НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НА ПРИКЛАДІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека»
Голомозенко Володимир Сергійович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.фіз.-мат.наук., доцент
Чепурна Олена Євгенівна

Одеса 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

ЗАВДАННЯ
на кваліфікаційну (бакалаврську) роботу
здобувачу Голомозенку Володимиру Сергійовичу

1. Тема роботи: «Формування політики безпеки на об’єктах інформаційної діяльності на прикладі органів місцевого самоврядування»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)
Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Формування політики безпеки на об’єктах інформаційної діяльності на прикладі органів місцевого самоврядування» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 14 літературних джерел за переліком посилань. Робота виконана на 41 сторінці загального тексту та 33 сторінках основного тексту.

Метою роботи є аналіз сучасного стану питань інформаційної безпеки в органах місцевого самоврядування та розробка стратегічних напрямків для підвищення рівня захисту їхніх інформаційних ресурсів. У роботі розглянуто принципи та поняття інформаційної безпеки, визначено основні загрози та вразливості інформаційних систем, а також запропоновано механізми захисту від кіберзагроз та кібератак. Проаналізовано існуючі стандарти та рекомендації у сфері інформаційної безпеки, а також оцінено сучасний стан захисту інформації в органах місцевого самоврядування.

Результати роботи можуть бути використані при розробці та впровадженні політик інформаційної безпеки в органах місцевого самоврядування, а також для підвищення рівня захисту інформаційних ресурсів в інших державних та приватних установах.

Можливими напрямками подальших досліджень є розробка нових методів і засобів захисту інформації, а також удосконалення існуючих стратегій з метою підвищення їх ефективності в умовах постійно зростаючих загроз інформаційної безпеки.

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ОРГАНИ МІСЦЕВОГО САМОВРЯДУВАННЯ, ПОЛІТИКА БЕЗПЕКИ.

ABSTRACT

Qualification paper on the topic "Development of Security Policies for Information Activity Objects on the Example of Local Government Bodies" for obtaining the first (bachelor's) level of higher education in specialty 125 Cybersecurity, educational program: Cybersecurity, contains 14 literary sources according to the list of references. The work is completed on 41 pages of the general text and 33 pages of the main text.

The aim of the work is to analyze the current state of information security issues in local government bodies and to develop strategic directions for enhancing the level of protection of their information resources. The paper examines the principles and concepts of information security, identifies the main threats and vulnerabilities of information systems, and proposes mechanisms for protection against cyber threats and cyber-attacks. Existing standards and recommendations in the field of information security are analyzed, and the current state of information protection in local government bodies is assessed.

The results of the work can be used in the development and implementation of information security policies in local government bodies, as well as to enhance the level of protection of information resources in other public and private institutions.

Possible directions for further research include the development of new methods and means of information protection, as well as the improvement of existing strategies to increase their effectiveness in the face of constantly growing information security threats.

INFORMATION SECURITY, CYBERSECURITY, INFORMATION PROTECTION, LOCAL GOVERNMENT BODIES, SECURITY POLICY.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КБ – Кібербезпека

СУІБ – Система управління інформаційною безпекою

ISO/IEC –International Organization for Standardization / International Electrotechnical Commission (міжнародна організація зі стандартизації / міжнародна електротехнічна комісія)

GDPR – General Data Protection Regulation (загальний регламент захисту даних)

CIA – Confidentiality, Integrity, Availability (конфіденційність, цілісність, доступність)

SIEM – Security Information and Event Management (управління інформацією та подіями безпеки)

DDoS – Distributed Denial of Service (розподілене відмовлення в обслуговуванні)

ЗМІСТ

ВСТУП

В сучасному цифровому світі інформація стала однією з найцінніших ресурсів. Органи місцевого самоврядування, які відповідають за ефективне управління містами та регіонами, надзвичайно залежать від інформаційних технологій та баз даних для виконання своїх функцій. Проте, разом із зростанням значення інформації збільшується й загроза її безпеці. Кіберзлочинці постійно вдосконалюють свої методи нападів, а потенційні загрози стають все більш складними і небезпечними. У цьому контексті важливо, щоб органи місцевого самоврядування приділяли особливу увагу питанням інформаційної безпеки та розробляли ефективні політики для захисту своїх інформаційних ресурсів.

Актуальність теми формування політики безпеки на об’єктах інформаційної діяльності, зокрема в органах місцевого самоврядування, особливо насичується в умовах військових конфліктів та відкритих суперництв. У таких умовах інформаційна безпека стає надзвичайно важливою для забезпечення стабільності та ефективності управління містами та регіонами. Небезпека кібератак та витоків конфіденційної інформації стає серйозною загрозою для функціонування органів місцевого самоврядування та захисту інтересів громадян.

Метою даної кваліфікаційної роботи є аналіз сучасного стану питань інформаційної безпеки в органах місцевого самоврядування та розробка стратегічних напрямків для підвищення рівня захисту їхніх інформаційних ресурсів. Це включає в себе огляд загроз, з якими стикаються органи місцевого самоврядування у цифровому середовищі, а також ідентифікацію недоліків та проблем, які варто вирішити для забезпечення ефективного захисту інформації.

Здатність забезпечувати безпеку інформаційних ресурсів є ключовим аспектом сучасного управління в умовах постійних загроз інформаційної безпеки. Правильно розроблена та ефективно впроваджена політика безпеки може допомогти зменшити ризики кібератак та забезпечити стабільність та безпеку в діяльності органів місцевого самоврядування.

Об’єктом дослідження є процес забезпечення інформаційної безпеки на об’єктах інформаційної діяльності, зокрема в органах місцевого самоврядування.

Предметом дослідження є методи, стратегії та практичні аспекти формування політики безпеки з метою захисту інформаційних ресурсів в органах місцевого самоврядування.

У даній роботі проводиться огляд сучасних методів технічного захисту інформації, а також вивчаються та аналізуються підходи до управління кібербезпекою в органах місцевого самоврядування.

Робота складається з трьох розділів. У першому розділі «Теоретичні аспекти формування політики безпеки» розглянуто загальні принципи та поняття інформаційної безпеки, а також механізми захисту від кіберзагроз та кібератак.

У другому розділі «Аналіз сучасного стану питань інформаційної безпеки» буде проведено огляд існуючих підходів до захисту інформації в органах місцевого самоврядування, виявлені недоліки та проблемні аспекти у сфері інформаційної безпеки.

У третьому розділі «Стратегії підвищення рівня захисту інформаційних ресурсів» будуть визначені стратегічні напрямки для підвищення інформаційної безпеки, розглянуті можливі заходи та політичні рішення для забезпечення безпеки інформаційних ресурсів органів місцевого самоврядування.

1 ТЕОРЕТИЧНІ АСПЕКТИ ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ

Теоретичні аспекти формування політики безпеки включають ряд ключових елементів, що визначають стратегічні та тактичні напрямки організації в галузі забезпечення безпеки інформації [8]. Ось детальний розгляд цих аспектів:

– Аналіз загроз і ризиків: політика безпеки повинна базуватися на глибокому аналізі потенційних загроз і ризиків, з якими стикається організація. Це включає в себе ідентифікацію потенційних загроз зовнішнього та внутрішнього середовища, оцінку ймовірності та впливу цих загроз на діяльність організації.

– Визначення цілей і завдань: після аналізу загроз і ризиків важливо визначити конкретні цілі та завдання політики безпеки. Ці цілі можуть включати захист конфіденційності, цілісності та доступності даних, забезпечення безпеки мереж та інфраструктури, а також забезпечення відповідності вимогам законодавства [8].

– Встановлення стратегій та процедур: політика безпеки повинна містити стратегії та процедури, спрямовані на досягнення визначених цілей. Це включає в себе розробку правил і стандартів безпеки, впровадження механізмів контролю та моніторингу, а також розробку планів реагування на інциденти безпеки.

– Залучення зацікавлених сторін: формування політики безпеки є командною зусиллям, яке вимагає участі всіх зацікавлених сторін, включаючи керівництво, власників бізнесу, відділ інформаційної безпеки та інших відділів. Важливо забезпечити розуміння та підтримку політики безпеки серед всіх зацікавлених сторін.

