Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Бобошка Олександра Володимировича*

академічної групи *125м-22з-1*

Спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка та дослідження системи управління інформаційної безпеки закладу фахової передвищої освіти*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н.,проф. Корнієнко В.І.			
розділів:				
спеціальний	д.т.н.,проф. Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Бобошку Олександру Володимировичу*** **академічної групи** ***125м-22з-1***
(прізвище, ім'я, по батькові) (шифр)

Спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка та дослідження системи управління інформаційної безпеки закладу фахової передвищої освіти***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів побудови СУІБ, а також принципів та підходів до створення політик інформаційної безпеки	03.09.2023 – 10.10.2023
Розділ 2	Розробка та дослідження СУІБ закладу фахової передвищої освіти	11.10.2023 – 24.11.2023
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень	25.11.2023 – 04.12.2023

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Бобошко О.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 8 рис., 13 табл., 4 додатки, 11 джерел.

Об'єкт дослідження є забезпечення інформаційної безпеки закладу фахової передвищої освіти.

Предметом дослідження є організація управління інформаційною безпекою закладу фахової передвищої освіти в сучасних умовах України.

Метою дослідження є процес побудови системи управління інформаційною безпекою ЗФПО.

Методи розробки: аналіз існуючих підходів та стандартів в побудові системи управління інформаційною безпекою, побудова системи управління інформаційною безпекою на базі Фахового коледжу ракетно-космічного машинобудування Дніпровського Національного університету імені Олеся Гончара.

У першому розділі проведено аналіз стандартів, принципів та підходів у побудові СУІБ, визначено актуальність та постановка задачі.

У спеціальній частині наведено опис інформаційної системи коледжу, який потребує впровадження системи управління інформаційною безпекою, наведено модель управління, класифікація загроз інформаційної безпеки закладу фахової передвищої освіти, організаційна структура системи забезпечення інформаційної безпеки закладу фахової передвищої освіти.

В економічному розділі визначено економічну доцільність розробки та впровадження системи управління інформаційною безпекою, а також проведено розрахунок витрат та економічний ефект.

Результати дослідження можуть бути застосовані при розробці системи управління інформаційною безпекою у будь-якому закладі фахової передвищої освіти.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЗАКЛАД ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

ABSTRACT

Explanatory note: 87 p., 8 fig., 13 tables, 4 appendices, 11 sources.

The object of the research is to ensure the information security of an institution of higher vocational education.

The subject of the research is the organization of information security management in the institution of higher vocational education in modern conditions in Ukraine.

The aim of the research is the process of constructing an information security management system for the institution.

Development methods: analysis of existing approaches and standards in the construction of information security management systems, construction of an information security management system based on the vocational college of rocket and space engineering of Dnipro National University named after Oles Honchar.

The first chapter analyzes the standards, principles, and approaches in the construction of ISMS, defines the relevance and sets the task.

In the special part, a description of the college's information system is provided, which requires the implementation of an information security management system. It includes a management model, classification of threats to the information security of the institution of higher vocational education, organizational structure of the information security provision system for the institution of higher vocational education.

The economic section determines the economic feasibility of developing and implementing an information security management system, as well as calculates the costs and economic effect.

The research results can be applied in the development of an information security management system in any institution of higher vocational education.

Keywords: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, INSTITUTION OF HIGHER VOCATIONAL EDUCATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗФПО	-	заклад фахової передвищої освіти
ІБ	-	інформаційна безпека
ІСУ	-	інформаційна система управління
СУІБ	-	система управління інформаційною безпекою
СЗІБ	-	системи забезпечення інформаційної безпеки
ТЗІ	-	технічний захист інформації
УІБ	-	управління інформаційною безпекою
ФКРКМ	-	Фаховий коледж ракетно-космічного машинобудування Дніпровського Національного Університету імені Олеся Гончара

ЗМІСТ

ВСТУП

Актуальність теми. Під інформаційною безпекою, згідно зі стандартами ISO, розуміють цілий комплекс засобів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Останнім часом все чіткіше стає помітний деякий перекіс: кажучи про інформаційну безпеку, в першу чергу мають на увазі захист від вірусів і хакерів. Але якщо попросити фахівців з безпеки розповісти про те, що їх хвилює, то найбільше занепокоєння викликають дії інсайдерів. Так, за даними досліджень, збиток від необережних і неправомірних дій співробітників в кілька разів перевищує за обсягом заподіяної шкоди збиток від дії вірусів, «хакерських» атак тощо. І незважаючи на те, що кількість інцидентів з вини зовнішніх і внутрішніх порушників спокою можна порівняти, у внутрішнього порушника, особливо якщо його дії свідомі, а не є помилкою, стимулів може бути більше: від банальної образи до матеріальної вигоди. А можливостей у нього набагато більше: він вже є легальним користувачем мережі, має доступ в тому числі й до конфіденційних ресурсів організації, може користуватися корпоративними додатками і даними в них на законних підставах.

Для освітнього середовища проблема є ширшою: обмеження доступу здобувачів освіти до інформації, яка може негативно впливати на їх формування та розвиток, тобто від негативної пропаганду різноманітного спрямування. Крім того, ще слабко усвідомлюється та частина проблеми, яка пов'язана з комунікацією в соціальних мережах, які сьогодні все частіше підмінюють живу спільноту. У віртуальному просторі діють абсолютно інші правила, де особистість з незміцнілою психікою не може ефективно протистояти загрозам. І сьогодні саме цей фактор починає виходити на перші ролі в забезпеченні інформаційної безпеки в її широкому розумінні: не лише технічній, але й в когнітивній сфері в усій її повноті.

Саме тому досить актуальним є питання побудови системи управління інформаційною безпекою, щоб урегулювати інформаційні потоки в ЗФПО та контролювати розповсюдження інформації в закладі.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

- сформулювати основні вимоги щодо побудови системи управління інформаційної безпекою ЗФПО,
- проаналізувати існуючий методичні матеріали щодо розробки і провести дослідження досвіду щодо впровадження систем управління інформаційною безпекою,
- розробити рекомендації щодо вдосконалення процесів розробки та впровадження системи управління інформаційною безпекою.

Об'єкт дослідження є забезпечення інформаційної безпеки закладу фахової передвищої освіти.

Предметом дослідження є організація управління інформаційною безпекою закладу фахової передвищої освіти в сучасних умовах України.

Метою дослідження є процес побудови системи управління інформаційною безпекою ЗФПО.

Методи розробки: аналіз існуючих підходів та стандартів побудови системи управління інформаційною безпекою, побудова системи управління інформаційною безпекою на базі Фахового коледжу ракетно-космічного машинобудування Дніпровського національного університету імені Олеся Гончара.

Результати дослідження можуть бути застосовані при розробці системи управління інформаційною безпекою у будь-якому закладі фахової передвищої освіти. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу ЗФПО у відповідності до можливостей та ресурсів.

1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Актуальність питання інформаційної безпеки в ЗФПО

Сучасні освітні установи широко використовують інформаційні технології для ведення журналів, контролю успішності, адміністративно-господарської діяльності тощо. На жаль, інформаційні системи, які використовуються у ЗФПО, в більшості випадків не відповідають навіть мінімальним вимогам, що пред'являються до безпечних систем.

Переважна більшість інформаційних систем не проходить жодної сертифікації, стандартизації, створюються буквально "на коліні" низько кваліфікованими розробниками, дуже часто на основі застарілих рішень. Перераховуючи проблеми, характерні для таких інформаційних систем, можна відзначити:

- Використання різноманітних та застарілих небезпечних платформ. Вразливості в інформаційних системах, базах даних та інших засобах інформаційних технологій регулярно виявляються, і будь-яка застаріла платформа повинна розглядатися як завідомо небезпечна, якщо не здійснені заходи з усунення цих проблем. У багатьох випадках інформаційні системи не пов'язані між собою, використовують різні платформи, що значно ускладнює їхнє використання та підтримку.
- Відсутність стандартизації. Незважаючи на зусилля створити уніфіковані інформаційно-технічні рішення, більшість навчальних закладів використовують ті рішення, які знаходяться під рукою.
- Використання публічного відкритого з'єднання. Будь-яка інформаційна система, яка претендує на безпеку, повинна організовувати передачу даних з використанням зашифрованих з'єднань за замовчуванням для уникнення перехоплення даних.

- Відсутність практики регулярного аудиту безпеки. Без постійної перевірки та виявлення потенційних проблем навіть якісно спроєктовані інформаційні системи можуть стати небезпечними при виявленні нових видів вразливостей.
- Низька кваліфікація обслуговуючого персоналу або відсутність посади фахівця з підтримки інформаційних систем взагалі. Якісна підтримка інформаційних систем вимагає регулярного моніторингу їхньої роботи.
- Використання піратського програмного забезпечення. Багато "взламаних" програм можуть містити троянський код, який полегшує проникнення в інформаційні системи. Крім того, піратське програмне забезпечення часто виключає можливість його оновлення, що не дозволяє протистояти новим загрозам.
- Недостатнє фінансування. Ця проблема є коренем всіх вищезазначених.

  Для вирішення усіх описаних проблем можна підходити на різних рівнях.
- Слід відзначити ще один фактор, який серйозно послаблює інформаційну безпеку, фактично анулюючи всі зусилля технічних служб. Йдеться про політику розповсюдження і зміни реквізитів доступу до інформаційних систем. Це не лише проблема освітніх установ, вона, на жаль, загальновизнана. При створенні інформаційного середовища в ЗФПО фактор політики управління реквізитами доступу, як правило, взагалі не враховується: паролі поширюються відкрито, не змінюються протягом багатьох років, часто їх знають студенти, які, не секрет, вміють користуватися сучасними інформаційними технологіями значно краще, ніж їхні батьки. Цей канал витоку, за статистикою, є основним, і закрити його в найближчому майбутньому не видається можливим. Немає сенсу витрачати зусилля хакерського спрямування для взлому пароля, якщо його легко можна вгадати, володіючи мінімумом інформації про користувача.

Незважаючи на те, що ми говоримо про елементарні правила інформаційної гігієни – навіть не безпеки – переважна більшість користувачів не має про це жодного уявлення. Проте ця проблема стає системною: якщо людина не знайома з

такими елементарними правилами інформаційної гігієни, вона з великою ймовірністю може стати жертвою шахраїв у майбутньому.

Розширений курс інформаційної безпеки зі всіма вказаними вище порушеними питаннями був би занадто обширним, але його основи можуть і мають включатися в програми підвищення кваліфікації персоналу ЗФПО, особливо з урахуванням того, що сучасний світ просто пронизаний інформаційними технологіями на всіх рівнях за вибухово низьким рівнем розуміння ризиків їх використання звичайним користувачем.

Оптимальним варіантом вирішення цих проблем могло б стати розроблення єдиної платформи для всіх освітніх установ і її централізована віддалена підтримка висококваліфікованими спеціалістами, які мають необхідні знання у сфері забезпечення безпеки інформаційних систем. Однак такий варіант можливий лише у далекій перспективі і виглядає ідеалістичним. Ще одним напрямком щодо забезпечення інформаційної безпеки технологічної інфраструктури є проведення регулярного аудиту систем, який може здійснюватися зовнішніми фахівцями. Однак, на практиці всі проблеми, що виникають, заклади освіти змушені вирішувати самостійно.

Питання управління інформаційною безпекою (ІБ) в закладах фахової передвищої освіти має велику актуальність і важливість, оскільки ці установи зберігають та обробляють значну кількість чутливої інформації. Ось деякі аспекти, які підкреслюють актуальність цього питання:

1) *Конфіденційність даних:* Заклади фахової передвищої освіти зберігають конфіденційну інформацію стосовно студентів, викладачів, досліджень та інших аспектів діяльності. Збереження конфіденційності є важливим елементом забезпечення довіри та дотримання законодавства.

2) *Доступність систем.* Управління інформаційною безпекою також стосується забезпечення доступності інформаційних ресурсів для студентів, викладачів та адміністративного персоналу. Запобігання відмовам, атакам та іншим загрозам забезпечує неперервну роботу систем.

3) *Освітні інформаційні ресурси.* Управління інформаційною безпекою також стосується надання доступу до освітніх ресурсів та платформ. Забезпечення доступності та захисту від несанкціонованого доступу до цих ресурсів впливає на якість навчання.

4) *Дотримання законодавства:* Заклади фахової передвищої освіти повинні відповідати ряду законодавчих вимог щодо захисту особистих даних. Недотримання цих вимог може призвести до санкцій та штрафів.

5) *Етичні питання*. Збереження етичних стандартів та запобігання порушень етики у роботі з інформацією є важливим аспектом управління інформаційною безпекою, особливо в освітньому середовищі. Управління інформаційною безпекою впливає на рівень довіри студентів, викладачів та інших зацікавлених сторін до установи. Заходи забезпечення безпеки допомагають підтримувати довіру до обробки особистих даних та конфіденційної інформації.

6) *Запобігання інцидентам безпеки.* Високий рівень усвідомленості та підготовки з управління інформаційною безпекою може допомогти запобігти інцидентів безпеки, таких як кібератаки, витоки даних та інші загрози.

7) *Соціальна інженерія та обізнаність персоналу*. Забезпечення безпеки також передбачає навчання персоналу та студентів з питань інформаційної безпеки для запобігання соціальному інжинірингу та іншим соціальним загрозам.

8) *Фільтрація небажаної інформації*. Ця група загроз безпосередньо пов'язана із протидією екстремістській ідеології, але не обмежується лише нею. При розгляді загроз доступу до небажаної інформації слід також враховувати питання поширення порнографії, провокаційних матеріалів, пропаганди наркотиків і алкоголю тощо.

9) *Проблеми регулювання використання соціальних мереж*. Саме в цій сфері здійснюється активний тиск на студентів, загрози залякування, а також відносно новий феномен кібербулінгу.

10) *Кібертероризм*. Незважаючи на те, що ця група загроз перебуває під контролем відповідних силових відомств, частково вона може розвиватися і на рівні закладів освіти. Створення безпечного інформаційно-технологічного середовища серйозно ускладнює можливі кібератаки на об'єкти освіти, які можуть призвести до

порушення функціонування управлінських автоматизованих систем і подальшого пошкодження інфраструктури. Слід відзначити, однак, що ця група загроз залишається поки що переважно гіпотетичною, оскільки заклади освіти через низьку їхню насиченість автоматизованими управлінськими системами не розглядаються як пріоритетні цілі для кібератак.

Враховуючи ці аспекти, заклади фахової передвищої освіти повинні активно розвивати та впроваджувати стратегії управління інформаційною безпекою для захисту своєї інформації та забезпечення безпеки всього освітнього процесу. У зв'язку з вищевикладеним метою роботи є створення системи управління інформаційною безпекою ЗФПО.

1.2 Ціль впровадження СУІБ.

Основною ціллю впровадження системи інформаційної безпеки (ІБ) у закладу ФПО є забезпечення конфіденційності, цілісності та доступності інформації. Це часто називається "трьома стовпами інформаційної безпеки" або принципами CIA:

Конфіденційність (Confidentiality): Гарантування, що інформація доступна лише тим, хто має на це право. Іншими словами, це забезпечення захисту інформації від несанкціонованого доступу. Конфіденційність – це один з основних принципів інформаційної безпеки, який визначає, що інформація має бути доступною та використовуватися тільки тим особам або системам, які мають на це відповідні права чи дозволи.

Основні аспекти конфіденційності включають:

- Захист від несанкціонованого доступу: Гарантування, що інформація залишається доступною лише тим особам чи системам, які мають право на її перегляд або використання.
- Шифрування: Застосування криптографічних методів для перетворення інформації таким чином, щоб тільки особи, які мають відповідний ключ, могли розшифрувати та отримати доступ до неї.

- Контроль доступу: Використання систем контролю доступу для регулювання та обмеження прав доступу до різних ресурсів та інформації.
- Управління ідентифікацією та аутентифікацією: Визначення осіб чи систем та встановлення їхньої ідентичності для надання або відмови у доступі відповідно до встановлених політик.
- Фізична безпека: Заходи безпеки для захисту фізичного доступу до інформаційних ресурсів, таких як захищені приміщення, замки, картки доступу тощо.

Конфіденційність особливо важлива для захисту конфіденційної інформації, такої як особисті дані, комерційні та бізнес-секрети, медична інформація та інші конфіденційні ресурси від несанкціонованого доступу та використання.

Цілісність (Integrity): Забезпечення того, щоб інформація залишалася недоторканною та не змінювалася несанкціоновано. Це означає запобігання несанкціонованим змінам або втраті інформації. Цілісність можна розділити на статичну та динамічну. Статична цілісність в контексті інформаційної безпеки вказує на стабільність та непорушність інформації на певному етапі часу або в конкретному стані системи. Це означає, що дані або система залишаються недоторканими і не зазнають змін або втрат у певний період часу, не враховуючи динамічних факторів.

