МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Євген ГОЛОВКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Євген ГОЛОВКО
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Головку Євгену Васильовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оцінка ефективності засобів та методів захисту інформації на підприємстві”,
керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби забезпечення інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати особливості управління інформаційною безпекою підприємства.
4.2. Дослідити основні засоби та методи захисту інформації на підприємстві.
4.3. Вивчити засоби підвищення ефективності захисту інформації на підприємстві, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2024	
4.	Дослідження основних засобів та методів захисту інформації на підприємстві.	22.04.2024	
5.	Вивчення засобів підвищення ефективності захисту інформації на підприємстві	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Євген ГОЛОВКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувач Головко Є.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оцінка ефективності засобів та методів захисту інформації на підприємстві"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ГОЛОВКО Євген у кваліфікаційній роботі проаналізував особливості управління інформаційною безпекою підприємства, дослідив основні засоби та методи захисту інформації на підприємств, вивчив засоби підвищення ефективності захисту інформації на підприємстві, розробив практичні рекомендації за темою дослідження.

ГОЛОВКО Євген показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ГОЛОВКА Євгена на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Головко Є.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ГОЛОВКА Євгена
на тему “Оцінка ефективності засобів та методів захисту інформації на підприємстві”

Актуальність.

Динамічний розвиток технологій, підвищення кількості цифрових платформ і збільшення обсягів обробки даних створюють унікальні виклики для забезпечення безпеки інформації. Однією з ключових причин актуальності цієї теми є постійне зростання кількості та складності кіберзагроз. Зловмисники намагаються експлуатувати вразливості в системах безпеки для отримання несанкціонованого доступу до конфіденційної інформації, викрадення даних або навіть впливу на нормальне функціонування підприємства.

Оцінка ефективності засобів та методів захисту інформації на підприємстві стає стратегічно важливою для забезпечення довіри стейкхолдерів. Клієнти, партнери та регулятори вимагають від організацій доведення, що їхні дані і системи належним чином захищені від можливих загроз. Важливо, щоб підприємства постійно моніторили та оцінювали свої засоби та методи захисту інформації, щоб забезпечити їхню актуальність і ефективність у протидії новітнім загрозам.

Важливо зазначити, що росте значущість вимірювання показників управління ризиками та оцінки ефективності заходів безпеки. Комплексне вивчення та оцінка ефективності засобів захисту інформації ідентифікуються як критичні аспекти для постійного вдосконалення систем управління ризиками та адаптації до змін у загрозах. Регулярне тестування та аудит систем захисту допомагають виявити слабкі місця та впровадити необхідні вдосконалення для підвищення рівня безпеки інформації на підприємстві.

Позитивні сторони.

Цією роботою звернулися до важливої та актуальної теми, пов'язаної з ефективністю засобів та методів захисту інформації на підприємстві, що відображає велику значущість цієї проблематики в сучасному цифровому світі.

Кваліфікаційна робота вражає ретельністю аналізу використовуваних методик та підходів до оцінки ефективності засобів та методів захисту інформації.

Чітко структурований вступ та висновок роблять роботу добре впорядкованою та логічно зв'язаною.

Акцент на рекомендаціях щодо підвищення ефективності захисту інформації на підприємстві є важливим аспектом роботи, що відображає сучасні тенденції в галузі інформаційної безпеки.

Недоліки.

Хоча робота добре структурована, варто розглянути можливість більш

детального розгляду окремих методик та їхнього порівняння, щоб надати читачеві глибше розуміння вибору конкретних підходів. Це дозволить визначити найбільш ефективні та відповідні методи захисту інформації для різних типів підприємств.

Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування обраної методики управління ризиками на конкретних кейсах чи в реальних умовах підприємства. Такий підхід дозволить оцінити практичну ефективність методів та адаптувати їх до специфічних потреб і умов різних організацій, забезпечуючи більш глибоке розуміння та удосконалення систем захисту інформації.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ГОЛОВКО Євген заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
к.т.н., доцент _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена оцінці ефективності засобів та методів захисту інформації на підприємстві. Робота складається зі вступу, трьох розділів, що містять 10 рисунків, висновківі списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 61 аркуш, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є оцінка ефективності засобів та методів захисту інформації на підприємстві.

Об'єктом дослідження є методи та засоби захисту інформації.

Предмет дослідження – особливості загроз та вразливостей інформації на підприємстві.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Як результат у роботі проаналізовано особливості управління інформаційною безпекою підприємства, досліджено основні засоби та методи захисту інформації на підприємстві; засоби підвищення ефективності захисту інформації на підприємстві, розроблено практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при оцінці ефективності засобів та методів захисту інформації у контексті інформаційної безпеки підприємства.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ОЦІНКА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАГРОЗИ ТА ВРАЗЛИВОСТІ ІНФОРМАЦІЇ, ЕФЕКТИВНІСТЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ.

ABSTRACT

The qualification work is devoted to the assessment of the effectiveness of information security tools and methods at an enterprise. The work consists of an introduction, three chapters containing 10 figures, conclusions and the list of references containing 45 items. The total volume of the work is 61 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to assess the effectiveness of means and methods of information security at the enterprise.

The object the study is methods and means of information protection.

The subject of the study is the peculiarities of threats and vulnerabilities of information at the enterprise.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to information security management were used in the work.

As a result, the work analyzed the peculiarities of enterprise information security management, investigated the main means and methods of information protection at the enterprise; measured improvement the efficiency of information protection at the enterprise, developed practical recommendations.

Field of application. The developed approaches can be used in assessing the effectiveness of information security tools and methods in the context of enterprise information security.

Keywords: INFORMATION SECURITY OF THE ENTERPRISE, ASSESSMENT OF INFORMATION SECURITY PROTECTION MEANS, THREATS AND VULNERABILITIES OF INFORMATION, EFFICIENCY OF INFORMATION SECURITY.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де де кіберзагрози стають все більшим викликом для підприємств, забезпечення ефективного захисту інформації на підприємствах є важливим, як ніколи. Аналіз та оцінка ефективності засобів, що використовуються на підприємстві, дозволять визначити вразливості в системі захисту інформації та прийняти потрібні заходи для запобігання негативним наслідкам.

З огляду на зазначене дослідження оцінки ефективності засобів та методів захисту інформації на підприємстві є актуальним науковим завданням.

Мета роботи полягає у дослідженні оцінки ефективності засобів та методів захисту інформації на підприємстві.

Об'єкт дослідження –методи та засоби захисту інформації

Предмет дослідження – особливості загроз та вразливостей інформації на підприємстві.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати особливості управління інформаційною безпекою підприємства.

2. Дослідити основні засоби та методи захисту інформації на підприємстві.

3. Вивчити засоби підвищення ефективності захисту інформації на підприємстві, розробити практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Як результат у роботі проаналізовано особливості управління інформаційною безпекою підприємства, досліджено основні засоби та методи захисту інформації на підприємстві; засоби підвищення ефективності захисту інформації на підприємстві, розроблено практичні рекомендації.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити правильну оцінку забезпечення безпеки інформації на підприємстві. Результати дослідження можуть допомогти оптимізувати систему захисту, спираючись на оцінку наявних методів та рекомендації щодо їх покращення.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

РОЗДІЛ 1 УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА ЯК ОСНОВА ЕФЕКТИВНОГО ЗАХИСТУ

Управління інформаційною безпекою є критичним елементом стратегії захисту для будь-якого підприємства в умовах сучасного цифрового середовища. Завдяки швидкому розвитку технологій та зростанню кількості кіберзагроз, ефективне управління інформаційною безпекою стає пріоритетом для забезпечення стабільності та успішності бізнесу.

Основою ефективного управління інформаційною безпекою є впровадження систематичного та комплексного підходу до захисту інформації в усіх аспектах діяльності підприємства. Першим кроком у цьому процесі є проведення аналізу потенційних загроз та вразливостей інформаційних систем підприємства. Це включає в себе ідентифікацію можливих кіберзагроз, оцінку рівня ризику та визначення пріоритетів для вжиття заходів з протидії.

Після аналізу загроз необхідно розробити стратегію інформаційної безпеки, яка враховуватиме конкретні потреби та особливості підприємства. Ця стратегія повинна включати в себе політики, процедури та технології, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації. Наприклад, вона може передбачати регулярні оновлення програмного забезпечення, впровадження механізмів аутентифікації та авторизації, а також навчання персоналу з питань кібербезпеки.

Ключовим елементом ефективного управління інформаційною безпекою є постійний моніторинг та оновлення заходів захисту відповідно до змін у загрозах та технологічному середовищі. Це включає в себе аналіз нових кіберзагроз, вчасне виявлення інцидентів безпеки та швидку реакцію на них. Крім того, важливою частиною управління інформаційною безпекою є постійне навчання та підвищення обізнаності персоналу з питань кібербезпеки [1].

Ефективне управління інформаційною безпекою є невід'ємною частиною стратегії захисту для будь-якого підприємства. Шляхом систематичного аналізу, розробки стратегії та постійного моніторингу підприємство може

забезпечити надійний захист своєї інформації та зберегти довіру своїх клієнтів і партнерів.