– Оцінка та аудит: політика безпеки повинна регулярно оцінюватися та аудитуватися з метою виявлення слабких місць та вдосконалення стратегій і процедур. Це дозволить організації підтримувати високий рівень безпеки і адаптувати свої підходи до змін у загрозах та технологічному середовищі.

1.1 Принципи і поняття інформаційної безпеки

Інформаційна безпека є складною та багатогранною областю, яка ґрунтується на ряді принципів та понять [3, 11]. Нижче розглянуті основні принципи та поняття інформаційної безпеки з прив’язкою до прикладів з діяльності органів місцевого самоврядування в Україні [9]:

1) Принцип відповідальності передбачає, що кожен працівник органу місцевого самоврядування має бути відповідальний за безпеку інформації, якою він оперує. Наприклад, керівник відділу має бути відповідальним за встановлення правил доступу до конфіденційної інформації та забезпечення їх виконання всіма працівниками [8].

2) Принцип етики покликаний забезпечити етичність та законність дій працівників у використанні інформації. Наприклад, використання персональної інформації мешканців для будь-яких цілей, окрім офіційних, може порушувати принцип етики.

3) Принцип демократії означає, що рішення про заходи забезпечення інформаційної безпеки мають бути прийняті на демократичних засадах, залучаючи всіх зацікавлених сторін [8]. Наприклад, розробка та впровадження правил доступу до інформації повинна проводитися з урахуванням думки всіх працівників органу.

4) Принцип обізнаності передбачає, що працівники повинні бути інформовані про загрози та ризики, пов’язані з інформаційною безпекою, та про заходи щодо їх запобігання. Наприклад, організація тренінгів та інформаційних кампаній з питань кібербезпеки.

5) Принцип протидії передбачає прийняття заходів для виявлення, запобігання та реагування на потенційні загрози для інформаційної безпеки. Наприклад, встановлення систем моніторингу та виявлення вторгнень для реагування на кібератаки.

6) Принцип оцінки ризиків передбачає проведення систематичного аналізу потенційних загроз та вразливостей для оцінки ризиків інформаційної безпеки.

Наприклад, оцінка ризиків використання застарілих програмних продуктів для обробки конфіденційної інформації.

7) Принцип перегляду передбачає систематичне переглядання та оновлення політик, процедур та технічних засобів інформаційної безпеки з метою забезпечення їхньої актуальності та ефективності. Наприклад, періодичні аудити та ревізії систем безпеки для виявлення можливих слабких місць та пропозицій щодо вдосконалення [8].

8) Принцип розробки та впровадження інформаційної безпеки покликаний забезпечити системний та узгоджений підхід до розробки, впровадження та підтримки заходів інформаційної безпеки в організації. Наприклад, етапна реалізація заходів забезпечення інформаційної безпеки, починаючи з аналізу потреб та закінчуючи впровадженням та контролем [8].

9) Принцип управління безпекою передбачає наявність чіткої системи управління безпекою, яка включає в себе структуру, процедури та механізми контролю за дотриманням політики інформаційної безпеки. Наприклад, визначення відповідальних осіб за впровадження та виконання політики інформаційної безпеки, а також механізмів звітності та контролю.

Поняття інформаційної безпеки можна розглядати з різних точок зору, враховуючи контекст її використання та потреби. Основними аспектами поняття інформаційної безпеки є:

1) Конфіденційність інформації є ключовим аспектом інформаційної безпеки. Вона означає, що лише уповноважені особи мають доступ до конфіденційної інформації, а несанкціонованим особам він недоступний. Це може бути досягнуто шляхом різних заходів, таких як застосування шифрування даних, управління правами доступу та контроль доступу до приміщень та обладнання.

2) Цілісність інформації забезпечує, що дані залишаються незмінними та недоторканими від несанкціонованих модифікацій. Це означає, що будь-які зміни або модифікації даних мають бути виявлені та запобіжні. Для досягнення цього можуть використовуватися хеш-функції та цифрові підписи, які дозволяють перевірити цілісність даних.

3) Доступність інформації – це принцип, який забезпечує, що інформація та ресурси доступні для користувачів у відповідний час та місце. Це важливо для підтримки продуктивності та ефективності роботи організації. Для забезпечення доступності можуть використовуватися резервне копіювання даних, моніторинг стану систем, а також механізми виявлення та відновлення випадків відмов [8].

4) Аутентифікація та авторизація – це процеси, які забезпечують перевірку ідентичності користувача та надання йому відповідних прав доступу. Аутентифікація визначає, хто саме намагається отримати доступ, тоді як авторизація визначає, що саме користувач може робити з отриманим доступом.

Ці принципи і поняття інформаційної безпеки є фундаментальними для розробки та впровадження ефективної стратегії захисту інформаційних ресурсів органів місцевого самоврядування. Їх реалізація дозволить забезпечити надійний захист конфіденційної інформації та зберегти довіру громадян до діяльності владних структур.

1.2 Загрози та вразливості інформаційних систем

Загрози та вразливості інформаційних систем є важливим етапом у розробці політики безпеки [4]. Правильна ідентифікація цих факторів дозволяє організації виявляти потенційні ризики та приймати необхідні заходи для їх запобігання.

Однією з найсерйозніших загроз є кібератаки. Це різні види атак, спрямованих на інформаційні системи з метою отримання конфіденційної інформації, завдання матеріальних збитків або руйнування репутації. Кіберзлочинці використовують різноманітні методи, такі як фішинг, віруси, шкідливі програми та атаки на мережеві протоколи, щоб отримати доступ до системи.

Другою загрозою є недостатній контроль над правами доступу. Недостатнє управління доступом може призвести до витоку конфіденційної інформації або навіть до несанкціонованого доступу до системи. Для запобігання цьому важливо встановити ефективні механізми аутентифікації та авторизації.

Третій аспект – відсутність оновлень та патчів. Недостатнє оновлення програмного забезпечення та встановлення патчів може створювати вразливості, які використовуються кіберзлочинцями для атак. Патчі виправляють виявлені вразливості та допомагають підтримувати безпеку системи на відповідному рівні [4].

Загрози інформаційних систем можуть бути різноманітні і включати в себе:

1) Кібератаки: це спроби несанкціонованого доступу до інформації або інших цифрових ресурсів з метою втручання, крадіжки або руйнування.

2) Віруси та шкідливі програми: це програмні коди, які призначені для нанесення шкоди інформаційним системам, включаючи видалення або крадіжку даних, відмову в обслуговуванні та інше.

3) Фішинг: це метод соціальної інженерії, коли атакуючі використовують підроблені електронні листи, вебсайти або повідомлення, щоб отримати конфіденційну інформацію від користувачів.

4) Деніал сервіс (DDoS) атаки: це спроби перевантаження серверів або мережі, щоб вони перестали працювати для легітимних користувачів.

5) Недбалість користувачів: це ситуації, коли користувачі вчиняють дії, які створюють загрози безпеці інформаційних систем, наприклад, використання слабких паролів або незахищених мереж Wi-Fi.

Вразливості інформаційних систем - це слабкі місця або дефекти, які можуть бути використані зловмисниками для злому або порушення безпеки системи. Ці вразливості можуть включати недоліки у програмному забезпеченні, погано налаштовані мережі, слабкі паролі, а також вразливості у фізичній безпеці [4]. Вони можуть призвести до втрати конфіденційності, цілісності та доступності даних, а також до порушення нормального функціонування системи. Управління вразливостями є важливою складовою безпеки інформаційних систем і включає в себе виявлення, аналіз та виправлення цих слабких місць для забезпечення захисту системи від потенційних загроз [8].

Відповідно до класу активів, до яких вони відносяться, уразливості класифікуються на кілька типів.