Статична цілісність може бути забезпечена різними методами та технологіями, включаючи:

- Хеш-суми (Hash Functions): Використання алгоритмів хешування для створення фіксованої довжини "хеш-суми" для файлу або даних. Будь-яка зміна в файлах призводить до зміни хеш-суми, що дозволяє виявити неправомірні зміни.
- Цифрові підписи (Digital Signatures): Використання криптографічних методів для створення цифрових підписів, які можна перевірити для забезпечення автентичності та цілісності даних.
- Захист від запису (Write Protection): Застосування прав доступу для об'єктів або даних, щоб унеможливити їхню зміну чи перезапис.

- Системи контролю версій (Version Control Systems): Використання систем, які ведуть історію змін файлів і можуть відновлювати попередні версії у випадку порушень цілісності.
- Фізична безпека: Захист фізичного доступу до обладнання та інфраструктури, що забезпечує стабільність системи.

Статична цілісність важлива для забезпечення стабільності та впевненості в тому, що дані або система залишаються непошкодженими відповідно до визначених стандартів і вимог безпеки. Однак, для вирішення комплексних викликів інформаційної безпеки, часто використовують і динамічні заходи безпеки для виявлення та реагування на нові загрози.

Динамічна цілісність в контексті інформаційної безпеки означає здатність системи або даних залишатися цілісними та недоторканими в умовах динамічних змін або атак. Динамічність може включати в себе зміни у складі системи, відновлення після інцидентів, а також застосування оновлень та змін у середовищі, що змінюється.

В інформаційній безпеці концепція динамічної цілісності підкреслює потребу в ефективних заходах безпеки, які дозволяють системі або даним залишатися недоторканими і функціональними, навіть коли змінюється середовище або виникають нові загрози.

Для досягнення динамічної цілісності можуть використовуватися такі підходи та технології:

- Системи виявлення вторгнень (IDS): Вони моніторять мережевий трафік і системні активності для виявлення аномальних або підозрілих змін.
- Системи відновлення після інциденту (Incident Response Systems): Розробка та впровадження планів відновлення, щоб систему можна було якнайшвидше відновити після інцидентів.
- Автоматизовані системи оновлення та конфігурації: Застосування автоматизованих інструментів для оновлення програмного забезпечення та конфігурації систем, забезпечення відсутності вразливостей.

- Безпека "за замовчуванням" (Security by Default): Конфігурування системи так, щоб вона була безпечною за замовчуванням, навіть до внесення змін або додавання нових елементів.
- Регулярні аудити та оцінки ризиків: Проведення регулярних оглядів системи для виявлення можливих загроз і оновлення стратегій безпеки на основі останніх ризиків.

Динамічна цілісність є важливим аспектом забезпечення стійкості та безпеки інформаційних систем у змінних умовах діяльності та еволюції загроз.

Доступність (Availability): Забезпечення доступу до інформації для тих, хто має на це право, коли це необхідно. Це включає заходи для запобігання втратам доступу до інформації через різні інциденти. Доступність в контексті інформаційної безпеки визначається як забезпечення того, щоб інформаційні ресурси, системи та дані були доступними для використання користувачами або системами, якщо це необхідно та визначено відповідно до встановлених стандартів та вимог.

Ключові аспекти доступності включають:

- Запобігання втратам сервісу: Забезпечення того, щоб система чи сервіс був доступний для користувачів у необхідний час із прийнятною продуктивністю, не допускаючи значущих перерв або втрати доступу.
- Мінімізація впливу відмов: Використання заходів, щоб зменшити можливість виникнення відмов та мінімізувати їхній вплив на доступність системи.
- Забезпечення відновлення після інцидентів: Використання методів відновлення після інцидентів, таких як резервне копіювання, щоб швидко відновити доступність після втрати даних чи системної відмови.
- Моніторинг та управління ресурсами: Систематичний моніторинг ресурсів для виявлення можливих проблем, а також ефективне управління ресурсами для оптимізації доступності.
- Заходи для захисту від відмов сервісу (Denial of Service, DoS): Розробка та впровадження заходів безпеки, щоб убезпечити систему від атак, спрямованих на припинення її нормальної роботи.

Доступність є важливим аспектом для бізнес-операцій, оскільки недоступність може вплинути на продуктивність, клієнтське обслуговування та інші ключові аспекти діяльності.

1.3 Вимоги міжнародних стандартів щодо розробки системи управління інформаційною безпекою.

Найбільш поширеним і загальновизнаним у світі збіркою рекомендацій в сфері захисту інформації є стандарт ISO / IEC 27001.

ISO/IEC 27001 є міжнародним стандартом, що встановлює вимоги до систем управління інформаційною безпекою. Цей стандарт розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC).

Основна мета ISO/IEC 27001 – забезпечити ефективний управлінський контроль над інформаційною безпекою в організації. Це включає в себе встановлення системи управління, ідентифікацію ризиків і прийняття заходів для їх зменшення чи управління.

Отримання сертифікату відповідності за ISO/IEC 27001 свідчить про те, що організація встановила ефективну систему управління інформаційною безпекою та дотримується встановлених стандартом вимог.

Стандарт ISO/IEC 27001 по праву вважається найбільш концептуальним і комплексним. Його історія (Рис.1.1) почалася в 80-х роках минулого століття, коли Центр комп'ютерної безпеки Департаменту торгівлі і промисловості Великобританії опублікував рекомендації DTI CCSC User's Code of Practice.

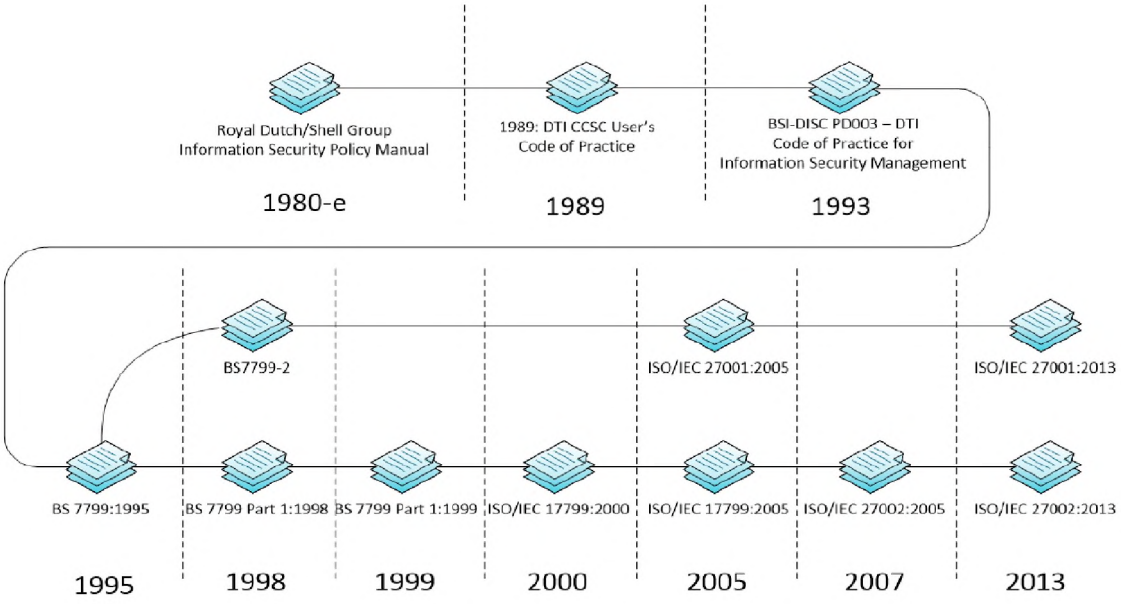

Рис. 1.1. Хронологія розвитку стандарту ISO/IEC 27001

В даний час серія 27xxx містить більше 30 стандартів з різних напрямків системи управління інформаційної безпеки (СУІБ), починаючи з рівня стратегічного управління і контролю СУІБ і закінчуючи технічними рекомендаціями щодо застосування окремих програмно-технічних і організаційних заходів захисту інформації. Всі ці стандарти можна розділити на кілька груп (рис. 1.2).

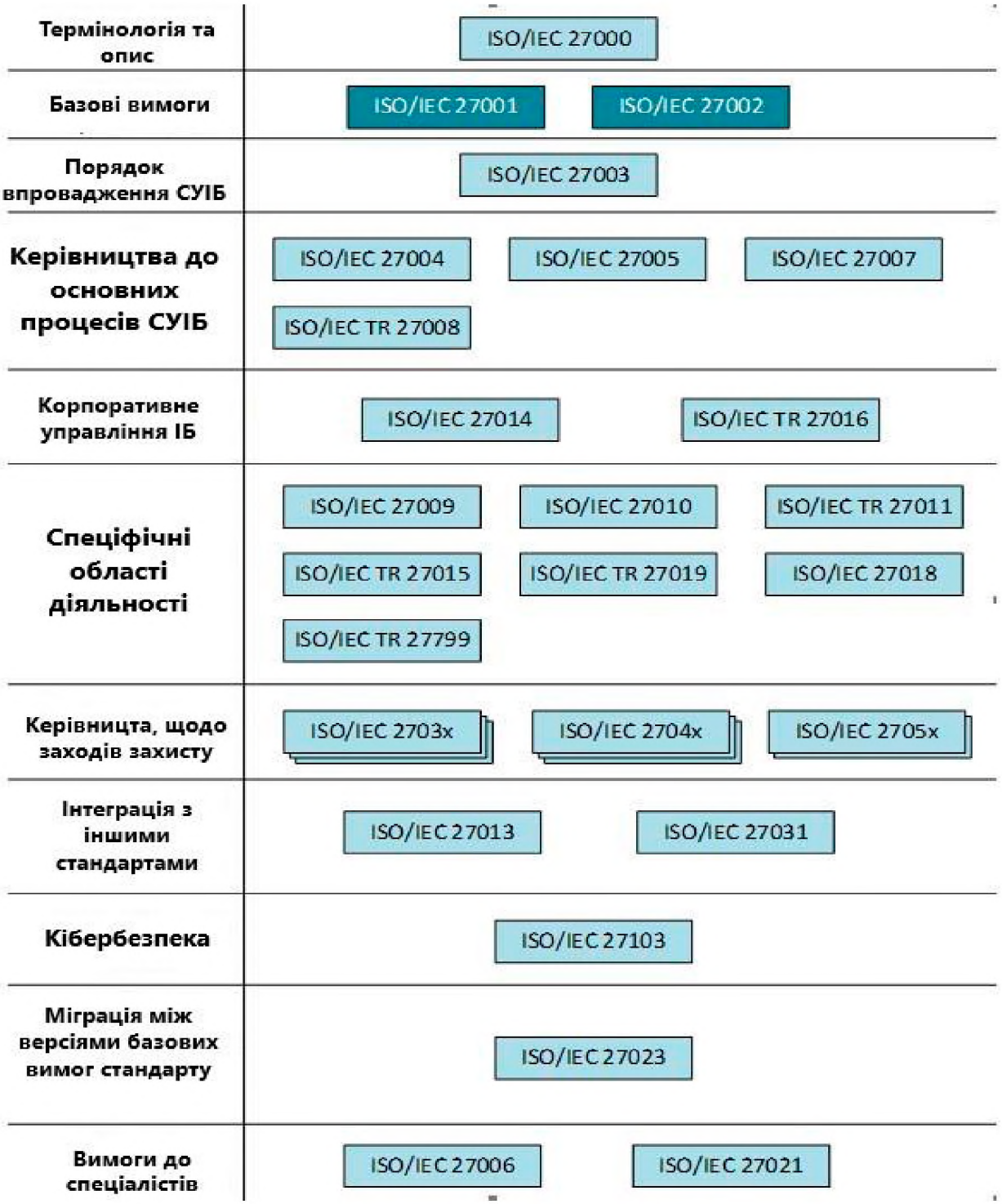

Рис. 1.2. Групування стандартів серії 27xxx

Підхід до управління інформаційною безпекою в даний час визначається двома взаємопов'язаними стандартами: ISO / IEC 27001 та ISO / IEC 27002 (рис. 1.3).

Рис. 1.3. Управління інформаційною безпекою

Основну роль тут відіграє стандарт ISO / IEC 27001, який містить рекомендації щодо менеджменту ІБ в організації на основі широко використовуваного в корпоративному середовищі циклу управління якістю PDCA (Plan, Do, Check, Act). Стандарт ISO / IEC 27002 носить скоріше довідковий характер, описуючи набір можливих заходів захисту інформації, з яких організація може вибрати необхідні саме їй.

Стандарт ISO / IEC 27001 дає рекомендації щодо функціонування СУІБ як комплексної системи, спрямованої на захист інформаційних активів організації від загроз і, отже, мінімізацію ризиків.

Основні етапи впровадження системи управління інформаційною безпекою за стандартом ISO/IEC 27001 включають:

1. Область застосування: Стандарт охоплює всі види організацій і встановлює універсальні принципи, які можуть бути застосовані для будь-якої форми і розміру організації.

2. Керівництво: Вимагає від керівництва встановлення політики інформаційної безпеки та активної участі в управлінні інформаційною безпекою.

3. Оцінка ризиків: Визначає необхідність проведення оцінки ризиків та впровадження заходів для їх управління.

4. Заходи безпеки: Встановлює необхідність впровадження технічних та організаційних заходів для забезпечення інформаційної безпеки.

5. Моніторинг та оцінка: Вимагає впровадження моніторингу та оцінки ефективності СУІБ, а також постійного вдосконалення.

6. Документація: Стандарт визначає необхідність документування політики інформаційної безпеки, процедур та інших важливих аспектів управління інформаційною безпекою.

Таким чином, пропонований підхід дозволяє застосовувати стандарт для реалізації СУІБ в організаціях будь-якого масштабу і рівня нормативної зарегульованості.

Відзначимо також, що ISO / IEC 27001 сумісний з іншими стандартами систем менеджменту якості, такими як ISO 9001, ISO 14000, ISO 31000, ISO / IEC 38500, ISO / IEC 20000, ISO / IEC 22301 та ін. Це дозволяє використовувати єдиний підхід і принципи, загальну термінологію, реалізувати інтегровані процеси за напрямками контролю якості продукції, що випускається, охорони навколишнього середовища, стратегічного управління та управління IT-сервісами, забезпечення безперервності діяльності організації, і, нарешті, інформаційної безпеки. Що, в свою чергу, дає можливість побудувати структуровану і прозору систему менеджменту організації і підвищити загальну ефективність відповідних процесів

1.4 Основні процеси управління інформаційною безпекою.

З точки зору цільового призначення процеси ІБ в організації класифікуються як процеси забезпечення та процеси управління. Процеси забезпечення ІБ призначені для реалізації безпосередніх організаційних і технічних функцій захисту активів компанії (технічних засобів, програмного забезпечення та інформаційних

активів). Процеси управління ІБ призначені для реалізації керуючих дій щодо системи забезпечення ІБ (СЗІБ).

Серед основних процесів управління інформаційною безпекою можна виділити наступні:

- підтримка в актуальному стані документаційного забезпечення ІБ;
- ідентифікація та класифікація активів компанії (об'єктів захисту);
- оцінка ризиків ІБ;
- робота з персоналом з питань ІБ;
- управління інцидентами ІБ;
- оцінка відповідності вимогам власних політик ІБ і вимогам регуляторів в області ІБ і ін.

Необхідно акцентувати увагу на тому, що забезпечення інформаційної безпеки ЗФПО – це не разова акція, а безперервна діяльність з планування, реалізації, вимірювання та вдосконалення процесів забезпечення і управління ІБ. Впровадження процесного підходу до управління інформаційною безпекою в умовах обмеженого штату підрозділів ІБ ускладнює створення, впровадження і підтримку СУІБ, особливо для ЗФПО.

Зокрема, видаються проблематичними здійснення і підтримка в актуальному стані результатів класифікації об'єктів захисту та оцінки ризиків ІБ без засобів автоматизації, враховуючи складність інформаційної інфраструктури, велику кількість прикладних систем, де обробляється інформація обмеженого доступу, великий перелік критичних активів, які підлягають захисту. Або ж, наприклад, впровадження і функціонування СУІБ з урахуванням процесного підходу вимагає обігу всередині системи значного обсягу документів. Зазначені особливості обумовлюють необхідність використання засобів автоматизації для підтримки процесів управління ІБ.

Аналіз ризиків – це основний рушійний процес СУІБ. Він виконується не тільки при створенні СУІБ, але і періодично при зміні бізнес-процесів організації і вимог з безпеки. Необхідно підібрати таку методику аналізу ризиків, яку можна було б використовувати з мінімальними змінами на постійній основі. Є два шляхи:

використовувати існуючі на ринку методики і інструментарій для оцінки ризиків або ж розробити свою власну методику, яка найкращим чином буде відповідати специфіці ЗФПО.

Типовими недоліками існуючих методик є:

- стандартний набір загроз і вразливостей, який часто неможливо змінити;
- прийняття в якості активів тільки програмно-технічних і інформаційних ресурсів – без розгляду людських ресурсів, сервісів і інших важливих ресурсів;
- загальна складність методики з точки зору її стійкого і повторюваного використання.