1.1 Аналіз основних загроз та вразливостей інформаційної безпеки на підприємствах

Сучасне цифрове середовище підприємства стикається з різноманітними загрозами та вразливостями в галузі інформаційної безпеки, які можуть суттєво підірвати їхню діяльність та завдати значних фінансових та репутаційних збитків. Аналіз основних загроз та вразливостей на підприємствах є критичним етапом у розробці ефективних стратегій захисту інформації та забезпеченні стійкості бізнесу.

Рис. 1 Основні загрози та вразливості інформаційної безпеки

Однією з основних загроз є кібератаки та вторгнення в інформаційні системи підприємств. Ці атаки можуть бути здійснені різними методами, включаючи віруси, черви, троянські коні, фішинг, ддос-атаки та інші. Вони спрямовані на викрадення конфіденційної інформації, порушення роботи систем та завдання шкоди репутації підприємства.

Кібератаки та вторгнення в інформаційні системи підприємств є серйозними загрозами, які можуть призвести до серйозних наслідків для їхньої діяльності. Ці атаки відрізняються за методами, цілями та рівнем складності, але всі вони спрямовані на отримання несанкціонованого доступу до інформації або на завдання шкоди інформаційним системам підприємств[2].

Однією з найпоширеніших форм кібератак є віруси, черви та троянські коні. Віруси є програмами, які вбудовуються в інші файли або програми і можуть самостійно розповсюджуватися між комп'ютерами. Черви є самореплікуючими програмами, які можуть поширюватися через мережу без необхідності взаємодії з користувачем. Троянські коні приховуються в звичайних програмах та виконують шкідливі дії без відома користувача.

Фішинг є методом атаки, при якому атакувачі використовують підроблені повідомлення або веб-сайти, щоб отримати конфіденційну інформацію, таку як паролі чи номери кредитних карток, від користувачів. Ці дані потім можуть бути використані для крадіжки грошей або для ідентифікації інших форм шахрайства[3].

Деніал сервіс (DDoS) атаки спрямовані на перевантаження серверів або мережевих ресурсів, що призводить до зниження доступності сервісу для законних користувачів. Ці атаки можуть призвести до значних втрат прибутку та підриву репутації підприємства.

Успішне протидіяння кібератакам та вторгненням в інформаційні системи підприємств вимагає вдосконаленої стратегії кібербезпеки. Це включає в себе застосування технічних заходів захисту, таких як антивірусне програмне забезпечення, фаєрфоли та системи виявлення вторгнень. Крім того, важливо проводити навчання персоналу з питань кібербезпеки та встановлювати політики та процедури для виявлення та реагування на кібератаки.

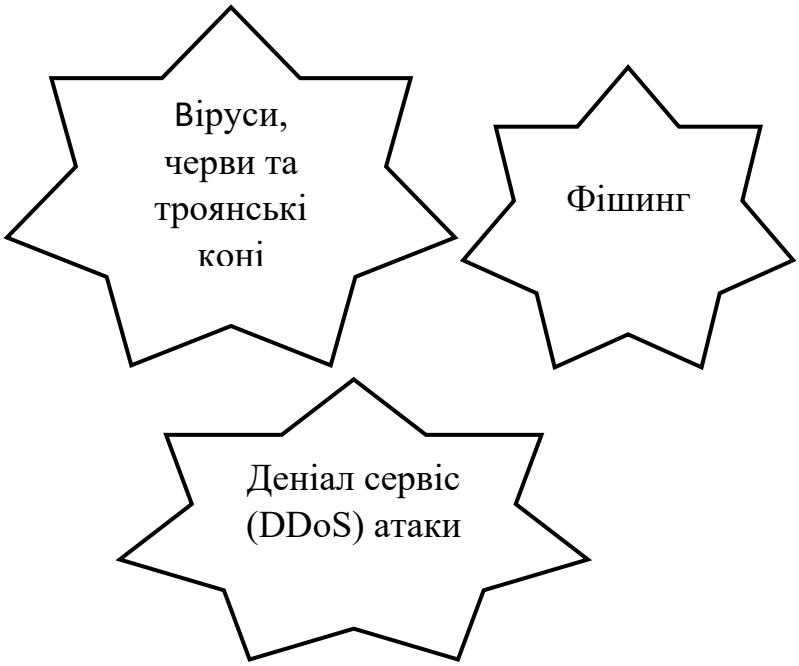

Рис. 2 Найпоширеніші форми кібератак

Великою загрозою є внутрішній фактор, а саме недбалість або зловживання працівників. Інсайдерські загрози можуть включати в себе неправильне використання привілеїв, крадіжку даних, недотримання політик безпеки та інші дії, які можуть призвести до компрометації конфіденційної інформації.

Недбалість або зловживання працівників є серйозною загрозою для інформаційної безпеки підприємства. Це може статися з метою отримання конфіденційної інформації, відволікання від нормальної діяльності підприємства або навіть завдання шкоди організації. Недбалість може бути випадковою, а зловживання - умисною[4].

Одним з прикладів недбалості може бути недбале використання паролів або неналежне зберігання конфіденційної інформації. Наприклад, працівник може використовувати слабкі паролі або надавати доступ до конфіденційної інформації неналежним особам.

Зловживання працівників може включати в себе намагання використовувати конфіденційну інформацію для особистої вигоди або для завдання шкоди підприємству. Наприклад, співробітник може намагатися використовувати конфіденційну інформацію для власного збагачення або для

ведення конкурентної діяльності. Також можливе зловживання доступом до інформаційних систем, наприклад, злам акаунтів або незаконне використання привілеїв доступу.

Ефективне протидіяння недбалості та зловживанню працівників вимагає впровадження відповідних політик та процедур управління доступом та моніторингу активності працівників. Це може включати в себе обмеження доступу до конфіденційної інформації лише необхідним працівникам, встановлення аудиту доступу для виявлення неправомірних дій та проведення регулярних навчань з питань етики та кібербезпеки. Також важливо мати механізми звітування про порушення політик та швидкі механізми реагування на них[5].

Недостатній рівень кібербезпеки та захисту даних може бути викликаний недоліками управління, відсутністю або недостатнім оновленням програмного забезпечення та обладнання, а також недостатньою освіченістю персоналу з питань інформаційної безпеки.

Недостатній рівень кібербезпеки та захисту даних становить серйозну загрозу для підприємств, оскільки відкриває шлях для кібератак та порушення конфіденційності, цілісності та доступності інформації. Ця проблема може виникати з різних причин, включаючи недостатність технічних засобів захисту, відсутність політик та процедур управління кібербезпекою, а також недостатню обізнаність персоналу з питань інформаційної безпеки.

Однією з причин недостатнього рівня кібербезпеки може бути відсутність або застарілість технічних засобів захисту. Наприклад, застаріле програмне забезпечення або обладнання може містити вразливості, які можуть бути використані зловмисниками для здійснення атак. Також недостатній рівень захисту може виникнути внаслідок неправильної конфігурації або неправильного використання доступних технічних засобів[6].

Недостатність політик та процедур управління кібербезпекою також може призвести до проблем. Відсутність чітких правил та відповідних процедур для захисту інформації може призвести до неправильного використання або

недостатнього захисту конфіденційних даних. Наприклад, відсутність політик паролів або процедур захисту даних може викласти організацію на ризик зламу акаунтів або втрати конфіденційної інформації.

Недостатня обізнаність персоналу з питань кібербезпеки також може стати фактором ризику. Наприклад, неправильне використання паролів або недбале ставлення до електронної пошти може стати джерелом загрози для безпеки інформації. Крім того, недостатня обізнаність персоналу з можливими кіберзагрозами може призвести до неправильної реакції на потенційні атаки та порушення безпеки.

В цілому, недостатній рівень кібербезпеки та захисту даних може стати серйозною загрозою для підприємства, оскільки відкриває йому двері для потенційних кібератак та порушень безпеки. Для запобігання цим проблемам необхідно вдосконалювати технічні засоби захисту, розробляти та впроваджувати ефективні політики та процедури управління кібербезпекою, а також проводити регулярне навчання та підвищення обізнаності персоналу з питань інформаційної безпеки.

Успішний аналіз основних загроз та вразливостей на підприємствах вимагає систематичного підходу та комплексного огляду всіх аспектів діяльності. Врахування цих загроз та вразливостей у розробці стратегій захисту та впровадження відповідних заходів може допомогти підприємствам забезпечити надійний захист інформації та зберегти стабільність свого бізнесу[7].

У висновку слід підкреслити, що аналіз основних загроз та вразливостей інформаційної безпеки на підприємствах є критичним етапом у розробці стратегій захисту. Він дозволяє ідентифікувати потенційні загрози та ризики, що стоять перед підприємствами, та визначити пріоритети для вжиття заходів з протидії. Аналіз допомагає зрозуміти, що кіберзагрози можуть мати різноманітний характер та джерела, включаючи як зовнішні, так і внутрішні фактори.

