки, від оцінки загроз до конкретних дій для мінімізації ризиків. Визначення чітких правил доступу до інформаційних ресурсів, а також впровадження сучасних методів захисту даних, таких як шифрування та моніторинг, є потрібним.

Система аудиту та моніторингу забезпечує постійне спостереження за станом інформаційної безпеки, що дозволяє оперативно реагувати на можливі загрози або інциденти. Навчання співробітників допомагає підвищити рівень обізнаності та відповідальності за дотримання вимог безпеки. Усі ці елементи повинні бути чітко прописані в політиці інформаційної безпеки.

Політика повинна бути гнучкою і адаптованою до змінюваних загроз та вимог законодавства. Успішне впровадження ПІБ дозволяє створити систему, яка знижує ризики від можливих загроз, забезпечує захист конфіденційної інформації та підтримує безперервність бізнес-процесів підприємства [22].

Створення служби захисту інформації (СЗІ) є одним із найважливіших кроків для забезпечення надійного захисту інформаційних активів підприємства. У сучасному світі зростаючі загрози в кіберпросторі, а також вимоги до забезпечення конфіденційності та цілісності даних зумовлюють необхідність створення спеціалізованих підрозділів, які б мали достатні ресурси та повноваження для ефективного захисту інформаційних систем підприємства. Основним завданням такої служби є розробка, впровадження та підтримка заходів, які забезпечують належний рівень безпеки інформації на всіх етапах її обробки та зберігання.

Служба захисту інформації повинна працювати на принципах інтеграції безпеки в усі бізнес-процеси підприємства, відповідати вимогам законодавства, а також забезпечувати сталий розвиток захисту від нових та наявних загроз. Для цього СЗІ повинна складатися з кваліфікованих фахівців та використовувати сучасні технології захисту інформації.

Таблиця 3.2 - Основні функції служби захисту інформації

Функція	Опис
Розробка політики безпеки	Визначення основних принципів безпеки, створення документів, що регламентують політику безпеки інформації на підприємстві, зокрема політики доступу, обробки та зберігання даних.
Аналіз загроз і ризиків	Проведення регулярних оцінок загроз та вразливостей для інформаційних систем підприємства, визначення потенційних ризиків та заходів для їх мінімізації.
Моніторинг і аудит	Постійне відслідковування стану безпеки інформаційних систем, моніторинг доступу до ресурсів, здійснення регулярних перевірок систем безпеки та аудиту подій для виявлення порушень та інцидентів.
Захист даних і мереж	Забезпечення захисту інформації шляхом впровадження технологій шифрування, антивірусного захисту, фаєрволів, VPN-мереж, а також фізичного захисту від несанкціонованого доступу до інформаційних систем підприємства.

Продовження таблиці 3.2

Навчання та підвищення кваліфікації	Організація регулярних тренінгів і навчальних програм для співробітників підприємства з питань безпеки, підвищення обізнаності про загрози та правильне використання корпоративних систем захисту.
Виявлення та реагування на інциденти	Оперативне реагування на інциденти безпеки, аналіз можливих наслідків, вжиття заходів для локалізації та усунення загроз, відновлення систем після атак або збоїв.

Створення служби захисту інформації передбачає не лише технічні, але й організаційні заходи, що включають визначення чіткої структури служби, її повноважень та функцій. Першим кроком є розробка політики безпеки підприємства, яка визначає основні принципи та вимоги щодо захисту інформації. Служба повинна активно працювати над аналізом загроз і ризиків, проводити регулярні оцінки вразливостей та визначати можливі напрямки вдосконалення заходів безпеки. Вона також має відповідати за моніторинг інформаційних систем, забезпечення захисту даних та мереж, організацію навчальних заходів для персоналу, а також вчасне реагування на інциденти безпеки.

Іншою складовою є навчання співробітників, адже навіть найсучасніші технічні засоби не здатні забезпечити повний захист без належної підготовки персоналу. Тому постійне підвищення кваліфікації і усвідомлене ставлення до безпеки інформації є досить необхідним.

Створення служби захисту інформації є ключовим кроком у забезпеченні інформаційної безпеки на підприємстві. Вона має не лише технічні завдання, а й організаційні, які включають розробку політики безпеки, проведення оцінки загроз, організацію навчання та реагування на інциденти. Встановлення чітких функцій і завдань для служби дозволить підприємству ефективно захищати свої інформаційні активи, знижувати ризики від загроз та забезпечувати стабільну роботу усіх інформаційних систем [25].

Людський фактор часто є найбільш уразливою ланкою в системі захисту, тому навчання співробітників має бути системним, регулярним і охоплювати

різні аспекти безпеки. Урамках цього процесу необхідно, щоб кожен співробітник розумів свої обов'язки щодо захисту інформації, а також був готовий до реагування на потенційні загрози та інциденти. План навчання персоналу має бути інтегрований з політикою безпеки підприємства та враховувати специфіку його діяльності.

Таблиця 3.3 - Основні етапи навчання персоналу з інформаційної безпеки

Етап	Опис
1. Визначення цілей навчання	Формулювання основних цілей навчання, таких як підвищення обізнаності щодо загроз, освоєння основних принципів захисту інформації, усвідомлення значення безпеки для підприємства.
2. Розробка навчальної програми	Створення комплексної програми навчання, що включає як теоретичні знання про інформаційну безпеку, так і практичні навички для вирішення реальних ситуацій. Програма має бути адаптована під різні категорії співробітників.
3. Організація тренінгів	Проведення тренінгів, семінарів, вебінарів для співробітників, які охоплюють аспекти захисту інформації, методи реагування на інциденти та основи користування захищеними системами.
4. Оцінка ефективності навчання	Вимірювання ефективності навчання за допомогою тестів, опитувань або практичних завдань, що дозволяють оцінити рівень засвоєння матеріалу та готовність співробітників до реальних загроз.
5. Постійне вдосконалення	Регулярне оновлення програм навчання з урахуванням нових загроз, змін у технологіях та законодавстві. Проведення повторних тренінгів і підвищення кваліфікації співробітників на основі отриманих результатів.

Процес навчання персоналу з інформаційної безпеки починається з визначення цілей, які повинні бути спрямовані на підвищення загальної обізнаності щодо безпеки інформації, знайомство з можливими загрозами і вразливостями, а також освоєння основних заходів і процедур щодо захисту інформаційних активів. Метою є не лише підвищення рівня знань, але й розвиток навичок реагування на загрози, що виникають у реальних умовах.

Далі розробляється навчальна програма, яка повинна бути адаптована для різних груп співробітників в залежності від їх посадових обов’язків. Наприклад, для керівників необхідно акцентувати увагу на стратегічних аспектах безпеки та управлінні ризиками, а для технічних працівників – на засобах захисту інформаційних систем та методах виявлення загроз [25].

Основними етапами навчання є тренінги та семінари, де співробітники можуть не лише отримати теоретичні знання, але й пройти практичні заняття, такі як симуляції кібератак або сценарії реагування на інциденти. Такі тренінги мають бути інтерактивними та зручними для учасників, щоб максимально залучити їх до процесу навчання.

Для оцінки ефективності навчання проводяться тестування та інші методи оцінки знань, що дозволяють з'ясувати, наскільки співробітники засвоїли матеріал. Значеннєвим є також періодичне оновлення навчальних програм для того, щоб вони відповідали актуальним вимогам і загрозам [24].

План навчання персоналу є компонентом стратегії забезпечення інформаційної безпеки підприємства. Ретельно продумане навчання дозволяє знизити ймовірність помилок з боку співробітників, підвищити рівень обізнаності та готовності до реагування на загрози, що значно знижує загальний рівень ризиків для підприємства. Регулярні тренінги, оновлені навчальні програми та ефективна оцінка результатів є ключовими елементами для підтримки високого рівня безпеки.

3.2. Технічні заходи

Система криптографічного захисту є основним елементом забезпечення конфіденційності, цілісності та аутентифікації інформації, яка передається або зберігається в системах обробки даних. Вона забезпечує надійний захист інформації від несанкціонованого доступу та змін шляхом використання криптографічних алгоритмів для шифрування, підпису та перевірки достовірності даних.

Криптографічний захист реалізується через використання алгоритмів симетричного та асиметричного шифрування, хеш-функцій, цифрових підписів та інших засобів для захисту інформаційних потоків. Симетричне шифрування використовує один ключ для шифрування та дешифрування даних, що забезпечує високу швидкість обробки даних, але потребує безпечного обміну ключами між сторонами. Асиметричне шифрування, в свою чергу, використовує пару ключів (публічний та приватний), що дозволяє забезпечити безпечний обмін інформацією навіть в умовах незахищених каналів зв'язку.

Основною метою використання криптографії є забезпечення конфіденційності переданої інформації, її цілісності, щоб вона не була змінена в процесі передачі, а також підтвердження її достовірності через механізми аутентифікації.

Криптографічний захист є складовою частиною загальної стратегії інформаційної безпеки, яка дозволяє запобігати несанкціонованому доступу до конфіденційних даних, їх модифікації або викраденню. Правильний вибір криптографічних методів та їх інтеграція в систему захисту підприємства дозволяють забезпечити надійний рівень безпеки в умовах сучасних загроз.

Система управління доступом (СУД) є механізмом, який дозволяє контролювати, хто, коли та які ресурси має доступ до інформації та інформаційних систем підприємства. Вона дозволяє організувати ефективний контроль над доступом до ресурсів, що допомагає мінімізувати ризики несанкціонованого доступу та витоків конфіденційної інформації [23].

Система управління доступом включає в себе визначення політик доступу, механізми аутентифікації та авторизації, а також моніторинг та аудит доступу до інформаційних ресурсів. Аутентифікація є процесом перевірки особи користувача, зазвичай через паролі, смарт-карти або біометричні дані. Авторизація ж визначає, чи має користувач право доступу до певних ресурсів на основі його ролі в організації або інших атрибутів.

Ще одним аспектом є реалізація принципу найменших привілеїв, при якому користувачі отримують лише ті права доступу, які необхідні для

виконання їхніх обов'язків. Це дозволяє значно зменшити ймовірність несанкціонованих дій та зловживань.

Система управління доступом є елементом захисту інформаційних ресурсів підприємства, оскільки без належного контролю доступу до даних та систем неможливо забезпечити достатній рівень інформаційної безпеки. Необхідною складовою є постійний моніторинг та коригування політик доступу відповідно до змін в організації [21].

Система захисту периметра мережі (Firewall) є першою лінією оборони для мережі підприємства, яка забезпечує захист від несанкціонованих вторгнень ззовні та обмежує доступ до внутрішніх мережевих ресурсів. Система реалізує політику безпеки шляхом фільтрації мережевого трафіку, що дозволяє контролювати з’єднання з іншими мережами або інтернетом.

Механізм роботи системи захисту периметра полягає в фільтрації мережевого трафіку на основі набору правил, що визначають, який трафік дозволяється, а який заблоковано. Система може бути побудована на основі різних технологій, таких як пакетні фільтри, проксі-сервери або інтелектуальні міжмережеві екрани нового покоління, що використовують методи аналізу контексту та поведінки трафіку.

Ці системи здатні блокувати доступ до конкретних адрес, портів або протоколів, а також проводити глибокий аналіз трафіку для виявлення шкідливих або аномальних дій. Захист периметра також включає в себе моніторинг та реагування на інциденти, що виникають у процесі роботи.

Система захисту периметра є необхідним компонентом для запобігання несанкціонованим спробам доступу до інформаційних ресурсів підприємства. Вона дозволяє захистити внутрішню мережу від зовнішніх загроз та зловмисних дій, мінімізуючи ризики інцидентів безпеки.

Система моніторингу та аудиту інформаційної безпеки підприємства включає в себе постійний моніторинг систем для виявлення несанкціонованої активності, а також здійснення аудиту для аналізу відповідності політикам безпеки та виявлення можливих вразливостей [15].

Основною метою системи моніторингу є збір і аналіз даних про всі операції, що відбуваються в інформаційній системі, в тому числі про спроби доступу, зміни даних і виявлення аномальної активності. Ці системи дозволяють своєчасно реагувати на загрози та інциденти безпеки, а також виконувати комплексну перевірку відповідності встановленим стандартам і політикам безпеки.

Система аудиту дозволяє зберігати детальні журнали подій, які можуть бути використані для відновлення картин інцидентів та перевірки дотримання стандартів безпеки. Вона також включає в себе механізми перевірки конфігурацій безпеки та оцінки вразливостей.

Система моніторингу та аудиту є частиною загальної стратегії управління інформаційною безпекою підприємства. Вона дозволяє своєчасно виявляти загрози, а також надавати необхідні дані для аналізу і прийняття рішень щодо підвищення рівня безпеки.

3.3. Документальне забезпечення КСЗІ

Технічне завдання (ТЗ) є етапом у процесі розробки будь-якого інформаційного або технологічного продукту. Воно визначає вимоги та критерії, яких повинна дотримуватись розробка для досягнення необхідного результату. Технічне завдання складається на основі загальних цілей проекту і включає в себе деталізовану інформацію щодо функціональних та нефункціональних вимог, а також ресурсних, технічних та юридичних аспектів. «додаток Б»

Метою ТЗ є чітке формулювання вимог, що дозволяють однозначно оцінити та оцінювати готовність розробленої системи до експлуатації, а також визначити обсяг робіт та ресурси, необхідні для їх виконання. У контексті створення систем захисту інформації або інформаційних систем, ТЗ має включати вимоги щодо безпеки, продуктивності, масштабованості, зручності в експлуатації і взаємодії з іншими системами [19].

У технічному завданні для інформаційної системи мають бути вказані такі аспекти [21]:

1. Визначення основної мети розробки системи, зокрема щодо захисту інформації, підтримки цілісності та конфіденційності даних, покращення ефективності бізнес-процесів тощо.
2. Детальні описи функцій, які має виконувати система. Це включає опис необхідних процесів і процедур, автоматизацію задач, а також вимоги до інтерфейсів та взаємодії з іншими системами.
3. Вимоги до продуктивності, безпеки, надійності, масштабованості та доступності системи. Ці аспекти дуже потрібні для забезпечення стійкості та ефективності роботи інформаційних систем.
4. Деталі, що стосуються апаратного і програмного забезпечення, архітектури системи, обмежень на інфраструктуру, вимог до платформи або середовища, у якому буде працювати система.
5. Опис криптографічних, мережевих та операційних заходів, спрямованих на захист даних від несанкціонованого доступу, витоків або атак. Це також включає в себе механізми аутентифікації, авторизації, захисту периметра та моніторингу.
6. Чітке визначення вимог до інтерфейсів з іншими системами або користувачами. Це може включати в себе визначення API, стандарти обміну даними, а також специфікації інтерфейсів для користувачів.
7. Чітко визначений графік виконання проекту, ключові етапи та бюджет, необхідний для виконання робіт.