У процесі аналізу ризиків для кожного з активів або групи активів проводиться ідентифікація можливих загроз і вразливостей, оцінюється ймовірність реалізації кожної із загроз і, з урахуванням величини можливих збитків для активу, визначається величина ризику, що відображає критичність тієї чи іншої загрози. Необхідно відзначити, що відповідно до вимог Стандарту в процедурі аналізу ризиків повинні бути ідентифіковані критерії прийняття ризиків та прийнятні рівні ризику. Ці критерії повинні базуватися на досягненні стратегічних, організаційних і управлінських цілей організації. Керівництво використовує дані критерії, приймаючи рішення щодо прийняття контрзаходів для протидії виявленим ризикам. Якщо виявлений ризик не перевищує встановленого рівня, він є прийнятним, і подальші заходи щодо його обробки не проводяться. У разі ж, коли виявлений ризик перевищує прийнятний рівень критичності загрози, вище керівництво повинне прийняти одне з таких можливих рішень:

- зниження ризику до прийнятного рівня за допомогою застосування відповідних контрзаходів;
- прийняття ризику;
- уникнення ризику;
- переведення ризику в іншу область, наприклад, за допомогою його страхування.

Як відомо, в основі СУІБ лежить модель безперервного поліпшення якості, також відома як цикл Демінга або цикл PDCA. Звідси стають очевидні чотири процеси СУІБ (рис. 1.4):

- Процес планування, метою якого є виявлення, аналіз та проєктування способів управління ризиками інформаційної безпеки. При створенні цього процесу слід розробити методику категоріювання інформаційних активів і формальної оцінки ризиків на основі даних про актуальні для нашої інформаційної інфраструктури загрози і вразливості;
- Процес впровадження спланованих методів обробки ризиків, що описує процедуру запуску нового процесу забезпечення інформаційної безпеки або модернізації існуючого. Особливу увагу слід приділити опису ролей і обов'язків, а також плануванню впровадження;
- Процес моніторингу функціонуючих процесів СЗІБ.
- Процес вдосконалення заходів безпеки відповідно до результатів моніторингу, що дає можливість здійснити коригувальні та профілактичні дії.

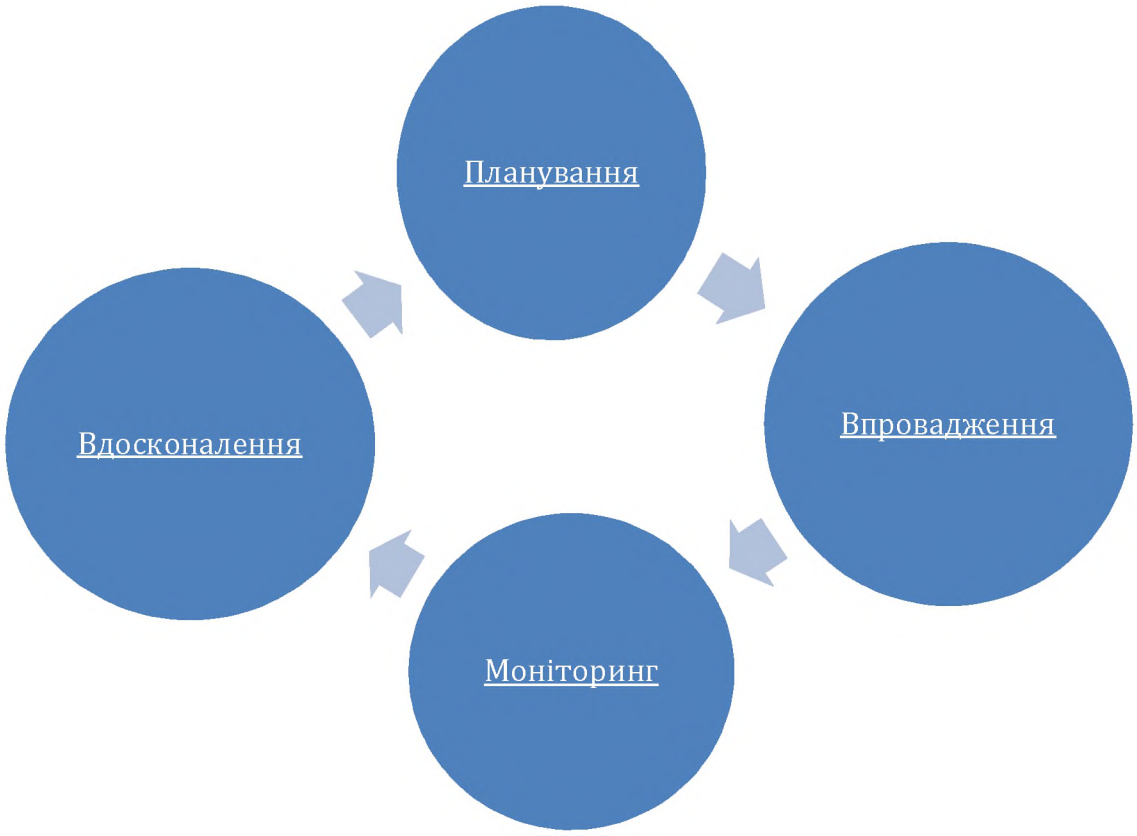

Рис. 1.4 Модель безперервного поліпшення якості

На практиці ці процеси описуються політикою управління інформаційною безпекою, яка є або частиною політики захисту інформації, або незалежним документом, представленим на найвищому рівні трирівневої структури бази даних регуляторних документів.

Для невеликих компаній, а також окремих підрозділів буде досить розробити методику формального аналізу інформаційних ризиків і передбачити процедуру перегляду процесів за результатами регулярного аудиту.

Таким чином, основними характеристиками управління інформаційною безпекою на сучасному етапі є комплексний підхід, оперативне прийняття управлінських рішень, персональна відповідальність.

Основними процесами управління інформаційною безпекою визначені: підтримка в актуальному стані документації ІБ, ідентифікація та класифікація активів, оцінка ризиків ІБ, робота з персоналом з питань ІБ, управління інцидентами ІБ, оцінка відповідності вимогам власних політик ІБ.

Не менш важливим фактором успішного впровадження СУІБ є створення робочої групи, відповідальної за впровадження СУІБ. До її складу мають увійти:

- керівництво ЗФПО;
- представники підрозділів, охоплених СУІБ.

1.5 Огляд моделей для побудови СУІБ.

Система управління інформаційною безпекою (СУІБ) використовує різні моделі для забезпечення конфіденційності, цілісності та доступності даних. Ось кілька ключових моделей, які можуть бути використані для побудови СУІБ

1) Модель CIA – це скорочення, яке в інформаційній безпеці вказує на три основні цінності чи аспекти, які повинні бути захищені в інформаційній системі чи організації. Під CIA розуміють такі терміни:

- Конфіденційність (Confidentiality): Забезпечення конфіденційності означає, що інформація повинна залишатися доступною тільки тим особам чи

системам, які мають на це право. Це включає контроль доступу та шифрування даних.

- Цілісність (Integrity): Цілісність передбачає, що інформація повинна залишатися непошкодженою та невідмінною. Тобто, дані не повинні бути змінені незаконно чи випадково, інакше, якщо зміни відбулися, це повинно бути виявлено та відновлено.
- Доступність (Availability): Доступність передбачає, що інформація та ресурси повинні бути доступними та використовуватися в той момент, коли вони потрібні. Це включає заходи для запобігання атакам, відновлення після інцидентів та забезпечення надійності систем.

Модель CIA є основоположною концепцією в інформаційній безпеці та використовується для розробки стратегій та заходів забезпечення безпеки інформації в різних сферах, включаючи комп'ютерні системи, мережі та організації.

2) **Модель DAD (Deny, Allow, Deny)**.

Модель DAD (Deny, Allow, Deny) може використовуватися в системах управління доступом (Access Control Systems). Ця модель представляє собою стратегію контролю доступу, де початкове відмовлення (Deny) є базовим рівнем доступу, за яким слідує дозвіл (Allow) і, в кінці кінців, знову відмовлення (Deny) на вищому рівні.

- Deny (Відмовити): Всі запити на доступ до ресурсу починаються з відмови. Це означає, що, якщо не існує явного дозволу на доступ, за замовчуванням доступ заборонений.
- Allow (Дозволити): Потім йде етап дозволу, де управління доступом дозволяє доступ до конкретних ресурсів, якщо у користувача або системи є відповідні права.
- Deny (Відмовити): Нарешті, на вищому рівні може бути правило відмови, яке перевизначить дозвіл на нижчому рівні. Таким чином, якщо у користувача було дозвіл на доступ, правило відмови на вищому рівні може його перевизначити.

Ця модель використовується для більш ретельного та гнучкого контролю доступу, дозволяючи адміністраторам більш детально визначити, які користувачі чи системи мають доступ до яких ресурсів.

3) **Модель RBAC (Role-Based Access Control)**.

Модель RBAC (Role-Based Access Control або модель контролю доступу на основі ролей) – це стратегія управління доступом, в якій призначення прав доступу відбувається на основі ролей, які визначаються в організації. Вона є однією з основних моделей управління доступом і широко використовується для забезпечення безпеки інформаційних систем та ресурсів.

Основні принципи моделі RBAC:

- Роль (Role): Ролі визначають функціональні обов'язки чи позиції в організації. Користувачі призначаються ролям, а ролі мають визначені права доступу.
- Права доступу (Permissions): Кожній ролі надаються конкретні права доступу, що визначають, які дії чи операції може виконати користувач, який належить до цієї ролі.
- Призначення ролей (Role Assignment): Процес призначення користувачам конкретних ролей на основі їхніх обов'язків або потреб.
- Авторизація (Authorization): Визначення, які конкретні дії дозволені користувачеві на основі його ролей та прав доступу.
- Аутентифікація (Authentication): Визначення і підтвердження ідентичності користувача, який намагається отримати доступ.

Переваги моделі RBAC включають простоту управління доступом, гнучкість та легкість адміністрування. Вона дозволяє ефективно регулювати права доступу в організації, спрощуючи управління забезпеченням безпеки.

4) **Модель Bell-LaPadula.**

Модель Bell-LaPadula є однією з основних моделей безпеки інформаційних систем та використовується для контролю доступу до конфіденційної інформації. Ця модель була розроблена в 1973 році Дейвідом Беллом і Леоном Ла Падулою, які працювали в області криптографії та безпеки.

Основні принципи Моделі Bell-LaPadula:

- Обов'язок нерозголошення (No Read Up): Забороняє користувачам читати інформацію вищого рівня безпеки, ніж у них встановлений рівень доступу.
- Обов'язок нерозповсюдження (No Write Down): Забороняє користувачам записувати інформацію нижчого рівня безпеки, ніж у них встановлений рівень доступу.
- Модель відсутності конфлікту інтересів (COI): Гарантує, що користувачі з різними рівнями доступу не можуть взаємодіяти таким чином, що порушує безпеку.

Ці принципи визначають, як інформація може бути доступна індивідам у системі та як нею можна маніпулювати. Модель Bell-LaPadula спрямована на запобігання втраті конфіденційності, забезпечуючи, що конфіденційна інформація не витікає до недозволених осіб.

Ця модель часто використовується в галузі військової, урядової та корпоративної безпеки, де важливо уникнути неправомірного доступу до конфіденційної інформації.

5) **Модель Biba**.

Модель Biba – це інша модель безпеки інформаційних систем, яка, так само як і модель Bell-LaPadula, розглядає питання контролю доступу до інформації. Ця модель була представлена Дейвідом Бібою в 1975 році і спрямована на забезпечення цілісності інформації.

Основні принципи Моделі Biba:

- Обов'язок чистоти (No Write Up): Забороняє користувачам запис або внесення змін до інформації вищого рівня безпеки, ніж встановлений у них рівень доступу.
- Обов'язок нерозголошення (No Read Down): Забороняє користувачам читати або отримувати інформацію нижчого рівня безпеки, ніж встановлений у них рівень доступу.
- Модель відсутності конфлікту інтересів (COI): Гарантує, що користувачі з різними рівнями доступу не можуть взаємодіяти таким чином, що порушує цілісність інформації.

Модель Biba спрямована на уникнення введення помилок чи змін у конфіденційні дані, що може впливати на їх цілісність. Вона часто застосовується в галузі фінансів, урядових структур, а також у будь-якому іншому контексті, де важлива надійність і цілісність інформації.

6) **Модель Clark-Wilson.**

Модель Clark-Wilson — це модель безпеки інформаційних систем, призначена для забезпечення цілісності даних. Вона була розроблена Девідом Кларком і Дейвідом Вільсоном і вперше представлена в 1987 році. Основний фокус цієї моделі – забезпечення і підтримка цілісності даних, що забороняє неправомірне або несанкціоноване їх модифікування.

Основні концепції Моделі Clark-Wilson:

- Інваріанти цілісності (Integrity Invariants): Модель визначає набір інваріантів цілісності, які повинні залишатися справжніми для системи в будь-який момент часу. Ці інваріанти обмежують доступ та зміну даних з метою збереження їхньої цілісності.
- Процес обслуговування (Transformation Procedures): Для зміни даних в моделі Clark-Wilson використовуються спеціальні процедури, відомі як процеси обслуговування. Ці процедури гарантують, що після зміни дані все ще відповідають інваріантам цілісності.
- Сертифікати (Certification): Важливою частиною моделі є процес сертифікації, який перевіряє, чи дотримуються дані визначених інваріантів цілісності. Це допомагає підтверджувати, що система залишається в безпечному стані.
- Обмеження доступу (Access Control): Модель обмежує доступ до даних та процедур, забезпечуючи, що тільки визначені процедури обслуговування можуть змінювати дані.

Модель Clark-Wilson широко використовується в області фінансів, банківської справи та інших областях, де важлива цілісність та відсутність неправомірного втручання в інформаційні ресурси.

7) **Модель Non-Interference**.

Модель Non-Interference (некерований вплив) – це концепція безпеки інформаційних систем, яка ставить за мету запобігання витоку конфіденційної інформації внаслідок дій внутрішніх суб'єктів або користувачів системи. Основна ідея полягає в тому, що користувачі на нижчому рівні безпеки не можуть впливати на конфіденційні дані на вищому рівні.

Основні принципи Моделі Non-Interference:

- Неінтерференція (Non-Interference): Система повинна забезпечити такий рівень ізоляції між різними рівнями безпеки, щоб дії користувачів на нижчому рівні не могли впливати на дані на вищому рівні.
- Відсутність витоків інформації (No Information Flow): Система має гарантувати, що конфіденційна інформація не просочується або не передається на рівень безпеки, який має менший рівень класифікації.
- Запобігання впливу (Prevention of Influence): Користувачі на нижчому рівні безпеки не повинні мати можливості впливати на роботу чи стан системи на вищому рівні безпеки.

Ця модель часто використовується в області військової, урядової та корпоративної безпеки, де важливо уникати витоків конфіденційної інформації та зберігати її в надійному стані. Модель Non-Interference допомагає підтримувати високий рівень безпеки в інформаційних системах, обмежуючи можливості несанкціонованого доступу і впливу.

Вибір конкретної моделі залежить від конкретних вимог і характеристик системи, а також від сфери застосування. Часто в СУІБ використовують комбінації різних моделей для комплексного захисту інформації

1.6 Принципи та підходи до створення політик інформаційної безпеки.

Існують різні принципи та підходи до створення політик інформаційної безпеки, які визначають стратегії та правила для забезпечення захисту інформації. Декілька типових принципів та підходів включають:

1) Модель найменшого доступу (Least Privilege):

Модель найменшого доступу (Least Privilege) є важливим принципом у сфері інформаційної безпеки. Основна ідея полягає в тому, щоб надавати користувачам або системним об'єктам лише ті права доступу, які є абсолютно необхідними для виконання їхніх конкретних обов'язків чи завдань. Кожен об'єкт повинен мати лише той рівень доступу, який необхідний для його роботи, і нічого більше.

Основні принципи моделі найменшого доступу включають:

- *Мінімізація привілеїв.* Користувачам або системним об'єктам призначаються тільки ті привілеї, які необхідні для їхньої діяльності.
- *Обмеження доступу.* Об'єкти мають доступ лише до ресурсів інформації або систем, які є необхідними для виконання їхніх завдань.
- *Принцип найменшої привілеї для адміністраторів.* Адміністраторам надається тільки той рівень доступу, який є абсолютно необхідним для виконання їхніх обов'язків. Вони не повинні мати більше привілеїв, ніж це необхідно.
- *Перевірка привілеїв.* Регулярно переглядаються та оновлюються права доступу для впевненості, що вони відповідають поточним потребам користувачів чи об'єктів системи.

Переваги моделі найменшого доступу включають зменшення ризиків, пов'язаних із несанкціонованим використанням привілеїв, обмеженням можливостей внутрішнього та зовнішнього вторгнення, а також полегшення адміністрування та управління правами доступу.

2) Модель найменшої функціональності (Least Functionality).