Недоліки управління, недбалість персоналу та недостатній рівень кібербезпеки можуть стати причиною серйозних проблем для підприємства, включаючи фінансові втрати та порушення репутації. Тому важливо систематично аналізувати та вдосконалювати заходи захисту, враховуючи нові тенденції у кіберзлочинності та зміни в технологічному середовищі[8].

Урахування цих аспектів у розробці стратегій захисту допомагає підприємствам забезпечити надійний захист інформації, зберегти довіру клієнтів та партнерів і зберегти стабільність свого бізнесу в умовах зростаючих кіберзагроз.

1.2 Вплив внутрішніх та зовнішніх загроз на управління інформаційною безпекою

Управління інформаційною безпекою є критично важливою складовою стратегічного керівництва та операційної діяльності будь-якого підприємства. На сучасному етапі розвитку технологій, коли підприємства зростають у віртуальному просторі та дедалі більше довіряють цифровим системам для зберігання, обробки та передачі інформації, важливо усвідомлювати, що інформаційна безпека стає ключовою складовою успішного функціонування та конкурентоспроможності.

Внутрішні загрози виникають з організаційної структури та діяльності самого підприємства. Це може бути недбале ставлення до безпеки інформації зі сторони співробітників, недостатня кваліфікація або недоліки в системі управління персоналом, а також вразливості в корпоративному програмному забезпеченні або мережевих ресурсах[9].

Внутрішні загрози в інформаційній безпеці підприємства є однією з найскладніших та найбільш важливих проблем, які потребують уваги та розв’язання. Ці загрози виникають внаслідок дій та недій персоналу, який має прямий доступ до конфіденційної інформації та інформаційних систем

підприємства. Вони можуть мати різні форми і проявлятися через недбале ставлення, недостатню обізнаність або навіть зловживання привілеями.

Однією з основних форм внутрішніх загроз є недбале ставлення до інформаційної безпеки зі сторони співробітників. Це може включати в себе використання слабких паролів, відкритий доступ до конфіденційної інформації, або недотримання політик та процедур безпеки, що може призвести до несанкціонованого доступу та ризику витоку даних.

Також внутрішні загрози можуть виникати через недостатню обізнаність персоналу з питань інформаційної безпеки. Недостатня або неправильна підготовка персоналу може призвести до неправильного розуміння ризиків та відповідних заходів захисту, що може відкрити двері для внутрішніх загроз.

Крім того, зловживання привілеями та доступом до інформації є ще однією серйозною формою внутрішніх загроз. Співробітники, які мають доступ до конфіденційної інформації або систем, можуть зловживати своїм статусом для незаконних цілей, використовуючи цю інформацію для особистої вигоди або для завдання шкоди підприємству[10].

Для запобігання внутрішнім загрозам необхідно вживати комплексних заходів, що включають в себе:

- *Розробка та впровадження політик безпеки:*

розробка чітких політик та процедур безпеки, які повинні бути відомі всьому персоналу та строго дотримуватися.

- *Навчання та підвищення обізнаності персоналу:*

регулярне проведення навчань та тренінгів з питань інформаційної безпеки для всього персоналу, щоб забезпечити правильне розуміння ризиків та процедур захисту.

- *Моніторинг та аудит безпеки:*

постійний моніторинг та аудит інформаційної безпеки, який дозволить вчасно виявляти та вирішувати внутрішні загрози.

- *Контроль доступу:*

обмеження доступу до конфіденційної інформації лише до необхідного персоналу та використання систем контролю доступу.

- *Постійне вдосконалення:*

постійне вдосконалення стратегій та заходів захисту для адаптації до змін в загрозах та технологіях.

Рис. 3 Комплексні заходи для запобігання внутрішнім загрозам

У цілому, внутрішні загрози є серйозним викликом для інформаційної безпеки підприємства, але за допомогою правильних стратегій та заходів захисту їх можна ефективно управляти та мінімізувати їхні наслідки.

Зовнішні загрози, у свою чергу, представлені атаками ззовні, що можуть бути здійснені з використанням широкого спектру технік та методів, таких як хакерські атаки, фішинг, віруси та інші форми кіберзлочинності[11].

Ці загрози можуть мати серйозні наслідки для підприємства, включаючи фінансові втрати, порушення конфіденційності та цілісності даних, порушення репутації, втрату клієнтів та партнерів, а також можуть завдати шкоди його бізнес-процесам та операціям. Відтак, важливою задачею для будь-якого підприємства є ефективне управління цими загрозами та забезпечення адекватного рівня захисту.

Зовнішні загрози є однією з найбільш серйозних та актуальних проблем в сфері інформаційної безпеки підприємства. Вони виникають ззовнішнього середовища та можуть бути представлені широким спектром загроз, включаючи кібератаки, хакерські вторгнення, соціально-інженерні атаки та інші форми кіберзлочинності. Ці загрози становлять серйозну загрозу для конфіденційності, цілісності та доступності інформації підприємства, а також можуть призвести до значних фінансових втрат та порушення репутації[12].

Однією з основних форм зовнішніх загроз є кібератаки, що можуть бути здійснені з використанням різних технік та методів, таких як вторгнення через вразливості програмного забезпечення, віруси, віруси-вимагачі, фішинг, деніал-оф-сервіс (DDoS) атаки тощо. Ці атаки можуть бути спрямовані на злам систем безпеки, крадіжку конфіденційної інформації, викрадення фінансових коштів або завдання шкоди репутації підприємства.

Крім того, соціально-інженерні атаки є ще однією серйозною формою зовнішніх загроз. Ці атаки використовують маніпуляцію та маніпулюють людським фактором для отримання конфіденційної інформації або доступу до систем підприємства. Наприклад, фішингові атаки можуть включати відправлення шахрайських електронних листів, які намагаються переконати співробітників надати свої логін та пароль або інші конфіденційні дані.

Для захисту від зовнішніх загроз необхідно вжити широкого спектру заходів, включаючи[13]:

- *Розвиток та впровадження технічних засобів захисту:*

використання мережевих заходів безпеки, систем виявлення вторгнень, антивірусного програмного забезпечення та інших технологій для виявлення та запобігання кібератакам.

- *Постійний моніторинг та аналіз загроз:*

проведення регулярного моніторингу та аналізу потенційних загроз для вчасного виявлення та вирішення потенційних проблем.

- *Навчання та підвищення обізнаності персоналу:*

проведення тренінгів та навчань для персоналу з питань кібербезпеки та соціально-інженерних атак для підвищення рівня обізнаності та захисту.

- *Забезпечення резервного копіювання та відновлення даних:*

регулярне створення резервних копій даних та розробка планів відновлення після інцидентів для забезпечення доступності та цілісності інформації.

- *Співпраця зі спеціалізованими організаціями та обмін інформацією:*

укладення партнерських угод зі спеціалізованими організаціями та участь у програмах обміну інформацією про кіберзагрози.

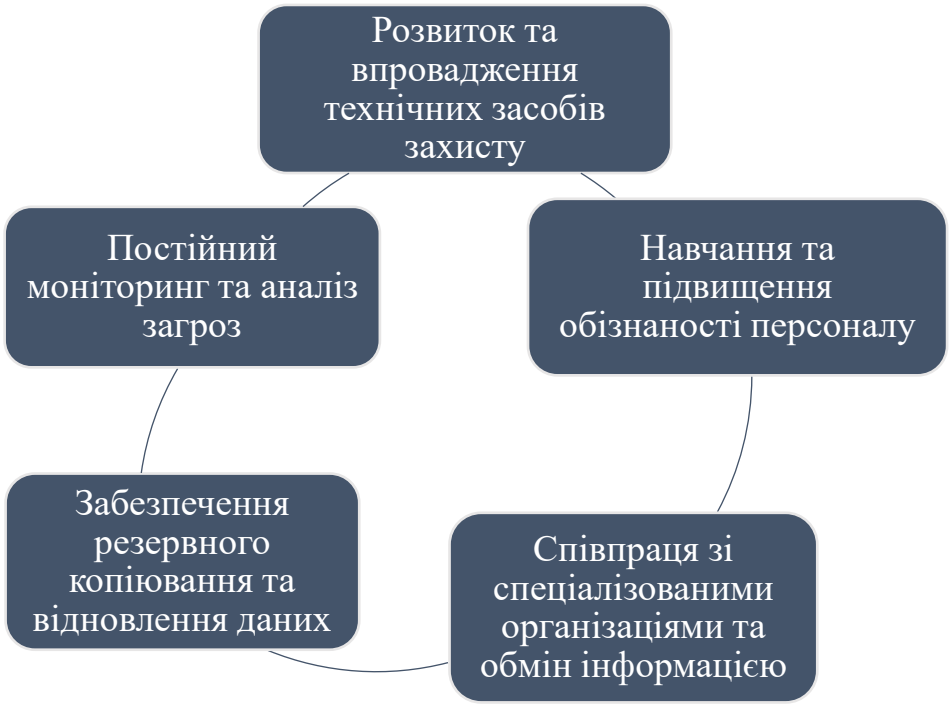

Рис. 4 Комплексні заходи для запобігання зовнішнім загрозам

Загальною метою цих заходів є забезпечення стійкості та надійності інформаційної інфраструктури підприємства в умовах постійно зростаючих зовнішніх загроз. Лише за допомогою комплексного підходу та активного виявлення та протидії зовнішнім загрозам підприємство може забезпечити ефективний захист своєї інформації та інформаційних ресурсів[14].