Технічне завдання є основою для успішної реалізації проекту, адже воно не лише визначає технічні вимоги, але й встановлює чітке розуміння того, що має бути розроблено. Деталізація вимог у ТЗ дозволяє ефективно планувати ресурси, час та інші аспекти, що є необхідними для досягнення поставлених цілей. Крім того, ТЗ служить як основа для оцінки виконання робіт і якості готової системи, що, в свою чергу, допомагає забезпечити необхідний рівень захисту та безпеки інформаційних ресурсів. «додаток В»

План захисту інформації — це документ, який описує стратегії, засоби та заходи, спрямовані на забезпечення безпеки інформації в організації. Він має на меті зменшення ризиків, пов’язаних з витоками або втратами даних, а також забезпечення конфіденційності, цілісності та доступності інформації на всіх етапах її обробки. План базується на принципах управління ризиками, що дозволяє мінімізувати загрози та вразливості.

Враховуючи значення інформаційних активів для успішної діяльності підприємства, необхідно розробити план, що забезпечує надійний захист від внутрішніх і зовнішніх загроз. Для цього варто врахувати не тільки технічні рішення, але й організаційні та юридичні аспекти, що впливають на безпеку.

План захисту інформації включає в себе кілька основних компонентів. Перше, що необхідно зробити для створення плану захисту — це провести ретельний аналіз потенційних загроз і вразливостей у системі. Необхідно визначити, які саме дані та ресурси потребують захисту, а також визначити можливі джерела ризиків. Це може включати технічні загрози (наприклад, віруси або хакерські атаки), організаційні загрози (неправомірний доступ працівників) або природні катастрофи (пожежі, затоплення) [24].

Варто ідентифікувати активи, які мають найбільшу цінність для підприємства та є необхідними для його функціонування. Це можуть бути бази даних, фінансові документи, стратегічні плани або інтелектуальна власність. Після визначення таких активів, потрібно встановити рівень їх захисту та головні засоби безпеки для їх збереження.

План повинен визначати політику доступу до інформаційних ресурсів, механізми аутентифікації та авторизації, а також рівні доступу для різних категорій користувачів. Включає в себе використання паролів, біометричних даних, ключів доступу, двофакторної аутентифікації та інших технологій для обмеження несанкціонованого доступу.

Необхідно визначити, які технічні засоби будуть використовуватись для захисту інформації. Це можуть бути криптографічні засоби, системи виявлення вторгнень (IDS), брандмауери, антивірусні програми та інші інструменти, які

допомагають захистити дані від атак, несанкціонованого доступу або пошкодження. Варто встановити чіткі політики і процедури щодо обробки та зберігання інформації. Це включає визначення стандартів щодо збереження та передачі даних, а також правила для роботи з мобільними пристроями, системами резервного копіювання та відновлення даних.

Для забезпечення ефективного захисту необхідно впровадити систему моніторингу і аудиту, що дозволяє здійснювати постійний контроль за станом безпеки. Це включає регулярні перевірки доступу, виявлення потенційних вразливостей, а також аналіз подій безпеки. Не менш необхідним є навчання співробітників, яке дозволяє підвищити рівень обізнаності з питань інформаційної безпеки. Систематичне проведення тренінгів та навчальних програм допомагає уникнути людських помилок, які можуть призвести до порушення безпеки.

Потрібно розробити чіткий план дій на випадок інцидентів безпеки. Це включає процедури для реагування на атаки, витоки даних, втрати інформації або порушення конфіденційності. Варто також мати план відновлення після катастроф, який забезпечить мінімальний час відновлення діяльності підприємства після інциденту.

Захист інформації є ключовим аспектом для будь-якої організації, що працює з необхідними або чутливими даними. Розробка ефективного плану захисту допомагає не тільки знизити ризики, але й забезпечити безперервність бізнес-процесів, зберегти репутацію та довіру клієнтів. Важливо, щоб план був не лише детальним і всебічним, але й постійно актуалізувався, щоб відповідати новим загрозам і технологіям [24].

Акти категоріювання інформації — це певний етап у системі управління інформаційною безпекою, що полягає в класифікації інформаційних активів за рівнями конфіденційності, значення та ризику, що стосуються їхнього використання, обробки та зберігання. Цей процес допомагає визначити необхідні заходи захисту для кожного виду інформації в залежності від її категорії. Категоріювання є необхідним для ефективної реалізації політики інформаційної

безпеки, оскільки дозволяє організувати захист інформації на всіх етапах її життєвого циклу, враховуючи специфіку даних та вимоги до їхнього захисту. «додаток В»

Акти категоріювання включають в себе визначення рівнів доступу, визначення умов для надання доступу до різних типів інформації, а також визначення засобів, необхідних для забезпечення належного захисту. Це дозволяє визначити, яка інформація є критичною для організації та потребує найвищого рівня захисту, а яка — може бути оброблятися з меншими обмеженнями [26].

Таблиця 3.4 - Акти категоріювання

Категорія інформації	Опис	Заходи захисту	Рівень доступу
Конфіденційна	Інформація, доступ до якої обмежений, її розкриття може призвести до серйозних наслідків.	Криптографічний захист, контроль доступу, обмеження передачі, регулярний моніторинг.	Доступ лише авторизованих осіб.
Інтернал	Внутрішня інформація, доступна тільки для працівників організації.	Обмежений доступ на основі ролей, захист за допомогою паролів та двофакторної аутентифікації.	Доступ обмежений для внутрішніх працівників.
Публічна	Інформація, що може бути вільно доступною для зовнішніх осіб, але все ж потребує контролю.	Моніторинг використання та доступу, мінімальний захист для забезпечення цілісності.	Вільний доступ для громадськості.
Сенситивна	Інформація, яка має бути захищена, але її розкриття не є критичним для організації.	Поглиблений контроль доступу, використання захищених каналів зв’язку.	Обмежений доступ для конкретних осіб або груп.

Акти категоріювання дозволяють класифікувати інформацію за рівнями значення та конфіденційності, що допомагає організації ефективно захищати її ресурси. Категорії інформації визначаються на основі значення для діяльності організації, ймовірності негативних наслідків у разі її порушення, а також необхідності її захисту. Після категоріювання встановлюються конкретні вимоги до захисту кожної категорії інформації, що включають механізми обмеження доступу, засоби криптографії та інші інструменти для забезпечення належної безпеки.

Акти категоріювання допомагають чітко визначити значення інформаційних активів і в залежності від цього впроваджувати необхідні заходи захисту. Правильне категоріювання дає змогу забезпечити належний рівень безпеки для кожного виду інформації та дозволяє організації ефективно керувати ризиками, пов'язаними з її використанням. В результаті створюється баланс між рівнем доступу до інформації та її захистом, що потрібно для сталого функціонування підприємства та запобігання можливим загрозам.

Модель загроз та порушника є інструментом для розуміння потенційних загроз для інформаційної безпеки організації. «додаток Д» Вона описує, які види атак чи порушень можуть бути здійснені, хто може бути відповідальним за ці дії (так звані порушники), а також якими методами і засобами вони можуть здійснювати свої дії. Розробка моделі загроз дозволяє організаціям визначити уразливості в своїх інформаційних системах і на їх основі побудувати ефективні стратегії захисту. Крім того, розуміння типів порушників і їх можливих дій дозволяє адаптувати систему безпеки для протидії конкретним загрозам [24].

Модель загроз включає аналіз можливих атак, вивчення характеристик порушників (наприклад, їхні мотивації, рівень кваліфікації, ресурси), а також оцінку наслідків таких атак для організації. Моделювання загроз є складовою процесу управління ризиками, оскільки дозволяє передбачити й оцінити ймовірність реалізації загроз і розробити відповідні заходи для їх запобігання.

Таблиця 3.5 - Модель загроз

Тип загрози	Опис загрози	Методи атаки	Можливий порушник
Атака через зовнішніх хакерів	Зовнішні хакери можуть використовувати вразливості в мережах і системах підприємства для незаконного доступу.	Фішинг, експлойти в ПЗ, атаки на периметр мережі, DDoS.	Незаконні хакери, зловмисники з метою крадіжки даних чи витрат.
Атака через внутрішніх осіб	Працівники або колишні співробітники можуть мати доступ до конфіденційної інформації та зловживати ним.	Несанкціоноване використання доступу, крадіжка даних, саботаж.	Співробітники або колишні співробітники організації.
Атака через фізичний доступ	Порушник може фізично доступити пристрої організації, щоб отримати дані або змінити налаштування системи.	Використання несанкціонованого доступу до комп'ютерної техніки.	Вандали, злочинці або несанкціоновані відвідувачі.
Атака через уразливості ПЗ	Атака, яка спричинена використанням вразливостей в програмному забезпеченні, що має доступ до систем.	Використання відомих уразливостей у ПЗ для атаки.	Хакери, зловмисники, що використовують автоматизовані інструменти.
Атака через соціальну інженерію	Вплив на людей для того, щоб отримати доступ до конфіденційної інформації, наприклад, через фішинг.	Обман, маніпуляція або використання психологічних методів для здобуття довіри.	Соціальні інженери, шахраї.

Модель загроз дозволяє систематизувати можливі сценарії атак, враховуючи їх характеристики та потенційних порушників. Кожна загроза має свій метод атаки, і вона може бути здійснена конкретними групами осіб або навіть автоматизованими системами. Наприклад, зовнішні хакери можуть використовувати фішинг або DDoS-атаки, щоб вивести з ладу сервери компанії, або знайти уразливості в програмному забезпеченні. У той же час, внутрішні працівники, маючи доступ до чутливих даних, можуть стати причиною витоку інформації або навіть її модифікації.

Розуміння загроз і типів порушників є ключовим для формування стратегії захисту. Наприклад, атака через соціальну інженерію потребує впровадження навчальних програм для співробітників, що дозволяють розпізнати фішинг чи інші методи маніпуляцій. З іншого боку, атаки через уразливості програмного забезпечення вимагають регулярних оновлень і патчів для усунення можливих вразливостей [26].

Модель загроз та порушників є інструментом для планування та реалізації заходів інформаційної безпеки. Вона дає змогу ідентифікувати найімовірніші загрози, оцінити потенційний вплив порушників і розробити відповідні контрзаходи. Це допомагає ефективно управляти ризиками, підвищувати рівень захисту інформації та забезпечити безпеку системи на всіх етапах її експлуатації.

3.4. Рекомендації щодо впровадження та атестації КСЗІ

План впровадження системи захисту інформації є комплексним документом, що містить всі етапи, методи і терміни реалізації заходів, спрямованих на забезпечення інформаційної безпеки організації. Цей план охоплює як організаційні, так і технічні аспекти, включаючи інфраструктуру, політики, процедурні зміни та навчання персоналу. Впровадження ефективної системи захисту інформації передбачає не тільки використання сучасних технологій, але й забезпечення безпеки на рівні процесів, людей та фізичної безпеки.

План впровадження допомагає організації сформулювати чіткі кроки для захисту від різноманітних загроз і вразливостей, а також визначити терміни, ресурси та відповідальних осіб для кожного етапу реалізації. Важливою частиною такого плану є моніторинг прогресу впровадження та коригування заходів відповідно до нових загроз або змін в організаційних цілях.

Таблиця 3.6 - План впровадження системи захисту інформації

Етап впровадження	Опис заходу	Терміни	Відповідальні особи	Ресурси
Оцінка поточного стану	Аналіз існуючої ситуації в організації, виявлення уразливостей та оцінка потреб у захисті інформації.	1 місяць	IT-спеціалісти, аналітики	Засоби моніторингу, аудити
Розробка стратегії захисту	Визначення основних принципів і напрямків політики захисту інформації в організації.	2 тижні	Директор з IT, керівник безпеки	Партнери з консалтингу
Вибір та закупівля засобів захисту	Вибір відповідних технологічних рішень (антивірусне ПЗ, міжмережеві екрани, системи управління доступом).	3 тижні	IT-відділ, закупівельна комісія	Бюджет на технології
Розробка політик безпеки	Створення та впровадження політик безпеки для всіх рівнів доступу та використання корпоративних даних.	1 місяць	Керівник безпеки, юрист	Зразки політик, консультації

Продовження таблиці 3.6

Впровадження навчання персоналу	Проведення тренінгів для співробітників щодо основ інформаційної безпеки та специфічних вимог організації.	2 місяці	HR-відділ, тренери	Навчальні матеріали, платформи
Тестування та моніторинг	Перевірка ефективності заходів на реальних даних, моніторинг роботи систем безпеки.	1 місяць	IT-відділ, аудитори	Тестові середовища, моніторинг
Оцінка та коригування заходів	Перегляд результатів тестування, коригування стратегії та заходів у разі виявлення нових загроз.	1 місяць	Керівник безпеки, IT-менеджер	Інструменти аудиту та аналізу

Розробка та впровадження плану інформаційної безпеки передбачає кілька етапів, кожен з яких має своє значення в загальній стратегії. Початковий етап полягає в оцінці поточного стану інформаційної безпеки, що дозволяє зрозуміти, які саме вразливості присутні в організації. Це може включати в себе аналіз існуючих технологічних рішень, огляд політик та процедур, а також інтерв'ю з персоналом, щоб виявити потенційні слабкі місця.

На наступному етапі розробляється стратегія захисту інформації, що включає основні напрями дій і визначення принципів, за якими буде організовано захист. Це може включати вибір між різними типами систем захисту, від антивірусного ПЗ до більш складних систем управління доступом та міжмережевими екранами [28].

Вибір та закупівля засобів захисту є ключовим етапом, на якому проводиться порівняння рішень, що відповідають вимогам організації, з

урахуванням бюджету та потреб у безпеці. Розробка політик безпеки дозволяє чітко визначити правила використання інформаційних систем, доступу до даних та організації роботи співробітників, щоб забезпечити максимальний рівень безпеки. «додаток Е»

Навчання персоналу є важливим етапом, оскільки навіть найкращі технологічні рішення не будуть ефективними, якщо співробітники не будуть знати, як правильно ними користуватися. Це включає в себе тренінги, семінари та інші заходи, що сприяють підвищенню рівня обізнаності.

Тестування та моніторинг дозволяють переконатися, що всі заходи безпеки працюють належним чином, а також виявити потенційні недоліки. Якщо під час тестування виявлено слабкі місця, необхідно коригувати стратегію захисту.

План впровадження системи інформаційної безпеки є комплексним і багатогранним процесом, що включає не лише закупівлю технологій, а й розробку політик, навчання персоналу та регулярний моніторинг системи безпеки. Кожен етап є потрібним для забезпечення надійного захисту даних і інформаційних ресурсів організації. Завдяки детальному плануванню та впровадженню всіх необхідних заходів можна знизити ризики витоків даних, зламів та інших загроз інформаційній безпеці організації.

Процедура атестації системи захисту інформації (СЗІ) є необхідною для підтвердження відповідності технічних і організаційних заходів вимогам безпеки інформації в організації. Атестація дозволяє оцінити ефективність існуючих заходів з захисту інформації, а також визначити їх відповідність встановленим стандартам, нормативним вимогам і внутрішнім політикам. Процес атестації також допомагає виявити слабкі місця в системах безпеки та запропонувати заходи для їх усунення [28].

Атестація проводиться на регулярній основі для того, щоб переконатися, що система захисту продовжує працювати належним чином і відповідає змінним вимогам або новим загрозам. Оскільки загрози та вразливості постійно еволюціонують, варто регулярно перевіряти і підтверджувати ефективність заходів захисту.