Модель найменшої функціональності (Least Functionality) вказує на підхід, коли система, програмне забезпечення або пристрій наділяються лише тими функціями, які абсолютно необхідні для їхнього основного призначення та ефективного функціонування. Забороняє користувачам використовувати будь-які функції чи послуги, які не є необхідними для виконання їхніх обов'язків. Цей принцип реалізується для мінімізації потенційних загроз безпеці, які можуть виникнути через надмірні функціональність або зайві можливості.

Основні ідеї найменшої функціональності включають:

- *Мінімізація атакованої поверхні*. Зменшення кількості можливостей і функцій, які можуть бути використані для здійснення атак.
- *Зменшення ризику.* Зниження загроз і ризиків шляхом видалення зайвих функцій або послуг.
- *Легше адміністрування та підтримка*. Зменшення складності управління та підтримки системи чи програмного забезпечення.
- *Максимальна фокусуваність на безпеці*. Концентрація лише на тих функціях, які є стратегічно важливими та безпечними.

3) Модель захисту всередині (Insider Threat Protection).

Модель захисту всередині – це стратегічний підхід до захисту інформації та ресурсів компанії від внутрішніх загроз. Вона спрямована на запобігання та виявлення можливих загроз з боку власних працівників, які мають доступ до конфіденційної інформації та ресурсів організації.

Основні аспекти моделі захисту всередині включають:

- *Виявлення аномалій.* Використання технологій для виявлення аномальних або непередбачених дій працівників, які можуть свідчити про небажану або зловмисну діяльність.
- *Моніторинг діяльності*. Систематичний моніторинг дій працівників та їхнього взаємодії з інформаційними ресурсами.
- *Політики та обмеження.* Встановлення політик безпеки, які обмежують доступ до конфіденційної інформації лише необхідним працівникам.
- *Навчання та обізнаність.* Проведення навчань для працівників з питань безпеки та досягнення розуміння щодо потенційних загроз.
- *Захист від втручання.* Використання технологій, що запобігають або ускладнюють несанкціоновану діяльність всередині мережі.
- *Аудит та аналіз.* Проведення систематичного аудиту та аналізу дій працівників для виявлення потенційно небезпечних ситуацій.
- *Відповідь на інциденти.* Розробка процедур та планів реагування на можливі загрози зсередини компанії.

Модель захисту всередині є важливою частиною стратегії інформаційної безпеки та дозволяє компаніям ефективніше впоратися з внутрішніми загрозами, щоб захистити свою конфіденційну інформацію та уникнути можливих втрат чи проблем.

4) Модель визначення правил (Rule-Based Policy).

Модель визначення правил (Rule-Based Policy) – це підхід до визначення політик безпеки, в якому встановлюються конкретні правила і обмеження для контролю доступу до ресурсів та забезпечення безпеки інформації в інформаційних системах.

Основні аспекти моделі визначення правил включають:

- *Правила доступу.* Визначення конкретних правил, які вказують, хто із користувачів або систем має доступ до конкретних ресурсів.
- *Умови виконання.* Встановлення умов, за яких правила стають активними або неактивними.
- *Авторизація.* Здійснення визначення прав доступу на основі заданих правил та умов.
- *Логіка визначення правил.* Використання логічних операцій (AND, OR, NOT) для визначення складних умов і обмежень.
- *Попередження та блокування.* Введення механізмів попередження або блокування доступу, якщо правила порушуються.
- *Аудит та моніторинг.* Забезпечення можливості ведення аудиту та моніторингу для виявлення подій, які порушують встановлені правила.
- *Зміна правил.* Можливість внесення змін до правил відповідно до змін в потребах організації чи змін в загрозах безпеці.
- *Масштабованість.* Здатність розширення та масштабування правил для врахування зростання ресурсів та обсягів даних.

Ця модель надає можливість деталізованого та гнучкого управління доступом на основі визначених правил і є популярним підходом в області інформаційної безпеки. Однак важливо враховувати, що успішна реалізація моделі визначення

правил вимагає уважного аналізу та управління правилами для забезпечення ефективної та безпечної роботи системи.

5) Модель ризик-орієнтованої політики (Risk-Based Policy).

Модель ризик-орієнтованої політики (Risk-Based Policy) - це підхід до визначення політик безпеки, який зосереджений на оцінці та управлінні ризиками в інформаційних системах. Замість того, щоб застосовувати стандартні правила для всіх користувачів чи ресурсів, ця модель визначає рівень ризику та встановлює політики відповідно до цього рівня.

Основні аспекти моделі ризик-орієнтованої політики включають:

- *Оцінка ризиків.* Систематичний аналіз і оцінка потенційних ризиків для інформаційних ресурсів та даних.
- *Класифікація ризиків.* Розподіл ризиків за категоріями, визначення їхнього впливу та ймовірності.
- *Визначення рівнів ризиків*. Встановлення порогових значень, які визначають рівні прийнятного ризику для організації.
- *Спрощення заходів захисту.* Налагодження заходів захисту та контролю відповідно до визначених рівнів ризиків.
- *Гнучкість політик.* Здатність адаптувати політики в залежності від змін у загрозах та збитках.
- *Пріоритизація заходів безпеки.* Визначення пріоритетів заходів безпеки на основі важливості та ризиків.
- *Контроль та моніторинг.* Забезпечення систематичного контролю та моніторингу ризиків для адаптації політик при необхідності.
- *Взаємодія з бізнес-процесами.* Інтеграція політик безпеки з бізнес-процесами для забезпечення спрощення та відповідності бізнес-цілям.

Модель ризик-орієнтованої політики дозволяє організаціям ефективно використовувати ресурси для захисту найбільш важливих та вразливих частин інформаційної інфраструктури, враховуючи конкретні ризики та потенційні втрати.

6) Модель контролю заходів (Compliance-Based Policy).

Модель контролю заходів – це підхід до визначення політик безпеки, який базується на вимогах та стандартах безпеки, що встановлюються зовнішніми агенціями чи організаційними стандартами. У цій моделі акцент робиться на виконанні конкретних нормативів та вимог щодо захисту інформації та ресурсів.

Основні аспекти моделі контролю заходів включають:

- *Встановлення стандартів безпеки.* Визначення набору правил, вимог і стандартів безпеки, які мають бути дотримані.
- *Внутрішні та зовнішні вимоги.* Урахування внутрішніх політик організації та зовнішніх стандартів, таких як регуляторні акти, законодавство чи стандарти галузі.
- *Аудит та перевірка відповідності.* Забезпечення процесів аудиту та перевірки, щоб переконатися, що усі вимоги та стандарти дотримуються.
- *Звітність та документація.* Ведення документації щодо виконання вимог, а також представлення звітів органам, що мають відношення до контролю заходів.
- *Санкції за порушення.* Встановлення санкцій або відповідальності за невиконання вимог та стандартів.
- *Постійна оновленість.* Адаптація політик та процедур для відповідності змінам у вимогах та стандартах.
- *Тренування та навчання персоналу.* Навчання персоналу щодо важливості та методів дотримання стандартів безпеки.
- *Моніторинг виконання.* Систематичний моніторинг дотримання політик та вимог за допомогою технічних та організаційних засобів.

Модель контролю заходів спрощує впровадження та визначення політик безпеки, оскільки базується на конкретних вимогах та стандартах, але також може вимагати значних ресурсів для забезпечення та підтримки відповідності.

7) Модель надійності (Assurance-Based Policy).

Модель надійності – це підхід до визначення політик безпеки, який зосереджений на забезпеченні надійності та впевненості у тому, що система безпеки діє так, як очікується, та виконує свої функції ефективно та безпечно.

Основні аспекти моделі надійності включають:

- *Визначення стандартів якості та надійності.* Встановлення конкретних стандартів та критеріїв для оцінки надійності системи.
- *Сертифікація та атестація.* Процес отримання сертифікатів або атестації, які підтверджують відповідність системи встановленим стандартам.
- *Аудит та ревізія.* Систематичні аудити та перевірки для переконання в тому, що політики безпеки та контрольні заходи відповідають стандартам.
- *Документування процесів.* Детальне документування всіх процесів, пов'язаних з надійністю системи.
- *Система управління якістю.* Впровадження системи управління якістю для забезпечення постійного вдосконалення та відповідності стандартам.
- *Тестування та верифікація.* Проведення тестів та верифікація, щоб переконатися в правильності та ефективності заходів безпеки.
- *Оновлення та підтримка.* Забезпечення постійного оновлення та підтримки системи для збереження відповідності стандартам надійності.
- *Постійна еволюція.* Систематична оцінка та оновлення політик та процедур для забезпечення найвищого рівня надійності.

Модель надійності покладається на проактивні заходи, спрямовані на забезпечення високого рівня довіри та впевненості у функціонуванні системи безпеки. Цей підхід особливо важливий в областях, де високий ступінь довіри та надійності є ключовими аспектами.

8) Дискреційна політика безпеки (DAC – Discretionary Access Control)

Дискреційна політика безпеки – це модель управління доступом в інформаційних системах, де власник ресурсу має право визначати, хто має доступ до цього ресурсу та які дозволи він має. У цій моделі доступ до об'єктів контролюється на рівні користувачів, а власник ресурсу може самостійно встановлювати, кому і в якому обсязі надається доступ.

Основні принципи дискреційної політики безпеки:

- *Власник ресурсу.* Власник (власники) ресурсу має (мають) повний контроль над доступом до свого ресурсу.

- *Дозволи та заборони*. Власник ресурсу встановлює, які конкретні користувачі чи групи користувачів мають доступ до ресурсу і які операції вони можуть виконувати.
- *Локальний контроль.* Контроль доступу реалізується на рівні окремих ресурсів, і власник ресурсу може встановлювати свої власні правила безпеки.
- *Гнучкість.* Модель дозволяє гнучко встановлювати правила безпеки, що робить її придатною для різних сценаріїв використання.

Основний недолік полягає в тому, що ця модель може бути менш ефективною в управлінні доступом для великих систем або в ситуаціях, де потрібно встановлювати однакові правила для багатьох користувачів.

9) Мандатна політика безпеки (MAC – Mandatory Access Control)

Мандатна політика безпеки – це модель управління доступом в інформаційних системах, де контроль над доступом до ресурсів здійснюється на основі формальних правил і обов'язкових мандатів, які встановлюються системним адміністратором чи адміністраторами безпеки. У цій моделі керівництво встановлює загальні правила доступу, яких обов'язково дотримуються усі користувачі та процеси системи.

Основні характеристики мандатної політики безпеки:

- *Централізований контроль.* Правила доступу визначаються централізовано адміністратором безпеки чи системним адміністратором і є обов'язковими для всіх користувачів.
- *Немає власника ресурсу.* У відміну від дискреційної політики безпеки, у мандатній моделі немає власника ресурсу, який може самостійно встановлювати правила доступу.
- *Мандати та класифікація.* Кожен суб'єкт та об'єкт у системі має мандат, який визначає рівень конфіденційності чи інших параметрів доступу. Об'єкти класифікуються, і суб'єкти мають доступ лише до тих об'єктів, які відповідають їхньому мандату.
- *Високий рівень безпеки.* Мандатна політика забезпечує високий рівень безпеки, оскільки вона обов'язкова для всіх користувачів і не допускає відхилення від встановлених правил.

- *Обмежена гнучкість.* Мандатна модель може бути менш гнучкою у порівнянні з дискреційною політикою, оскільки всі правила є обов'язковими і не піддаються зміні користувачем.

Мандатна політика безпеки часто використовується в системах, які вимагають високого рівня конфіденційності та контролю доступу, таких як військові системи, де важливо строго регламентувати доступ до ресурсів.

Ці моделі допомагають визначити рамки та принципи для розробки політик інформаційної безпеки, щоб забезпечити відповідний рівень захисту для організації.

10) Модель безпеки Microsoft.

Microsoft використовує модель безпеки, яка базується на кількох ключових принципах та фундаментальних підходах. Нижче розглянуті основні аспекти моделі безпеки Microsoft:

- *Принцип захисту від внутрішніх та зовнішніх загроз.* Microsoft вбудовує в свої продукти та сервіси механізми захисту від різних видів загроз, будь то віруси, зловмисний код або атаки з зовнішнього середовища.
- *Цикл розробки безпеки (SDL – Security Development Lifecycle).* SDL – це методологія, розроблена Microsoft для розробки безпечного програмного забезпечення. Вона включає у себе етапи визначення вимог, проєктування, реалізації, тестування та випуску.
- *Постійне оновлення та виправлення.* Microsoft регулярно випускає патчі та оновлення для своїх продуктів для усунення виявлених вразливостей та забезпечення стійкості до нових загроз.
- *Ідентифікація та автентифікація.* Microsoft розвиває та підтримує різноманітні механізми ідентифікації та автентифікації, включаючи різні методи багаторівневої аутентифікації.
- *Захист даних.* Послуги та продукти Microsoft надають інструменти для шифрування даних в спокої та під час передачі, контролю доступу та інші механізми захисту конфіденційності та цілісності інформації.
- *Моніторинг та виявлення загроз.* Вбудовані засоби моніторингу та виявлення аномалій допомагають вчасно виявляти та реагувати на потенційні загрози.

- *Всебічна оборона (Defense in Depth).* Майже всі продукти та сервіси Microsoft використовують стратегію всебічної оборони, що передбачає використання кількох шарів захисту для мінімізації ризиків.
- *Хмарні сервіси з безпеки.* Microsoft надає хмарні сервіси, такі як Microsoft 365 та Azure, і вбудовує в них різні засоби безпеки, включаючи управління правами, облік та аудит.

Ці принципи та підходи входять в комплексну модель безпеки Microsoft, яка постійно розвивається, щоб боротися із зростаючими загрозами в інформаційному середовищі.

11) Трирівнева модель політики безпеки.

Трирівнева модель політики безпеки – це концептуальна модель, яка визначає політику безпеки на трьох рівнях абстракції для забезпечення комплексного контролю та управління безпекою в інформаційних системах. Ці три рівні включають стратегічний, тактичний і технічний рівні.

Стратегічний рівень.

- Орієнтація на бізнес. Розглядається політика безпеки на високому рівні бізнесу. Визначаються стратегічні цілі та завдання організації щодо безпеки інформації.
- Управління ризиками. Визначаються і аналізуються потенційні загрози та ризики для інформаційної безпеки. Розробляються стратегії зменшення ризиків.

Тактичний рівень.

- Політики та стандарти. Визначення конкретних політик та стандартів, які повинні бути виконані для досягнення стратегічних цілей.
- Управління доступом. Розробка та впровадження стратегій контролю доступу до інформації для забезпечення конфіденційності, цілісності та доступності.

Технічний рівень.

- Технічні засоби безпеки. Визначення конкретних технічних засобів та заходів для реалізації політик та стандартів.

- Інцидентний менеджмент. Визначення та впровадження процедур виявлення, відповіді та відновлення від інцидентів безпеки.

Трирівнева модель політики безпеки дозволяє організаціям раціонально підходити до управління безпекою, забезпечуючи взаємодію між стратегічними цілями, тактичними положеннями та конкретними технічними рішеннями. Це допомагає створити комплексний підхід до безпеки, який враховує потреби бізнесу, технічні можливості та управлінські вимоги.

1.7 Порівняння принципів та підходів до створення політик ІБ.

В Таблиці 1.1 наведена інформація про порівняння принципів та підходів управління ризиками, які були розглянуті в попередньому розділі.