Ефективне управління інформаційною безпекою вимагає системного підходу та розробки комплексних стратегій, які враховують як внутрішні, так і

зовнішні загрози. Це включає в себе розробку та впровадження політик та процедур управління ризиками, вдосконалення технічних засобів захисту, проведення регулярних навчань та підвищення обізнаності персоналу, а також підтримку постійного моніторингу та аналізу загроз для оперативного реагування на них. Враховуючи постійні зміни в технологічному ландшафті та появу нових кіберзагроз, підприємства повинні бути готовими до постійного вдосконалення своїх стратегій та заходів захисту для забезпечення стійкості та надійності своєї інформаційної інфраструктури.

Системний підхід до управління інформаційною безпекою передбачає інтеграцію всіх аспектів цієї сфери діяльності в єдину систему, що працює відповідно до певних принципів та стратегій. Він базується на розумінні того, що безпека інформації - це не просто питання технічних заходів, але і впровадження відповідних політик, процедур, контролю та навчання персоналу.

Розробка комплексних стратегій управління інформаційною безпекою передбачає врахування як внутрішніх, так і зовнішніх загроз та ризиків. Це включає в себе такі кроки:

- *Оцінка ризиків:*

проведення комплексної оцінки ризиків, яка охоплює як внутрішні, так і зовнішні загрози. Це може включати аналіз існуючих систем безпеки, ідентифікацію потенційних вразливостей та визначення можливих наслідків для бізнесу в разі реалізації загроз.

- *Розробка політик і стандартів:*

розробка чітких політик та стандартів щодо захисту інформації, які враховують як внутрішні, так і зовнішні загрози. Ці політики повинні охоплювати такі аспекти, як управління доступом, захист даних, управління інцидентами та навчання персоналу.

- *Впровадження технічних засобів захисту:*

реалізація технічних засобів захисту, які допоможуть запобігти внутрішнім та зовнішнім загрозам. Це може включати в себе застосування

мережевих заходів безпеки, шифрування даних, використання систем виявлення вторгнень та інших технологій.

- *Навчання та підвищення обізнаності персоналу:*

здійснення регулярного навчання та підвищення обізнаності персоналу з питань інформаційної безпеки. Це допоможе зменшити ризик внутрішніх загроз, оскільки добре навчений персонал буде краще розуміти потенційні загрози та вміти вчасно реагувати на них.

- *Моніторинг і аналіз:*

постійний моніторинг і аналіз інформації щодо потенційних загроз та інцидентів. Це дозволяє вчасно реагувати на нові загрози та адаптувати стратегії захисту відповідно до змін в середовищі.

Рис. 5 Основні кроки до розробки комплексних стратегій управління інформаційною безпекою

У цілому, розробка комплексних стратегій управління інформаційною безпекою, які враховують як внутрішні, так і зовнішні загрози, є ключовим елементом успішного захисту підприємства від потенційних ризиків та забезпечення його стійкості та надійності.

Варто підкреслити, що управління інформаційною безпекою є надзвичайно важливим аспектом діяльності будь-якого підприємства в сучасному цифровому світі. Внутрішні та зовнішні загрози становлять серйозні виклики для безпеки інформації та можуть призвести до серйозних наслідків для бізнесу. Важливо враховувати різноманітність цих загроз та приділяти належну увагу розробці та впровадженню ефективних стратегій захисту[15].

Успішне управління інформаційною безпекою вимагає постійного вдосконалення технічних та організаційних заходів захисту, а також активного залучення персоналу до процесу захисту інформації. Відповідальність за забезпечення безпеки інформації лежить на всіх рівнях організації, від керівництва до кожного працівника. Лише шляхом поєднання технічних, організаційних та людських ресурсів підприємства можуть ефективно протистояти загрозам і забезпечити стійкість та надійність своєї інформаційної інфраструктури.

Висновок до розділу 1

Управління інформаційною безпекою підприємства є критично важливою складовою для забезпечення його стійкості та ефективності в умовах сучасного цифрового світу. Цей розділ надає глибокий аналіз основних загроз та вразливостей, які можуть зіткнутися з підприємством, а також стратегій та заходів, які можна вжити для їх управління та мінімізації ризиків.

Внутрішні загрози, такі як недбале ставлення до безпеки, недостатня обізнаність персоналу та зловживання привілеями, потребують уваги та контролю з боку керівництва підприємства. Відповідні політики та процедури безпеки, регулярне навчання персоналу та контроль доступу до конфіденційної інформації можуть допомогти зменшити внутрішні загрози та мінімізувати їхні наслідки.

Зовнішні загрози, такі як кібератаки та соціально-інженерні атаки, потребують комплексного підходу до захисту. Використання технічних засобів захисту, моніторингу та аналізу загроз, навчання персоналу та співпраці зі

спеціалізованими організаціями можуть допомогти ефективно виявляти та протидіяти зовнішнім загрозам.

У цілому, управління інформаційною безпекою підприємства вимагає постійного вдосконалення стратегій та заходів захисту, а також активного залучення персоналу до процесу безпеки. Лише шляхом комплексного підходу та системного управління можна забезпечити ефективний захист інформації та забезпечити стійкість підприємства в умовах постійно зростаючих загроз.

РОЗДІЛ 2 АНАЛІЗ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

2.1 Аналіз сучасних засобів та методів захисту інформації на підприємства

Технічні засоби захисту інформації включають у себе широкий спектр технологій, що застосовуються для забезпечення безпеки даних та інформаційних ресурсів. Ці засоби можуть включати програмне забезпечення, такі як антивіруси, що моніторять та блокують шкідливі програми та незаконний доступ до систем. Крім того, до технічних засобів захисту можуть входити заходи управління доступом, багаторівнева аутентифікація та моніторинг виявлення вторгнень, що допомагають управляти та контролювати доступ до систем та даних. Ці технічні засоби є важливою складовою інформаційної безпеки та допомагають зменшити ризики витоку та несанкціонованого використання даних.

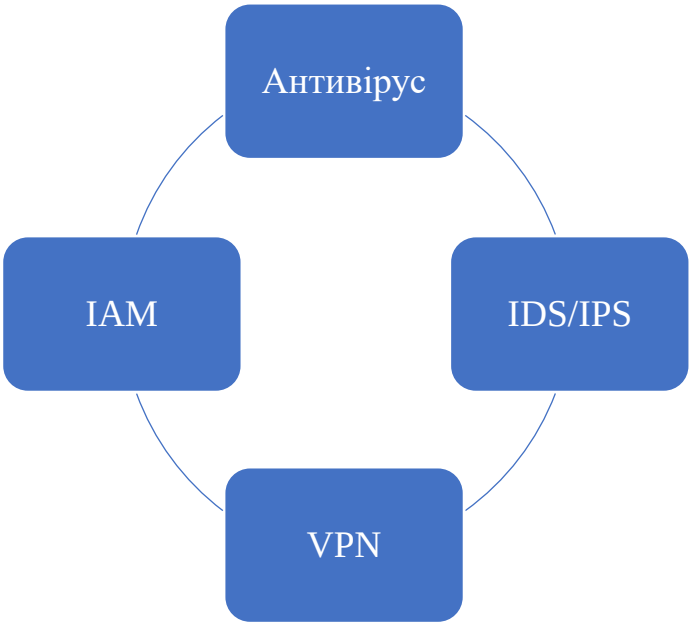

Рис. 2.1. Технічні засоби захисту інформації

Антивірусне програмне забезпечення (антивірус) — це спеціалізований програмний продукт, розроблений для виявлення комп'ютерних вірусів і різноманітних небажаних або шкідливих програм, а також для відновлення файлів, які були заражені або модифіковані такими програмами. Крім того, антивірусні програми виконують профілактичні функції, запобігаючи зараженню або модифікації файлів та операційної системи шкідливим кодом. Антивірусні програми виконують низку важливих завдань для забезпечення безпеки комп'ютерів та інших цифрових пристроїв[16].

Антивіруси здійснюють планове сканування системи, що дозволяє автоматично перевіряти комп'ютер у певні проміжки часу для виявлення та видалення шкідливих програм. Сканування в реальному часі постійно моніторить систему для негайного виявлення та блокування загроз.

Існує ряд ключових показників ефективності, які використовуються для оцінки роботи антивірусного програмного забезпечення. Вони допомагають забезпечити високий рівень захисту та продуктивності комп’ютерів в системі організації[17]:

- *Оновлення вірусних баз:*

щоденне користування Інтернетом або завантаження файлів піддає комп'ютер ризику зараження шпигунськими програмами, шкідливими програмами, вірусами, троянами та іншими загрозами. Антивірусні програми постійно оновлюють свої бази даних вірусів, щоб ефективно протистояти новим загрозам, забезпечуючи максимальний захист робочого комп'ютера.