Таблиця 3.7 - Процедура атестації системи захисту інформації

Етап атестації	Опис заходу	Терміни	Відповідальні особи	Ресурси
Оцінка поточного стану безпеки	Аналіз існуючої системи захисту інформації та перевірка її відповідності вимогам безпеки.	1 місяць	IT-відділ, керівник безпеки	Аудиторські інструменти
Визначення критеріїв атестації	Формулювання чітких вимог і критеріїв, яким повинна відповідати система захисту інформації.	2 тижні	Керівник безпеки, юрист	Стандарти безпеки
Проведення аудиту СЗІ	Виконання технічного і організаційного аудиту для оцінки ефективності захисту.	2 місяці	Аудитори, IT-фахівці	Платформи для тестування
Підготовка звіту	Формулювання результатів аудиту, виявлення вразливостей і слабких місць, а також рекомендацій щодо вдосконалення.	1 місяць	Аудитори, керівник безпеки	Звіти, рекомендації
Оцінка результатів атестації	Оцінка відповідності результатів аудиту вимогам політики інформаційної безпеки.	1 тиждень	Керівник безпеки, директор IT	Інструменти для аналізу
Внесення коригувань	Реалізація змін і вдосконалень на основі результатів атестації та рекомендацій.	1-2 місяці	IT-відділ, персонал безпеки	Ресурси для модифікацій

Процедура атестації СЗІ зазвичай складається з кількох етапів. Спочатку проводиться оцінка поточного стану безпеки, що дозволяє отримати уявлення про наявність або відсутність уразливостей у поточній системі захисту. Цей етап включає перевірку всіх компонентів СЗІ, починаючи від технічних засобів, таких як програмне забезпечення для шифрування, до організаційних процедур, зокрема політик доступу і навчання персоналу.

Наступним кроком є визначення критеріїв атестації. Це потрібно для того, щоб чітко зрозуміти, яким вимогам повинна відповідати система для отримання атестату відповідності. Крім того, критерії атестації мають допомогти перевірити, наскільки захищеною є інформація в контексті загроз, що існують на даний момент.

Проведення аудиту є практичною частиною атестації, коли спеціалісти з безпеки використовують різні інструменти для тестування ефективності системи захисту. Це може включати сканування на наявність вразливостей, перевірку рівня шифрування, тестування захисту від несанкціонованого доступу та інші методи перевірки [27].

Після аудиту готується звіт, який містить результати перевірки, виявлені проблеми, а також рекомендації щодо удосконалення системи захисту інформації. Звіт є основою для прийняття рішень про те, що потрібно змінити чи вдосконалити для покращення рівня безпеки.

Оцінка результатів атестації дозволяє організації визначити, чи відповідає її система захисту інформації вимогам нормативних документів і внутрішнім політикам. Це також допомагає розуміти, які саме аспекти потребують вдосконалення або додаткових заходів.

Внесення коригувань після атестації є певним етапом для реалізації змін на основі виявлених слабких місць. Це може включати модернізацію програмного забезпечення, зміни в організаційних процесах або додаткові тренінги для персоналу.

Атестація системи захисту інформації є необхідною для забезпечення належного рівня безпеки в організації. Вона допомагає виявити слабкі місця в

існуючій системі, що дозволяє своєчасно вжити заходів для їх усунення. Крім того, атестація сприяє покращенню відповідності нормативним вимогам, стандартам безпеки та внутрішнім політикам, що забезпечує надійний захист інформаційних ресурсів організації від зовнішніх і внутрішніх загроз.

Оцінка ефективності системи захисту інформації (СЗІ) є частиною управління інформаційною безпекою в організації. Це дозволяє визначити, наскільки добре реалізовані заходи з захисту інформації виконують свої функції, і чи відповідають вони вимогам безпеки в умовах постійно змінюваного середовища загроз. Оцінка ефективності повинна проводитися на регулярній основі, щоб забезпечити відповідність до стандартів і забезпечити стійкість організації перед новими загрозами.

Оцінка ефективності може включати в себе аналіз результатів впровадження заходів захисту, перевірку їх здатності зберігати конфіденційність, доступність і цілісність даних, а також виявлення можливих слабких місць у системі захисту.

Підтримка та модернізація СЗІ є аспектами для забезпечення безпеки інформаційних систем, оскільки загрози, технології та вимоги до захисту постійно змінюються. Ось чому регулярна адаптація і вдосконалення заходів захисту є необхідними для збереження належного рівня безпеки [24].

Таблиця 3.8 – Деталі проведення заходів

Етап	Опис заходу	Терміни	Відповідальні особи	Ресурси
Оцінка поточної ефективності	Проведення аналізу рівня захисту інформації на основі існуючих інструментів та методів.	1 місяць	ІТ-відділ, керівник безпеки	Інструменти моніторингу та тестування

Продовження таблиці 3.8

Визначення недоліків	Виявлення вразливостей і слабких місць, які можуть впливати на ефективність системи захисту.	2 тижні	Керівник безпеки, аудитори	Звіти про вразливості
Оцінка відповідності вимогам	Перевірка того, чи відповідає система захисту актуальним вимогам та стандартам безпеки.	2 тижні	ІТ-відділ, аудитори	Вимоги стандартів безпеки
Рекомендації щодо модернізації	Формулювання заходів з вдосконалення системи захисту для усунення виявлених недоліків.	1 місяць	Керівник безпеки, ІТ-відділ	Ресурси для реалізації змін
Реалізація змін	Внесення коригувань до СЗІ відповідно до рекомендацій, модернізація та оновлення засобів захисту.	2-3 місяці	ІТ-відділ, персонал безпеки	Нові технології для захисту
Оцінка ефективності після змін	Перевірка результатів впровадження змін та вдосконалень, оцінка їх впливу на рівень безпеки.	1 місяць	Керівник безпеки, аудитори	Інструменти тестування

Оцінка ефективності системи захисту інформації має на меті визначити, чи відповідає вона вимогам безпеки, чи ефективно реалізуються заходи з захисту від зовнішніх та внутрішніх загроз, а також чи зберігається належний рівень цілісності, доступності та конфіденційності інформації. Цей етап включає в себе аналіз усіх елементів системи, таких як програмне забезпечення, апаратні засоби, мережеві елементи та організаційні заходи. Оцінка може проводитись за допомогою різних інструментів моніторингу та тестування, що дозволяє виявити слабкі місця у захисті інформаційних ресурсів [28].

Визначення недоліків є наступним етапом після оцінки ефективності. Тут проводиться більш детальний аналіз виявлених уразливостей та слабких місць, які можуть вплинути на безпеку системи. Це можуть бути вразливості в програмному забезпеченні, порушення процедур безпеки або недостатня кваліфікація персоналу.

Оцінка відповідності вимогам дозволяє визначити, чи відповідає існуюча система захисту актуальним нормативним вимогам і стандартам безпеки. Це також дозволяє виявити відхилення від політик і стандартів, що визначені організацією для забезпечення безпеки.

Рекомендації щодо модернізації спрямовані на вдосконалення системи захисту інформації. На основі аналізу ефективності та виявлених недоліків розробляються конкретні пропозиції щодо впровадження нових засобів захисту, оновлення старих технологій, а також зміни в організаційних процесах для підвищення рівня безпеки.

Реалізація змін є наступним етапом, на якому здійснюються необхідні вдосконалення системи захисту. Це може включати оновлення програмного забезпечення, впровадження нових інструментів криптографії або моніторингу, а також зміни в політиках доступу або тренінгах для персоналу.

Після реалізації змін проводиться нова оцінка ефективності, щоб перевірити, чи покращився рівень безпеки і чи відповідає система новим вимогам. Це допомагає переконатися, що впроваджені зміни мають позитивний вплив на рівень захисту інформації [29].

Оцінка ефективності та модернізація системи захисту інформації є безперервними процесами, які дозволяють підтримувати належний рівень безпеки в організації. Регулярне оновлення системи, відповідно до змін у загрозах і вимогах, є необхідним для запобігання потенційним загрозам і для забезпечення стійкості організації до нових викликів. Внесення коригувань і вдосконалень на основі регулярних оцінок ефективності допомагає підтримувати актуальність і надійність заходів захисту.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Охорона праці та безпека в надзвичайних ситуаціях є частиною забезпечення ефективної та безпечної роботи підприємства. Вона передбачає комплекс заходів, спрямованих на захист життя, здоров’я та працездатності працівників, а також на забезпечення належних умов для мінімізації ризиків у разі виникнення надзвичайних ситуацій (НС). В умовах постійно зростаючої складності робочих процесів та технічних систем, надзвичайно варто забезпечити не лише безпеку праці на підприємстві, але й здатність оперативно реагувати на можливі НС, зменшуючи їх наслідки для людей і навколишнього середовища [29].

Таблиця 4.1 - Охорона праці та безпека в надзвичайних ситуаціях

Етап	Опис заходу	Терміни	Відповідальні особи	Ресурси
Аналіз умов праці	Оцінка потенційних ризиків для здоров'я працівників та умов праці на кожному робочому місці.	1 місяць	Відділ охорони праці, керівники	Засоби захисту працівників
Розробка плану заходів з охорони праці	Розробка та затвердження комплексного плану заходів щодо забезпечення безпеки праці на підприємстві.	2 місяці	Керівник охорони праці	План, нормативні документи
Проведення навчань для працівників	Організація регулярних навчань щодо безпеки праці, інструктажів з використання засобів захисту.	1 місяць	Відділ охорони праці	Навчальні матеріали, тренажери

Продовження таблиці 4.1

Підготовка до надзвичайних ситуацій	Розробка інструкцій та планів щодо дій персоналу у разі виникнення НС, проведення тренувань та евакуацій.	3 місяці	Керівники підрозділів, відділ НС	План дій, обладнання для тренувань
Впровадження системи моніторингу	Встановлення системи моніторингу та аналізу ризиків для своєчасного виявлення потенційних небезпек.	2 місяці	ІТ-відділ, охорона праці	Програмне забезпечення, датчики
Аудит та оцінка ефективності заходів	Перевірка результативності впроваджених заходів щодо охорони праці та безпеки у надзвичайних ситуаціях.	6 місяців	Відділ охорони праці, аудитори	Звіти, інструменти аудиту

Оцінка умов праці є першим етапом у забезпеченні охорони праці. Це включає виявлення потенційно небезпечних факторів на робочих місцях, таких як шкідливі або небезпечні умови, що можуть загрожувати здоров'ю працівників. Аналіз проводиться за допомогою інструментів оцінки ризиків, інспекцій і медичних оглядів, які дозволяють виявити осередки можливих небезпек.

Розробка плану заходів з охорони праці передбачає створення документа, що регламентує всі аспекти охорони праці на підприємстві. Це включає заходи, спрямовані на усунення чи мінімізацію ризиків, а також створення норм і стандартів безпеки, необхідних для виконання робіт.

Працівники повинні бути обізнані з існуючими загрозами і відповідними заходами безпеки. Також варто проводити практичні заняття з використання

засобів індивідуального захисту, засобів першої допомоги, а також тренування на випадок надзвичайних ситуацій.

Підготовка до надзвичайних ситуацій включає розробку спеціальних планів дій у випадку виникнення надзвичайних ситуацій. Це включає евакуацію персоналу, забезпечення готовності спеціального обладнання, організацію тренувань для працівників, а також розробку інструкцій, що регламентують дії в умовах НС [25].

Моніторинг та система раннього попередження про потенційні загрози є необхідним для швидкої реакції на будь-які зміни, які можуть призвести до небезпеки. Встановлення відповідних датчиків і систем моніторингу дозволяє своєчасно виявляти небезпечні ситуації, що може запобігти їх розвитку або знизити шкоду від них.

Аудит та оцінка ефективності передбачає перевірку виконаних заходів і аналіз їх результативності. Це дозволяє виявити слабкі місця в системі охорони праці та безпеки в надзвичайних ситуаціях і оперативно їх усувати, покращуючи загальну ефективність управління безпекою на підприємстві.

Охорона праці та безпека в надзвичайних ситуаціях є необхідними складовими частинами забезпечення стабільної і безпечної роботи підприємства. Наявність добре розробленої і ефективно впровадженої системи охорони праці, а також наявність належних підготовчих заходів до надзвичайних ситуацій, дозволяють значно знизити ризики для життя і здоров’я працівників. Ретельна оцінка ефективності, регулярне навчання персоналу і своєчасне впровадження заходів на основі аналізу поточних загроз дозволяють оперативно реагувати на будь-які зміни у робочому середовищі і забезпечити належний рівень безпеки для всіх учасників процесу.

4.1 Охорона праці при роботі на персональному комп'ютері

Під час роботи на персональному комп'ютері важливо дотримуватись заходів безпеки, аби мінімізувати ризики для здоров'я, пов'язані з використанням електричних пристроїв та тривалою роботою за екраном.

Перед початком роботи необхідно переконатися в належному стані обладнання: кабелі повинні бути правильно підключені, а розетки — відповідати стандартам безпеки. Також потрібно перевірити наявність заземлення для запобігання ураженню електричним струмом.

Для комфортної роботи монітор має бути розташований на оптимальній відстані від очей, а рівень освітлення не повинен викликати відблисків або перенапруження зору. Це допоможе уникнути втоми очей і негативного впливу на зір.

Робоче місце повинно бути організовано так, щоб забезпечити правильну посадку та зручність. Стілець має бути з регулюванням висоти, а стіл — зручний для роботи, щоб не виникало напруження в руках або спині.

Важливо регулярно робити перерви для відпочинку. Рекомендується проводити вправи для очей і змінювати позу, щоб запобігти розвитку хронічних захворювань, пов’язаних з сидячою роботою.

По завершенні робочого дня комп'ютер та інші пристрої повинні бути вимкнені відповідно до інструкцій, а робоче місце — прибрано. Потрібно також проводити регулярне вологе прибирання для підтримки чистоти і гігієни.

У разі виявлення несправностей у роботі комп'ютера або інших пристроїв, необхідно терміново звернутися до відповідальних осіб або технічного спеціаліста для усунення проблем.

4.2. Безпека під час роботи на персональному комп'ютері .

1) Перевірка обладнання та робочого місця. Перед початком роботи важливо перевірити стан персонального комп'ютера. Усі кабелі повинні бути

надійно підключені до відповідних розеток, а пристрої — належним чином заземлені. Це дозволяє знизити ризик ураження електричним струмом та забезпечити стабільну роботу комп'ютера.

2) Налаштування монітора для зручності зору. Для комфортної роботи монітор повинен бути розташований на відстані 50-70 см від очей користувача, а верхній край екрану має бути на рівні очей або трохи нижче. Таке розташування зменшує навантаження на зір і знижує ризик розвитку дискомфорту в очах. Освітлення робочого простору має бути помірним, щоб уникнути відблисків на екрані.

3) Правильна поза при роботі за комп'ютером. Для комфортної роботи слід використовувати стілець, що має регульовану висоту, з підтримкою для спини. Положення рук на клавіатурі повинно бути таким, щоб зап’ястя були розслаблені і не зазнавали перенапруження. Стіл має бути на такій висоті, щоб користувач міг без зусиль дістатися до всіх елементів комп'ютера.