Таблиця 1.1 – Порівняння політик управління інформаційною безпекою

Модель	Переваги	Недоліки
найменшого доступу	Мінімізація ризиків Захист від внутрішніх загроз Зменшення атакованості Більша контрольованість Легше виявлення аномалій Забезпечення принципу необхідності Сприяння принципу неперетину Легше управління авторизацією Виконання вимог в регулятивних актах	Складність впровадження Можливі труднощі для адміністраторів Підвищений обсяг роботи при зміні ролей Виклики у визначенні необхідних прав доступу Вплив на продуктивність Вартість імплементації
найменшої функціональності	Зменшення атакованості Спрощений моніторинг та управління Менше вразливостей Легша адаптація до стандартів безпеки Зменшення ризиків пов'язаних з людським фактором Ефективна оборона	Обмежений зручністю використання Адміністративне ускладнення Потреба у великій увазі до деталей Можливість атак на інші частини системи Неадекватна реакція на зміни
захист всередині	Мінімізація ризиків Принцип найменших привілеїв Контроль доступу на основі контексту Зменшення поверхні атаки Можливість виявлення порушень Більша прозорість	Обмежена захищеність від зовнішніх загроз Неадекватна відповідь на нові загрози Внутрішні загрози та зловживання привілеями Помилки конфігурації та адміністративні вразливості Витратність на моніторинг та управління доступом Неспроможність у виявленні деяких загроз Обмежена готовність до зовнішніх атак Висока потреба у внутрішній координації та співпраці

Продовження таблиці 1.1

Модель	Переваги	Недоліки
визначення правил	Прозорість: Керованість Контроль доступу Автоматизація Захист від недбалості	Статичність Недостатня гнучкість Системні обмеження Потенційна неефективність Низька реактивність
ризик-орієнтованої політики	Гнучкість Спрямованість на пріоритети Інтеграція в бізнес-процеси Орієнтованість на реальні загрози Постійна оцінка ризиків	Суб'єктивність оцінки ризиків Недостатній рівень усвідомлення ризиків Складність визначення вагомості ризиків Приховані ризики Необхідність постійного моніторингу Складність керування ризиками великої кількості Вартість і ресурси Спроби зловживання
контролю заходів	Спрощення управління безпекою Конкретні заходи для захисту Спрямованість на конкретні загрози Ефективність та точність заходів Поліпшення виконання стандартів	Реактивний характер Залежність від точкових рішень Важкість визначення всіх можливих загроз Високі витрати на обслуговування Неефективність у визначенні внутрішніх загроз Обмежений погляд на безпеку
надійності	Стійкість до атак Швидке відновлення Гнучкість та адаптивність Зменшення впливу вразливостей Система моніторингу та виявлення Ефективне управління ризиками Забезпечення послуги без перерви Забезпечення відновлюваності даних	Вартість Складність Залежність від технологій Людський фактор Обмежені резервні ресурси Застарілість
Дискреційна	Гнучкість Простота в реалізації Індивідуалізація доступу Легкість в адмініструванні Масштабованість	Слабка гранулярність доступу Залежність від користувачів Складне управління правами Відсутність централізованого контролю Ризик інсайдерських загроз Обмежені можливості аудиту
Мандатна	Строгий контроль Ефективна управління привілеями Спрощення аудиту та відслідковування Мінімізація ризиків безпеки Забезпечення дотримання внутрішніх та зовнішніх вимог	Витрати та складність Необхідність постійного оновлення Обмежена гнучкість Людський фактор Призначеність для конкретного контексту
Microsoft	Інтегрованість Широкий функціонал Облачні сервіси Постійні оновлення Аналітика та моніторинг Інтелектуальна безпека Співпраця та відкриті стандарти Гнучкість та масштабованість	Вразливості Залежність від вендора Обмеженість безпекових можливостей у деяких версіях Великий обсяг атак Проблеми з приватністю Споживання ресурсів Спростування діагностичних інструментів
Трирівнева	Простота і зрозумілість Легка сегментація Гнучкість впровадження Ефективне управління ризиками Забезпечення консистентності	Спрощеність Загальні стандарти Обмеженість в управлінні ризиками Недостатня адаптованість Неусунення внутрішніх загроз

Отже з вище розглянутих моделей найбільш перспективною та оптимальною для наших цілей е трирівнева модель у сукупності з моделлю Microsoft, з застосуванням підходів найменшого доступу, найменшої функціональності тощо.

1.8 Стандарт, орієнтований на управління ризиками ІБ

ISO 27005 – це стандарт із серії 2700x, що описує підхід до організації всього процесу з управління ризиками інформаційної безпеки. Представлена в стандарті методика оцінки є класичною і має за недоліки зайву академічність і загальність формулювань. Даний стандарт описує настанови і рекомендується до ознайомлення з метою формування загального уявлення про організацію процесу з управління ризиками ІБ [1].

Що мається на увазі під «ризиком» в даному стандарті: ризик – ефект невизначеності на цілі (ефект – це відхилення від передбачуваного (позитивного і / або негативного). Ризик зазвичай виражається у вигляді комбінації наслідків події ІБ і відповідної ймовірності її виникнення. Невизначеність – це недостатність (навіть часткова) інформації, пов'язаної з розумінням події або знаннями про подію, її наслідками або можливістю виникнення.

Процес менеджменту ризиків інформаційної безпеки складається з визначення обставин, оцінки ризику, обробки ризику, прийняття ризику, обміну інформацією щодо ризику, а також моніторингу та перегляду ризику (Рис. 1.5).

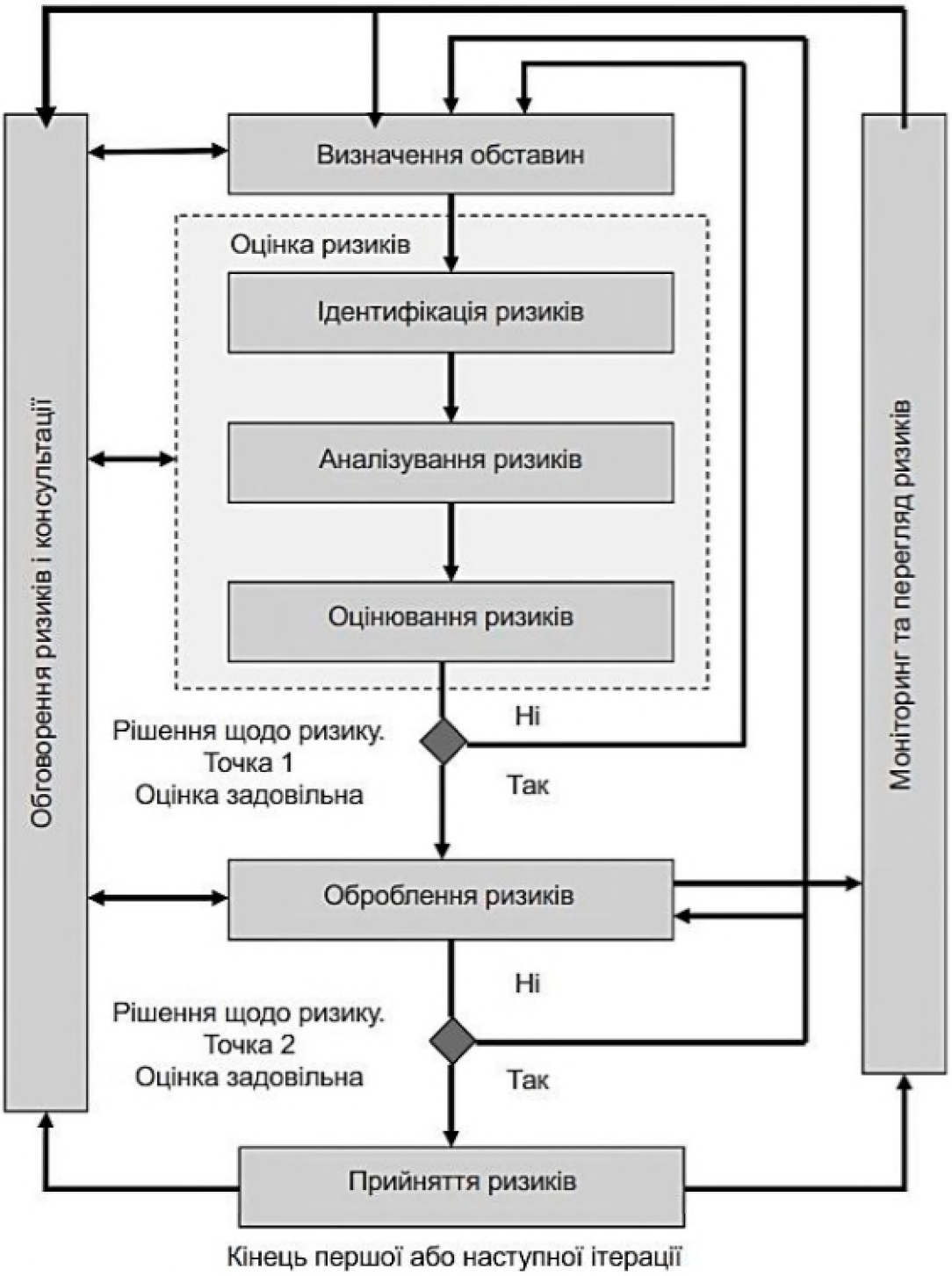

Рис. 1.5 – Ілюстрація процесу управління ризиками ІБ за стандартом ISO 27005

На етапі визначення обставин визначаються зовнішні та внутрішні обставини для управління ризиками ІБ, що передбачає встановлення базових критеріїв, необхідних для управління ризиками інформаційної безпеки, визначення сфери застосування та її меж й забезпечення функціонування управління ризиками інформаційної безпеки прийнятого для організації.

Базові критерії:

- критерії зіставлення ризиків;
- критерії впливу;
- критерії приймання ризиків.

Оцінка ризиків складається з таких дій:

- ідентифікація ризику;
- аналіз ризиків;
- зіставлення ризиків.

Метою ідентифікації ризику є визначення того, що могло б статися, щоб спричинити потенційні втрати, і щоб отримати уявлення про те, як, де і чому ці втрати можуть виникати. [4] Етапи, які входять в ідентифікацію ризику, повинні збирати вхідні дані для дії щодо аналізу ризику:

1. Ідентифікація активів СУІБ (активом є щось, що має цінність для організації і, отже, потребує захисту);
2. Ідентифікація загроз;
3. Ідентифікація існуючих засобів контролю;
4. Ідентифікація вразливостей;
5. Ідентифікація наслідків.

Методологія аналізу ризиків може бути якісною чи кількісною, або їх комбінацією залежно від обставин.

Рівні ризиків повинні порівнюватися з критеріями оцінювання ризику і критеріями прийняття ризику.

Для оцінювання ризиків підприємства виміряні ризики повинні порівнюватися з критеріями оцінювання ризику.

Для обробки ризику є чотири варіанти: модифікація ризику, прийняття ризику, усунення ризику і розподілення ризику.

1.9 Методика проведення оцінки ризиків OCTAVE Allegro

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) розроблено в стінах університету Карнегі-Меллон у травні 2007 року. Методика використовується для якісної оцінки ризиків інформаційної безпеки.[2]

Нас цікавить найактуальніша на даний момент в ряді OCTAVE методологія, а саме OCTAVE Allegro. Метод має на меті узагальнення та оптимізацію процесу оцінювання ризиків інформаційної безпеки установи та забезпечення можливості отримання необхідних результатів, при цьому, з мінімальною витратою ресурсів. Працівники, технології, інформаційні системи, об'єкти, що належать до інформації чи сфери інформаційних послуг, в межах якої вони знаходяться, розглядаються методом окремо. Оцінка ризиків проводиться персоналом та кваліфікованими спеціалістами, що є відповідальними за інформаційну безпеку.

Згідно з методикою OCTAVE Allegro, управління ризиками інформаційної безпеки складається з восьми етапів, а також допоміжного етапу визначення пріоритетів.

На *першому етапі* проводиться визначення критеріїв вимірювання ризиків, які є набором якісних параметрів, що використовують для оцінки ризиків. Дані параметри також цілком можуть оцінювати імовірність виникнення ризику, можливі збитки чи інші наслідки для установи чи організації. Окрім того, на цьому етапі виділяються найбільш критичні напрями діяльності установи чи організації, для яких додатково можна встановити певні рівні прийнятного ризику.

На *другому етапі* здійснюють розробку профілів для ІТ-активів установи чи організації. Профіль – це опис активу, який включає унікальні характеристики, певні особливості та якості інформаційної безпеки, а також цінність і вимоги. Профіль кожного активу вказується на одному аркуші, які формують основу для подальшого процесу визначення загроз і ризиків.

На *третьому етапі* визначається оточення ІТ-активів, тобто проводиться опис місця, де обробляють, передають чи зберігають активи. Всі ризики оточення

передаються на самі активи, що особливо актуально для активів, що надаються організації чи установі зовнішніми постачальниками.

Четвертий етап передбачає визначення областей для занепокоєння. Цей етап починає процес визначення ризиків за участі всієї проєктної команди, шляхом визначення високорівневих областей та типів ризиків для ІТ-активів, які є об'єктом аналізу.

Під час *п`ятого кроку* проводиться визначення сценаріїв реалізації загроз. Даний метод виділяє наступні типи загроз:

- користувацькі помилки під час використання технічних засобів;
- помилки користувачів під час фізичного доступу до активів;
- технічні проблеми чи проблеми іншого характеру.

Для всіх ІТ-активів можна визначити сценарії реалізації загроз, завдяки виділенню цих типів загроз, і описати їх можливий вплив на актив та визначити імовірність їх реалізації, яка вимірюється за трибальною шкалою. Для спрощення даний метод пропонує використовувати спеціальні опитувальники.

Шостий етап полягає у процесі визначення ризиків на основі інформації про найімовірніші сценарії реалізації загроз, а також проводиться аналіз їх впливу на активи установи чи організації.

На сьомому етапі проводиться аналіз ризиків на основі інформації, що була отримана під час проведення попередніх етапів, а також здійснюється оцінка впливу всіх визначених загроз на основний напрям діяльності установи чи організації. Окрім цього проводиться групування цих ризиків відповідно до визначених на першому етапі критеріїв.

І на *останньому кроці* обирається підхід для обробки ризиків, тобто визначається стратегія, що буде використовуватися для їх обробки. Це відбувається на основі визначеного рівня впливу цих ризиків на установу чи організацію.

На основі цього опису можна виділити наступні переваги методології OCTAVE Allegro під час його практичного застосування:

- простота та прозорість методу під час аналізу та оцінки ризиків, що дозволяє розпочати процес в найкоротші терміни, без тривалого дослідження методики та документації;

- ітеративність дозволяє поетапно збільшувати глибину та якість аналізу ризиків для інформаційної системи на основі реальних потреб установи чи організації та доступних їй ресурсів;

- прийнятні трудовитрати на процес аналізу та оцінки ризиків роблять можливою їх реалізацію з використанням мінімальних ресурсів та у короткі терміни;

- можливість повторення результатів спрощують реалізацію цих процесів для їх виконавців.

Проте, варто зазначити, що методу OCTAVE Allegro притаманні наступні недоліки:

- не дозволяє оцінити ризики в грошовому еквіваленті, що суттєво обмежує використання методу в створенні техніко-економічного обґрунтування, визначенні необхідних інвестицій на введення в використання засобів захисту в установі чи організації;

- в методології відсутні допоміжні матеріали, а саме каталоги з загрозами, вразливостями, їх можливими наслідками та заходами по забезпеченню інформаційної безпеки, що збільшує необхідність фахових знань для тих, хто виконує процеси аналізу та управління ризиками даним методом.

Попри це, методологія OCTAVE отримала широке застосування для проведення якісної оцінки та управління ризиками інформаційної безпеки. Вона найбільш придатна для установ та організацій, які проводять процес впровадження управління ризиками інформаційних безпеки вперше та відчувають потребу в покроковому поділі цих ризиків в залежності від рівня їх впливу. Також, з використанням даного методу в установи чи організації є можливість проводити інтеграцію процесу управління ризиками ітеративно.

1.10 Структурно-логічна схема дій з розробки СУІБ

Рішення про створення СУІБ повинно прийматися вищим керівництвом організації. Таким чином керівництво висловлює свою підтримку початку даного процесу, що є ключовим фактором для успішного впровадження СУІБ в організації. При цьому керівництво повинно усвідомлювати кінцеву мету даного заходу.

Для виконання цілей інформаційної безпеки дії з розробки системи управління інформаційною безпекою мають наступний структурно-логічний вигляд (рис.1.6):

- Визначення мети та обсягу системи управління інформаційною безпекою (СУІБ):
  - Визначення стратегічних цілей безпеки інформації.
  - Встановлення обсягу інформаційних активів, які потрібно захищати.
- Аналіз ризиків:
  - Оцінка потенційних загроз безпеці інформації.
  - Визначення вразливостей в існуючих інформаційних системах.
  - Оцінка ймовірності виникнення ризиків та їхніх наслідків.
- Розробка політики безпеки:
  - Визначення основних принципів і стратегій безпеки інформації.
  - Встановлення стандартів і правил для користувачів та адміністраторів.
- Розробка інфраструктури безпеки:
  - Впровадження заходів фізичної безпеки (обмеження доступу, захист приміщень).
  - Розгортання технічних засобів захисту (фаєрволи, антивіруси, системи виявлення вторгнень).
- Тренування персоналу:
  - Проведення навчань і тренінгів з питань інформаційної безпеки.
  - Забезпечення свідомості персоналу щодо правил безпеки та процедур реагування на інциденти.
- Моніторинг і виявлення інцидентів:

- Впровадження систем моніторингу та виявлення аномалій в мережах і системах.

- Розробка процедур реагування на інциденти та планів відновлення роботи.

- Аудит і вдосконалення:

- Проведення періодичних аудитів системи безпеки.

- Аналіз і вдосконалення стратегій та процедур інформаційної безпеки на основі виявлених слабких місць.

- Забезпечення відповідності:

- Впровадження процедур та технічних засобів для забезпечення відповідності стандартам безпеки та регулюючим вимогам.