- *Оновлення антивірусного програмного забезпечення*:

антивірусні програми не тільки оновлюють вірусні бази, але й саме програмне забезпечення. Антивіруси потребують регулярного оновлення до останніх версій. Це забезпечує інтеграцію нових функцій безпеки та виправлення можливих вразливостей. Автоматичні оновлення допомагають зберігати програму в актуальному стані без втручання користувача.

- *Сканування в режимі реального часу*:

ця функція забезпечує постійне сканування файлів та папок під час доступу до них. Сканер працює у фоновому режимі, невпинно перевіряючи систему на наявність загроз. Це дозволяє виявляти та нейтралізувати інфекції одразу, як тільки вони з'являються.

- *Сканування за вимогою*:

дана опція дозволяє користувачеві самостійно ініціювати сканування окремих файлів, папок або навіть цілих дисків у будь-який час. Це корисно для перевірки конкретних об'єктів, які можуть бути підозрілими.

- *Сканування за розкладом*:

антивірусне програмне забезпечення дозволяє налаштовувати автоматичне сканування системи у визначений час. Наприклад, сканування може бути заплановане під час перезавантаження системи, що дозволяє виявити та видалити загрози до активізації операційної системи.

- *Автоматичне сканування зовнішніх носіїв*:

при підключенні знімних носіїв, таких як USB-накопичувачі або зовнішні жорсткі диски, антивірус автоматично сканує їх на наявність загроз. Це запобігає поширенню вірусів через переносні пристрої.

- *Сканування стиснутих файлів*:

антивірусні програми можуть розпаковувати та сканувати файли, що мають кілька рівнів стиснення. Вони підтримують широкий спектр типів декомпресії та форматів кодування, що дозволяє ефективно перевіряти архіви на наявність шкідливого вмісту.

- *Захист файлообмінників (P2P)*:

антивірусне програмне забезпечення перевіряє файли, завантажені через популярні пірингові мережі. Це забезпечує додатковий рівень захисту під час обміну файлами в мережі.

- *Захист електронної пошти*:

сканує вхідні та вихідні повідомлення електронної пошти, виявляючи та блокуючи повідомлення, що містять вірусні інфекції. Це запобігає поширенню шкідливого ПЗ через електронну пошту.

- *Евристичний аналіз*:

використовується для оцінки підозрілих об'єктів шляхом моделювання їх поведінки у безпечному віртуальному середовищі. Це дозволяє виявляти нові та невідомі загрози, які ще не внесені до вірусної бази даних.

- *Захист миттєвих повідомлень*:

перевіряє файли, завантажені через програми обміну миттєвими повідомленнями, запобігаючи завантаженню заражених вірусами файлів.

- *Захист від шкідливих скриптів*:

виявляє та блокує шкідливі скрипти, що можуть надходити з Інтернету або інших джерел, зокрема збережених на диску чи в кеші браузера. Це запобігає запуску небезпечних сценаріїв, які можуть завдати шкоди системі.

- *Веб-щит*:

захищає комп'ютер під час перегляду веб-сторінок та завантаження файлів з Інтернету. Веб-щит виявляє та блокує відомі або потенційні загрози, що можуть надходити з Інтернету, такі як зламані веб-сторінки.

- *Антивірусна технічна підтримка*:

команда фахівців з антивірусної підтримки забезпечує актуальність програмного забезпечення, видаляє віруси та шкідливі програми, а також забезпечує загальну безпеку вашого ПК. Підтримка доступна цілодобово, надаючи найкращі послуги для захисту комп'ютера.

- *Захист паролем*:

антивірусне програмне забезпечення дозволяє встановити пароль для захисту від несанкціонованого доступу до програми або її окремих функцій. Це забезпечує додатковий рівень безпеки, запобігаючи несанкціонованому внесенню змін у налаштування антивірусу.

Отже, антивірусне програмне забезпечення є необхідним елементом захисту сучасних комп'ютерних систем. Воно забезпечує широкий спектр функцій, які допомагають захистити систему від численних кіберзагроз, зберегти дані в безпеці та підтримувати високу продуктивність комп'ютера.

Регулярне оновлення антивірусу і дотримання основних правил кібергігієни значно підвищує рівень захисту від потенційних атак.

IDS/IPS (Intrusion Detection and Prevention System) – це програмні або апаратні системи, призначені для виявлення та запобігання вторгненням, забезпечуючи мережну та комп'ютерну безпеку[18].

IDS – пасивна система виявлення, яка аналізує весь мережевий трафік у режимі реального часу. Її завданням є виявлення можливих загроз і повідомлення про них адміністратору або іншим засобам безпеки. IDS не модифікує мережеві пакети даних і не впливає на роботу мережевої інфраструктури. Вона працює шляхом моніторингу трафіку і виявлення аномалій або підозрілих дій, які можуть свідчити про спробу вторгнення.

Існує три основних типи виявлення для IDS: виявлення зловживань, виявлення аномалій та гібридне виявлення[19].

Виявлення зловживань, також відоме як сигнатурне виявлення, полягає в пошуку відомих шаблонів вторгнення в мережі або на хості. Кожна атака має специфічну сигнатуру, яка може включати корисне навантаження пакета або IP-адресу джерела. IDS спрацьовує, якщо виявить атаку, яка відповідає одній із сигнатур у базі даних відомих атак. Основною перевагою цього підходу є висока точність виявлення відомих атак, оскільки система чітко розпізнає визначені загрози. Однак цей метод має значні недоліки: він неефективний проти нових або невідомих атак, які ще не мають зареєстрованих сигнатур, зокрема вразливостей типу "нульового дня".

Виявлення аномалій ґрунтується на визначенні нормального стану мережі або хоста, який називається базовою лінією. Будь-яке відхилення від цієї базової лінії розглядається як потенційна загроза. Наприклад, IDS, заснована на виявленні аномалій, може створити базову лінію, враховуючи загальний мережевий трафік, послуги, що надаються кожним хостом, послуги, що використовуються кожним хостом, та обсяг активності протягом дня. Якщо зловмисник отримує доступ до внутрішнього ресурсу вночі, коли зазвичай активність мінімальна, IDS піднімає тривогу. Головною перевагою цього

підходу є здатність виявляти нові та невідомі атаки, які не мають попередньо визначених сигнатур. Проте встановлення точної базової лінії для мережі є складним завданням, і частота помилкових спрацьовувань може бути високою, що ускладнює ефективну роботу системи.

Гібридне виявлення поєднує в собі переваги обох вищезгаданих методів. Цей підхід використовує як сигнатурне виявлення, так і виявлення аномалій, забезпечуючи більш збалансований рівень захисту. Гібридні системи мають нижчий рівень помилкових спрацьовувань у порівнянні з методами виявлення аномалій, а також здатні виявляти нові атаки, завдяки чому вони є більш універсальними. Поєднання цих двох методів дозволяє досягти високої точності та ефективності виявлення загроз, забезпечуючи комплексний підхід до безпеки мережі.

IPS – активна система, яка не тільки виявляє загрози, але й здатна запобігти доставці небезпечних пакетів даних. IPS функціонує подібно до брандмауера, блокуючи небезпечний трафік, що може загрожувати безпеці мережі. На відміну від IDS, IPS активно втручається в роботу мережі, модифікуючи або блокуючи пакети даних, які були ідентифіковані як загроза.

Існують різні типи підходів, що використовуються в IPS для захисту мережі:

- *IPS на основі сигнатур*:

цей підхід зазвичай застосовується у багатьох рішеннях IPS. Сигнатури, які ідентифікують шаблони, властиві найпоширенішим атакам, додаються до пристроїв. Цей метод також відомий як зіставлення шаблонів. Сигнатури можуть бути додані, налаштовані та оновлені для боротьби з новими атаками. Основною перевагою цього підходу є висока точність виявлення відомих атак, але він неефективний проти нових та невідомих загроз.

- *IPS на основі аномалій*:

відомий також як профіль-орієнтований метод, він намагається виявити активність, яка відрізняється від нормальної активності, визначеної в системі.

Цей підхід може бути реалізований через статистичне або нестатистичне виявлення аномалій.

- *IPS, заснована на політиці*:

цей підхід орієнтований на забезпечення дотримання політики безпеки організації. Система піднімає тривогу, якщо виявляє дії, що порушують політику безпеки, що створена організацією. Політика безпеки записується на пристрої IPS, що дозволяє виявляти та запобігати порушенням, забезпечуючи дотримання внутрішніх правил безпеки.

- *IPS на основі аналізу протоколів*:

подібний до підходу на основі сигнатур, але з більш глибокою перевіркою пакетів. Цей метод перевіряє правильність налаштувань протоколів і може робити більш детальний аналіз трафіку. Це дозволяє більш гнучко виявляти деякі типи атак, що можуть залишитися непоміченими при звичайному сигнатурному аналізі. Основною перевагою є здатність виявляти складні атаки, але цей метод може вимагати більше ресурсів для обробки трафіку.