4) дійснення перерв для запобігання втоми. Регулярні перерви є важливою частиною безпеки. Рекомендується кожні 20 хвилин робити невелику паузу на 20 секунд, щоб відпочити очам і подивитися на об'єкт, що знаходиться на відстані 6 метрів. Це допомагає знизити ризик втоми очей і покращити концентрацію.

5) Захист від шкідливих програм. Для забезпечення безпеки важливо мати актуальне антивірусне програмне забезпечення, що захищає комп'ютер від шкідливих атак. Крім того, слід регулярно оновлювати програмне забезпечення та використовувати брандмауери для запобігання доступу зловмисників до комп'ютера через мережу.

6) Ергономіка робочого місця. Для зменшення навантаження на хребет і суглоби необхідно правильно налаштувати робоче місце. Важливо змінювати позу, сидячи за комп'ютером, а також використовувати спеціальні підставки для клавіатури та миші, що допомагають знизити навантаження на руки.

7) Захист особистої інформації. Для забезпечення безпеки особистих даних слід використовувати складні паролі, а також активувати двофакторну

автентифікацію, де це можливо. Всі важливі файли повинні бути зашифровані, і доступ до них потрібно обмежувати лише авторизованим користувачам.

8) Завершення робочого дня. Наприкінці робочого дня слід вимикати комп'ютер і відключати всі периферійні пристрої від мережі. Це не тільки зберігає енергоресурси, а й знижує ймовірність технічних несправностей, а також забезпечує більшу безпеку від несанкціонованого доступу.

ВИСНОВКИ

У ході дослідження проаналізовано нормативно-правову базу України у сфері захисту інформації, що включає законодавчі акти, постанови Кабінету Міністрів України (КМУ) та нормативні документи, які регулюють інформаційну безпеку в Україні. Зокрема, детально розглянуто основні закони, такі як Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», а також підзаконні акти, які визначають порядок створення та сертифікації КСЗІ. Особливу увагу приділено аналізу ролі державних органів у регулюванні інформаційної безпеки, таких як Державна служба спеціального зв’язку та захисту інформації України.

Окремо досліджено міжнародні стандарти, зокрема ISO 27001, які є ключовими для забезпечення відповідності української системи захисту інформації світовим стандартам. Порівняння положень цих стандартів із національними документами дозволило виявити напрями, які потребують удосконалення, такі як інтеграція кращих практик управління ризиками та впровадження інноваційних технологій.

Вивчено еволюцію систем захисту інформації в Україні, що дозволило зрозуміти зміни підходів до захисту даних на різних етапах розвитку країни: від перших нормативних актів у 1990-х роках до сучасних підходів, які включають використання криптографічного захисту та автоматизованих систем моніторингу загроз. Особливо підкреслено розвиток галузі в контексті зростання кіберзагроз та потреби в інтеграції міжнародного досвіду.

Проведено порівняльний аналіз українських систем захисту інформації з міжнародними стандартами, що дозволило ідентифікувати переваги та недоліки існуючих практик. Розглянуто, яким чином застосовуються міжнародні стандарти на рівні українських підприємств і організацій, зокрема в частині сертифікації КСЗІ, управління доступом до даних та моніторингу інцидентів інформаційної безпеки.

Здійснено оцінку інформаційної безпеки обраного державного підприємства. У рамках цієї оцінки визначено можливі загрози, такі як несанкціонований доступ, витік інформації, кібератаки, а також вразливості, викликані як технічними недоліками систем, так і організаційними прорахунками. Проведено аналіз ризиків із використанням сучасних методик, що дозволило сформувати базу для розробки відповідних заходів захисту.

Обґрунтовано необхідність створення Комплексної системи захисту інформації (КСЗІ) для підприємства. Розробка цієї системи враховує специфіку діяльності організації, рівень критичності оброблюваних даних, а також можливі сценарії загроз. Акцент зроблено на інтеграції комплексних заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації.

Розроблено основні елементи КСЗІ, які включають як технічні, так і організаційні заходи. Зокрема, створено політику інформаційної безпеки, яка враховує потреби підприємства у забезпеченні конфіденційності, цілісності та доступності даних. У політиці визначено механізми контролю доступу, класифікацію інформації, застосування криптографічних технологій, а також заходи з управління інцидентами безпеки.

Запропоновано створення організаційної структури, яка забезпечуватиме реалізацію заходів із захисту інформації. Ця структура включатиме службу інформаційної безпеки, яка відповідатиме за моніторинг, аудит, а також впровадження політики безпеки. Для забезпечення ефективності впроваджено розподіл обов’язків серед співробітників та визначено роль керівництва у підтримці системи.

Рекомендовано інтеграцію сучасних технічних засобів захисту, таких як системи управління доступом, засоби криптографічного захисту, системи моніторингу кіберзагроз та резервного копіювання. Впровадження таких засобів дозволить оперативно реагувати на інциденти, запобігати несанкціонованому доступу до даних та забезпечувати їх відновлення у разі пошкодження.

Загалом запропонований підхід до створення КСЗІ дозволяє забезпечити як технічний, так і організаційний захист інформації. Він сприятиме відповідності національним та міжнародним стандартам, підвищенню рівня безпеки підприємства та ефективному використанню сучасних технологій у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.
2. Дзьобань О. П., Панфілов О. Ю., Чемчекаленко Р. А. Методологічний контекст дослідження проблеми інформаційної безпеки. Зовнішня торгівля: економіка, фінанси, право. 2014. № 2. С. 171–180.
3. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)
4. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.
5. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.
6. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)
7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)
8. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.

9. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.
10. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081
11. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).
12. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
13. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства / Наше право. 2016. № 1. С. 17–23.
14. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
15. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
16. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.
17. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".

18. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".
19. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".
20. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
21. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.
22. Положення про організацію освітнього процесу в Тернопільському національному технічному університеті імені Івана Пулюя - наказ №4/7-340 від 21.05.2015 із змінами від 25.06.2019 - наказ №4/7-622 від 27.06.2019 та від 14.04.2020 - наказ №4/7-243 від 15.04.2020.
23. Положення про кваліфікаційні роботи студентів Тернопільського національного технічного університету імені Івана Пулюя - наказ №4/7-241 від 15.04.2020.
24. Положення про екзаменаційну комісію з атестації здобувачів вищої освіти ТНТУ ім.І.Пулюя - наказ №4/7-339 від 21.05.2015.
25. Положення про оцінювання здобувачів вищої освіти ТНТУ ім.І.Пулюя - наказ №4/7-542 від 11.07. 2016 зі змінами від 21.05.2019 - наказ №4/7-524 від 05.06.2019 та зі змінами від 31.10.2019 - наказ №4/7-970 від 01.11.2019.
26. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. — [Чинний від 2000.12.04]. — К. : ДСТСЗІ СБУ, 2000. — № 53.— (Нормативний документ системи технічного захисту інформації).
27. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

28. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.
29. Muzh, V., & Lechachenko, T. (2024). Computer technologies as an object and source of forensic knowledge: challenges and prospects of development. Scientific Journal of TNTU, 115(3), 17–22.

ДОДАТОК А

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18–19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професор.
Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.
Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.
Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень – завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.
Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. – 238 с.

М34

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com
Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УКД 004.056
З. В. Олекшій
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

«ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ»

UDC 004.056
Z. V. Olekshii

«PROTECTION OF CONFIDENTIAL INFORMATION IN CONDITIONS OF MARTIAL LAW»

В умовах ввоєнного стану гостро постала необхідність посилення захисту інформації з обмеженим доступом в автоматизованих системах. Кіберзагрози зі сторони агресора зумовили впровадження нових підходів до створення систем захисту. Особливо цінним є збереження конфіденційності в роботі державних підприємств оборонної сфери, оскільки інформація, що має стратегічне значення для безпеки країни, може бути використана для організації кібератак. Невдалі спроби захистити таку інформацію можуть мати катастрофічні наслідки для національної безпеки.

Невід'ємною складовою захисту конфіденційної інформації є швидка адаптація існуючих систем до умов воєнного часу. Підвищений рівень кіберзагроз вимагає впровадження більш ефективних засобів криптографії, антивірусного захисту, а також технологій моніторингу та виявлення аномальної активності в реальному часі. Такі заходи здатні зменшити ризики витоків важливої інформації та несанкціонованого доступу до державних систем [1].

В умовах военного стану значну роль у захисті інформації відіграють як організаційні, так і технічні заходи. Першочерговим завданням є забезпечення безпеки на всіх етапах обробки даних – від їх створення та збереження до передачі та використання в межах організацій. Це включає створення багаторівневих систем контролю доступу, впровадження шифрування на всіх рівнях, а також обмеження доступу до інформації для мінімальної кількості осіб.

Окремо варто зазначити важливість навчання персоналу, особливо в умовах екстремальних ситуацій. Підвищення обізнаності про сучасні загрози та правильне поводження з конфіденційними даними є важливою частиною стратегії захисту інформації. Адже людський фактор, зокрема помилки або недбалість співробітників, часто є основною загрозою для витоку інформації. Крім того, на тлі воєнного стану зростає значення захисту інформації від впливу зовнішніх загроз, таких як кібератаки або спроби знищення критичної інфраструктури [2].

Актуальним є створення систем, здатних автоматично виявляти й блокувати несанкціоновані спроби доступу до систем, а також запобігати можливим атакам з використанням шкідливого програмного забезпечення. У цьому контексті застосування сучасних технологій, таких як блокчейн для забезпечення цілісності даних і штучний інтелект для автоматичного виявлення аномальних дій, є важливими елементами захисту [3].

Не менш важливим є адаптація державних нормативно-правових актів до умов воєнного часу. Потрібно запровадити нові підходи до класифікації інформації, враховуючи специфіку загроз, що виникають в умовах війни. Врахування військових стандартів, наказів захисту інформації, що вже використовуються в країнах, де інформаційна безпека є пріоритетом, дозволяє удосконалити національні регуляції й привести їх у відповідність до сучасних вимог [4].

Таким чином, захист конфіденційної інформації в умовах воєнного стану є комплексним завданням, яке включає в себе технічні, організаційні та правові заходи. Це дозволяє забезпечити не лише захист критично важливої інформації від зовнішніх загроз, але й зберегти її цілісність, доступність і конфіденційність у найскладніших умовах.

Література

1. Шкварчук, В. В. Кіберзагрози та заходи їх мінімізації в умовах війни. – Київ: Національний університет оборони України, 2021. – 280 с.
2. Smith, J. Cybersecurity in Times of Crisis: Emerging Technologies and Practices. New York: Tech Press, 2022. – 180 p.
3. The Role of Blockchain in Enhancing Information Security in Wartime» – Journal of Cybersecurity Research, 2023.
4. Харченко, Ю. М. Інформаційна безпека в умовах сучасних загроз. – Київ: Літера, 2019.

Додаток Б

ТИПОВЕ ТЕХНІЧНЕ ЗАВДАННЯ
на створення комплексної системи захисту інформації автоматизованої системи класу “1”

2024

Зміст

Перелік скорочень

АС	–	автоматизована система
ДТЗС	–	допоміжні технічні засоби та системи
ЗПЗ	–	загальне програмне забезпечення
ІзОД	–	інформація з обмеженим доступом
ІТС	–	інформаційно-телекомунікаційна система
КЗЗ	–	комплекс засобів захисту, до складу якого за необхідності входять технічні, програмні, програмно-апаратні та апаратні засоби захисту інформації від несанкціонованого доступу
КС	–	комп’ютерна система
КСЗІ	–	комплексна система захисту інформації
НД	–	нормативний документ
НЖМД	–	накопичувач на жорсткому магнітному диску
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПДТР	–	протидія технічним розвідкам
ПЕМВ	–	побічні електромагнітні випромінювання і наведення
ПЕОМ	–	персональна електронно-обчислювальна машина
ПЗ	–	програмне забезпечення
ПЗ ПЗП	–	програмне забезпечення постійного запам’ятовуючого пристрою
ПМВ	–	програма та методики випробувань
СЗІ	–	служба захисту інформації
СПЗ	–	спеціальне програмне забезпечення
ТЗ	–	технічне завдання
ТЗІ	–	технічний захист інформації

1. Терміни та визначення

У цьому ТЗ використовуються терміни та визначення згідно з Законом України “Про захист інформації в інформаційно-телекомунікаційних системах”, ДСТУ 3396.2-97 “Захист інформації. Технічний захист інформації. Терміни та визначення”, НД ТЗІ 1.1-003-99 “Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу”, ДСТУ 2938-94 “Системи оброблення інформації. Основні положення. Терміни та визначення”.

2. Загальні відомості

2.1. Це ТЗ визначає вимоги до комплексу організаційних та інженерно-технічних заходів щодо забезпечення захисту інформації в типових автоматизованих системах класу “1”.

2.2. Вимоги цього ТЗ є обов’язковими для установ та організацій, а також підприємств, об’єднань підприємств.

2.3. Під типовою АС розуміється автоматизована система, склад якої та умови функціонування визначені в цьому ТЗ.

2.4. Створення типової КСЗІ в ІКС типової АС класу “1” в установах здійснюється шляхом реалізації для цієї АС вимог даного ТЗ.

2.5. Після завершення створення КСЗІ проводиться дослідна експлуатація ІКС і КСЗІ та державна експертиза. Порядок проведення державної експертизи визначається наказами Адміністрації Держспецзв’язку України. Експертиза КСЗІ проводиться відповідно до типових програми та методик, які погоджені з Адміністрацією Держспецзв’язку України.

2.6. Умовне позначення КСЗІ: типова КСЗІ АС класу “1” з СІ.

2.7. Шифр теми: “Таурег СІ”.

2.8. Замовник: начальник установи.

2.9. Виконавець: штатна служба захисту інформації в інформаційно-комунікаційній системі установи.

2.10.Початок робіт: визначається керівником установи.

2.11. Закінчення робіт: визначається наказом керівника установи.

2.12. Підстава для проведення робіт: вимоги Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”, дозвіл на проведення робіт з технічного захисту інформації для власних потреб.

2.13. Фінансування робіт здійснюється за рахунок утримання.

2.14. Технічне завдання оформлено відповідно до вимог НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі”.

3. Мета і призначення комплексної системи захисту інформації

3.1. Метою створення КСЗІ є захист ІзОД в типовій АС класу “1” від загроз порушення конфіденційності, цілісності, доступності інформації.

3.2. Для забезпечення безпеки інформації на всіх стадіях життєвого циклу типової АС класу “1” її КСЗІ повинна передбачати застосування наступних заходів та засобів захисту інформації:

організаційні заходи;

інженерно-технічні заходи (програмні засоби захисту від несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів).

Захист інформації повинен забезпечуватися на всіх технологічних етапах обробки інформації в усіх режимах функціонування.

3.3. КСЗІ типової АС класу "1" призначена для:

забезпечення ідентифікації, автентифікації користувачів, керування та контролю доступу користувачів АС до ІзОД;

блокування несанкціонованих дій з технологічною інформацією;

блокування спроб доступу до ІзОД, модифікації чи знищення ІзОД користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора;

забезпечення цілісності комплексу засобів захисту;

забезпечення реєстрації даних про події, що відбуваються в системі і мають відношення до безпеки інформації;

створення замкнутого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм, а також від впровадження і поширення комп'ютерних вірусів;

запобігання можливостям реалізації загроз для ІзОД в АС;

здійснення контролю за забезпеченням захисту ІзОД та за збереженням її матеріальних носіїв.