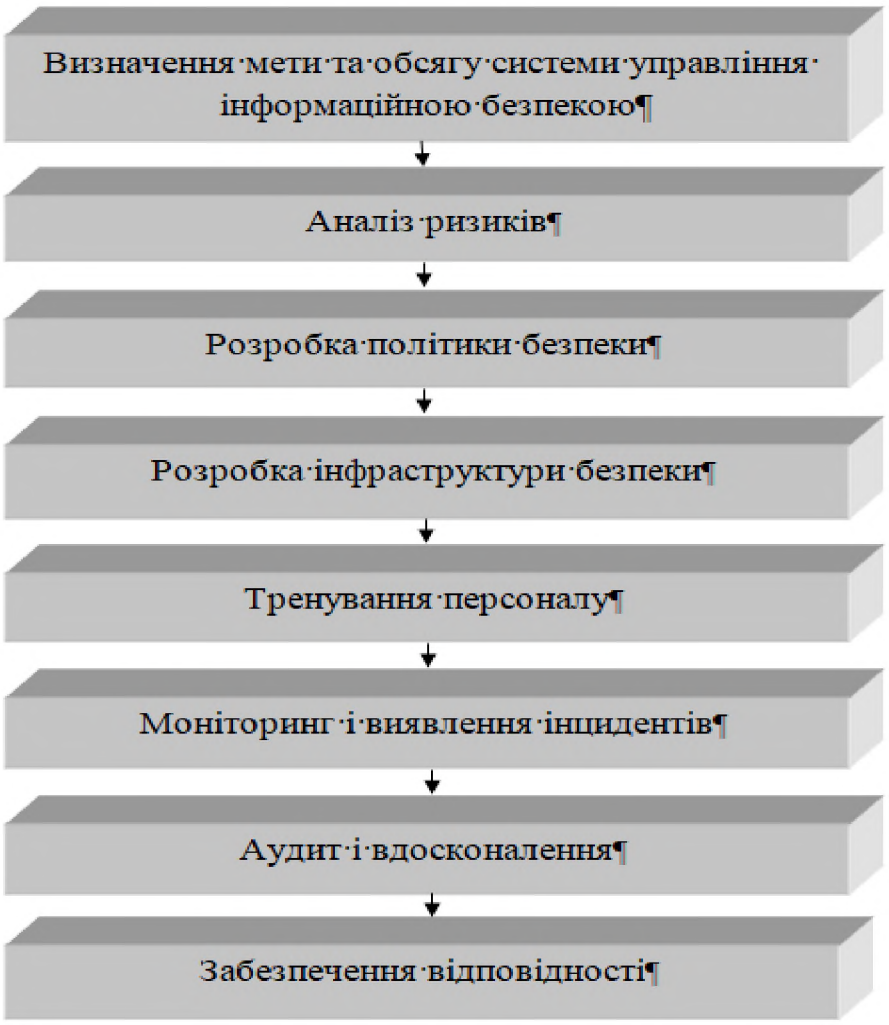

Рис.1.6 – Структурно-логічна схема дій з розробки СУІБ.

Це загальний огляд, і конкретні кроки можуть змінюватися в залежності від конкретних потреб і характеристик підприємства.

1.11 Висновки. Постановка задачі

У цьому розділі були досліджені стандарт ISO/IEC 27001 щодо розробки системи управління інформаційною безпекою, стандарт ISO 27005, що описує підхід до організації всього процесу з управління ризиками інформаційної безпеки, розглянуті основні процеси, моделі для побудови і забезпечення ефективності СУІБ. Зроблено огляд принципів та підходів до створення політик інформаційної безпеки, проведено їх порівняння. Розглянута методика проведення оцінки ризиків OCTAVE Allegro.

На основі проведеного аналізу, можна зробити висновок, що оптимальним варіантом для вибору моделі управління ризиками інформаційної безпеки є трирівнева модель, для оцінки ризиків запропоновано використовувати методику OCTAVE Allegro. У наступному розділі буде наведено побудову СУІБ ЗФПО на прикладі фахового коледжу.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Структура інформаційної систем.

Для розуміння області застосування СУІБ розглянемо організаційно-штатну структура закладу фахової передвищої освіти. Вона може варіюватися залежно від типу і розміру закладу освіти, його спеціалізації та організаційних вимог. Нижче наведено організаційно-штатна структура ЗФПО на прикладі Фахового коледжу ракетно-космічного машинобудування Дніпровського національного університету імені Олеся Гончара (рис.2.1)

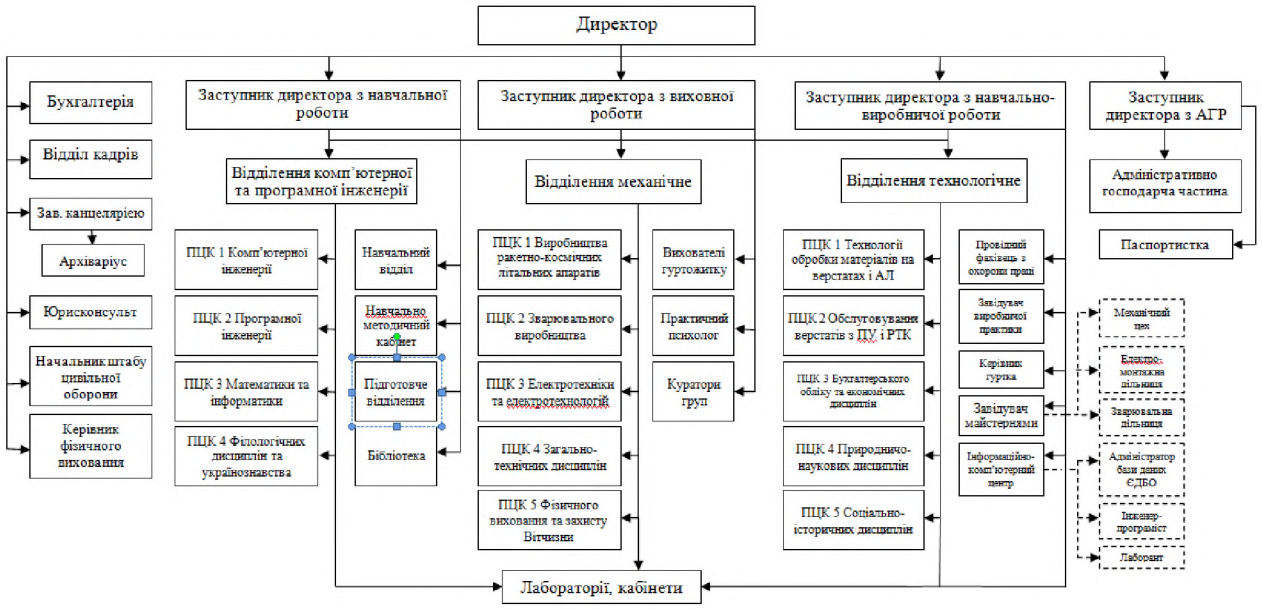

Рис.2.1 Організаційно-штатна структура ЗФПО ФКРКМ

Найбільш важливі підрозділи та посади з точки зору циркулюючої в них чутливої та важливої інформації виділені зеленим кольором (рис.2.2).

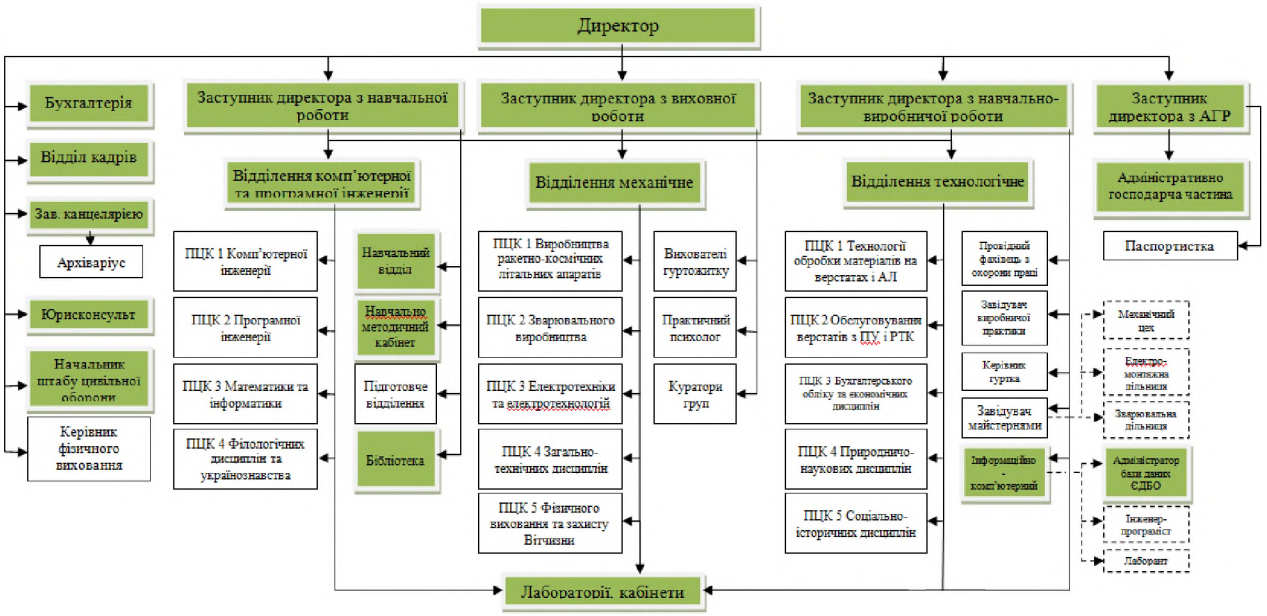

Рис.2.2 – Найбільш важливі підрозділи та посади з точки зору циркулюючої в них чутливої та важливої інформації.

Опис їх функції наведено в таблиці 2.1

Таблиця 2.1 – Опис функції підрозділів та посад

№ п/п	Найменування	Основні функції
1	Директор	Стратегічне планування; Управління персоналом; Фінансове управління; Комунікації та взаємодія з громадськістю; Управління інформаційною безпекою; Співпраця з органами влади
2	Бухгалтерія	Облік фінансових операцій; Розрахунок заробітної плати; Фінансове планування і бюджетування; Ведення обліку матеріальних цінностей та обладнання
3	Відділ кадрів	управління кадрами
4	Зав. канцелярією	Організація робочих процесів; керування документацією; взаємодія з клієнтами та персоналом; Ведення архіву документації
5	Заступник директора з навчальної роботи	Організація навчального процесу; взаємодія з педагогічним колективом
6	Заступник директора з виховної роботи	Організація виховної роботи; контроль дисципліни та порядку; співпраця з батьками; організація заходів культурного характеру
7	Заступник директора з навчально-виробничої роботи	Організація Навчально-Виробничого Процесу; Контакти з Партнерами; Вирішення Організаційних Питань

Продовження таблиці 2.1

№ п/п	Найменування	Основні функції
8	Заступник директора з АГР	Організація робочого простору; Безпека та охорона; Вирішення адміністративних питань
9	Зав. відділення	Управління персоналом; Планування і контроль робіт; Забезпечення порядку і безпеки; Впровадження стратегічних ініціатив
10	Голови ЦК	Організація роботи циклової комісії;
11	Навчальний відділ	Організація навчального процесу; Ведення обліку відвідуваності та успішності студентів; Взаємодія з викладачами;
12	Бібліотека	Забезпечення доступу до різних джерел інформації, таких як книги, періодичні видання, електронні ресурси і т.д
13	Адміністратор бази даних ЄДБО	Надання даних коледжу до систему ЄДЕБО; впровадження заходів забезпечення конфіденційності та захисту даних; формування звітів та аналіз
14	Інформаційно-комп'ютерний центр	Адміністрування мережі; Технічна підтримка; Безпека інформації; Управління базами даних; Навчання користувачів; Оновлення та моніторинг апаратного забезпечення; IT-стратегія та консультування
15	Комп'ютерні лабораторії, кабінети	Доступ до інформаційних ресурсів; Розвиток програмування; Тестування та оцінка; Комунікація та співпраця

Інформаційна система закладу освіти призначена для підтримки інформаційних ресурсів та потоків, надання користувачам інформаційно-обчислювального середовища та інших послуг, необхідних їм для виконання своїх функцій.

Інформаційна система закладу освіти – організаційно-технічна система, в котрій реалізуються інформаційні технології, і передбачається використання апаратного і програмного забезпечення, необхідного для реалізації процесів збирання, обробки, накопичення, зберігання, пошуку і поширення інформації. Основою інформаційної системи навчального закладу є територіально розподілені комп'ютерні системи, елементи яких розміщені в окремих будівлях, на різних поверхах цих будівель і пов'язані між собою транспортним середовищем. Основу апаратних засобів таких систем становлять персональні обчислювальні машини, периферійні та інші допоміжні пристрої, засоби зв'язку. Склад програмних засобів визначається можливостями апаратури і характером вирішуваних завдань.

Можна виділити такі елементи інформаційної системи:

- апаратне забезпечення;
- програмне забезпечення;
- інформаційні ресурси;
- робочі місця користувачів;
- власне користувачі.

Апаратне забезпечення – це канали і засоби зв'язку, вузли комутації, сервери тощо.

Програмне забезпечення інформаційної системи закладу освіти об'єднує системне програмне забезпечення, необхідне для підтримки функціонування самої системи, інструментарій користувача та навчальне програмне забезпечення.

До інформаційних ресурсів належать матеріали в електронному вигляді, які можуть використовувати користувачі в освітньому процесі.

Зважаючи на це, можна побудувати структуру інформаційної системи закладу. Дана модель інформаційної систем зображена на рисунку 2.3.

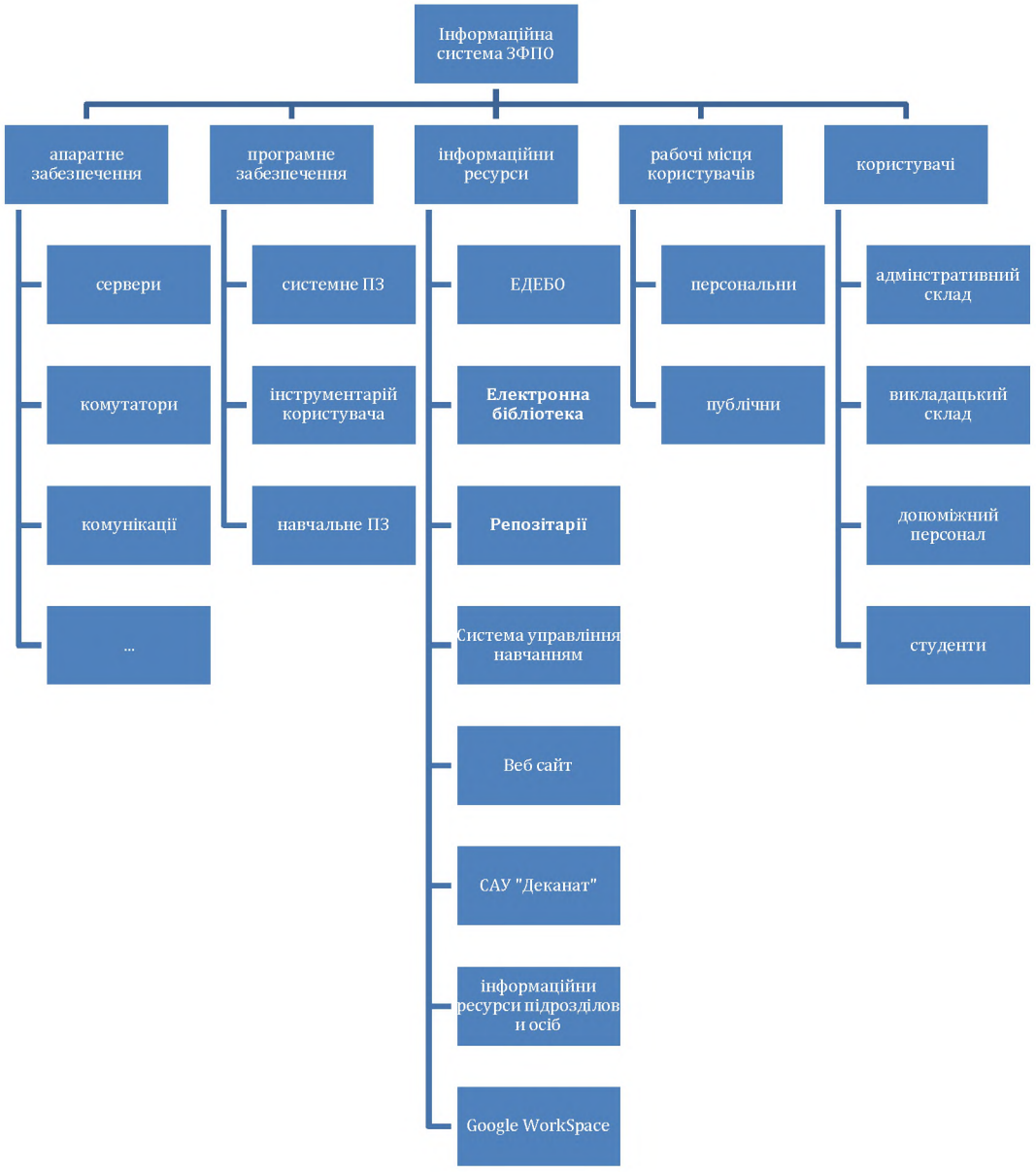

Рис. 2.3 Структура інформаційної систем ЗФПО ФКРКМ.

Межі СУІБ включають організаційні одиниці, підрозділи, інформаційні системи та інші складові ЗФПО.