Першим типом вразливостей є ті, що стосуються апаратного забезпечення. Це означає, що апаратні пристрої можуть бути вразливі до різних умов довкілля, таких як вологість, пил, забруднення або незахищене зберігання. Наприклад, вологість може призвести до корозії контактів або короткого замикання електричних компонентів. Пил і забруднення можуть затримувати тепло і призводити до перегріву пристроїв. Незахищене зберігання може призвести до фізичного пошкодження або втрати даних через несприятливі умови.

Другим видом вразливостей є програмне забезпечення. Це означає, що програми можуть мати помилки або дефекти, які можуть бути використані зловмисниками для виконання небажаних дій або отримання несанкціонованого доступу. Недостатнє тестування програм може призвести до пропуску критичних вад, які стають джерелом вразливостей. Відсутність аудиту програмного коду може ускладнити виявлення і усунення помилок.

Третій тип вразливостей стосується комп’ютерних мереж. Це означає, що мережеві з’єднання можуть бути незахищеними або вразливими до атак. Наприклад, відсутність шифрування трафіку може дозволити зловмисникам перехоплювати та зчитувати конфіденційні дані. Незахищена мережева архітектура може мати слабкі точки, які можна експлуатувати для незаконного доступу до системи.

Четвертий вид вразливостей стосується персоналу. Це означає, що люди, які мають доступ до системи, можуть становити ризик через недоліки найму або недостатню підготовку. Наприклад, якщо працівники не проходять достатню школу з інформаційної безпеки, вони можуть бути недостатньо обізнані з потенційними загрозами та правилами безпеки.

П’ятий вид вразливостей стосується самого вебсайту. Це означає, що веб-ресурси можуть містити вразливості, які дозволяють зловмисникам отримувати несанкціонований доступ або впливати на користувачів через шкідливе вміст або атаки [4]. Ненадійні джерела живлення на веб-сайті можуть бути джерелом шкідливих програм або коду, які можуть завдати шкоди відвідувачам.

Останнім типом вразливостей є організаційні. Це означає, що внутрішні процеси та політики організації можуть бути недостатньо ефективними для захисту від кіберзагроз. Наприклад, відсутність регулярних перевірок безпеки може дозволити виявити уразливості пізно, коли вже завдано шкоди. Відсутність планів безперервності може ускладнити відновлення роботи після кібератаки [5].

Щодо програмного забезпечення, існує кілька поширених типів вразливостей, таких як порушення безпеки доступу до пам’яті, помилки перевірки введених даних та невірна підтримка інтерпретації метасимволів командної оболонки. Причини вразливостей можуть бути пов’язані з фундаментальними недоліками дизайну операційних систем, переглядом вебсайтів, помилками в програмному забезпеченні та необмеженим введенням користувачів. Наслідки вразливостей можуть бути серйозними, тому виявлення та усунення їх важливо для забезпечення безпеки інформаційних систем [9].

Порушення безпеки може мати серйозні наслідки, такі як втрата конфіденційної інформації, порушення цілісності даних або навіть виток особистої інформації користувачів. Це може призвести до великих фінансових втрат, порушення репутації компанії або навіть правових наслідків.

Для виявлення та усунення вразливостей інформаційних систем використовуються різні методи. Наприклад, проведення зондування, або пошуку вразливостей, що дозволяє ідентифікувати потенційні проблеми у системі. Також важливо вести моніторинг системи та встановлювати оновлення, які містять заходи безпеки. Інші практики включають в себе використання інструментів, що допомагають у виявленні потенційних загроз та небезпек, а також впровадження стратегій управління інформаційною безпекою, які відповідають вимогам стандартів, таких як ISO/IEC 27002.

Оскільки нові уразливості постійно виявляються, важливо пам’ятати про постійну пильність і приймати відповідні заходи для захисту системи від потенційних атак.

Поміж методів інформування про вразливості інформаційних систем є дискусія. Деякі експерти вважають, що важливо негайно повідомляти про будь-які

знайдені уразливості, дозволяючи розробникам швидко виправити їх та застосувати необхідні заходи безпеки. Інші вважають, що інформацію про вразливості слід розголошувати тільки тим користувачам, які піддаються найбільшому ризику, а повну інформацію публікувати лише після затримки або зовсім не публікувати, щоб уникнути можливих зловживань [4].

Забезпечення захищеності та цілісності інформаційних систем вимагає постійного моніторингу, встановлення оновлень та використання спеціальних інструментів для виявлення можливих загроз. [8] Уразливості можуть існувати у всіх основних операційних системах, включаючи Microsoft Windows, Mac OS, різні варіанти UNIX (у тому числі GNU / Linux) і OpenVMS. Тому, для зменшення ймовірності їх використання, необхідна постійна увага та вжиття відповідних заходів безпеки [5].

1.3 Механізми захисту від кіберзагроз та кібератак

Механізм захисту від кіберзагроз включає комплекс заходів, спрямованих на запобігання, виявлення та відновлення після кібератак. Першим кроком є розробка та впровадження політик і стандартів безпеки, які визначають правила та процедури для захисту інформаційних активів організації. Ці політики повинні охоплювати всі аспекти інформаційної безпеки, включаючи захист мережі, захист даних, керування доступом та навчання персоналу.

Другим кроком є використання технічних засобів захисту, таких як антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень та системи моніторингу безпеки. Ці засоби допомагають виявляти та блокувати потенційні загрози перед тим, як вони зможуть завдати шкоди.

Третій крок – це постійна підтримка та оновлення програмного забезпечення та апаратного забезпечення. Це включає в себе встановлення патчів та оновлень для виправлення виявлених вразливостей, а також оновлення програмного забезпечення до останніх версій з метою отримання нових функцій та підвищення безпеки [8].

Четвертий крок – навчання та свідоме ставлення персоналу до кібербезпеки. Це включає проведення навчань та тренінгів з питань кібербезпеки, регулярну інформаційну розсилку з попередженнями про потенційні загрози та встановлення політик щодо використання інформаційних технологій на робочому місці.

П’ятий крок – це реагування на інциденти та відновлення після кібератак. Це включає розробку та впровадження планів реагування на інциденти, які визначають процедури для виявлення, відключення та відновлення після кібератаки. Також важливо проводити аналіз інцидентів з метою вдосконалення заходів захисту та попередження майбутніх атак.

В сучасному цифровому світі захист від кібератак стає все більш важливим для підприємств і організацій будь-якого розміру. Механізм захисту від кібератак включає комплекс заходів, спрямованих на запобігання, виявлення та відновлення після кібератак.

Першим кроком у механізмі захисту від кібератак є розробка і впровадження комплексу заходів з превентивного захисту. Це включає налаштування брандмауерів, інтеграцію систем виявлення вторгнень та застосування інших технічних засобів захисту мережі та інформаційних систем.

Другим етапом є постійний моніторинг та аналіз діяльності мережі та інформаційних систем для виявлення аномальних поведінок, підозрілих активностей або спроб несанкціонованого доступу. Це включає в себе використання систем виявлення вторгнень, моніторингу журналів подій та аналізу відхилень від типових моделей поведінки.

Третім кроком є розробка та впровадження планів реагування на кібератаки, які визначають процедури для виявлення, ізоляції та відновлення після інцидентів. Ці плани повинні включати чіткі кроки для виявлення діяльності зловмисників, зупинки розповсюдження загрози та відновлення нормального функціонування систем.

Четвертим етапом є навчання персоналу щодо кібербезпеки, включаючи навчання про процедури захисту, розпізнавання підозрілих активностей та поведінки, а також процедури реагування на інциденти.

П’ятим кроком є постійне оновлення та вдосконалення заходів захисту відповідно до змін у загрозах кібербезпеки та нових технологій. Це включає в себе вивчення нових загроз, аналіз інцидентів, а також впровадження патчів та оновлень для виправлення виявлених вразливостей [2].

Отже, механізми захисту від кіберзагроз та кібератак стають невід’ємною частиною сучасного бізнесу і організаційного управління. Інтегрований підхід до кібербезпеки, який включає розробку політик безпеки, моніторинг, планування реагування та навчання персоналу, дозволяє ефективно запобігати, виявляти та відновлюватися після кібератак. Ці механізми допомагають забезпечити надійний захист інформаційних активів і зберегти довіру в цифровому середовищі.