3.4. Нормативно-правовою базою щодо захисту інформації та створення КСЗІ в ІТС типової АС класу "1" є:

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31.05.05 № 2594-IV (зі змінами);

Закон України "Про інформацію" від 02.10.92 № 2657-XII (зі змінами);

Закон України "Про доступ до публічної інформації" від 13.01.11 № 2939-VI;

Закон України "Про захист персональних даних" від 01.06.10 № 2297-VI;

Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229/99;

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені ПКМУ від 29.03.06 № 373 (зі змінами);

ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

Тимчасове положення про категорування об’єктів в Україні (ТПКО-95), затверджене наказом Державного комітету країни з питань ДС та ТЗІ від 10.07.95 № 35;

НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.99 № 22;

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.99 № 22;

НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.99 №22;

НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБУ від 28.04.99 № 22 (зі змінами);

НД ТЗІ 3.7-003-2023. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом ДСТСЗІ СБ України від 08.11.05 № 125;

НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв’язку від 25.03.11 №65.

Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затверджений наказом Адміністрації Держспецзв`язку України від 26.03.07 № 45;

Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв’язку України від 16.05.07 № 93;

4. Загальна характеристика типової автоматизованої системи класу “1” та умов її функціонування

4.1 Згідно з НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” АС відноситься до класу “1” автоматизованих систем, як одномашинний багатокористувацький обчислювальний комплекс, який може обробляти інформацію кількох ступенів обмеження доступу.

4.2 Особливості функціонування: в кожний момент часу з комплексом може працювати тільки один користувач, з числа осіб, допущених до роботи. Усі користувачі, допущені до роботи з АС, повинні мати однакові повноваження (права) щодо доступу до інформації загального користування, яка оброблюється в АС.

Адміністратор безпеки повинен мати повноваження (права) щодо доступу до технологічної інформації АС.

4.3 Друкування, реєстрація, обіг, зберігання та знищення службової інформації в АС повинні здійснюватись відповідно до вимог чинного законодавства.

4.4 Найвищий ступінь обмеження доступу до інформації, яка може оброблятися в типовій АС класу “1” – “ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ”.

Ступінь обмеження доступу до інформації, яка буде оброблятись в конкретній АС визначається наказом керівника установи під час введення АС в експлуатацію.

4.5 Типова АС класу “1” призначена для:

введення інформації за допомогою клавіатури, сканера, з зовнішніх носіїв;

узагальнення, формалізації інформації, виконання інформаційно-розрахункових задач, опрацювання текстових, графічних документів, електронних таблиць тощо;

копіювання та архівування даних;

зберігання інформації;

друкування документів.

До складу типової АС класу “1” входять:

технічні засоби;

програмні засоби;

комплекс засобів захисту (від несанкціонованого доступу);

інформація, яка обробляється;

адміністратор безпеки;

користувачі.

4.6 Характеристика обчислювальної системи.

4.6.1 До складу типової АС повинна входити обчислювальна система, що складається з одного автоматизованого робочого місця на базі ПЕОМ, загального та спеціального програмного забезпечення (далі – ПЗ), в тому числі антивірусного.

4.6.2 АС класу “1” не повинна мати ліній зв’язку з іншими персональними комп’ютерами, локальними мережами та глобальною мережею Інтернет.

4.6.3 АС класу “1” не повинно мати у своєму складі бездротових інтерфейсів.

4.6.4 Склад технічних засобів.

Типова АС класу “1” будується на базі ПЕОМ у складі:

процесор архітектури x86 з частотою не нижче 1 ГГц;

оперативна пам’ять не менше 512 Мб;

відеокарта (окрема або вбудована в материнську плату) з підтримкою з підтримкою DirectX не нижче 9 версії;

пристрій НЖМД (HDD);

пристрій для НГМД 3.5 (за необхідністю);
пристрої DVD-ROM, DVD-RW (один або кілька, за необхідністю);
носій (ї) USB-Flash (за необхідністю);
монітор (пристрій відображення);
клавіатура;
графічний маніпулятор типу “миша”;
принтер (за необхідністю);
сканер (за необхідністю);
багатофункціональний пристрій (за необхідністю);
фільтр-подовжувач для мережі електроживлення (за необхідністю);
засіб безперебійного живлення типу APC Back-UPS або інший (за необхідністю).

4.6.5 Загальні технічні характеристики АС-1 повинні бути наведені в паспорті на АРМ та формулярі АС.

4.6.6 Програмне забезпечення (ПЗ) типової АС класу “1” повинне мати належним чином оформлені документи (ліцензії, сертифікати, експертні висновки тощо). До складу ПЗ входить загальне програмне забезпечення (ЗПЗ) та спеціальне програмне забезпечення (СПЗ).

4.6.7 ЗПЗ типової АС класу “1” формується з урахуванням вимог щодо підтримки:
можливості створення та оброблення документів різних форматів (файли типів docx, doc, rtf, xls, vsd, ppt, txt, lex, cdr, bmp, jpg, tif, pcx, psd, pdd, pdf, nsf, html, xml тощо);
використання пристроїв для друку;
використання пристроїв для сканування (за необхідності);
проведення операцій резервного копіювання;
проведення операцій архівування даних;
проведення операцій відновлення системи після збоїв;
функцій захисту інформації, що обробляється в типовій АС класу “1” (ідентифікації та автентифікації користувачів, управління доступом, реєстрації системних подій тощо).

ЗПЗ типової АС класу “1” формується на базі операційної системи та інших програмних засобів загального призначення і включає:
ПЗ постійного запам’ятовуючого пристрою (ПЗ ПЗП);

операційна система з вбудованим комплексом засобів захисту, на який одержаний сертифікат відповідності або позитивний експертний висновок в галузі ТЗІ;
антивірусне ПЗ, на яке одержаний сертифікат відповідності або позитивний експертний висновок в галузі ТЗІ;
драйвери периферійних пристроїв;
офісні пакети (наприклад, типу MS Office).
В залежності від завдань, які вирішуються за допомогою АС класу “1” до

ЗПЗ додатково може бути включено:

графічні пакети;

файловий менеджер;

ПЗ перевірки орфографії та перекладу;

ПЗ оптичного розпізнавання текстів;

ПЗ керування базами даних;

ПЗ для програмування інформаційно-розрахункових завдань;

архіватор WinRar тощо.

4.6.8 СПЗ типової АС класу “1” формується з урахуванням вимог щодо підтримки:

стирання інформації;

формування та перевірки електронно-цифрового підпису;

обліку контрольних сум файлів тощо.

4.6.9 Склад апаратного та програмного забезпечення АС вказується у “Формулярі на автоматизовану систему класу “1”).

4.6.10 Факт інсталяції програмного забезпечення фіксується в Акті інсталяції програмного забезпечення в АС класу “1”.

4.7 Характеристика середовища користувачів

4.7.1 Експлуатація типової АС класу “1” здійснюється працівниками однієї установи, який за своїми функціональними обов’язками працює з відомостями однієї тематики (змісту).

4.7.2 Посадові особи, що мають доступ до типової АС класу “1” (персонал АС), відносяться до наступних груп:

адміністратор безпеки, який має повноваження щодо встановлення, конфігурації та керування комплексом засобів захисту інформації;

користувачі, які мають певні повноваження щодо оброблення службової інформації;

технічний персонал, який забезпечує працездатність АС та порядок у робочих приміщеннях АС.

Посадові особи АС не є недбалими, навмисно недбалими або зловмисними (ворожими).

4.7.3 Адміністратор безпеки є працівником штатної служби захисту інформації установи. Адміністратор безпеки може бути на декілька типових АС класу “1” установи.

4.7.4 На адміністратора безпеки покладаються обов’язки щодо інсталяції, відновлення працездатності, видалення та тестування програмного забезпечення. Крім того, до функцій адміністратора безпеки належать конфігурування КЗЗ, контроль подій, періодичні перевірки працездатності засобів захисту інформації, повсякденний контроль виконання вимог щодо захисту інформації користувачами, виконання інших функцій забезпечення безпеки інформації. Адміністратор безпеки входить до складу СЗІ.

4.7.5 Користувачі володіють необхідною авторизацією доступу. Користувачі діють взаємоузгодженим чином та мають право доступу до інформації (п. 4.8.3), що зберігається на НЖМД у відповідності до вимог п. 4.8.4.

4.7.6 На адміністратора безпеки покладаються обов'язки з оновлення баз даних антивірусного програмного забезпечення. Порядок проведення вказаного оновлення визначається в Інструкції щодо порядку забезпечення антивірусного захисту інформації в ІКС.

4.7.8 Обов'язки користувачів при роботі з інформаційними ресурсами типової АС класу "1", порядок копіювання, друку, сканування та стирання інформації визначаються відповідними інструкціями.

4.8 Характеристика інформації, яка обробляється.

4.8.1 Інформація, що обробляється в типовій АС класу "1", класифікується за ступенем обмеження доступу (грифом обмеження доступу), за персоналізацією (категорією доступу), за правами доступу та за формою представлення.

4.8.2 За ступенем обмеження доступу інформація поділяється на:

відкриту;

службову (зі ступенем обмеження доступу "для службового користування").

4.8.3 За персоналізацією (належністю) інформація поділяється на:

технологічна інформація: файли КЗЗ, файли адміністратора безпеки з інформацією, яка не призначена для колективного використання (ознайомлення, копіювання, модифікації або знищення). Файли адміністратора безпеки зберігаються в підкаталогах адміністратора безпеки на НЖМД та/або на зовнішніх носіях інформації, закріплених за адміністратором безпеки;

інформація користувачів: файли користувача з інформацією, яка не призначена для колективного використання. При цьому, ці файли зберігаються в особистих підкаталогах кожного з користувачів на НЖМД та/або на зовнішніх носіях інформації, закріплених за кожним з користувачів особисто;

інформація загального користування: файли загального користування, що призначені для колективного використання (ознайомлення, копіювання, модифікації або знищення). При цьому, ці файли зберігаються у спеціально визначеному каталозі (далі – груповий каталог) на НЖМД, а копії цих файлів можуть зберігатися на зовнішніх носіях будь-якого з користувачів. В груповому каталозі, як правило, створюються підкаталоги для однотипних за змістом (темою) документів.

4.8.4 За правами доступу інформація, в загальному вигляді, поділяється наступним чином:

до технологічної інформації, що представлена у вигляді файлів КЗЗ та є інформацією, яка призначена для адміністрування типової АС класу "1" (ключі реєстру, ідентифікаційні дані, паролі, матриці доступу, дані настройки системи, журнали реєстраційних подій, бази даних захисту тощо, далі – дані

адміністрування) – доступ надається адміністратору безпеки та технологічним системним процесам користувачів згідно до їх повноважень. До технологічної інформації, яка представлена у вигляді файлів адміністратора безпеки і зберігається в підкаталогах адміністратора безпеки – надається доступ тільки адміністратору безпеки. Створення файлів (підкаталогів) в підкаталогах адміністратора безпеки дозволяється тільки адміністратору безпеки;

до інформації користувачів, яка представлена у вигляді файлів користувачів і зберігається в особистих підкаталогах кожного з користувачів – надається доступ тільки власникам цих особистих підкаталогів та адміністратору безпеки. Створення файлів (підкаталогів) в особистих підкаталогах кожного з користувачів дозволяється тільки власникам особистих підкаталогів та адміністратору безпеки;

до інформації загального користування, яка представлена у вигляді файлів загального користування і зберігається в груповому каталозі, надається доступ усім користувачам та адміністратору безпеки з можливістю ознайомлення з інформацією, її копіюванням, модифікацією або знищенням. Створення файлів (підкаталогів) в груповому каталозі дозволяється усім користувачам та адміністратору безпеки.

4.8.5 За формою представлення (формат електронного вигляду) інформація поділяється на:

документи текстових редакторів;
текстові файли;
документи редакторів з підготовки презентацій;
документи редакторів електронних таблиць;
документи HTML;
документи PDF;
документи Adobe Acrobat;
растрові зображення, наприклад Adobe Fhotoshop;
векторні зображення, наприклад Corel Draw;
аудіо, відео файли тощо.

4.9 Характеристика технології обробки інформації

4.9.1 В АС застосовується технологія обробки інформації, яка характеризується наступними ознаками:

службова інформація зберігається на машинних носіях інформації (НЖМД, магнітних носіях малої ємності, носіях USB-Flash та оптичних носіях CD (DVD));

усі користувачі, які мають доступ до носія інформації, мають однакові повноваження щодо доступу до всіх даних, які розміщені на носії інформації, на весь час функціонування КСЗІ;

усі користувачі, які мають доступ до НЖМД, мають однакові повноваження щодо доступу до всіх даних, які розміщені в груповому каталозі;

кожен з користувачів має доступ до всіх даних, які розміщені в особистому підкаталозі цього користувача, та не має доступу до даних, що розміщені в особистих підкаталогах інших користувачів та адміністратора;

засобами КЗЗ реалізована заборона доступу користувачів до будь-яких носіїв USB-Flash, за винятком тих, що були зареєстровані в системі адміністратором безпеки встановленим порядком;

взаємодія типових АС класу "1" між собою та з іншими АС здійснюється шляхом використання спеціально виділених магнітних носіїв малої ємності, оптичних носіїв CD (DVD) з грифом "для службового користування";

типова АС не має підключень (у тому числі тимчасових) до технічних засобів, які не належать до даної АС.

4.9.2 Машинні носії інформації реєструються і видаються користувачам встановленим порядком.

4.10 Характеристика фізичного середовища

4.10.1 До фізичного середовища типової АС класу "1" відноситься:

приміщення, в яких розташовано автоматизовану систему з усіма її компонентами (обчислювальна система, сховище носіїв інформації та програмного забезпечення, робочі місця користувача та обслуговуючого персоналу тощо);

засоби енергопостачання, заземлення, життєзабезпечення та сигналізації;

допоміжні технічні засоби та засоби зв'язку.

4.10.2 Одна або декілька типових АС класу "1" розгортаються в окремому приміщенні (приміщеннях) в межах контрольованої території. При цьому, в одному приміщенні допускається розгортання ПЕОМ різних категорій.

4.10.3 Доступ на контрольовану територію установи обмежений, здійснюється за перепустками та контролюється особами призначеними для здійснення охорони.

Доступ до приміщення обмежений та контролюється в робочий час користувачами, які працюють з АС, а в неробочий час – особою, яка призначена для здійснення охорони, якому приміщення здається під охорону.

4.10.4 В неробочий час МНСІ (за винятком НЖМД) зберігаються в сейфах.

Категорування приміщення та технічних засобів здійснюється відповідно до "Тимчасового положення про категоріювання об'єктів", затвердженого наказом Державної служби України з питань ТЗІ від 10.07.95 № 35 та наказу Міністра оборони України від 17.12.08 № 06.

4.10.5 Особливості функціонування об'єктів:

тип об'єкту – наземний (підземний тощо);

АС функціонують у робочий час, за виключенням робіт під час навчань, тренувань, непередбачених робіт.