Ці підходи можуть бути комбіновані в одній системі IPS для забезпечення більш комплексного захисту мережі, що дозволяє виявляти та запобігати різноманітним типам загроз.

VPN (Virtual Private Network) – це технологія, що забезпечує безпечний та зашифрований обмін даними через інтернет, надаючи користувачеві приватність та конфіденційність. Підключаючись до VPN, пристрої організації створюють захищене з'єднання з VPN-сервером, що шифрує всі передані дані. Це забезпечує захист даних від прослуховування та забезпечує анонімність під час використання Інтернету[19].

Однією з ключових функцій VPN є зміна IP-адреси. Замість використання реальної IP-адреси, VPN призначає віртуальну IP-адресу з іншого місця, що дозволяє приховати справжню локацію. Крім того, VPN дозволяє отримати доступ до ресурсів мережі з будь-якого місця. З допомогою VPN можна

безпечно підключитися до корпоративної мережі з будь-якого місця і використовувати її ресурси так, ніби ви знаходитесь в офісі організації[20].

Системи керування ідентифікацією та доступом (Identity and Access Management, IAM) представляють собою важливий інструмент для організацій, дозволяючи їм ефективно керувати широким спектром ідентифікаційних даних. Ці системи охоплюють такі частини системи, як користувачі, програмне та апаратне забезпечення, а також пристрої IoT[21].

Рис. 2.2. Принцип роботи IAM

Зростаюче використання додатків в організаціях створює ряд проблем у сфері IAM. Ці проблеми можна розділити на фінансові, безпекові, відповідність нормативним вимогам та простоту використання[22]:

- *Фінансові проблеми:*

керування кількома обліковими даними для входу в систему негативно впливає на продуктивність роботи користувачів і призводить до виникнення зайвих завдань, таких як керування паролями для численних додатків. Проблеми, пов'язані з паролями, включаючи забуті паролі та часті скидання, призводять до значних витрат часу та коштів для організацій.

- *Проблеми з безпекою:*

неефективні політики безпеки та непослідовне застосування заходів безпеки створюють ризики для безпеки організації. Неналежне управління ідентифікаційними даними та повільні процеси деактивації сприяють виникненню вразливих місць у системі безпеки, що ускладнює збереження конфіденційності, цілісності та доступності конфіденційної інформації.

- *Проблеми з дотриманням нормативних вимог:*

жотримання нормативних вимог, таких як SOX та HIPAA, є необхідним для уникнення юридичних санкцій та фінансових втрат. Організації повинні продемонструвати можливість аудиту та контролювати дані, щоб забезпечити відповідність нормативним вимогам, що вимагає ефективних процесів управління ідентифікацією та доступом.

- *Проблеми зі зручністю використання:*

зростаюча складність автентифікації та попит на персоналізований контент погіршують користувацький досвід і продуктивність. Працівники стикаються з труднощами в отриманні доступу до необхідної інформації та управлінні численними обліковими даними для входу в систему. Попит на опції самообслуговування, такі як скидання паролів, має важливе значення для покращення користувацького досвіду та спрощення доступу до необхідних додатків, мінімізації розчарувань та неефективності.

Організаційні заходи захисту інформації включають у себе стратегії, політики та процедури, що встановлюються для забезпечення безпеки даних та інформаційних ресурсів в організації. Ці заходи можуть включати розробку політик безпеки інформації, які визначають правила та вимоги щодо обробки та зберігання даних, а також встановлення процедур контролю доступу та

моніторингу активності користувачів. Крім того, організаційні заходи можуть включати проведення навчань та навчальних програм з питань інформаційної безпеки для персоналу, а також регулярну перевірку та аудит систем безпеки для виявлення потенційних загроз і вразливостей. Всі ці заходи спрямовані на зменшення ризиків витоку, втрати або несанкціонованого доступу до інформації в організації[23].

Політика інформаційної безпеки визначає рамки для захисту даних та виконання сертифікаційних вимог. Вона включає набір правил і принципів, що керується компанією, щоб забезпечити безпеку в цій сфері.

Побудова політики інформаційної безпеки передбачає кілька ключових кроків. Спочатку виконавче керівництво встановлює правила високого рівня, що окреслюють концепцію безпеки компанії. Потім ці правила трансформуються в організаційні стандарти та інструкції, в яких детально описується, що потрібно зробити, щоб відповідати політиці. Організаційні стандарти забезпечують основу, тоді як правила містять детальні інструкції щодо впровадження політики. Після того, як політика розроблена, фокус переноситься на її впровадження на всіх рівнях організації[24].

Впровадження політики безпеки часто є найскладнішим етапом. Він вимагає навчання та тренування співробітників щодо нових вимог, щоб забезпечити їх розуміння та дотримання. Для підвищення обізнаності використовуються різні канали комунікації, такі як повідомлення, внутрішня мережа та інформаційні розсилки. Програма навчання, підготовки та підвищення обізнаності з питань безпеки (SETA) відіграє вирішальну роль у боротьбі зі зловживанням безпекою, передаючи знання про ризики та наголошуючи на обов'язках працівників.

Моніторинг, перегляд та оцінка політики безпеки є важливими для її ефективності. Регулярні оцінки забезпечують відповідність загрозам і нормативним вимогам, що постійно змінюються. Автоматизовані системи можуть допомогти у плануванні перевірок та попередженні про значні зміни.

Крім того, аналіз порушень безпеки та аудиторської інформації допомагає визначити сфери для вдосконалення та забезпечення дотримання політики[25].

Оцінка ризику є методом визначення й оцінки потенційних небезпек, впливу та ризиків. Управління ризиками — це процес ретельного аналізу альтернативних політичних заходів і вибір найбільш ефективних регуляторних дій на підставі отриманих результатів оцінки ризиків. Цей процес враховує соціальні, економічні та політичні аспекти для прийняття обґрунтованих рішень щодо управління потенційними негативними наслідками.

Цей підхід використовує різні інструменти і методи, адаптовані до конкретних умов. Надаючи уявлення про причини, наслідки та ймовірність ризиків, оцінка ризиків допомагає особам, які приймають рішення, та зацікавленим сторонам глибше зрозуміти потенційні загрози та ефективність існуючих засобів контролю. Крім того, вона слугує критично важливим фактором для визначення найбільш прийнятних стратегій управління ризиками.

Аналіз ризиків, найважливіший компонент процесу оцінювання, передбачає заглиблення в тонкощі ідентифікованих ризиків. Він допомагає визначити, чи потребують ризики лікування, і допомагає у виборі найбільш підходящих методів і стратегій лікування. Шляхом оцінки наслідків, ймовірностей та ефективності існуючих засобів контролю аналіз ризиків дає кількісну оцінку рівнів ризиків, що використовується в процесі прийняття рішень в організації[26].

Залежно від складності ризику та наявності даних використовуються різні методи, включаючи якісні, напівкількісні та кількісні підходи. У той час як кількісний аналіз забезпечує практичну цінність наслідків і ймовірностей, напівкількісні та якісні методи залишаються ефективними альтернативами, коли детальні дані або детальний аналіз є недоцільними або непотрібними. Зрештою, обраний підхід забезпечує адекватне розуміння ризиків та управління ними з метою пом'якшення потенційного впливу на цілі організації.

Фізичні засоби захисту інформації включають усі види обладнання, систем і інфраструктури, які застосовуються для забезпечення безпеки

фізичного доступу до інформаційних ресурсів. Ці засоби можуть включати системи контролю доступу, такі як біометричні сканери відбитків пальців або картки доступу, фізичні бар'єри, такі як двері з електронними замками або огородження, а також системи відеоспостереження для відстеження активності користувачів. Ці заходи спрямовані на запобігання несанкціонованому доступу до конфіденційної інформації та фізичного збереження даних у безпечному середовищі. Крім того, фізичні заходи захисту можуть включати заходи для захисту від природних катастроф, таких як пожежі або повені, наприклад, використання систем автоматичного сповіщення та пожежних сигналізацій для оперативного реагування на небезпеку[27].

Контроль доступу до приміщень є ключовим елементом фізичного захисту інформації. Він забезпечує безпеку та обмежує доступ до критично важливих зон, таких як серверні кімнати, архіви, та інші місця, де зберігається конфіденційна інформація. Також важливо зазначити, що контроль доступу передбачає ведення журналів доступу, де фіксуються всі спроби входу та виходу з приміщень, що дозволяє відстежувати дії користувачів і швидко виявляти можливі загрози. Регулярні аудити системи контролю доступу також допомагають підтримувати її ефективність та вчасно виявляти і усувати вразливості.