1.4 Стандарти та рекомендації у сфері інформаційної безпеки

Стандарти у сфері інформаційної безпеки є сукупністю методів, процедур та правил, які призначені для захисту конфіденційності, цілісності та доступності інформації в комп’ютерних системах. Вони охоплюють управління ризиками, захист від несанкціонованого доступу, криптографічний захист інформації, а також захист персональних даних [13]. Ці стандарти можуть бути встановлені організаціями або прийняті національними або міжнародними організаціями з метою забезпечення найвищого рівня безпеки в інформаційних системах [7].

Історія стандартів у сфері інформаційної безпеки налічує кілька десятиліть. Початкові роботи у цій області відбувалися у 1990-х роках в рамках Стенфордського консорціуму з досліджень з питань інформаційної безпеки та політики. З того часу стандарти у цій сфері постійно розвиваються завдяки співпраці між користувачами та постачальниками на різних національних та міжнародних форумах.

Міжнародні стандарти у сфері інформаційної безпеки включають в себе такі документи, як ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, а також BS 7799 [10]. Ці стандарти описують системи управління інформаційною безпекою та практичні правила управління інформаційною безпекою. Вони становлять основу для

розробки та впровадження заходів з підвищення безпеки інформаційних систем у різних країнах світу [7].

Система управління інформаційною безпекою (СУІБ) є набором процедур та практик, які спрямовані на ефективне управління ризиками та захист інформації в організації. Вона включає в себе розробку політик безпеки, ідентифікацію та оцінку ризиків, впровадження технічних та організаційних заходів, а також контроль та аудит безпеки інформації.

Захист від несанкціонованого доступу у сфері інформаційної безпеки охоплює широкий спектр технічних та організаційних заходів. Це включає в себе реалізацію сильних методів аутентифікації, контроль доступу до систем та даних, моніторинг активності користувачів, а також навчання персоналу щодо безпечних практик роботи з інформацією.

Криптографічний захист інформації у сфері інформаційної безпеки використовує різноманітні шифрувальні алгоритми та протоколи для захисту конфіденційної інформації від несанкціонованого доступу під час передачі через мережу або зберігання на пристроях [13]. Використання криптографії дозволяє забезпечити конфіденційність та цілісність даних у віртуальному середовищі.

Захист персональних даних у сфері інформаційної безпеки включає в себе різні заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності особистої інформації [8]. Це включає в себе шифрування даних, обмеження доступу до них, реалізацію правил щодо обробки особистої інформації, а також впровадження заходів безпеки для запобігання несанкціонованому доступу до цих даних.

Зважаючи на постійно зростаючу складність кіберзагроз і кібератак, рекомендації у сфері інформаційної безпеки стають критично важливими для будь-якої організації чи користувача. Давайте розглянемо кожну з них докладніше:

1) Регулярні аудити та тестування безпеки: аудити безпеки є важливим етапом для виявлення слабких місць в інфраструктурі та програмних засобах. Тестування на проникнення дозволяє експертам виявити потенційні вразливості, які можуть бути використані зловмисниками [4].

2) Захист мережі: брандмауери та системи виявлення вторгнень створюють бар’єри, що мінімізують ризики витоку даних та незаконного доступу. Моніторинг мережі дозволяє оперативно виявляти аномальні патерни трафіку, що може свідчити про атаку.

3) Аутентифікація та авторизація: сильна аутентифікація є важливою для забезпечення тільки легітимним користувачам доступу до системи [8]. Комбінація факторів аутентифікації, таких як пароль та біометричні дані, забезпечує високий рівень безпеки.

4) Шифрування даних: шифрування даних гарантує, що навіть у випадку несанкціонованого доступу до інформації, зловмисники не зможуть прочитати її. Це особливо важливо для конфіденційних даних, таких як особиста інформація або фінансові дані.

5) Освіта та навчання персоналу: найбільша загроза для безпеки часто виникає через людський фактор. Навчання персоналу з питань кібербезпеки допомагає створити свідомих користувачів, які вміють виявляти та уникати потенційних загроз [2].

6) Створення планів реагування на інциденти: безпека не може бути абсолютною, тому важливо мати плани дій для реагування на інциденти. Швидка реакція та ефективне відновлення після атаки допомагають зменшити збитки.

7) Резервне копіювання даних: регулярне створення резервних копій даних забезпечує можливість відновлення інформації у випадку втрати або пошкодження основного джерела.

8) Створення культури безпеки: культура безпеки, що поширюється на всіх рівнях організації, сприяє створенню середовища, де кожен працівник відчуває відповідальність за захист інформації.

Ці рекомендації допомагають побудувати повноцінну систему захисту, що забезпечує ефективний захист від кіберзагроз.

2 АНАЛІЗ СУЧАСНОГО СТАНУ ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасний стан інформаційної безпеки характеризується комплексністю викликів і загроз, які стикаються користувачі та організації в цифровому середовищі. Ось кілька ключових аспектів сучасного стану інформаційної безпеки:

1) Різноманітність загроз: загрози від кібератак набули різноманітних форм і рівнів складності. Вони включають в себе атаки з використанням шкідливих програм, фішинг, DDoS-атаки, крадіжку даних, розкрадання ідентифікаційних даних та інші.

2) Глобальний масштаб: кіберзагрози не обмежуються географічними межами. Зловмисники можуть атакувати будь-яку точку світу, використовуючи мережу Інтернет як засіб для швидкого та анонімного здійснення атак.

3) Зростаюча складність технологій: швидкий розвиток технологій, таких як хмарні обчислення, Інтернет речей (IoT), штучний інтелект (AI) та блокчейн, створює нові можливості для зловмисників і водночас ускладнює завдання забезпечення безпеки [8].

4) Підвищена увага до захисту даних: востанні роки споживачі стали більш свідомими щодо захисту своїх персональних даних. Це призвело до посилення вимог до організацій з їх обробки та зберігання.

5) Реакція законодавства: у багатьох країнах посилюються вимоги до захисту даних, що виражається у введенні нових правил і законодавчих актів, таких як Загальний регламент з захисту даних (GDPR) в Європейському Союзі та Цифровий Єдиний ринок в Сполучених Штатах.

6) Зростання інвестицій у кібербезпеку: організації вкладають все більше ресурсів у засоби та технології кібербезпеки, оскільки вони усвідомлюють важливість захисту своєї інформації та систем від потенційних загроз.

7) Загалом, сучасний стан інформаційної безпеки вимагає постійного удосконалення стратегій, технологій та практик, щоб ефективно відповідати на зростаючі виклики і загрози в цифровому середовищі.

Аналіз сучасного стану інформаційної безпеки, враховуючи ключові виклики та тенденції:

1) Виклики безпеки даних: з розвитком технологій та збільшенням обсягу цифрових даних зростає й ризик їх втрати або порушення. Кількість кібератак, спрямованих на організації з метою крадіжки чутливих даних, постійно зростає.

2) Необхідність забезпечення конфіденційності та цілісності даних: захист конфіденційності та цілісності даних стає критичним завданням для багатьох секторів, зокрема для медичних установ, фінансових організацій та урядових установ [6].

3) Зростання кількості пристроїв IoT: підключення все більшої кількості пристроїв до мережі Інтернет (IoT) створює нові можливості для кіберзлочинців. Недостатня безпека цих пристроїв може призвести до серйозних кібератак на підприємства та приватних користувачів.

4) Соціальна інженерія: широке поширення соціальної інженерії дозволяє кіберзлочинцям отримувати доступ до систем та інформації шляхом маніпулювання людьми. Ця тенденція показує, що технічні заходи безпеки не завжди є достатніми для захисту від кіберзагроз.

5) Потреба відповідності: законодавство про захист даних стає все більшим фактором в сфері інформаційної безпеки. Організаціям потрібно не лише забезпечити безпеку своїх систем, але й дотримуватися вимог регуляторів щодо захисту даних, таких як GDPR в Європейському Союзі або HIPAA в Сполучених Штатах.