2.2 Модель управління ІБ

Трирівнева модель управління інформаційною безпекою (ІБ) визначає троїсту структуру для ефективного впровадження та управління інформаційною безпекою в організації. Ця модель враховує різні рівні відповідальності та функцій в організації,

сприяючи взаємодії та впровадженню кращих практик. Нижче подано загальний огляд трирівневої моделі управління інформаційною безпекою:

- Стратегічний рівень (організаційний);
- Тактичний рівень (процедурний);
- Операційний рівень (програмно-технічний).

Управління ІБ на *організаційному рівні* включає в себе розробку та впровадження стратегій, політик, процедур та структур, спрямованих на забезпечення високого рівня безпеки інформації в організації. Її реалізація забезпечується за допомогою контролю виконання посадових інструкцій персоналом. Необхідно також встановити персональну відповідальність кожного співробітника, закріплену на юридичному рівні. ІБ на організаційному рівні є основною в запобіганні витоку інформації. У більшості випадків витік інформації відбувається з вини співробітників, які мають до неї доступ. Особливо це актуально там, де є доступ до конфіденційних даних, які обробляються в ІС. До цього може привести недостатня обізнаність з питань ІБ співробітниками ЗФПО.

Управління ІБ на *процедурному рівні* включає розробку, впровадження та управління процедурами, які спрямовані на захист інформаційних активів та забезпечення ефективного управління ризиками

Управління ІБ на *програмно-технічному рівні* включає реалізацію технічних заходів та використання програмних рішень для захисту інформаційних ресурсів організації. Модель комплексного забезпечення режиму інформаційної безпеки досягається за рахунок структуризації керуючих впливів по рівнях або областях відповідальності

В таблиці 2.2 наведена структура управління ІБ з урахуванням рівнів відповідальності, класів керуючих впливів та критеріїв безпеки

Таблиця 2.2 - Структура управління ІБ

Рівень	Класи керуючих впливів і критерії безпеки
Організаційний рівень	• управління персоналом; • управління доступом; • управління ризиками; • створення культури безпеки; • розмежування відповідальності; • аудит та внутрішній контроль; • управління інцидентами; • створення політик та стандартів безпеки
Процедурний рівень	• Розробка конкретних політик, що визначають правила та вимоги для забезпечення конфіденційності, цілісності та доступності інформації; • Визначення процедур для надання та зняття прав доступу до інформаційних ресурсів; • Організація навчань та тренінгів з питань ІБ для персоналу; • Розробка та впровадження політик та процедур для захисту конфіденційної інформації та запобігання втратам даних; • Визначення процедур для керування інфраструктурою та технічним середовищем з точки зору ІБ;
Програмно-технічний рівень	• регулярне оновлення та патчі; • управління ідентифікацією та аутентифікацією; • шифрування даних; • моніторинг та детекція загроз; • створення резервних копій та відновлення; • системи захисту від вірусів та зловмисних програм; • безпека мережі; • управління ключами.

2.3 Класифікація загроз інформаційної безпеки ЗФПО.

Уразливостям інформаційного ресурсу закладу освіти та їх наслідкам в повній мірі притаманні такі ж самі негативні прояви, як й іншим закладам і установам держави [3]. Це збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу і використання інформаційних ресурсів, незаконного копіювання інформації, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах. Разом з тим для закладів освіти є й особливості, що пов'язані із блокуванням доступу до відкритої інформації при дистанційному навчанні, введення хибних теоретичних і оціночних даних, ведення електронного діалогу від особи викладача або студента.

Територіально розподілена структура інформаційної системи закладу створює ряд передумов для реалізації величезної кількості потенційних загроз інформаційній безпеці, що можуть завдати шкоди всім складовим інформаційної системи. Розмаїття таке значне, а випадковість появи атак, мета їх застосування і оснащеність так стрімко зростає, що це не дозволяє передбачити кожну загрозу. Тому, аналізуючи характеристики загроз, треба вибирати протидії з позицій здорового глузду, одночасно виявляючи не тільки самі загрози, розмір потенційного збитку, але і поєднувати окремі випадки застосувань в підгрупи джерел і зменшувати загальну уразливість системи та застосовувати принцип диференціації рівня захисту на основі оцінювання ризиків.

Ці особливості впливають на необхідність визначення, що захищати в першу чергу: яку інформацію, які інформаційні системи. Необхідним є впровадження зрозумілого ранжування цінної інформації, місць її зберігання та можливих ризиків.

Модель порушника інформаційної безпеки повинна відображати причини і мотиви його дій, його можливості, апріорні знання, мету дій, їх пріоритетність, шляхи досягнення (способи реалізації вихідних загроз, місце і характер дії, можливу тактику, мотиви поведінки). Взагалі це може бути декілька моделей дій

зловмисника, що відображають різний рівень його підготовленості, що пояснює розподіл джерел за ознакою – категорія порушника інформаційної безпеки.

Для ЗФПО типовими категоріями стають ті, що беруть участь в життєдіяльності закладу, суттєво впливають на стан інформаційної безпеки, мають наступні характеристики і оцінки:

- *студент*. Загрози з боку студентів можливі за декількома напрямками. По-перше, це неконтрольований вихід в Інтернет, що тягне за собою різке збільшення трафіку і нецільове витрачання інформаційного ресурсу. Нелегальне скачування може призвести до зараження вірусами мережі, що відповідно, призводить до обмеження доступу великого контингенту студентів і викладачів або навіть повного блокування мережі. По-друге, заклад освіти – це місце підвищеної активності і концентрації хакерів-початківців. Юнацький максималізм, бажання випробувати свої знання і справити враження на однокурсників спонукає студентів зламати мережу, заблокувати вихід в Інтернет, отримати адміністративний доступ, влаштувати вірусну епідемію або вчинити інші комп'ютерні правопорушення. Це веде до зриву занять або блокування доступу до мережі. По-третє об'єктивна зміна життєвих цінностей вносить певні труднощі в забезпечення безпеки самого освітнього процесу, бо застосовується:

- широке використання в студентському середовищі сучасних інформаційно-комунікаційних технологій для складання заліків та іспитів (ноутбуки, планшети, смартфони із бездротовим доступом до Інтернету);
- підробки відпрацювання та захисту практичних і лабораторних занять, курсових робіт і проєктів;
- плагіат на стадії виконання рефератів, курсових робіт і проєктів тощо.

До четвертого напрямку загроз відносяться можливі розкрадання, в тому числі, комп'ютерного обладнання та бібліотечного фонду. Тут втрати мають суто матеріальний характер, пов'язаний з необхідністю відновлення ресурсів. І останній напрям загроз – це ненавмисні помилки студентів, що має наслідками

вихід з ладу обладнання, зрив занять, обмеження доступу інших користувачів до інформації;

- *співробітник*. Серед загроз з боку співробітників ЗФПО можна виділити такі:
- в області відкритої інформації – це неправомірне використання веб-доступу, так як практично всі викладачі та співробітники мають вільний, слабо контрольований доступ в Інтернет;
- в області конфіденційної інформації, що має характер службової таємниці, – це витік, розголошення, модифікація інформації, що може нанести шкоду діяльності чи іміджу закладу;
- халатність і безвідповідальність співробітників, що тягне за собою реалізацію загроз і пов'язані з цим збитки;
- ненавмисні помилки при роботі з обчислювальною технікою, так як не всі співробітники мають відповідну кваліфікацію;

- *відвідувач*. Дана категорія осіб практично не має фізичного доступу до інформаційної системи закладу освіти. Можливості їх обмежені, вони можуть здійснювати тільки поодинокі дії, скориставшись недбалістю або безвідповідальністю працівників, однак збиток від їх дій може бути істотним;
- *хакер-одинак*. Використовує стандартні комп'ютерні програми для реалізації відомих вразливостей. Це може бути і студент, що має доступ як з середини мережі, так і віддалений доступ. Дії його носять експериментальний характер, фінансова мотивація – не головне. Йому цікаво зламати сайт, отримати доступ до конфіденційної інформації, до серверів організації, до систем адміністрування, контролю і управління інформаційною системою. Дії його можуть завдати шкоди цілісності мережі. Найчастіше його дії носять несистемний характер, і він зупиняється після першого успішно проведеного злому. У той же час, він може мати і чисто матеріальний інтерес, розраховуючи на підключення та використання каналів зв'язку з високою пропускною здатністю;
- *хакерська група* - переслідує суто матеріальний інтерес. Володіючи достатніми сумарними знаннями в області комп'ютерних технологій, такі зловмисники

можуть організувати сканування інформаційної системи закладу освіти з метою виявлення нових вразливостей, самостійно написати програми для експлуатації цих вразливостей. Вони діють цілеспрямовано і можуть отримати доступ до різних фінансовим документів, влаштувати потужні атаки на інформаційну систему з повним виводом її з ладу, що може завдати істотної матеріальної шкоди закладу;

- *злочинні угрупування і організації*. - ЗФПО виконують важливу соціально роль, спрямовану на виховання молоді, де зосереджена велика кількість людей у віці від 14 до 18 років. Тому заклади стають мішенню для дії злочинних угруповань та організацій для проведення різних терористичних актів, поширення наркотиків і завоювання впливу на молоді незміцнілі уми з боку різних політичних партій, екстремістських угруповань і релігійних сект. Ця група зловмисників представляє серйозну загрозу як для закладу в цілому, так і для його інформаційного середовища. Залежно від цілей, подібні організації можуть мати досить високий фінансовий потенціал і підготовлених фахівців.

2.4 Ідентифікація активів.

Ідентифікація активів є важливим етапом в процесі управління інформаційною безпекою та оцінки ризиків. Цей процес передбачає визначення та класифікацію всіх інформаційних ресурсів, які мають цінність для організації.

У рамках цієї роботи немає можливості розглянути весь перелік активів даного закладу в силу його великої кількості. Принцип оцінки ризиків залишається однаковим не дивлячись на кількість. Для проведення оцінки ризиків розглянемо невеликий набір активів.

На кроці заповнення таблиці інвентарю активів створюється повний список всіх інформаційних ресурсів організації. Він може включати дані, обладнання, програмне забезпечення, комунікаційні засоби, людські ресурси та інші елементи. Активи потрібно класифікувати відповідно до їх значення для організації, визначити місцезнаходження активу та його цінність. для визначених активів потрібно

провести оцінку їх імовірної вартості або той грошовий еквівалент збитку, який може бути нанесений внаслідок розголошення, видалення або зміни даного активу. Щоб полегшити процес оцінки ризиків інформаційної безпеки, виразимо цінність активів за допомогою балів . Розподіл подано в таблиці 2.3 та 2.4

Таблиця 2.3 – Класифікація інформаційних активів за ступенем їх впливу на заклад

Цінність активу	**Опис**
[8, 10]	Особливо висока цінність
[5, 8)	Висока цінність
[2, 5)	Середня цінність
< 2	Низька цінність

Таблиця 2.4 Ідентифікація активів

№	Матеріальні активи		
		місцезнаходження	Вартість активу (S)
1.1	Сервер зберігання даних	серверна	10 балів
1.2	ПК Адміністратора ЄДЕБО	14 каб.	7 балів
1.3	ПК відділу бухгалтерії	19 каб. бухгалтерія	8 балів
1.4	Система управління навчанням Moodle	сервер віртуальних машин	10 бали

2.5. Ідентифікації загроз

На другому етапі оцінки ризиків інформаційної безпеки проводимо процес визначення загроз інформаційним ресурсам та у відповідність їм ставимо вразливості. Дана відповідність подана в таблиці 2.5

Таблиця 2.5 Загрози інформаційним ресурсам та відповідні їм вразливості.

№	Загрози	Уразливості
1	Атаки, що викликають відмову в обслуговуванні	низька пропускна здатність мережі Системи, які не ефективно управляють ресурсами Неправильне опрацювання великої кількості запитів Системи, які не мають обмежень або перевірок щодо швидкості обробки запитів
2	Отримання несанкціонованого доступу до системи /мережі	Використання слабких або неякісних методів аутентифікації Використання вразливостей у програмному забезпеченні Отримання фізичного доступу до обладнання
3	Крадіжка носіїв інформації, обладнання	Зберігання носіїв інформації за межами сейфа Відсутність системи контролю доступу Відсутність системи сигналізації Відсутність захисту від проникнення
4	Умисне знищення інформації	Відсутність розмежування доступу Відсутність системи резервного копіювання
5	Ненавмисне знищення інформації	Відсутність системи резервного копіювання

Продовження таблиці 2.5

№	Загрози	Уразливості
6	Дії шкідливих програм	Не встановлено сертифіковане антивірусне програмне забезпечення Відсутність оновлень ПЗ
7	Віддалений запуск додатків	Відсутність засобів між мережевого екранування
8	Стихійне лихо	Відсутність джерел безперебійного живлення
9	Фізичне Пошкодження	Відсутність системи кондиціювання, забруднення, пошкодження водою

Загрози та відповідні їм засоби нейтралізації подано в таблиці 2.6

Таблиці 2.6 Загрози та відповідні їм засоби нейтралізації

№	Загроза	Засіб нейтралізації загрози	Чи присутній на об'єкті даний засіб захисту	
			Так	Ні
1	Атаки, що викликають відмову в обслуговуванні	Встановлення фаєрволів та систем запобігання вторгненням для виявлення та блокування атак	+	
		Збільшення пропускної здатності та оптимізація мережевої інфраструктури для витримки атак	+	

Продовження таблиці 2.6

№	Загроза	Засіб нейтралізації загрози	Чи присутній на об'єкті даний засіб захисту	
			Так	Ні
2	Отримання несанкціонованого доступу до системи /мережі	Використання сильних паролів	+	
		двофакторної аутентифікації		+
		оновлення програмного забезпечення	+	
		Застосування фізичних контрольних заходів		+
3	Крадіжка носіїв інформації	Сейфи для зберігання носіїв інформації	+	
		Система контролю доступу		+
		Система відеоспостереження	+	
		Сигналізація		+
		Захист від проникнення		+
4	Умисне знищення інформації	Аутентифікація та авторизація для обмеження доступу до інформації	+	
		Резервні копії важливих даних		+
		Блокування доступу під час звільнення	+	
		Системи виявлення вторгнень		+
5	Ненавмисне знищення інформації	Аутентифікація та авторизація для обмеження доступу до інформації	+	
		Резервні копії важливих даних		+

Продовження таблиці 2.6

№	Загроза	Засіб нейтралізації загрози	Чи присутній на об'єкті даний засіб захисту	
			Так	Ні
6	Дії шкідливих програм	Антивірусне програмне забезпечення	+	
		Оновлення програмного забезпечення	+	
		Фільтрація веб-трафіку		+
		Резервні копії важливих даних		+
7	Віддалений запуск додатків	Антивірусне програмне забезпечення	+	
		Брандмауер	+	
		Обмеження прав користувачів	+	
		Централізоване управління політикою безпеки	+	
		Оновлення системи та програмного забезпечення	+	
		Мережеві політики	+	
8	Стихійне лихо	Встановлення системи безперебійного живлення		+
9	Фізичне пошкодження	Встановлення системи кондиціювання	+	
		технічна профілактика		+
		система виявлення протікання		+

Список загроз необхідно переглядати щорічно і додавати в нього інформацію, на підставі даних про інциденти ІБ, які трапилися у закладу або поза ним, і з використанням інших загальнодоступних джерел

Також на даному етапі доцільно визначити імовірність реалізації загроз - Р. Дана відповідність подана в таблиці 2.7

Таблиці 2.7 Визначення імовірності реалізації загроз

Імовірність реалізації загроз **(Р)**	**Опис**
Р=0 Ймовірність реалізації загроз - дуже низька. Очікувана частота реалізації загроз не перевищує 1 разу на 1-3 роки.	на об'єкті дослідження присутні всі засоби захисту Здатність реалізувати загрозу низька або джерело загрози недостатньо мотивоване. Діючі засоби захисту ускладнюють реалізацію загрози. Рівень вразливості низький. Відсутня статистика або інша інформація, яка б вказувала, що інцидент може статися. Використання вразливості можливо тільки при наявності прав адміністратора
Р=1 Ймовірність реалізації загроз - низька. Очікувана частота реалізації загроз не перевищує 1 разу на 1 рік.	на об'єкті дослідження присутні більш ніж 75% засобів захисту Здатність реалізувати загрозу низька або джерело загрози недостатньо мотивоване. Діючі засоби захисту ускладнюють реалізацію загрози. Рівень вразливості низький. Відсутня статистика або інша інформація, яка б вказувала, що інцидент може статися. Використання вразливості можливо тільки при наявності прав адміністратора
Р=3 Ймовірність реалізації загроз - середня. Очікувана частота реалізації загроз - приблизно 3 раз в 1 рік.	на об'єкті дослідження присутні от 25 до 75% засобів захисту Джерело загрози мотивоване, існують передумови для реалізації загрози. Інформація про уразливість опублікована для широкої аудиторії, проте необхідні спеціальні технічні засоби для реалізації загрози. Використання вразливості можливо при наявності прав зареєстрованого користувача
Р=5 Ймовірність реалізації загрози - висока. Очікувана частота реалізації загрози – от 5 разів на рік.	на об'єкті дослідження присутні менш ніж 25% засобів захисту Джерелом загрози можуть бути співробітники компанії. Інформація про уразливість опублікована для широкої аудиторії. Існує статистика або інша інформація, яка вказує на те, що загроза скоріше за все здійсниться або можуть існувати серйозні причини або мотиви атакуючого, щоб здійснити такі дії

В опитувальній таблиці (таблиця 2.5) , ми бачимо, що відсутні 44% засобів захисту, отже, Р = 3.