Ресурси АС в оренду стороннім організаціям не здаються. Відкриття приміщень, де встановлені ПЕОМ, здійснюється відповідними особами або черговим військової частини (установи) у відповідності із затвердженими списками.

Доступ до приміщень, де розміщені АС, користувачів та інших осіб здійснюється відповідно до затвердженого списку згідно порядку, що визначений службою захисту інформації в ІКС (СЗІ в ІТС) та затверджений керівником установи.

Обробка службової інформації в АС в присутності сторонніх осіб (осіб, які не відносяться до керівництва установи, користувачів або адміністраторів), заборонена.

4.11 Потенційні загрози інформації в АС та можливі наслідки їх реалізації.

Загрози інформації, що обробляється в АС, можуть мати суб'єктивну або об'єктивну природу. Загрози, що мають суб'єктивну природу, включають в себе випадкові (ненавмисні) та навмисні.

4.11.1 Загрози суб'єктивного характеру.

Джерелом загроз суб'єктивного характеру можуть бути навмисні чи ненавмисні дії осіб, які можуть отримати фізичний доступ в категороване приміщення АС та до машинних носіїв.

4.11.1.1 Навмисні загрози.

До навмисних загроз відносяться:

порушення фізичної цілісності об'єкта (окремих компонентів, пристроїв, обладнання, носіїв інформації). Джерело загрози – люди. Наслідки– порушення конфіденційності, цілісності, спостереженості, доступності;

порушення режимів функціонування (виведення з ладу) систем життєзабезпечення об'єкта (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.). Джерело загрози – люди. Наслідки – порушення цілісності, доступності;

порушення режимів функціонування об'єкта (обладнання і програмного забезпечення). Джерело загрози – люди, програми. Наслідки – порушення конфіденційності, цілісності, спостереженості, доступності;

застосування комп'ютерних вірусів. Джерело загрози – люди, програми, апаратура. Наслідки – порушення цілісності, спостереженості;

впровадження програмних закладок та апаратних закладних пристроїв. Джерело загрози – люди, програми, апаратура. Наслідки – порушення конфіденційності, цілісності, спостереженості, доступності;

використання (шантаж, підкуп тощо) з корисливою метою персоналу об'єкту. Джерело загрози – люди. Наслідки – порушення конфіденційності, цілісності;

крадіжки носіїв інформації, виробничих відходів (роздруківок, записів, тощо). Джерело загрози – люди. Наслідки – порушення конфіденційності;

несанкціоноване копіювання інформації. Джерело загрози – люди, програми. Наслідки – порушення конфіденційності;

читання залишкової інформації з оперативної пам’яті ПЕОМ, НЖМД. Джерело загрози – люди, апаратура, програми. Наслідки – порушення конфіденційності;

одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”). Джерело загрози – люди, програми. Наслідки – порушення конфіденційності, цілісності;

впровадження і використання забороненого політикою безпеки програмного забезпечення або несанкціоноване використання ПЗ. Джерело загрози – люди, програми. Наслідки – порушення конфіденційності, цілісності, спостереженості;

навмисне пошкодження носіїв інформації. Джерело загрози – люди. Наслідки – порушення цілісності, доступності;

неправомірна зміна режимів роботи об’єкта (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад форматування носіїв інформації). Джерело загрози – люди, програми. Наслідки – порушення конфіденційності, цілісності, спостереженості;

невиконання організаційних вимог розпорядчих документів, чинних для військової частини та АС. Джерело загрози – люди. Наслідки – порушення конфіденційності, цілісності, спостереженості.

4.11.1.2 Випадкові загрози.

До випадкових загроз суб’єктивного характеру відносяться:

вплив фізичного середовища у разі аварії, стихійного лиха (землетрус, повінь, пожежа). Джерело загроз – люди, природні явища. Наслідки – порушення цілісності, спостереженості, доступності;

ненавмисне ураження ПЗ комп’ютерними вірусами. Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності;

ненавмисне пошкодження носіїв ІзОД. Помилки при введенні даних в АС. Джерело загрози – люди. Наслідки – порушення цілісності, спостереженості, доступності;

ненавмисні дії, що можуть призвести до розголошення ІзОД, паролів, атрибутів розмежування доступу, втрати атрибутів тощо. Джерело загрози – люди. Наслідки – порушення конфіденційності;

некомпетентне застосування засобів захисту. Джерело загрози – люди. Наслідки – порушення конфіденційності, цілісності, доступності, спостереженості.

4.11.2 Загрози об’єктивного характеру.

До загроз об’єктивного характеру відносяться:

зміна умов фізичного середовища (вологість, запиленість, коливання температури). Джерело загрози – природні явища. Наслідки – порушення доступності, цілісності;

збої і відмови у роботі обладнання та технічних засобів. Джерело загрози – апаратура. Наслідки – порушення цілісності, спостереженості, доступності.

4.11.3 Наведені потенційні загрози інформації в АС можуть впливати на порушення вимог конфіденційності, цілісності і доступності інформації, а також спостереженості за діями користувачів, що визначає необхідність впровадження відповідних заходів з захисту інформації.

5. Вимоги до типової комплексної системи захисту інформації типової автоматизованої системи класу “1”

5.1 Загальні вимоги

Архітектура АС повинна дозволяти розв’язання функціональних завдань у замкненому середовищі.

Робота АС у штатних режимах повинна бути можливою лише за умови функціонування КСЗІ.

Організаційні та підготовчі заходи щодо технічного захисту інформації повинні проводитися одночасно і складати перший етап робіт зі створення КСЗІ, на якому повинні бути уточнені потенційні загрози безпеці інформації.

Порядок проведення робіт щодо розроблення КСЗІ повинний відповідати ДСТУ 3396.0-96, ДСТУ 3396.1-96, НД ТЗІ 3.7-003-05.

Захист програмних та інформаційних ресурсів повинен забезпечуватися програмними засобами та організаційними заходами.

Для реалізації частини політики безпеки інформації, яка покладається на програмні засоби і відповідає реальній моделі загроз, КЗЗ повинен мати такі функціональні можливості:

забезпечення входу в систему та завантаження операційної системи за умови введення особистих логіну (псевдоніма) і паролю;

контроль інсталяції програмного забезпечення;

підтримка функцій адміністратора безпеки в АС;

реєстрація дій користувачів по відношенню до ресурсів системи;

забезпечення цілісності інформаційних ресурсів (у тому числі і антивірусний захист);

перевірка цілісності та працездатності КЗЗ;

надання користувачам прав доступу до ресурсів АС згідно прийнятої політики безпеки, та їх ліквідація по закінченню строку дії;

розмежування повноважень користувачів до ресурсів АС;

контроль за запуском процесів та їх виконанням;

розмежування доступу користувачів до логічних дисків, каталогів, файлів;

блокування роботи у разі відсутності користувача більш встановленого періоду часу з наступною ідентифікацією та автентифікацією користувача;

керування процесом завантаження операційного середовища;

заборона доступу користувачів до будь-яких носіїв USB-Flash, за винятком тих, що були зареєстровані в системі адміністратором безпеки встановленим порядком.

Виконання завдань повинне здійснюватися зареєстрованими користувачами у функціонально замкненому середовищі із забезпеченням доступу до ресурсів АС, що обмежені рамками завдань.

Організаційні заходи повинні включати:

планування заходів захисту інформації;

визначення та встановлення обов'язків із захисту інформації підрозділів та осіб, що приймають участь в обробці інформації;

визначення технологічних процесів обробки інформації з урахуванням вимог із захисту інформації;

встановлення порядку впровадження та модернізації засобів обробки інформації, програмних та технічних засобів захисту інформації;

організацію фізичного та протипожежного захисту АС;

розробку правил та порядку контролю функціонування КСЗІ;

розробка організаційно-розпорядчих документів, доведення їх вимог до особового складу;

визначення адміністратора безпеки, користувачів;

закріплення технічних засобів за посадовими особами;

планування та здійснення контролю безпеки інформації та використання ресурсів системи;

заборона використання носіїв інформації без антивірусної перевірки;

організація системи зберігання та реєстрації ідентифікаторів і паролів користувачів;

планування та забезпечення відновлення системи після збоїв;

забезпечення перепускного режиму до контрольованої зони та в приміщення, де встановлені АС;

організацію навчання особового складу з питань захисту інформації.

5.2 Опис політики безпеки інформації, яку повинен реалізовувати КЗЗ

5.2.1 КЗЗ повинний забезпечувати наступні правила безпеки:

користувачі системи повинні бути підзвітними в їх діях в межах АС, всі спроби входу в АС (автентифікації), завершення сеансу роботи з АС, інші події, що мають відношення до безпеки інформації повинні реєструються в журналах реєстрації, доступ до цих журналів повинен мати лише адміністратор безпеки;

доступ до ресурсів АС повинен надаватися тільки тим користувачам, які пройшли автентифікацію;

КЗЗ повинний забезпечувати розмежування доступу користувачів до інформації;

КЗЗ повинний забезпечувати необхідний рівень цілісності та доступності інформації при збоях, відмовах та обслуговуванні системи;

захист службової інформації повинен забезпечуватись протягом всього періоду її існування в АС.

5.2.2 Об'єктами типової АС класу "1" є:

активні об'єкти (суб'єкти доступу) – користувачі автоматизованої системи та процеси, які діють від імені користувача відповідно до наданих користувачам прав;

пасивні об'єкти (ресурси АС, що знаходяться під керуванням КЗЗ і характеризується певними атрибутами):

томи (логічні диски);

каталоги (підкаталоги, папки) файлової системи;

файли даних користувачів;

тимчасові файли, що створюються операційною системою та іншим програмним забезпеченням під час роботи;

файли операційної системи та іншого програмного забезпечення;

файли КЗЗ з технологічною інформацією, яка призначена для адміністрування типової АС класу “1” (ключі реєстру, ідентифікаційні дані, паролі, настройки системи, реєстраційних подій, бази даних захисту тощо);

принтери;

сканери;

багатофункціональні пристрої;

області пам’яті (оперативної, постійної).

5.2.3 Принципи керування доступом до інформації, правила розмежування інформаційних потоків

До файлів (підкаталогів) КЗЗ з технологічною інформацією, яка призначена для адміністрування АС, надається доступ тільки адміністратору безпеки та технологічним системним процесам користувачів згідно до їх повноважень. До файлів (підкаталогів) адміністратора безпеки, які зберігаються в підкаталогах адміністратора безпеки, надається доступ тільки адміністратору безпеки. Створення файлів (підкаталогів) в підкаталогах адміністратора безпеки, дозволяється тільки адміністратору безпеки.

До файлів (підкаталогів), які зберігаються в особистих підкаталогах користувачів, доступ надається тільки власникам цих особистих підкаталогів та адміністратору безпеки. Створення файлів (підкаталогів) в особистих підкаталогах кожного з користувачів дозволяється тільки власникам особистих підкаталогів та адміністратору безпеки.

Для файлів (підкаталогів), що знаходяться безпосередньо в особистих підкаталогах користувачів, право власника об’єкта (файлу або підкаталогу) іншим користувачам не передається.

У типовій АС класу “1” повинне бути реалізоване довірче керування доступом, яке повинно дозволяти користувачеві передавати іншим користувачам повноваження по доступу (читання, зміна, запис, видалення файлу) до створених ним файлів, шляхом копіювання цих файлів з зовнішніх носіїв або особистого каталогу до групового каталогу, або створення файлів безпосередньо в груповому каталозі.

Користувачі повинні отримувати повний доступ (на читання, створення, зміну, запис, виконання, видалення файлу (підкаталогу) або інший, відповідний до наведеного, набір) до інформації, яка зберігається в групових каталогах.

5.2.4 Маркування носіїв ІзОД в типовій АС класу “1” повинно здійснюватись з використанням наступних атрибутів:

гриф обмеження доступу;

реєстраційний номер;

ідентифікатор діловодства;

підпис особи, що здійснила реєстрацію.

5.2.5 Основні атрибути доступу користувачів, процесів і пасивних об’єктів.

5.2.5.1 Основні атрибути доступу користувачів і процесів

Кожному користувачу та групі користувачів повинен визначатися обліковий запис, який представляється набором атрибутів[5)] (табл. 1):

Таблиця 1

Атрибут	Опис атрибута
Ім’я облікового запису	Використовується для представлення облікового запису в зручному для читання вигляді
Ідентифікатор безпеки	Ідентифікатор використовується для однозначного представлення облікового запису користувача або групи користувачів в межах системи
Пароль	Використовується для автентифікації облікового запису адміністратора безпеки або користувача при вході до системи
Група	Використовуються, щоб зв’язати членів групи користувачів з єдиним обліковим записом
Повноваження	Використовуються для зв’язку повноважень користувачів або груп користувачів з відповідним обліковим записом
Права на вхід до системи	Визначає право користувача щодо варіантів його входу в систему
Керуюча інформація	Використовується для контролю додаткових атрибутів облікового запису, що стосуються безпеки (час дії облікового запису, термін дії пароля та ін.)

Після успішної автентифікації в системі, КЗЗ для кожного користувача повинен створювати маркер доступу, який містить набір атрибутів безпеки суб’єкту. Маркери повинні асоціюватися з кожним процесом, що виконується від імені визначеного користувача. В маркері повинна міститися наступна інформація[6)]:

ідентифікатор безпеки користувача;

ідентифікатори безпеки відповідних груп, членами яких є даний користувач;

Примітка:

[5)]Склад набору атрибутів, які входять до облікового запису, може бути уточнений на етапі розробки робочої документації КСЗІ.

[6)]Інформація, яка міститься в маркері доступу, може бути уточнена на етапі розробки робочої документації КСЗІ.

список повноважень користувача (на читання, створення, зміну, запис, виконання, видалення файлу (папки) або інший відповідний набір[7)]);

встановлений по замовченню вибірковий список доступу (для об'єктів, що будуть створюватися даним користувачем).

Примітка:

[7)]Інформація, що входить до списку повноважень користувача, може бути уточнена на етапі розробки робочої документації КСЗІ.

5.2.5.2 Основні атрибути доступу пасивних об'єктів

Атрибути доступу пасивних об'єктів повинні зберігатися в дескрипторах безпеки (для кожного об'єкту призначається дескриптор безпеки), які містять[8)]:

номер версії дескриптора;

ідентифікатор власника об'єкта;

вибірковий список доступу, який містить інформацію про права доступу (на читання, створення, зміну, запис, виконання, видалення файлу (папки) або інший відповідний набір[9)]) до захищеного об'єкта.

Дескриптори повинні бути представлені в таблиці дескрипторів.

Вибірковий список доступу об'єкта повинен складатися із записів керування доступом. Кожний запис керування доступом має визначати:

тип запису (дозволити/заборонити);

права доступу (на читання, створення, зміну, запис, виконання, видалення файлу (папки) або інший відповідний набір[10)]), що надані конкретному користувачеві або групі користувачів, у вигляді бітової маски;

ідентифікатор безпеки користувача або групи користувачів.

КЗЗ повинний забезпечувати призначення списку доступу кожного захищеного об'єкта в момент його створення.

Примітка:

[8)]Інформація, яка міститься в дескрипторі безпеки, може бути уточнена на етапі розробки робочої документації КСЗІ.

[9)]Інформація, що входить до вибіркового списку доступу, може бути уточнена на етапі розробки робочої документації КСЗІ.