6) Необхідність постійного оновлення технологій: швидкість змін в сфері кібербезпеки вимагає постійного оновлення технологій та підвищення кваліфікації персоналу. Сучасні кіберзагрози постійно еволюціонують, і організаціям потрібно бути готовими до викликів, які вони ставлять [2].

Узагальнюючи, сучасний стан інформаційної безпеки відображає складність та динаміку цифрового світу. Організаціям необхідно постійно оновлювати свої стратегії та заходи забезпечення безпеки, щоб відповідати на зростаючі виклики та тенденції в цій області [8].

2.1 Огляд існуючих підходів до захисту інформації в органах місцевого самоврядування

Огляд підходів до захисту інформації в органах місцевого самоврядування є важливим кроком у забезпеченні ефективного функціонування цих установ. У зв’язку зі зростанням кількості цифрових загроз та вразливостей, збереження конфіденційності, цілісності та доступності даних стає дедалі важливішою задачею для місцевих органів влади.

Першим кроком у формуванні ефективної політики безпеки інформації є розробка і впровадження систем управління інформаційною безпекою. Ці системи мають включати в себе не лише технічні заходи захисту, але й організаційні та адміністративні процедури, спрямовані на мінімізацію ризиків і підвищення реагування на потенційні загрози.

Створення чіткої політики безпеки є ще одним ключовим аспектом. Ця політика повинна визначати правила та процедури щодо обробки, зберігання та передачі інформації, а також встановлювати відповідальність за її дотримання. Регулярне навчання персоналу з питань інформаційної безпеки також є важливим елементом, оскільки воно допомагає усвідомити загрози та прийняти належні заходи для їх запобігання.

Постійний моніторинг та аудит систем безпеки є обов’язковими етапами для виявлення можливих загроз та вразливостей. Це дозволяє оперативно реагувати на потенційні проблеми та вчасно вживати відповідних заходів для їх усунення.

Використання сучасних технологій, таких як шифрування даних та системи моніторингу безпеки, може допомогти підвищити рівень захисту. Шифрування даних дозволяє забезпечити конфіденційність інформації під час її передачі та зберігання, тоді як системи моніторингу безпеки надають можливість виявляти незвичайну активність та вчасно реагувати на потенційні загрози.

Крім того, співпраця та обмін інформацією з іншими установами є важливим аспектом захисту інформації в органах місцевого самоврядування. Це дозволяє обмінюватися досвідом та кращими практиками у сфері інформаційної безпеки, а

також підтримувати взаємну підтримку та координацію у разі виникнення кризових ситуацій.

2.2 Виявлення недоліків та проблемних аспектів у сфері інформаційної безпеки

Виявлення недоліків у сфері інформаційної безпеки є критичним етапом у процесі забезпечення безпеки та захисту даних [8]. Цей процес допомагає ідентифікувати потенційні проблеми, ризики та вразливості в існуючій системі безпеки, що може виявитися ключовим для запобігання кібератак та негативних наслідків для організації [4].

Один із способів виявлення недоліків - проведення регулярних аудитів інформаційної безпеки. Ці аудити включають оцінку технічних та організаційних заходів безпеки, перевірку відповідності з внутрішніми та зовнішніми стандартами безпеки, а також оцінку ефективності заходів захисту даних.

Додатковим способом є моніторинг систем безпеки та аналіз журналів подій. Це дозволяє виявляти незвичайну активність, атаки або інші потенційно шкідливі події, які можуть вказувати на існування недоліків у системі безпеки.

Також важливо проводити оцінку ризиків, щоб ідентифікувати потенційні загрози та визначити їх вплив на організацію. Це допомагає приймати обґрунтовані рішення щодо вдосконалення системи безпеки та вироблення пріоритетів у сфері захисту даних.

Нарешті, важливо мати процедури та механізми для збору та аналізу зворотного зв’язку від користувачів та співробітників організації. Це дозволяє виявляти проблеми та недоліки з точки зору кінцевих користувачів, що може допомогти у виявленні та вирішенні проблем у сфері інформаційної безпеки.

Проблемні аспекти у сфері інформаційної безпеки становлять серйозні виклики для організацій і можуть мати різноманітні характеристики та наслідки. Деякі з них включають:

1) Недостатня усвідомленість ризиків: багато організацій не розуміють повністю потенційні загрози і ризики, яким піддаються їхні інформаційні ресурси. Це може призвести до недооцінки потенційних загроз та неправильного розподілу ресурсів для захисту даних.

2) Брак фінансування та ресурсів: недостатнє фінансування і недостатні ресурси можуть ускладнити впровадження ефективних заходів інформаційної безпеки. Багато організацій можуть виявити, що вони не мають достатніх коштів або персоналу для захисту даних належним чином.

3) Технічні вразливості та недоліки в системах: швидкий розвиток технологій призводить до з'яви нових вразливостей у системах, які можуть бути використані зловмисниками для атак. Брак адекватного оновлення та захисту може залишити системи вразливими перед сучасними загрозами.

4) Соціальна інженерія та людський фактор: багато атак відбуваються через маніпулювання людським фактором, використовуючи соціальну інженерію. Наприклад, фішингові атаки можуть використовувати психологічні та маніпулятивні методи, щоб отримати доступ до конфіденційної інформації.

5) Законодавчі та регуляторні вимоги: багато організацій зіткнуться зі складнощами виконання законодавчих та регуляторних вимог у сфері інформаційної безпеки. Це може включати в себе вимоги до зберігання, захисту та обробки конфіденційної інформації, такої як особисті дані клієнтів.

6) Недостатня усвідомленість персоналу: недостатня підготовка персоналу з питань безпеки може призвести до недбалого відношення до захисту даних і збільшити ризик інцидентів безпеки.

Недостатня усвідомленість ризиків, обмежені фінансові ресурси, технічні вразливості, соціальна інженерія та інші фактори можуть призвести до серйозних наслідків, таких як втрата даних, порушення конфіденційності і порушення законодавства [4].

Для ефективного управління інформаційною безпекою необхідно вживати комплексних заходів, які включають у себе як технологічні рішення, так і вдосконалення процесів та підготовку персоналу. Потрібно постійно оновлювати

політики безпеки, проводити регулярні навчання та тренінги персоналу, а також вживати заходів щодо виявлення та мінімізації ризиків.

Враховуючи всі ці аспекти, можна зробити висновок, що інформаційна безпека вимагає постійної уваги та інвестицій з боку організацій, але забезпечує надійний захист від потенційних загроз і забезпечує безперебійне функціонування бізнесу [3, 11].

2.3 Визначення стратегічних напрямків для підвищення інформаційної безпеки

Стратегічні напрямки для підвищення інформаційної безпеки – це ключові напрямки діяльності, спрямовані на забезпечення надійного захисту інформаційних ресурсів організації. Ці напрямки включають в себе широкий спектр заходів, спрямованих на запобігання кіберзагрозам та забезпечення відповідного реагування на них [8].

Вони охоплюють такі аспекти, як фінансування ініціатив з інформаційної безпеки, підвищення свідомості персоналу, розробка та впровадження ефективних політик та процедур безпеки, посилення технічного захисту інформаційних систем, а також підвищення готовності до реагування на інциденти безпеки [12].

По-перше, важливо розглянути забезпечення відповідного фінансування ініціатив з інформаційної безпеки. Це означає виділення достатніх ресурсів на розробку та впровадження стратегій безпеки, включаючи закупівлю технічних засобів захисту, навчання персоналу та організацію аудитів безпеки.

По-друге, необхідно покращити свідомість персоналу про питання інформаційної безпеки. Це може бути досягнуто через проведення навчальних семінарів, тренінгів та інформаційних кампаній, які підвищують усвідомленість про потенційні загрози та процедури безпеки.

По-третє, важливо розробити і впровадити ефективні політики та процедури безпеки. Це включає в себе створення інструкцій та стандартів щодо обробки,

зберігання та передачі конфіденційної інформації, а також встановлення механізмів контролю та відповідальності за їх дотримання.