Рис. 2.3 Модель системи контролю доступу до приміщень

Фізичний захист серверів та мережевого обладнання має важливе значення для захисту IT-інфраструктури від несанкціонованого доступу, крадіжок, пошкоджень та екологічних загроз. Ключовим компонентом є

контроль доступу. Контроль навколишнього середовища підтримує оптимальні умови за допомогою систем опалення, вентиляції та кондиціонування, щоб запобігти перегріванню або пошкодженню від вологи. Заходи фізичної безпеки, такі як сейфові шафи, камери та укріплені двері, захищають від несанкціонованого доступу або крадіжки. Протипожежний захист включає детектори диму, пожежну сигналізацію та системи пожежогасіння, такі як спринклери або газові системи. Надійний захист електропостачання досягається за допомогою джерел безперебійного живлення і резервних генераторів для захисту від перебоїв і стрибків напруги. Впровадження фізичного резервування та планів аварійного відновлення забезпечує швидке відновлення у випадку катастроф. Постійний моніторинг і спостереження запобігають несанкціонованому доступу та забезпечують докази інцидентів, пов'язаних з безпекою. Регулярні перевірки виявляють вразливі місця та забезпечують дотримання політик безпеки, підвищуючи загальний рівень захисту серверів та мережевого обладнання[28].

Отже, постійне вдосконалення заходів безпеки є критично важливим через постійний розвиток нових загроз. Кіберзлочинці використовують сучасні технології для створення складніших методів атак, тому організації повинні регулярно оновлювати свої стратегії безпеки. Динамічний характер загроз вимагає адаптації до нових вразливостей і забезпечення ефективного захисту інформації.

2.2 Методика оцінки рівня вразливості та потенційних загроз інформаційній безпеці підприємства

Методика оцінки рівня вразливості та потенційних загроз інформаційній безпеці підприємства складається з кількох етапів, які включають ідентифікацію активів, аналіз вразливостей, визначення загроз, оцінку ризиків і розробку стратегії реагування. Спочатку здійснюється ідентифікація активів, які потребують захисту, таких як дані, системи, мережеве обладнання та

персонал. Далі проводиться аналіз вразливостей, щоб визначити слабкі місця в існуючих системах безпеки. Після цього визначаються потенційні загрози, які можуть скористатися цими вразливостями, включаючи зовнішні атаки, внутрішні витоки інформації та природні катастрофи.

Наступним етапом є оцінка ризиків, яка полягає у визначенні ймовірності та можливих наслідків реалізації кожної загрози. Цей процес дозволяє встановити пріоритети для найбільш критичних ризиків. На завершення розробляється стратегія реагування, яка включає заходи з усунення або мінімізації ризиків, підвищення рівня безпеки та план дій у разі інциденту. Такий підхід забезпечує комплексний захист інформаційних активів підприємства і дозволяє оперативно реагувати на нові загрози. Розглянемо кожен з етапів детальніше[29]:

- *Ідентифікація інформаційних активів:*

зосереджується на виявленні індивідуальних ризиків, які визначаються як ймовірність негативних подій, що становлять загрозу. Ризики оцінюються на основі їхньої ймовірності та потенційного впливу. Ідентифікація ризиків включає два підетапи: визначення критично важливих інформаційних активів, а потім виявлення їхніх вразливостей і потенційних загроз.

- *Визначення потенційних загроз:*

передбачає ідентифікацію всіх можливих загроз, які можуть вплинути на конфіденційність, цілісність та доступність інформаційних ресурсів організації. Також важливо визначити джерела та їх наслідки для орагіназції. Це дозволяє ефективніше розробляти стратегії захисту та мінімізувати ризики, пов'язані з інформаційною безпекою.

- *Аналіз вразливостей:*

оцінювання систем, мереж та програмного забезпечення на предмет потенційних слабкостей, які можуть бути використані зловмисниками для незаконного доступу або атак. Після ідентифікації вразливостей проводиться оцінка їхнього потенційного впливу на безпеку організації та розробка стратегій їхнього виправлення або запобігання.

- *Розробка стратегії управління ризиками:*

визначення пріоритетних заходів для зниження ризиків, розробка технічних, організаційних та фізичних заходів.

- *Впровадження заходів захисту.*
- *Планування реагування на інциденти:*

Розробка чітких процедур для виявлення, аналізу та відновлення після інцидентів. Реагування на інциденти повинно бути організованим, швидким і ефективним, щоб мінімізувати збитки та відновити нормальне функціонування бізнесу.

Отже, методика оцінки рівня вразливості та потенційних загроз інформаційній безпеці підприємства створює можливість розробки та впровадження ефективних стратегій захисту, а також дозволяє приймати обґрунтовані рішення щодо виділення ресурсів на запобігання потенційним ризикам. Також цей процес визначає готовність організації до виникнення ризиків та вирішує завдання мінімізації негативних наслідків.

2.3 Методи оцінки ефективності засобів захисту інформації

Від тестування на проникнення до аналізу показників безпеки – кожен підхід відіграє життєво важливу роль в оцінці та посиленні загального стану безпеки організацій. Розуміючи та впроваджуючи ці методи оцінки, компанії можуть виявити слабкі місця, зменшити ризики та створити надійний захист від кіберзагроз, що еволюціонують[30].

Аудит інформаційної безпеки є ключовим елементом в забезпеченні ефективності та надійності систем захисту даних. Внутрішній аудит проводиться власними силами компанії та спрямований на регулярну перевірку дотримання внутрішніх політик та процедур безпеки. Він дозволяє виявити можливі проблеми, вразливості та ризики та прийняти вчасні заходи для їх усунення. Зовнішній аудит залучає незалежних експертів, що дозволяє об'єктивно оцінити системи безпеки та виявити можливі прогалини або

вразливості, які можуть залишитися непоміченими внутрішнім відділом. Цей підхід допомагає компаніям забезпечити високий рівень захисту даних та запобігти можливим кіберзагрозам.

Внутрішній аудит інформаційної безпеки включає в себе оцінку дотримання політик безпеки, виявлення вразливостей у системах, аналіз процедур управління доступом та перевірку ефективності заходів захисту даних. Цей процес проводиться регулярно для забезпечення постійної відповідності до встановлених стандартів безпеки.

Зовнішній аудит, у свою чергу, виконується незалежними аудиторами або фахівцями з інформаційної безпеки, які мають об'єктивний погляд на стан систем захисту даних. Вони використовують спеціальні методи та інструменти для виявлення потенційних загроз та рекомендацій щодо поліпшення безпеки.

Обидва типи аудиту важливі для підтримки високого рівня безпеки інформації та захисту конфіденційності, цілісності та доступності даних[31].

Тестування на проникнення, відоме як пентестинг, є стратегічним методом для оцінки безпеки систем та мереж. Цей процес включає в себе ретельне використання реальних методів атак, які симулюють дії зловмисників, з метою виявлення потенційних вразливостей і ризиків безпеки. Експерти, які здійснюють пентестинг, використовують різноманітні техніки та інструменти для тестування систем на стійкість до вторгнень і оцінки їхньої здатності відбивати атаки. Результати цього процесу дозволяють ідентифікувати слабкі місця в захисті інформації та приймати відповідні заходи для їх усунення.

Пентестинг є важливою складовою стратегії кібербезпеки, оскільки він допомагає організаціям покращити свої заходи захисту та зменшити ризики кібератак. Процес пентестингу може бути виконаний як внутрішніми експертами з безпеки, так і залученням зовнішніх консультантів, які мають великий досвід у проведенні аналізу безпеки. Такий підхід дозволяє організаціям отримати об'єктивну оцінку їхньої інформаційної безпеки та розробити ефективні стратегії захисту даних[32].

Аналіз журналів та моніторинг подій є важливою складовою системи кібербезпеки для виявлення, відстеження та відповіді на потенційні загрози та інциденти. Цей процес передбачає постійний збір, аналіз і обробку журналів з різних інформаційних систем, таких як сервери, мережеві пристрої та додатки. Збираючи дані з цих джерел, команди забезпечення інформаційної безпеки можуть виявити підозрілу активність, яка може вказувати на спроби несанкціонованого доступу або атаки.

Використання інструментів для автоматизованого аналізу подій безпеки (SIEM) дозволяє швидше та ефективніше обробляти великі обсяги журналів, виявляючи відхилення від типових зразків поведінки та спрацьовуючи сповіщення про потенційні загрози. Додаткові інструменти аналізу можуть включати системи виявлення вторгнень та системи виявлення аномальної поведінки, які допомагають ідентифікувати атаки на ранніх стадіях.

Однак ефективність аналізу журналів і моніторингу подій залежить від точності і повноти зібраних даних, а також від швидкості реагування на виявлені загрози. Тому важливо постійно оновлювати та вдосконалювати процеси аналізу та реагування, враховуючи нові методики та технології, що дозволяють підвищити ефективність та швидкість.

Оцінка відповідності стандартам та нормативам також є ключовою складовою процесу забезпечення інформаційної безпеки. Вона передбачає перевірку та аналіз відповідності засобів захисту інформації міжнародним стандартам, таким як ISO/IEC 27001, NIST та іншим, а також регуляторним вимогам, що стосуються конкретної галузі або країни[33].

Цей процес включає перевірку того, чи відповідають заходи безпеки встановленим нормам та вимогам, а також аналіз результатів аудитів та інспекцій. Результати таких аудитів допомагають визначити, наскільки ефективно інформаційна система або процеси безпеки відповідають вимогам стандартів.