[10)]Види прав доступу можуть бути уточнені на етапі розробки робочої документації КСЗІ.

5.2.6 Правила розмежування доступу користувачів і процесів до пасивних об'єктів

5.2.6.1 У типовій АС повинні бути встановлені наступні правила розмежування доступу:

Якщо суб'єкт робить спробу виконати яку-небудь операцію або отримати доступ до захищеного об'єкта, КЗЗ повинний виконати перевірку атрибутів доступу і встановити, чи є операція дозволеною для конкретного користувача. КЗЗ повинний реалізовувати правила довірчого керування доступом до об'єктів, які ґрунтуються на співставленні повноважень, визначених у маркері доступу суб'єкта,

з одного боку, та масці дескриптора безпеки об’єкта, з другого боку. Доступ до об’єкта надається при їх співпаданні.

Суб’єкт, що створює об’єкт, визначає його розташування в ієрархії об’єктів АС.

5.2.6.2 При встановленні прав доступу до об’єктів під час їх копіювання або переміщення в АС, повинні використовуватися наступні правила:

якщо об’єкт копіюється в межах одного тому (наприклад, NTFS) або на інший том, новий скопійований об’єкт успадковує права доступу папки, що одержує цей об’єкт. Суб’єкт, який здійснює копіювання, стає власником об’єкта-копії;

якщо об’єкт переміщується в межах одного тому, то об’єкт зберігає свої початкові права доступу;

якщо об’єкт переміщується з одного тому на інший том, то об’єкт успадковує права доступу папки, що одержує цей об’єкт. Суб’єкт, який здійснює переміщення, стає власником об’єкта-копії;

якщо об’єкт переміщується або копіюється з тому на зовнішній носій інформації, об’єкт втрачає всі права доступу. Забезпечення цілісності та доступності таких об’єктів здійснюється режимними (організаційними) заходами[11)].

Примітка:

[11)]Шляхом налаштування КЗЗ повинна бути реалізована заборона на передачу прав доступу до файлів, що знаходяться в особистих каталогах, іншим користувачам.

5.2.7 Основні вимоги щодо адміністрування КЗЗ і реєстрації дій користувачів типової АС класу “1”.

5.2.7.1 КЗЗ повинен надавати змогу адміністратору безпеки:

встановлювати та керувати параметрами безпеки окремого користувача та групи користувачів;

визначати повноваження для користувачів та груп користувачів на вхід в АС та виконання системних задач (запуск програм на виконання);

дозволяти або забороняти реєстрацію подій, визначати категорії подій, що підлягають аудиту, вказувати тип контрольованої події (успіх/відмова), керувати (створення, видалення та очищення) журналами реєстрації;

встановлювати обмеження на паролі адміністратора безпеки та користувачів, що використовуються (максимальний, мінімальний термін дії пароля, мінімальна довжина пароля, відповідність пароля вимогам складності, вимога неповторюваності паролів або інший відповідний набір);

визначати параметри блокування облікових записів (часовий проміжок блокування облікового запису, часовий проміжок, після якого здійснюється обнуління лічильника блокування або інший відповідний набір);

керувати дисковими квотами на томах.

5.2.7.2 КЗЗ повинний підтримувати набір засобів аудиту, призначених для моніторингу та виявлення небажаних умов і подій, які виникають в обчислювальному середовищі. Моніторинг системних подій повинен виявляти

порушників системи безпеки, а також фіксувати спроби фальсифікації та видалення даних, які знаходяться в АС.

5.3 Вимоги до КСЗІ типової АС класу “1” в частині захисту від несанкціонованого доступу

5.3.1 КЗЗ повинний забезпечувати захист файлів адміністратора безпеки та файлів КЗЗ з інформацією, що призначена для адміністрування АС (ключі реєстру, ідентифікаційні дані, паролі, матриці доступу, дані настройки системи, журнали реєстраційних подій, бази даних захисту тощо).

Права доступу до цих об’єктів належать виключно адміністратору безпеки. Передача адміністратором безпеки прав доступу до цих об’єктів іншим користувачам заборонена.

Права доступу до кожного захищеного об’єкта, що містить дані адміністрування, повинні встановлюватись в момент його створення або ініціалізації.

Імпорт та експорт захищених об’єктів, що містять дані адміністрування, заборонені.

5.3.2 Функціональний профіль захищеності інформації від несанкціонованого доступу в типовій АС класу “1” повинен включати набір послуг, не нижчий ніж наступний:

КД-2, КО-0, ЦД-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2.

5.3.3 Вимоги до функціональних послуг

5.3.3.1 Вимоги до забезпечення конфіденційності

Шляхом виконання організаційних вимог та налаштувань КЗЗ у відповідності до вимог п. 5.2.3 повинні забезпечуватися елементи реалізації рівня мінімальної адміністративної конфіденційності, а саме:

політика реалізації мінімальної адміністративної конфіденційності повинна розповсюджуватися на файли даних системи захисту, файли ведення журналу реєстрації подій, функціональні програми КЗЗ;

КЗЗ повинен надавати адміністратору безпеки права доступу до процесів, що обслуговують ведення бази даних системи захисту (псевдоніми та паролі користувачів, повноваження щодо доступу тощо);

КЗЗ повинен надавати адміністратору безпеки права доступу до процесів, що обслуговують ведення та аналіз захищеного журналу, в якому реєструються події, визначені політикою безпеки послуги НР-2;

доступ до файлів даних системи захисту, файлів ведення захищеного журналу, в якому реєструються події, визначені політикою безпеки, повинен мати тільки адміністратор.

У відповідності до обраного профілю захищеності конфіденційність технологічної інформації, яка призначена для адміністрування АС (представлена у вигляді файлів КЗЗ), інформації адміністратора безпеки (представлена у вигляді файлів адміністратора безпеки), інформації, яка зберігається в особистих

підкаталогах користувачів та інформації, яка зберігається в групових каталогах, має забезпечуватися функціональними послугами “Довірча конфіденційність” на рівні “Базова довірча конфіденційність” (КД-2) та “Повторне використання захищених об’єктів” (КО-0).

Базова довірча конфіденційність (КД-2).

Політика базової довірчої конфіденційності повинна відноситися до наступних об’єктів, які містять інформацію з обмеженим доступом: підкаталоги адміністратора безпеки, особисті підкаталоги користувачів, груповий каталог, призначений для обміну файлами даних між користувачами, файли даних, тимчасові файли, що створюються операційною системою та іншим програмним забезпеченням під час роботи з файлами даних.

Примітка:

[12)]Розмежування фізичного доступу користувачів до файлів секретних даних, що зберігаються на з’ємних машинних носіях інформації (наприклад, фізичного доступу користувачів до НЖМД), досягається виконанням організаційних вимог та вимог режиму секретності в частині поводження з машинними носіями інформації.

КЗЗ повинен забезпечувати реалізацію принципів керування доступом до інформації, наведених в п. 5.2.3.

КЗЗ повинен здійснювати розмежування доступу відповідно до правил, наведених в п. 5.2.6, на підставі атрибутів доступу користувача та дескриптору безпеки захищеного об’єкта.

Запити на зміну прав доступу до об’єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, та дескриптору безпеки захищеного об’єкта (п. 5.2.5).

КЗЗ повинен надавати користувачу можливість визначати в списку доступу об’єкта, що належить його домену – конкретних користувачів або групи користувачів, які мають право одержувати (читати) інформацію від об’єкта, модифікувати або видаляти об’єкт.

КЗЗ повинен надавати користувачу можливість визначати в списку доступу процесу, що належить його домену – конкретних користувачів або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об’єкта повинні встановлюватись в момент його створення або ініціалізації.

Як частина політики довірчої конфіденційності повинні виконуватися правила збереження атрибутів доступу об’єктів під час їх експорту і імпорту. КЗЗ повинен здійснювати збереження атрибутів доступів об’єктів у відповідності до порядку, наведеного в п. 5.2.6.2.

Повторне використання захищених об’єктів (КО-0).

Політика повторного використання об’єктів, що реалізується КЗЗ, стосується тих об’єктів АС, які містять інформацію з обмеженим доступом (адміністратора безпеки, користувачів або загального користування), та ресурси яких поділяються між користувачами АС.

До множини захищених об’єктів, на які поширюються вимоги цієї послуги, повинні відноситись сегменти пам’яті на НЖМД, які використовуються

програмним забезпеченням, що здійснює обробку інформації з обмеженим доступом адміністратора безпеки, користувачів та/або інформації загального користування.

Механізм керування пам'яттю повинний реалізовувати взаємну ізоляцію адресного простору процесів і очищення пам'яті після її звільнення.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкту повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, семантичний зміст інформації, що міститься в даному об'єкті, повинен стати недосяжним.

5.3.3.2 Вимоги до забезпечення цілісності.

У відповідності до обраного профілю захищеності цілісність має забезпечуватися функціональною послугою "Довірча цілісність" на рівні "Мінімальна довірча цілісність" (ЦД-1).

Політика мінімальної довірчої цілісності повинна відноситися до об'єктів, що містять технологічну інформацію (файли КЗЗ та файли адміністратора безпеки), об'єктів, що містять інформацію користувачів (файли користувачів), об'єктів групового каталогу (файли загального користування), тимчасові об'єкти, що створюються програмним забезпеченням під час роботи з файлами адміністратора та користувачів (тимчасові файли).

КЗЗ повинен забезпечувати реалізацію принципів керування доступом до інформації, наведених в п. 5.2.3.

КЗЗ повинен здійснювати розмежування доступу відповідно до правил, наведених в п. 5.2.6, на підставі атрибутів доступу користувача та дескриптору безпеки захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, та дескриптору безпеки захищеного об'єкта.

КЗЗ повинен надавати користувачу можливість визначати в списку доступу захищеного об'єкта, що належить його домену – конкретних користувачів або групи користувачів, які мають право одержувати (читати) інформацію від об'єкта, модифікувати або видаляти об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Як частина політики довірчої цілісності повинні виконуватися правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту. КЗЗ повинен здійснювати збереження атрибутів доступів об'єктів у відповідності до порядку, наведеного в п. 5.2.6.2.

5.3.3.2 Вимоги до забезпечення доступності.

У відповідності до обраного профілю захищеності доступність має забезпечуватися функціональною послугою “Відновлення після збоїв” на рівні “Автоматизоване відновлення” (ДВ-2).

Політика відновлення, що реалізується КЗЗ, відноситься до таких типів відмов типової АС класу “1”: збої, відмови та переривання в роботі програмного забезпечення (відмови або переривання процесів завантаження АС, ініціалізації та перевірки цілісності КЗЗ, процедур автентифікації користувачів, процедур ведення журналу реєстрації подій).

Після відмови АС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення АС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути АС до нормального функціонування.

Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести АС до стану, з якого повернути її до нормального функціонування може тільки адміністратор безпеки.

КЗЗ повинний включати набір інструментів діагностики і забезпечувати, залежно від обставин виникнення і типу збою, можливість вибору наступних засобів відновлення, за допомогою яких можна безпечним чином повернути АС до нормального функціонування:

завантаження операційної системи в безпечному режимі (має використовуватися при збоях, що порушують процес завантаження операційної системи) – повинно здійснюватися в базовій конфігурації з настройками за умовчанням і мінімальним набором драйверів пристроїв. В безпечному режимі повинна підтримуватися можливість запуску і зупинення служб, зміни настройки АС, видалення програм або драйверів, які ймовірно стали причиною виникнення збою;

завантаження останньої вдалої конфігурації (має використовуватися якщо причиною збою є зміни в конфігурації, що сталися після останнього завантаження системи) – повинно дозволяти швидко відновити базу даних системної інформації (реєстр) і відмінити зміни, які сталися в у відповідному розділі бази даних системної інформації (ключі реєстру) з моменту останнього вдалого завантаження системи;

відновлення системи (використовується для відміни змін в конфігурації, які призвели до збою, при успішному завантаженні ОС або при завантаженні в безпечному режимі) – повинно забезпечувати створення копій системних файлів, відстеження кожної зміни в системних файлах і запис стислих копій цих файлів в захищений каталог.

5.3.3.3 Вимоги до забезпечення спостереженості.

У відповідності до обраного профілю захищеності спостереженість має забезпечуватися функціональними послугами “Реєстрація” на рівні “Захищений журнал” (НР-2), “Ідентифікація і автентифікація” на рівні “Одиночна

ідентифікація і автентифікація користувачів" (НИ-2), "Достовірний канал" на рівні "Однонаправлений достовірний канал" (НК-1), "Розподіл обов'язків" на рівні "Виділення адміністратора" (НО-1), "Цілісність КЗЗ" на рівні "КЗЗ з контролем цілісності" (НЦ-1), "Самотестування" на рівні "Самотестування при старті" (НТ-2).

Захищений журнал (НР-2).

КЗЗ повинен бути здатним здійснювати реєстрацію таких подій, що мають безпосереднє відношення до безпеки:

вхід/вихід користувача в систему (псевдонім користувача, дата, час);

реєстрація та видалення із системи користувачів (псевдонім користувача, дата, час);

зміна пароля (псевдонім користувача, дата, час);

створення та знищення файлів, які зберігаються на НЖМД, зміна прав доступу;

доступ програм до файлів адміністратора безпеки, файлів користувачів та файлів загального користування;

копіювання файлів адміністратора безпеки, файлів користувачів та файлів загального користування;

друкування документів;

факти порушення (спроби порушення) цілісності КЗЗ;

завантаження операційної системи, завершення її роботи;

зміна конфігурації;

спроби запуску програм, не дозволених політикою безпеки;

спроби інсталяції програмного забезпечення та встановлення (реєстрації) носіїв USB-Flash, не дозволених політикою безпеки;

спроби перевищення встановлених обмежень на використання ресурсів.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події.

Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або знищення.

Адміністратор безпеки повинний мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Одиночна ідентифікація і автентифікація користувачів (НИ-2).

Кожний користувач повинен однозначно ідентифікуватися КЗЗ на підставі введеного імені (псевдоніму).

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача на підставі введеного ним пароля.

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути у відповідності до п. 5.2.5 цього ТЗ.

Перш ніж дозволити будь-якому користувачу та адміністратору безпеки виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача на підставі введеного їм пароля.

Для визначення псевдоніму та паролю повинна використовуватися буквено-цифрова клавіатура. Кількість символів у паролі повинна бути не менше 8.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого ознайомлення, модифікації або знищення.

Однонаправлений достовірний канал (НК-1).

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації користувача.

Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем шляхом вибору або вводу свого особистого псевдоніму (ідентифікатору) під час початкової ідентифікації та вводу особистого паролю під час початкової автентифікації.

Політика достовірного каналу повинна передбачати обов'язковий вихід користувача із системи (шляхом виходу користувача із системи, перезавантаження або вимкнення ОС) після завершення ним роботи.

Політика достовірного каналу стосується всіх користувачів та компонентів програмного забезпечення, які задіяні для реалізації механізмів КЗЗ.

Виділення адміністратора (НО-1).

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора безпеки і звичайного користувача і притаманні їм функції.