По-четверте, необхідно посилити технічний захист інформаційних систем. Це може включати встановлення сучасних систем антивірусного захисту, брандмауерів, систем виявлення вторгнень та інших заходів захисту, які допоможуть запобігти кібератакам та несанкціонованому доступу.

Нарешті, важливо підвищити готовність до реагування на інциденти безпеки. Це означає розробку та впровадження планів надзвичайних ситуацій, які визначають процедури реагування на кібератаки, втрату даних та інші інциденти безпеки, а також проведення регулярних тренувань та вправ для персоналу з цих питань.

Ці стратегічні напрямки дозволяють організаціям ефективно реагувати на зростаючі загрози кібербезпеки та забезпечувати відповідний рівень захисту своїх інформаційних активів. Крім того, вони сприяють покращенню свідомості персоналу, підвищенню технічного рівня безпеки та впровадженню сучасних практик управління ризиками [12]. Такий комплексний підхід дозволяє зменшити вразливість організації перед кіберзагрозами та збільшити її стійкість до потенційних інцидентів безпеки [2].

2.4 Розгляд можливих заходів та політичних рішень для забезпечення безпеки інформаційних ресурсів органів місцевого самоврядування

При розгляді можливих заходів для забезпечення безпеки інформаційних ресурсів органів місцевого самоврядування можна врахувати наступні аспекти:

– Аудит безпеки: проведення систематичного аналізу стану безпеки інформаційних систем для виявлення потенційних загроз та вразливостей.

– Впровадження політик безпеки: розробка та впровадження політик, процедур та стандартів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів [8].

– Навчання та навчання персоналу: організація тренінгів, семінарів та інших навчальних заходів для персоналу з питань кібербезпеки та впровадження кращих практик безпеки [2].

– Захист мережі: встановлення захисних механізмів на рівні мережі, таких як брандмауери, виявлення вторгнень, контроль доступу тощо.

– Захист даних: використання шифрування даних, забезпечення резервного копіювання та відновлення даних, контроль доступу до конфіденційної інформації.

– Моніторинг та аналіз загроз: постійне відстеження та аналіз потенційних загроз безпеці, виявлення аномальних активностей та реагування на них вчасно.

– Співпраця зі сторонніми експертами: залучення зовнішніх консультантів та експертів з кібербезпеки для аудиту та розробки стратегій захисту [2].

– Регулярне оновлення програмного забезпечення: забезпечення своєчасного оновлення всього програмного забезпечення та патчів безпеки для усунення виявлених вразливостей [8].

– Реагування на інциденти безпеки: розробка планів реагування на інциденти безпеки, включаючи процедури виявлення, відновлення та комунікації у випадку інциденту.

Ці заходи допомагають створити комплексну систему захисту інформаційних ресурсів органів місцевого самоврядування та забезпечити їхню надійність та стійкість до кіберзагроз.

Політичні рішення для забезпечення безпеки інформаційних ресурсів органів місцевого самоврядування можуть включати [8]:

– Розробка та прийняття законодавства: ухвалення законів та нормативних актів, які встановлюють вимоги до захисту інформації в органах місцевого самоврядування, включаючи обов’язкові стандарти безпеки та відповідальність за їх порушення [7].

– Фінансова підтримка: виділення достатніх фінансових ресурсів на впровадження та підтримку заходів з кібербезпеки, включаючи придбання необхідного обладнання та програмного забезпечення, оплату послуг експертів та консультантів.

– Створення організаційних структур: утворення спеціалізованих відділів або комітетів з кібербезпеки, які відповідають за розробку та впровадження стратегій захисту інформаційних ресурсів, а також координацію дій у разі кіберінцидентів.

– Партнерство з іншими рівнями влади: співпраця з центральними урядовими органами, іншими місцевими владами та міжнародними організаціями для обміну досвідом та ресурсами у сфері кібербезпеки.

– Підвищення свідомості громадськості: проведення інформаційних кампаній та навчальних заходів для мешканців та працівників органів місцевого самоврядування з питань кібербезпеки та заходів профілактики кіберзагроз [2].

– Стимулювання розвитку кібербезпеки: надання пільг та підтримки для компаній та організацій, які активно інвестують у заходи з кібербезпеки, що сприяє створенню конкурентоспроможної та безпечної інформаційної інфраструктури.

– Взаємодія з приватним сектором: співпраця з приватними компаніями та бізнес-асоціаціями для обміну інформацією про кіберзагрози та спільного розв’язання проблем безпеки [6].

Ці політичні рішення сприяють створенню сприятливого середовища для ефективного захисту інформаційних ресурсів органів місцевого самоврядування.

3 СТРАТЕГІЇ ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Підвищення рівня захисту інформаційних ресурсів є надзвичайно важливим завданням для будь-якої організації в сучасному цифровому світі. Для досягнення цієї мети можна використовувати різноманітні стратегії [14].

Спочатку, регулярне аудитування безпеки стає ключовим етапом у процесі забезпечення інформаційної безпеки. Проведення періодичних аудитів дозволяє виявляти потенційні вразливості та проблеми, що можуть бути використані зловмисниками [4].

Далі, важливо впроваджувати сучасні технології захисту, такі як мультифакторна аутентифікація, шифрування даних, системи виявлення вторгнень та інші. Це допомагає у запобіганні кіберзагроз та збільшує загальний рівень безпеки інформації.

Створення культури безпеки серед персоналу є ще однією важливою стратегією. Залучення персоналу до усвідомлення важливості інформаційної безпеки за допомогою навчання, тренінгів та регулярного інформування про потенційні загрози допомагає підвищити рівень обізнаності та відповідальності.

Також, впровадження строгих політик безпеки, що включають в себе правила доступу до інформації, процедури реагування на інциденти та інші аспекти захисту, є необхідним кроком для забезпечення безпеки інформаційних ресурсів [8].

Моніторинг та реагування на підозрілі активності або інциденти також має велике значення. Постійний моніторинг заходів безпеки та швидке реагування на будь-які підозрілі ситуації дозволяє запобігти потенційним загрозам та зберегти безпеку даних.

Загалом, поєднання цих стратегій із відповідною політикою та практиками безпеки допомагає організаціям забезпечити ефективний захист їх інформаційних ресурсів [14].

3.1 Створення та застосування планів інформаційної безпеки

Створення плану інформаційної безпеки - це процес, що вимагає уважного аналізу потенційних загроз та ризиків, а також розробки конкретних стратегій і заходів для їх запобігання. Ось кроки, які зазвичай включаються у процес створення плану інформаційної безпеки:

1. Аналіз ризиків: перший етап полягає в ідентифікації потенційних загроз безпеці інформації та оцінці їхнього впливу на організацію. Це може включати аналіз зовнішніх загроз, таких як кібератаки, і внутрішніх загроз, наприклад, помилки персоналу або несправності обладнання.

2. Визначення цілей і стратегій: на основі результатів аналізу ризиків визначаються конкретні цілі та стратегії для захисту інформації [14]. Ці цілі можуть включати забезпечення конфіденційності, цілісності та доступності інформації, а також зменшення впливу можливих загроз [8].

3. Розробка політик та процедур: створюються політики та процедури, які визначають правила та стандарти для захисту інформації. Це може включати правила доступу до інформації, процедури реагування на інциденти безпеки, а також навчання персоналу щодо кібербезпеки [7].

4. Впровадження та навчання: план інформаційної безпеки впроваджується в організації, а персонал проходить навчання з питань безпеки інформації. Це допомагає забезпечити виконання політик та процедур безпеки та підвищити обізнаність персоналу щодо кібербезпеки.

5. Перевірка та оновлення: план інформаційної безпеки періодично переглядається та оновлюється з урахуванням нових загроз та технологій. Це дозволяє забезпечити ефективність плану в умовах швидко змінюючогося кіберландшафту.

Після розробки плану інформаційної безпеки необхідно його впровадити та застосовувати в організації. Ось деякі ключові кроки, які включаються у процес застосування плану:

1. Впровадження політик та процедур: політики та процедури, розроблені в рамках плану, повинні бути впроваджені в організаційну культуру та ділові процеси. Це може включати встановлення прав доступу до систем та даних, впровадження механізмів контролю доступу та виконання інших заходів безпеки.