2.6 Ідентифікація та обробка ризиків

Для визначення ризику інформаційної безпеки скористаємося формулою:

$$R = S*P \quad (2.1)$$

де S - цінність активу; P - ймовірність реалізації загрози; R - ризик інформаційної безпеки.

Оцінивши ступінь ризику, ми можемо сформувати план по його зниженню. Даний план наведений в таблиці 2.8.

Таблиця 2.8 План зниження ступеню ризику

P	№	S	R	Величина ризику	План по зниженню ризику
1	1.1	10	10	Особливо висока	Довготривалий
	1.2	7	7	висока	
	1.3	8	8	висока	
	1.4	10	10	Особливо висока	
3	1.1	10	30	Особливо висока	Не надто терміновий
	1.2	7	21	висока	
	1.3	8	24	висока	
	1.4	10	30	Особливо висока	
5	1.1	10	50	Особливо висока	Критично. Списки завдань на найближчий час
	1.2	7	35	висока	
	1.3	8	40	висока	
	1.4	10	50	Особливо висока	

З наведених даних в таблиці 2.8, можна підсумувати, що план по зниженню ризику є індивідуальним для кожної імовірності реалізації загроз.

Різики з низьким рівнем приймаються. Середні ризики є потенційно прийнятними за погодженням з керівництвом закладу. Високі ризики вимагають негайної обробки.

Тепер можна перейти до фінального етапу, а саме процесу оцінки ризику інформаційної безпеки. за методикою OCTAVE Allegro. Результати даного дослідження наведені в таблицях 2.9 – 2.12

Таблиця 2.9 Профіль активу

Актив організації	Сервер зберігання даних
Цінність активу, S	10
Імовірність реалізації загрози, P	3
Показник ризику інформаційної безпеки, R	30
Величина ризику	Особливо висока
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Фільтрація веб-трафіку
	Резервні копії важливих даних
	Захист від проникнення
	Система контролю доступу
	Захист від проникнення
	Системи виявлення вторгнень

Таблиця 2.10 Профіль активу

Актив організації	ПК Адміністратора ЕДЕБО
Цінність активу, S	7
Імовірність реалізації загрози, P	3
Показник ризику інформаційної безпеки, R	21
Величина ризику	висока
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Резервні копії важливих даних
	Система контролю доступу
	Захист від проникнення
	Технічна профілактика

Таблиця 2.11 Профіль активу

Актив організації	ПК відділу бухгалтерії
Цінність активу, S	8
Імовірність реалізації загрози, P	3
Показник ризику інформаційної безпеки, R	24
Величина ризику	висока
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Фільтрація веб-трафіку
	Резервні копії важливих даних
	Захист від проникнення
	Система контролю доступу

Таблиця 2.12 Профіль активу

Актив організації	Система управління навчанням MOODLE
Цінність активу, S	10
Імовірність реалізації загрози, P	3
Показник ризику інформаційної безпеки, R	30
Величина ризику	Особливо висока
План по зниженню ризику	Не надто терміновий
Заходи для зниження ризику	Резервні копії важливих даних

Таким чином формується профіль по кожному активу.

Насправді, методика OCTAVE Allegro не складний в користуванні метод якісної оцінки інформаційних ризиків. Вона дає змогу проведення процесу оцінювання персоналом будь-якої установи самостійно, без залучення фахівців з спеціалізованих організацій. Формуючи якісну оцінку системи безпеки, можна виробити чіткий план проведення заходів для зниження ризиків. Аналізуючи проведену роботу, можна з впевненістю сказати, що система захисту інформацій ЗФПО на прикладі ФКРКМ знаходиться в задовільному стані.

Жоден з розглянутих інформаційних активів не потребує оперативного втручання, проте можна скористатись рекомендаціями для покращення стану системи інформаційної безпеки в перспективі.

2.7 Організаційна структура системи забезпечення інформаційної безпеки ЗФПО

Підсумовуючи все вище сказане, можемо сформувати організаційну структуру системи забезпечення інформаційної безпеки ЗФПО у вигляді сукупності наступних рівнів:

- Рівень 1 Керівництво організації
- Рівень 2 IT підрозділ (або особа відповідальна за IT напрямок)
- Рівень 3 Кінцеві користувачі

На першому рівні керівництвом закладу формуються:

- концепція забезпечення ІБ;
- політика інформаційної безпеки;
- положення про інформаційну безпеку закладу;
- положення про розподіл прав доступу користувачів інформаційних систем;

На другому рівні підрозділом IT формуються:

- план забезпечення безперервної роботи і відновлення працездатності інформаційних систем в кризових ситуаціях;
- методика проведення повного аналізу та управління ризиками, пов'язаними з порушеннями інформаційної безпеки;
- журнал обліку нештатних ситуацій;
- інструкція по внесенню змін до списків користувачів і наділення їх повноваженнями доступу до інформаційних ресурсів закладу;
- інструкція щодо внесення змін до складу і конфігурацію технічних і програмних засобів інформаційних систем;
- інструкція по роботі співробітників в мережі Інтернет;
- інструкція по роботі співробітників в інформаційних системах закладу;
- інструкція з організації парольного захисту;
- інструкція з організації антивірусного захисту;

- інструкція користувачеві інформаційних систем з дотримання режиму інформаційної безпеки;
- інструкція з резервного копіювання інформації.

2.8 Висновок

Проведено аналіз інформаційної структури ЗФПО на прикладі ФКРКМ. Досліджені загрози інформаційної безпеки ЗФПО. Побудована модель порушника. Розроблено опис моделі управління ІБ, наведено приклад оцінки ризиків деяких інформаційних активів ЗФПО ФКРКМ. Описана організаційна структура системи забезпечення інформаційної безпеки ЗФПО.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності впровадження запропонованого підходу в побудові СУІБ ЗФПО . Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування СУІБ;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту.

3.1 Розрахунок капітальних (фіксованих) витрат.

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на впровадження СУІБ визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки СУІБ

Трудомісткість на впровадження СУІБ визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – витрати праці на підготовку та описання поставленої задачі, $t_{тз}$=17;

$t_в$ – витрати праці на збір потрібної інформації нормативно-правової бази, $t_в$=25;

$t_м$ – витрати на аналіз та обробку інформації, $t_м$=30;

$t_р$ – витрати на створення основних елементів системи, $t_м$=60;

$t_д$ – тривалість підготовки технічної документації, $t_д$=60.

Отже,

$$t = t_{тз} + t_в + t_м + t_р + t_д = 17+25+30+60+10= 192 \text{ години}$$

Розрахунок витрат на розробку СУІБ .

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

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 16575,36+1472,64 =18048 \text{ грн}$$

$$З_{зп} = t\ З_{іб} = 192*86,33 = 16575,36 \text{ грн.}$$

де t – загальна тривалість розробки СУІБ, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч}= t*С_{мч}=192*7,67=1472,64 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0,8 \cdot 4 \cdot 1,68 + \frac{9100 \cdot 0,3}{1920} + \frac{8400 \cdot 0,2}{1920} = 7,67 \text{ грн}$$

Для реалізації запропонованого підходу може бути використано стандартне апаратне забезпечення, яке вже наявне на підприємстві, тому капітальні витрати не виникають.

Витрати на налагодження системи інформаційної безпеки становитимуть 3000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 18048+3000 = 21048 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, грн;

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

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

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

$К_{навч}$ – витрати на навчання персоналу,

$К_{н}$ – витрати на налагодження суіб.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування СУІБ:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

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

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

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

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

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

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 8000 грн.

Річний фонд заробітної плати ІТ персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_{з} = З_{осн} + З_{дод}, \text{ грн.}$$

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16500 грн. Додаткова заробітна плата – 5% від основної заробітної плати.

Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки.

Отже,

$$С_з = (16500*12 + 16500*12*0,05)*0,2= 41580 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2023 р. складає 22%.

$$С_{єв} = 41580*0,22 = 9147,6 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос} = 21048*0,02 = 420,96$ грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 8000+41580+9147,6+420,96 = 59148,56 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 59148,56 \text{ грн.}$$

3.3 Оцінка можливого збитку

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16200 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15100 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 13 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 240 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 2000 грн.;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 25.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

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

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{15100 \cdot 13}{176} \cdot 4 = 4461{,}36 \text{ грн},$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{15100 \cdot 13}{176} \cdot 6 = 6692{,}05 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{16200 \cdot 1}{176} \cdot 2 = 184{,}09 \text{ грн.}$$

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

$$П_в = 6692{,}05+184{,}09+2000 = 8876{,}14 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{240000}{2080} \cdot (4+2+6) = 1384{,}62 \text{ грн.}$$

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

$$U = 4461{,}36+8876{,}14+1384{,}62 = 14722{,}12 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{25} 14722{,}12 = 368053 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи СУІБ

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації загрози (25%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки, отже було розраховано:

$$E = 368053*0,25 - 59148,56 = 32864,69 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності СУІБ

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI=32864,69/ 21048 = 1,56 \text{ частки}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (13%);

$N_{інф}$ – річний рівень інфляції, (10%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,56 > (13 - 10)/100 = 1,56 > 0,03.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}$$

$$T_0 = 1 / 1,56 = 0,64 \text{ років.}$$

3.6 Висновок

Отже, згідно з наведеними розрахунками можливо зробити висновок, що обґрунтування впровадження СУІБ є економічно доцільним.

Капітальні витрати, які складають 21048 грн, дозволяють отримати ефект величиною 32864,69 грн. Відповідно до отриманих значень показників економічної ефективності можна зазначити, що такий підхід дозволить отримувати 1,56 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 1,56). Термін окупності при цьому складатиме 0,64 року.

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об’єктів прав інтелектуальної власності) та кількістю об’єктів прав інтелектуальної власності, право на авторство яких може бути порушеним.

ВИСНОВКИ

У кваліфікаційній роботі магістра проведено аналіз актуальності питання інформаційної безпеки в закладі фахової передвищої освіти. Актуальною проблемою системи фахової передвищої освіти в Україні за останні роки є аналіз використання веб-технологій для дистанційного навчання в умовах пандемії та воєнного стану. Вимушений перехід багатьох закладів освіти у веб-простір вимагає аналізу безпеки користування різноманітними сервісами. Важливим є дослідження загроз інформаційної безпеки для персональних даних студентів та викладачів, систем оцінювання, збору та зберігання даних. Також використання он-лайн сервісів в освіті підвищує вимоги до автентифікації користувачів, бо дистанційне навчання у багатьох випадках ускладнює об'єктивність оцінювання знань. Разом з тим, використання веб-технологій може полегшити збір даних, зменшити паперовий документообіг між викладачем та здобувачами, спростити доступ до матеріалів лекцій, методичних вказівок та іноді навіть покращити комунікацію між учасниками освітнього процесу. В ході аналізу визначені стандарти щодо розробок систем управління інформаційною безпекою та організації процесу управління ризиками інформаційної безпеки. Все це є головними елементами щодо побудови системи управління інформаційної безпеки ЗПФО. Проведено аналітичний огляд принципів та підходів до створення політик інформаційної безпеки, проведено їх порівняння. Розглянута методика проведення оцінки ризиків OCTAVE Allegro. Наведена структурно-логічна схема дій з розробці СУІБ. На основі проведеного аналізу, визначені задачі щодо побудови оптимального варіанту для вибору моделі управління ризиками інформаційної безпеки. Визначено, що такою моделлю є трирівнева модель. Також визначено, що методика OCTAVE Allegro може бути найефективнішою для оцінки ризиків у СУІБ ЗФПО на прикладі фахового коледжу. Розроблена структурна схема інформаційної системи ЗПФО. Представлено модель управління інформаційною безпекою ЗПФО. Проведена оцінка можливих загроз інформаційної безпеки ЗПФО. Виконана ідентифікація активів, ідентифікація загроз, ідентифікація та обробка ризиків в розробленій системі забезпечення інформаційної

безпеки. Розглянуто особливості організації інформаційної безпеки ЗФПО. Визначені головні загрози ІБ. Наведено декілька моделей управління інформаційною безпекою. Представлено принципи та підходи до створення політик інформаційної безпеки, а також проведений їх порівняльний аналіз. На основі отриманих даних побудована модель загроз та модель порушника, які притаманні ЗФПО. Здійснений вибір методики для управління ризиками інформаційної безпеки ЗФПО. На прикладі ЗФПО ФКРКМ досліджено та впроваджено розроблену СУІБ. Сформована модель управління інформаційною безпекою, яка забезпечена трьома рівнями. Впровадження системи управління ІБ дає можливість вибрати економічно ефективні елементи контролю, що зменшують ризик до прийнятного рівня.

У кваліфікаційній роботі проведено обґрунтування економічної ефективності впровадження СУІБ в ЗФПО.

Досвід розробки та дослідження системи управління інформаційною безпекою ФКРКМ може бути використаний для створення СУІБ інших закладів фахової передвищої освіти.

ПЕРЕЛІК ПОСИЛАНЬ

1 ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. - Київ: ДП "УкрНДНЦ", 200.335. - 60с

2 Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Електронний ресурс]. Режим доступу : https://insights.sei.cmu.edu/library/introducing-octave-allegro-improving-the-information-security-risk-assessment-process/

3. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : спец. 12.00.01 / Максименко Ю. Є. – К., 2007. – 22 с.

4. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / Берко А. Ю., Висоцька В. А., Рішняк І. В. // Вісник Національного університету —Львівська політехніка‖. – 2008. – № 610. – С. 20–33.

5. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних сис- тем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачно- го, 2014. — Вип. 8 (124).— ISSN 1681–7710. — С. 128–134.

6. Information technology — Security techniques–Information security risk management: ISO/IEC 27005 : 2008 [Електронний ресурс]. — Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=42107.

7. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : спец. 12.00.01 / Максименко Ю. Є. – К., 2007. – 22 с.

8. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : Офіційне Інтернет-представництво Президента України http: // www.president.gov.ua

9. Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%Dl %80#Text

10. Закон України «Про захист персональних даних» (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) / Спосіб доступу: URL: https://zakon.rada.gov. ua/laws/show/2297-17#Text

11 ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість аркушів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	45	
6	А4	Спеціальна частина	22	
7	А4	Економічний розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Бобошко_ОВ.ppt

2 Диплом Бобошко_ОВ.doc

ДОДАТОК В. Відгук керівника економічного розділу

Бобошко Олександр Володимирович у кваліфікаційній роботі представил опис об'єкту, а саме систему управління інформаційною безпекою закладу фахової передвищої освіти. Проведено розрахунок собівартості впровадження системи. Проведено розрахунок економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень. При виконанні кваліфікаційної роботи Бобошко О.В. виявив достатні теоретичні та практичні знання та належним чином виконав усі розрахункові завдання. Календарний графік щодо виконання економічного розділу витримувався. Завдання економічного розділу виконані у повному обсязі. Економічний розділ кваліфікаційної роботи Бобошка Олександра Володимировича заслуговує оцінки _____

Керівник розділу,
к.е.н., доц. _____ Пілова Д.П.
(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22з-1 Бобошко О.В. на тему: «Розробка та дослідження системи управління інформаційної безпеки закладу фахової передвищої освіти»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 87 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на розробку та дослідження системи управління інформаційної безпеки.

Система управління інформаційною безпекою використовується для забезпечення ефективного захисту інформації від несанкціонованого доступу, руйнівної дії, витоку чи втрати. Дані системи мають дуже широке застосування у більшості сфер де необхідний захист інформації, що свідчить про актуальність теми кваліфікаційної роботи.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів побудови сучасних систем управління інформаційною безпекою сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У спеціальному розділі наведено опис інформаційної системи коледжу, який потребує впровадження системи управління інформаційною безпекою, наведено модель управління, класифікація загроз інформаційної безпеки закладу фахової передвищої освіти, організаційна структура системи забезпечення інформаційної безпеки закладу фахової передвищої освіти, наведена методика оцінки ризиків кібербезпеки.

Наукова новизна результатів полягає у запропонованому підході до побудови системи управління інформаційною безпекою закладу фахової передвищої освіти, представленій методиці оцінки ризиків. Практична цінність роботи полягає у тому, що цей підхід можна використовувати у закладі фахової

передвищої освіти для покращення захисту інформаційних ресурсів в умовах обмежених матеріальних та фінансових можливостей.

До недоліків роботи слід віднести недостатню проробку окремих питань. Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Бобошко О.В. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,

д.т.н., професор **В.І. Корнієнко**