Роль адміністратора безпеки повинна забезпечувати виконання функцій інсталяції, настройки та підтримки працездатності програмного забезпечення, встановлення користувачам прав доступу до ресурсів, контролю подій, реагування на інциденти, інших функцій безпеки.

Роль звичайного користувача повинна бути обмежена функціями, необхідними для роботи з файлами користувача та файлами загального користування.

Фізична особа повинна мати можливість виступати в певній ролі лише у тому разі, якщо у процесі автентифікації вона визначена як особа, якій притаманна ця роль.

КЗЗ з контролем цілісності (НЦ-1).

Перевірка цілісності програмних компонентів КЗЗ повинна виконуватися за допомогою порівняння цих файлів та файлів-еталонів, які використовуються для відстеження коректності файлів, що перевіряються.

Контроль цілісності програм та даних, що входять до КЗЗ, повинен здійснюватися при кожному включені АС або завантаженні операційної системи.

Контроль полягає у перевірці наявності всіх зазначених компонентів та відповідності їх контрольних характеристик еталонним значенням.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен зареєструвати цю подію у журналі реєстрації і (або) автоматично відновити відповідність компонента еталону або перевести АС до стану, з якого повернути її до нормального функціонування може тільки адміністратор безпеки.

З метою недопущення порушення політики безпеки необхідно унеможливити використання в АС програмного забезпечення, яке не має відповідного дозволу та не призначене для обробки секретної інформації, зокрема засобів налагодження програмного забезпечення, засобів моніторингу за процесами та ресурсами АС тощо.

КЗЗ повинний підтримувати наступні режими контролю цілісності:

негайний контроль цілісності;

однократний контроль цілісності при наступному завантаженні АС;

контроль цілісності при кожному завантаженні АС.

Самотестування при старті (НТ-2).

Завантаження операційної системи повинно здійснюватися під контролем КЗЗ, який контролює процес завантаження та ініціалізації системних сервісів та зупиняє систему при виникненні критичних проблем.

Повинні бути реалізовані процедури, які призначені для оцінки правильності функціонування КЗЗ: КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності своїх критичних функцій.

Тести повинні виконуватися за запитом адміністратора безпеки та при ініціалізації КЗЗ.

5.3.4 Вимоги до рівня гарантій.

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань КЗЗ. Рівень гарантій реалізації функціонального профілю захищеності має бути не нижчим за Г2, згідно до НД ТЗІ 2.5-004-99.

5.3.5 Вимоги до випробування комплексу засобів захисту.

Головний виконавець повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття.

Головний виконавець повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування.

Головний виконавець повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з’явилися нові “слабкі місця”.

Порядок проведення випробувань повинний відповідати вимогам НД ТЗІ 3.7-003-05.

5.4 Вимоги до захисту інформації від витоку технічними каналами у типовій АС класу “1” не висуваються.

6. Вимоги до складу проектної та експлуатаційної документації

В ході виконання роботи розробляються:

Наказ про створення служби захисту інформації в АС (штатної або позаштатної).

Положення про службу захисту інформації в АС.

Накази щодо організації робіт, призначення комісій та відповідальних.

Протокол про визначення вищого ступеня обмеження доступу до інформації.

Акт обстеження на ОІД.

Акти категорування ОІД (ТЗПІ).

Перелік категорованих ОІД.

Поіменні списки на доступ в режимні приміщення (зони, території) та до обробки інформації в ІКС.

Акти інсталяції програмного забезпечення.

План захисту інформації в ІКС (з наступними основними розділами: Модель загроз, Модель порушника, Політика безпеки).

Формуляр на АС класу “1”.

Інструкція (настанова) адміністратору безпеки з інсталяції та ініціалізації комп’ютерної системи.

Інструкція (настанова) адміністратору безпеки щодо конфігурування параметрів безпеки комп’ютерної системи.

Інструкція щодо порядку забезпечення антивірусного захисту інформації в ІТС.

Інструкції (настанова, посібник) адміністратору безпеки та користувачам від НСД.

Журнал обліку роботи на ПЕОМ.

Програма та методики випробувань ІКС і КСЗІ.

Акт приймання ІКС та КСЗІ у дослідну експлуатацію, протоколи випробувань.

Наказ про проведення дослідної експлуатації ІКС та КСЗІ.

Акт про завершення дослідної експлуатації КСЗІ (про завершення робіт зі створення КСЗІ).

Заява про проведення експертизи КСЗІ в ІКС (з Переліком відомостей про КСЗІ в ІТС).

7. Етапи виконання робіт

7.1 Створення служби захисту інформації (штатної або позаштатної) в ІТС.

Проведення робіт та розробка таких документів:

Наказ про створення служби захисту інформації в ІТС (штатної або позаштатної).

Положення про службу захисту інформації в ІТС.

Накази щодо організації робіт зі створення КСЗІ, призначення комісій та відповідальних (закріплення ТЗПІ за працівниками, категорування ОІД (ТЗПІ), випробувань ІТС і КСЗІ, адміністратора безпеки).

7.2 Аналіз загроз для інформації та розробка політики безпеки інформації в ІКС.

Проведення робіт та розробка таких документів:

Акт обстеження на ОІД.

Акти категорування ОІД (ТЗПІ).

Перелік категорованих ОІД.

Поіменні списки на доступ в режимні приміщення (зони, території) та до обробки інформації в ІКС.

План захисту інформації в ІКС (з наступними основними розділами: Модель загроз, Модель порушника, Політика безпеки).

7.3 Розробка робочої документації КСЗІ.

Проведення робіт та розробка таких документів:

Інструкція (настанова) адміністратору безпеки з інсталяції та ініціалізації комп’ютерної системи.

Інструкція (настанова) адміністратору безпеки щодо конфігурування параметрів безпеки комп’ютерної системи.

7.4 Розробка експлуатаційної документації КСЗІ.

Проведення робіт та розробка таких документів:

Інструкція щодо забезпечення безпеки інформації (забезпечення режиму секретності під час обробки секретної інформації) в ІКС.

Інструкція щодо порядку забезпечення антивірусного захисту інформації в ІКС.

Інструкції (настанова, посібник) адміністратору безпеки та користувачам від НСД.

Журнал обліку роботи на ПЕОМ.

Журнал обліку копіювання інформації на ПЕОМ.

Журнал обліку стирання інформації на ПЕОМ.

7.5 Пусконалагоджувальні роботи.

Здійснюється інсталяція та захищена конфігурація програмного забезпечення ІКС і КСЗІ.

Проведення робіт та розробка таких документів:

Акти інсталяції програмного забезпечення.

Програми та методики випробувань КТЗІ.

7.6 Випробування КСЗІ.

Проводяться випробування КСЗІ.

Проведення робіт та розробка таких документів:

Програма та методики випробувань ІКС і КСЗІ.

Акт приймання ІКС та КСЗІ у дослідну експлуатацію, протоколи випробувань.

7.7 Дослідна експлуатація КСЗІ.

Проводиться навчання користувачів та дослідна експлуатація КСЗІ.

Проведення робіт та розробка таких документів:

Наказ про проведення дослідної експлуатації ІКС та КСЗІ.

Акт про завершення дослідної експлуатації КСЗІ (про завершення робіт зі створення КСЗІ).

7.8 Державна експертиза КСЗІ.

Надання Заяви про проведення експертизи КСЗІ в ІКС з Переліком відомостей про КСЗІ в ІКС до Уповноваженого органу.

Надання організації-виконавцю експертизи комплекту документації.

Проведення робіт організацією-виконавцем експертизи.

Опрацювання експертами організації-виконавця експертизи КСЗІ Протоколів виконання робіт.

Узагальнення організацією-виконавцем результатів робіт в Експертному висновку та подання примірників Експертного висновку, разом із примірниками протоколів та проектом Атестату відповідності до Уповноваженого органу.

Реєстрація Атестату відповідності в Адміністрації Держспецзв'язку України.

Одержання Замовником експертизи КСЗІ Атестату відповідності та першого примірнику Експертного висновку.

7.9 Надання дозволу на обробку інформації з обмеженим доступом в типовій АС класу "1" шляхом видання наказу керівника установи "Про введення КСЗІ АС класу "1" в експлуатацію".

7.10 Супроводження КСЗІ.

Виконання робіт з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

8. Порядок внесення змін і доповнень до технічного завдання

8.1 Зміни до затвердженого ТЗ на створення КСЗІ типової АС класу "1", необхідність внесення яких виявлена у процесі виконання робіт, повинні оформлюватися окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому рівні, що і основний документ.

8.2 Доповнення до ТЗ на створення КСЗІ повинно складатися з вступної частини і змінюваних розділів (пунктів). У вступній частині повинна бути визначена причина опрацювання доповнення. В змінюваних розділах (пунктах) повинні наводитись номери та зміст змінюваних, нових або пунктів що скасовуються.

9. Порядок проведення випробувань типової комплексної системи захисту інформації типової автоматизованої системи класу "1"

9.1 Випробування проводяться Головним виконавцем у відповідності до Типової програми і методик випробувань типової КСЗІ типової АС класу “1” (ПМВ).

9.2 Випробування типової КСЗІ повинні проводитися на об’єкті Замовника у відповідності до ПМВ.

9.3 Для проведення випробувань типової КСЗІ призначається комісія.

9.4 За результатами випробувань КСЗІ складається Акт приймання ІКС та КСЗІ у дослідну експлуатацію, до якого додаються протоколи випробувань.

9.5 Державна експертиза проводиться згідно до вимог Типової програми та методик проведення державної експертизи типової КСЗІ, яка погоджується з Державною службою спеціального зв’язку та захисту інформації України.

10. Дозвіл на здійснення обробки службової інформації в типової АС класу “1” надається керівником установи за наявності атестату відповідності на комплексну систему захисту інформації.

ДОДАТОК В

Про створення комплексної
системи захисту інформації
автоматизованої системи класу
“1” ПЕОМ №

Згідно з вимогами Закону України “Про захист інформації в інформаційно-комунікаційних системах”, Постанови Кабінету Міністрів України від 29.03.2006 року № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”, Типового технічного завдання на створення комплексної системи захисту інформації автоматизованої системи класу “1” .

1. Створити комплексну систему захисту інформації автоматизованої системи класу “1” ПЕОМ № 0000.

2. Відповідальним за створення комплексних систем захисту інформації АС класу “1” ПЕОМ № 0000_____ .

3. Для проведення обстеження ОІД, обстеження середовища функціонування інформаційно-телекомунікаційної системи, категорування ОІД призначити комісію.

4. 4. Для проведення інсталяції програмного забезпечення в АС класу “1” ПЕОМ № 0000 призначити комісію.

ДОДАТОК Г

ЗАТВЕРДЖУЮ

“___”_____ _____року

АКТ
категоріювання об’єкта електронно-обчислювальної техніки у приміщення.

1. Підстава для категоріювання – наказ
про створення КСЗІ АС класу “1” від 00.00.20___ № 00.

2. Вид категоріювання – чергове. Раніше встановлена
категорія – ЧЕТВЕРТА.

Попередній акт категоріювання інв. № 00.

3. На ОІД здійснюється обробка інформації за допомогою технічного засобу (ПЕОМ зав. № 0000000).

4. Вищий ступінь інформації з обмеженням доступу, що обробляється технічним засобом на об’єкті – “Для службового користування” що становлять службову інформацію
(ПСІ – 2017)) – ст.0000, ст.0000, ст.0000.

5. Умови розташування ОІД – ЗВИЧАЙНІ.

6. Встановлена категорія – ЧЕТВЕРТА.

Голова комісії:

0.0.0000000

Члени комісії:

“___”_____20___ року

ДОДАТОК Д

ЗАТВЕРДЖУЮ

“___” _____ _____року

М.П.

МОДЕЛЬ ПОРУШНИКА

для інформації з обмеженим доступом, що обробляється

в автоматизованій системі класу “1” .

Модель порушника - абстрактний формалізований опис дій порушника, який відображає його практичні та теоретичні можливості, час та місце дії і т.ін.

Метою порушника можуть бути:

М1 - мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

М2 - нанесення збитків шляхом знищення (пошкодження) матеріальних та інформаційних цінностей.

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу робочої станції засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами робочої станції. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

Р1 - перший рівень визначає найнижчий рівень можливостей проведення діалогу з робочою станцією — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

Р2 - другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

Р3 - третій рівень визначається можливістю управління функціонуванням робочою станцією, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

Р4 - четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів робочої станції, аж до включення до складу робочої станції власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має повну інформацію про робочі станції і КЗЗ.

По відношенню до робочої станції порушники можуть бути внутрішніми:

- посадові особи служби захисту інформації;

- користувачі, які мають повноваження щодо обробки службової інформації в АС класу “1”;

- інші посадові особи;

або зовнішніми:

- особи, що мають доступ до АС класу “1” або до приміщення де розташовано АС класу “1”.

За рівнем знань про робочі станції усіх порушників можна класифікувати як таких, що:

З1 - володіють інформацією про функціональні особливості робочих станцій, основні закономірності формування в них масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

З2 - володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

З3 - володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації серверів та робочих станцій;

З4 - володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

С1 - використовують засоби АС класу “1”;

С2 - використовують штатні телекомунікаційні засоби або недоліки проектування КСЗІ для реалізації спроб НСД;

С3 - використовують способи і засоби активного впливу на технологічне обладнання, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

Т1 - з одержанням доступу до серверів АС класу “1”;

Т2 - з одержанням доступу до робочих місць користувачів робочих станцій;

Т3 - з одержанням доступу до місць накопичення і зберігання даних;

Т4 - з одержанням доступу до засобів адміністрування серверів та робочих станцій і засобів керування КСЗІ.

Формальний опис моделі порушника наводиться в табл. 1.

Таблиця 1

№ з/п	Категорії осіб, з числа яких може бути порушник	Мета		Рівень можливостей				Рівень знань				Характер дій			Місце здійснення дій			
		М1	М2	Р1	Р2	Р3	Р4	З1	З2	З3	З4	С1	С2	С3	Т1	Т2	Т3	Т4
1.	Посадові особи служби захисту інформації	+	+	+	+	+	+	+	+	+	+	-	+	+	+	+	+	+

2.	Користувачі, які мають повноваження щодо обробки інформації в АС класу “1”	+	+	+	+	+	+	+	+	+	-	-	+	+	+	+	+	-
3.	Інші посадові особи	+	+	+	+	+	+	+	+	-	-	-	+	+	+	+	+	-
4.	Особи, що мають доступ до АС класу “1”	+	-	+	+	+	-	+	+	+	+	+	+	+	+	-	-	-

Керівник служби захисту інформації в ІТС Ініціали ПРІЗВИЩЕ

ДОДАТОК Е

ЗАТВЕРДЖУЮ
(посада керівника установи)

_____
(посада,підпис, ініціали, прізвище)
“___” _____20__ року
М.П.

АКТ
інсталяції програмного забезпечення
(АС зав. № _____)

“__” _____ 20__ року м. _____

1. Склад комісії
2. Перелік програмного забезпечення, що встановлено та джерела його надходження.
3. Перелік документів, які використовувались під час інсталяції (інструкції, настанови тощо)
4. Висновки комісії щодо результатів проведення інсталяції.

Голова (члени) комісії:_____
(посада, підписи)