2. Навчання персоналу: всі співробітники повинні бути ознайомлені з політиками та процедурами безпеки інформації та проходити регулярне навчання з питань кібербезпеки. Це допоможе забезпечити відповідність стандартам безпеки та підвищити обізнаність персоналу щодо потенційних загроз.

3. Моніторинг та аналіз: проведення постійного моніторингу систем та даних на предмет потенційних загроз та виявлення вразливостей. Це дозволить своєчасно реагувати на можливі інциденти безпеки та запобігти їхньому подальшому розвитку.

4. Реагування на інциденти: встановлення механізмів реагування на інциденти безпеки, включаючи процедури виявлення, оцінки та відновлення після інциденту. Швидке та ефективне реагування на інциденти дозволяє мінімізувати їхні наслідки та зберегти безпеку систем та даних.

5. Оновлення та удосконалення: план інформаційної безпеки повинен періодично оновлюватися та удосконалюватися відповідно до змін у загрозах та технологіях. Регулярні аудити безпеки та оновлення політик і процедур допоможуть забезпечити відповідність плану сучасним вимогам безпеки.

Впровадження плану інформаційної безпеки є критичним етапом у забезпеченні безпеки організаційних інформаційних ресурсів. Це дозволяє організації не лише ідентифікувати потенційні загрози та вразливості, але і вживати необхідні заходи для їх запобігання та мінімізації наслідків інцидентів безпеки [4]. Шляхом впровадження політик, навчання персоналу, моніторингу та реагування на інциденти, організація може створити ефективну систему захисту, яка забезпечить конфіденційність, цілісність та доступність її інформаційних активів. Постійне оновлення та удосконалення плану дозволяє організації залишатися реагуючою на змінні умови та нові загрози, що можуть виникати у сфері кібербезпеки.

3.2 Налагодження моніторингових та контрольних процедур

Налагодження моніторингових та контрольних процедур є ключовим етапом у забезпеченні безпеки інформаційних ресурсів організації. Давайте розглянемо кожен етап та процедури, які входять у цей процес:

1. Моніторингові процедури:

– збір даних: спеціалізовані програмні засоби здійснюють постійний збір даних про діяльність на комп’ютерах та в мережі організації. Ці дані включають в себе журнали подій, відомості про використання ресурсів та іншу інформацію, яка може вказувати на потенційні загрози безпеці.

– аналіз даних: зібрані дані проходять через процес аналізу, де вони перевіряються на виявлення аномалій, незвичайних патернів чи ознак вразливостей. Це може включати виявлення підозрілих активностей, несподіваних змін у системі чи незвичайного трафіку в мережі.

– реагування на події: якщо виявлено потенційну загрозу, система автоматично або за участю адміністраторів запускає процес реагування. Це може включати блокування доступу до певних ресурсів, сповіщення адміністраторів про події або автоматичні заходи для мінімізації збитків.

2. Контрольні процедури:

– перевірка відповідності стандартам: ці процедури включають періодичні аудити та оцінки, які перевіряють, чи відповідають існуючі заходи безпеки встановленим стандартам та політикам. Якщо виявляються невідповідності, вони фіксуються та вживаються заходи для їх усунення.

– усунення недоліків: якщо під час аудитів чи інших контрольних процедур виявляються недоліки, адміністратори вживають відповідних заходів для їх усунення. Це може включати оновлення програмного забезпечення, налаштування політик безпеки чи проведення додаткового навчання для персоналу.

– моніторинг ефективності: після вжиття заходів з усунення недоліків проводиться моніторинг, щоб переконатися, що вони ефективно працюють. Це може включати перевірку журналів подій, аналіз трафіку та оцінку рівня ризику.

3. Спеціалізовані програмні засоби:

– системи моніторингу безпеки (SIEM): SIEM системи збирають, аналізують та візуалізують дані про безпеку з різних джерел для виявлення загроз та реагування на них.

– антивірусне програмне забезпечення: ці програми сканують комп’ютери на предмет вірусів, троянців та інших шкідливих програм, допомагаючи запобігти їх поширенню та виявленню.

– Firewall: фаерволи контролюють трафік в мережі та блокують небажаний доступ до комп’ютерів та ресурсів організації.

Ці процедури та програмні засоби разом створюють систему моніторингу та контролю, яка допомагає організаціям ефективно виявляти та реагувати на потенційні загрози безпеці.

3.3 Оцінка ефективності та розвиток стратегій безпеки

Оцінка ефективності стратегій безпеки важлива для забезпечення того, що вони відповідають потребам та досягають поставлених цілей [8]. Для цього можна використовувати різні методи та підходи:

1. Аналіз результатів: проведення регулярного аналізу результатів застосування стратегій дозволяє визначити їхню ефективність [14]. Це може включати оцінку зменшення кількості інцидентів безпеки, зменшення витрат на відновлення після інцидентів та покращення загального рівня безпеки організації.

2. Задання ключових показників ефективності (KPI): визначення ключових показників ефективності дозволяє оцінити досягнення конкретних цілей безпеки. Наприклад, KPI може включати кількість виявлених та заблокованих загроз, час реакції на інциденти, витрати на безпеку тощо.

3. Проведення аудитів безпеки: регулярні аудити безпеки дозволяють перевірити відповідність заходів безпеки стандартам та виявити можливі недоліки. Результати аудитів можуть бути використані для вдосконалення стратегій безпеки та покращення їх ефективності.

4. Залучення експертів: залучення експертів у сфері безпеки для оцінки стратегій та їхнього впливу дозволяє отримати об’єктивну оцінку їхньої ефективності та поради щодо подальших дій.

5. Навчання та розвиток персоналу: підвищення кваліфікації персоналу та забезпечення їхньої обізнаності з питань безпеки дозволяє підвищити ефективність заходів безпеки та виявлення потенційних загроз.

Загальна оцінка ефективності стратегій безпеки визначається їхньою здатністю до виявлення, запобігання та врегулювання інцидентів безпеки, а також забезпеченням відповідності стандартам безпеки та потребам організації [14].

Розвиток стратегій безпеки є постійним процесом, оскільки з розвитком технологій та появою нових загроз необхідно адаптувати заходи безпеки для забезпечення відповідності поточним вимогам [8]. Ось деякі ключові аспекти розвитку стратегій безпеки:

1. Моніторинг та аналіз: постійний моніторинг загроз та вразливостей дозволяє своєчасно виявляти нові загрози та впроваджувати відповідні заходи безпеки. Аналіз інцидентів та уроків, вивчених з них, допомагає удосконалювати стратегії та запобігати подібним ситуаціям у майбутньому.

2. Адаптація до нових технологій: розвиток нових технологій, таких як хмарні сервіси, штучний інтелект та Інтернет речей, потребує постійного оновлення стратегій безпеки для забезпечення їхньої ефективності та відповідності сучасним вимогам безпеки.

3. Залучення експертів: співпраця з експертами у сфері безпеки дозволяє отримати нові ідеї та підходи до захисту інформації та виявлення потенційних загроз.

4. Постійне навчання персоналу: забезпечення навчання персоналу з питань безпеки та підвищення їхньої обізнаності є важливим елементом розвитку стратегій безпеки. Персонал повинен бути свідомим про поточні загрози та знати, як діяти у випадку інциденту.

5. Тестування та вдосконалення: проведення регулярних тестів та вправ, включаючи симуляції інцидентів, дозволяє виявляти слабкі місця у стратегіях безпеки та вносити необхідні зміни для їх поліпшення [14].

6. Управління ризиками: постійний аналіз та оцінка ризиків дозволяє вчасно виявляти потенційні загрози та приймати заходи для їх запобігання або зменшення наслідків.

Розвиток стратегій безпеки є невід'ємною частиною процесу забезпечення безпеки інформації в організації і вимагає постійного удосконалення та адаптації до змін в сфері технологій та загроз безпеці [8].

3.4 Висновки та рекомендації щодо стратегій підвищення рівня захисту інформаційних ресурсів

Висновки щодо стратегій підвищення рівня захисту інформаційних ресурсів вказують на кілька ключових аспектів. По-перше, важливо визнати, що інформаційна безпека вимагає системного підходу, який об'єднує технічні, організаційні та культурні аспекти [9]. Технологічні інновації можуть сприяти підвищенню захисту, але вони повинні супроводжуватися відповідними політиками, процедурами та навчанням персоналу [11].

Другий аспект полягає в необхідності постійного моніторингу і аналізу загроз для адаптації стратегій захисту. Кіберзагрози постійно змінюються, тому стратегії безпеки повинні бути гнучкими і адаптивними, готовими реагувати на нові виклики та загрози.

Крім того, ефективні стратегії захисту вимагають участі всього колективу організації. Залучення персоналу до процесу забезпечення безпеки, навчання їх виявленню та запобіганню кіберзагрозам, а також створення безпечної культури в організації є ключовими складовими успішної стратегії захисту [14].

У підсумку, стратегії підвищення рівня захисту інформаційних ресурсів вимагають поєднання технологічних інновацій з відповідними політиками,

процедурами та культурними змінами. Тільки такий комплексний підхід може забезпечити ефективний захист в умовах постійно зростаючих кіберзагроз.

Рекомендації для подальших досліджень у цій області можуть включати:

1) глибше дослідження новітніх технологій і методів кіберзахисту, таких як штучний інтелект, машинне навчання та аналіз великих обсягів даних. Важливо вивчити їхні можливості та обмеження для ефективного застосування в сфері інформаційної безпеки.

2) аналіз новітніх кіберзагроз та трендів у кібербезпеці для розробки стратегій захисту, які відповідають сучасним викликам.

3) вивчення практик кібербезпеки в різних секторах економіки та країнах для виявлення найкращих підходів та взаємного обміну досвідом [6].

4) розвиток нових методів оцінки ризиків та визначення вразливостей в інформаційних системах для забезпечення більш ефективного управління кібербезпекою.

5) вивчення впливу регулятивного середовища та законодавства на кібербезпеку, включаючи аналіз їхнього впливу на практики захисту та можливість розвитку нових стандартів.

6) дослідження психологічних аспектів кібербезпеки, таких як поведінкові патерни користувачів та вплив соціально-інженерних атак на безпеку інформаційних систем.

7) вивчення проблеми кібербезпеки в контексті міжнародних відносин та глобальної безпеки для розробки спільних стратегій протидії кіберзагрозам на міжнародному рівні [2].

Ці рекомендації можуть сприяти подальшій розробці та вдосконаленню стратегій інформаційної безпеки та забезпечити більш ефективний захист в умовах постійно змінюючогося кіберпростору.

ВИСНОВОК

У сучасному цифровому світі інформаційна безпека є однією з ключових умов ефективного функціонування будь-якої організації, включаючи органи місцевого самоврядування. Зважаючи на зростання кіберзагроз і вдосконалення методів кіберзлочинців, забезпечення захисту інформаційних ресурсів стає пріоритетним завданням. Кваліфікаційна робота на тему «Формування політики безпеки на об’єктах інформаційної діяльності на прикладі органів місцевого самоврядування» спрямована на всебічний аналіз сучасного стану питань інформаційної безпеки та розробку ефективних стратегій для підвищення рівня захисту інформації.

Перший розділ роботи розглядає теоретичні аспекти формування політики безпеки, включаючи принципи та поняття інформаційної безпеки, основні загрози та вразливості інформаційних систем, а також механізми захисту від кіберзагроз і кібератак. Визначено, що ключовими елементами ефективної політики інформаційної безпеки є конфіденційність, цілісність та доступність інформації. Для досягнення цих цілей використовуються різні методи захисту, такі як криптографія, багатофакторна аутентифікація, системи виявлення і запобігання вторгненням (IDS/IPS) та інші.

Другий розділ присвячений аналізу сучасного стану інформаційної безпеки в органах місцевого самоврядування. Проведено огляд існуючих підходів до захисту інформації, виявлено основні недоліки та проблемні аспекти, що потребують вирішення. Аналіз показав, що багато органів місцевого самоврядування стикаються з проблемами недостатнього фінансування, нестачі кваліфікованих кадрів та застарілих технологій. Водночас, впровадження міжнародних стандартів і рекомендацій у сфері інформаційної безпеки, таких як ISO/IEC 27001 та NIST, може значно підвищити рівень захисту інформаційних ресурсів.

Третій розділ роботи зосереджений на розробці стратегічних напрямків для підвищення рівня захисту інформаційних ресурсів органів місцевого самоврядування. Запропоновано низку заходів, включаючи впровадження

сучасних технологій захисту інформації, проведення регулярних аудитів безпеки, підвищення кваліфікації працівників та розробку детальних планів реагування на інциденти. Особливу увагу приділено важливості моніторингу та контролю за станом інформаційної безпеки, а також співпраці з іншими державними та приватними організаціями для обміну досвідом і кращими практиками.

Таким чином, кваліфікаційна робота демонструє комплексний підхід до вирішення проблеми інформаційної безпеки в органах місцевого самоврядування. Розроблені рекомендації та стратегічні напрямки можуть бути використані для підвищення рівня захисту інформаційних ресурсів, що в свою чергу забезпечить стабільність та ефективність управління на місцевому рівні. Важливим результатом роботи є розуміння того, що інформаційна безпека повинна бути інтегрованою частиною загальної стратегії управління, а не розглядатися як окремий технічний аспект.

Подальші дослідження у цій сфері можуть бути спрямовані на розробку нових методів і засобів захисту інформації, а також на удосконалення існуючих стратегій з метою підвищення їх ефективності в умовах постійно зростаючих загроз. Це дозволить забезпечити ще більший рівень безпеки інформаційних ресурсів та знизити ризики, пов’язані з кіберзлочинністю та іншими загрозами у цифровому середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хмелевський, Р.М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності. *Сучасний захист інформації*. 2019. №4 URL: http://surl.li/tzobc
2. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. *Підручник. Видання друге.* 2019. Одеська національна академія зв’язку ім. О.С. Попова. URL: http://surl.li/txmbi
3. Безуглий Д.С. Інформаційна безпека України: огляд останніх тенденцій. *Науковий журнал: Фізико-математична освіта.* 2020 . URL: http://surl.li/tzobp
4. Вразливості інформаційних та комунікаційних систем. URL: http://surl.li/tzocc
5. Уразливість (інформаційні технології). *Матеріал з вікіпедії – вільної енциклопедії*. URL: http://surl.li/vfnr
6. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Дубовий Я. В. Кіберзагрози в освітньому секторі. 2022. URL: http://surl.li/tzocu
7. Стандарти кібербезпеки. *Матеріал з вікіпедії – вільної енциклопедії*. URL: https://en.wikipedia.org/wiki/Cybersecurity_standards
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017р. № 2163-VIII. Дата оновлення 04.04.2024р. URL: https://zakon.rada.gov.ua/laws/show/2163-19
9. Інформаційна, комунікаційна та кібер-вразливість країни: причини та наслідки. 2019.URL: https://ecpl.com.ua/news/14844/
10. Стандарти інформаційної безпеки. *Матеріал з вікіпедії – вільної енциклопедії*. URL: http://surl.li/bjch
11. Виздрик В. С., Мельник О. М. Інформаційна безпека в Україні: сучасний стан. *Національна академія сухопутних військ імені гетьмана П.Сагайдачного,* 2023. URL: http://surl.li/tzodc
12. Великий В., Мороз Ю., Полотай О. Методи технічного захисту інформації у сфері інформаційної безпеки. *Кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка», кафедра управління*

інформаційною безпекою Львівського державного університету безпеки життєдіяльності. 2020. URL: http://surl.li/tznyz

13. Криптографічний захист інформації. *Матеріал з вікіпедії – вільної енциклопедії*. URL: http://surl.li/lwje
14. Рада національної безпеки і оборони України. Стратегія кібербезпеки України (2021-2025 роки). 2021р. URL: http://surl.li/tzodk