Важливою частиною оцінки відповідності є визначення заходів для усунення будь-яких виявлених невідповідностей і підвищення рівня безпеки.

Це може включати впровадження додаткових технічних та організаційних заходів, а також актуалізацію процедур та політик інформаційної безпеки.

Метрики та ключові показники ефективності (KPI) дозволяють визначити та моніторити рівень безпеки в організації шляхом вимірювання різних параметрів. Ці метрики можуть включати кількість інцидентів, час реагування на них, відсоток виявлених вразливостей. Аналізуючи ці дані, можна виявити області, які потребують поліпшення, що дозволяє приймати обґрунтовані рішення щодо удосконалення системи безпеки[34].

Застосування метрик та KPI допомагає організаціям ефективно керувати процесом забезпечення інформаційної безпеки, забезпечуючи вчасну реакцію на потенційні загрози та постійне вдосконалення системи захисту.

Підсумовуючи, ці методи в комплексній системі оцінки ефективності засобів захисту інформації допоможуть підприємствам забезпечити ефективність засобів захисту та підтримувати високий рівень безпеки в умовах постійно змінюваних загроз.

Висновок до розділу 2

Важливість ефективних засобів та методів захисту інформації на підприємствах не можна переоцінити, оскільки інформаційна безпека є ключовим елементом стійкості та успішного функціонування будь-якої організації. Сучасні засоби захисту інформації включають різноманітні технології та інструменти, які допомагають запобігти несанкціонованому доступу, забезпечити конфіденційність, цілісність та доступність даних. Серед цих засобів важливу роль відіграють системи виявлення та запобігання вторгненням, шифрування даних, антивірусні програми, а також системи управління інформаційною безпекою, які забезпечують комплексний підхід до захисту інформації.

Методика оцінки рівня вразливості та потенційних загроз інформаційній безпеці підприємства включає кілька важливих етапів. Перший етап передбачає

ідентифікацію активів, що потребують захисту, та аналіз вразливостей, які можуть бути використані зловмисниками. Далі слідує визначення можливих загроз та оцінка ризиків, що дозволяє зрозуміти, які саме загрози є найбільш ймовірними та які з них можуть мати найбільш серйозні наслідки для підприємства. Останнім етапом є розробка стратегії реагування, що включає заходи з мінімізації ризиків та підвищення рівня захисту.

Методи оцінки ефективності засобів захисту інформації включають використання різних метрик та ключових показників ефективності (KPI), таких як кількість виявлених вразливостей, час реагування на інциденти та кількість успішних атак, що були відвернені. Такі метрики дозволяють не тільки оцінити поточний стан інформаційної безпеки, але й виявити слабкі місця та області, які потребують вдосконалення. Використання як внутрішніх, так і зовнішніх аудитів допомагає підприємствам отримати незалежну оцінку ефективності їхніх заходів безпеки та внести необхідні корективи для підвищення рівня захисту.

Таким чином, постійний моніторинг, оцінка та вдосконалення заходів безпеки є ключовими компонентами ефективного управління інформаційною безпекою на підприємствах. Сучасні технології та методики забезпечують комплексний підхід до захисту, що дозволяє підприємствам не тільки захищати свої активи, але й швидко адаптуватися до нових загроз та викликів.

РОЗДІЛ 3 ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Рекомендації щодо підвищення ефективності захисту інформації на підприємстві

Забезпечення інформаційної безпеки організацій нині є однією з необхідних умов їх конкурентоспроможного існування. Безпека даних спрямована на захист даних під час їх створення, зберігання, управління та передачі. Тому необхідно забезпечувати та підвищувати якісь найдійного захисту інформації в організації.

Як вже було розглянуто в попередньому розділі, розробка та впровадження політик безпеки забезпечує надійний захист інформаційних ресурсів підприємства та сприяє зниженню ризиків. Інформаційні загрози та технології швидко еволюціонують, тому політики безпеки повинні відповідати новим реаліям. Це вимагає постійного моніторингу поточної ситуації в сфері кібербезпеки, аналізу нових ризиків та впровадження відповідних змін до існуючих правил і процедур. Регулярний аудит політик дозволяє виявляти слабкі місця та своєчасно вносити необхідні корективи.

Проведення регулярних тренінгів з інформаційної безпеки для всіх співробітників допомагає створити культуру безпеки та забезпечити розуміння основних принципів захисту даних. Ці тренінги повинні охоплювати широкий спектр тем, включаючи захист конфіденційної інформації, безпечне користування інтернетом, управління паролями та правила безпечної роботи з електронною поштою[35].

Інформування співробітників про актуальні загрози та методи їх уникнення, такі як фішинг та соціальна інженерія, є не менш важливим. Регулярне оновлення інформації про нові загрози та навчання методам їх виявлення і уникнення допомагає знизити ризики успішних атак на підприємство.

Розробка програм навчання для нових співробітників та регулярне оновлення знань існуючих є також важливим аспектом загальної стратегії безпеки. Нові співробітники повинні отримувати повне введення в політику та процедури безпеки підприємства одразу після прийняття на роботу. Водночас, постійні працівники повинні регулярно проходити повторні тренінги та оновлення знань, щоб бути в курсі останніх змін у політиках безпеки та нових загроз.

Також в попередньому розділі були розглянуті сучасні технічні засоби захисту, впровадження яких може відіграти ключову роль в системі безпеки організації. До цих сучасних засобів відносяться системи виявлення та запобігання вторгнень (IDS/IPS), управління ідентифікацією та доступом (IAM) та антивіруси. Необхідно зазначити, що цими засобами перелік не обмежується. До них можна включити також шифрування даних та брандмауери[36].

Використання сильних алгоритмів шифрування для захисту даних як у стані спокою, так і під час передачі, значно знижує ризик несанкціонованого доступу до конфіденційної інформації. Шифрування дозволяє перетворити дані у форму, що недоступна для розуміння без відповідного ключа дешифрування, що унеможливлює прочитання інформації зловмисниками навіть у разі її перехоплення або витоку.

Для ефективного захисту даних важливо використовувати сучасні стандарти шифрування, такі як AES (Advanced Encryption Standard), який забезпечує високий рівень безпеки та швидкість. Крім того, необхідно впроваджувати протоколи шифрування для захисту даних під час передачі, наприклад, SSL/TLS для захисту веб-трафіку. Важливим аспектом є управління ключами шифрування, які повинні зберігатися в безпечних сховищах і бути доступними лише уповноваженим користувачам. Регулярна ротація ключів та використання апаратних засобів захисту, таких як апаратні модулі безпеки (HSM), допомагає знизити ризик компрометації ключів[37].

Також варто забезпечити шифрування даних на рівні дисків та файлових систем, що додатково захищає інформацію у випадку фізичної втрати або крадіжки пристроїв.

Брандмауери (фаєрволи) контролюють та фільтрують вхідний та вихідний трафік, запобігаючи несанкціонованому доступу до мережі підприємства. Брандмауери можуть бути як апаратними, так і програмними, і їх комбінація забезпечує більш надійний захист. Апаратні брандмауери встановлюються на фізичних пристроях і працюють незалежно від операційної системи, що дозволяє їм бути більш стійкими до зломів і відмов. Програмні брандмауери, в свою чергу, забезпечують більш гнучке налаштування і можуть бути інтегровані безпосередньо в операційну систему або мережеве програмне забезпечення[38].

Основною функцією брандмауерів є створення бар'єра між внутрішньою безпечною мережею підприємства та зовнішніми загрозами з Інтернету. Вони аналізують пакети даних, що надходять, і визначають, чи дозволити їм пройти до мережі або заблокувати. Це дозволяє запобігати різноманітним атакам, таким як спроби вторгнення, розповсюдження шкідливого програмного забезпечення та несанкціонований доступ до конфіденційної інформації. Налаштування брандмауерів повинне бути ретельно продумане і відповідати специфічним потребам підприємства.

Процес впровадження передових сучасних технічних засобів захисту є комплексним і вимагає детального планування та системного підходу. Першим етапом цього процесу є оцінка поточного стану інформаційної безпеки на підприємстві. Це включає виявлення вразливих місць, аналіз існуючих засобів захисту та визначення потенційних загроз. На основі цього аналізу розробляється стратегія впровадження нових технічних засобів захисту, яка враховує специфіку діяльності підприємства та його потреби.

Наступним кроком є вибір відповідних технологій та рішень. Після вибору відповідних технологій здійснюється їх впровадження в існуючу інфраструктуру підприємства. Це може включати встановлення нового

обладнання, налаштування програмного забезпечення та конфігурацію систем управління безпекою. Особлива увага приділяється сумісності нових засобів захисту з існуючими системами, щоб уникнути можливих конфліктів та забезпечити безперервність роботи. Після інтеграції нових засобів захисту проводиться тестування їхньої ефективності. Це включає симуляцію атак та оцінку здатності систем виявляти та відбивати загрози. За результатами тестування можуть бути внесені корективи до налаштувань для досягнення оптимальної продуктивності.

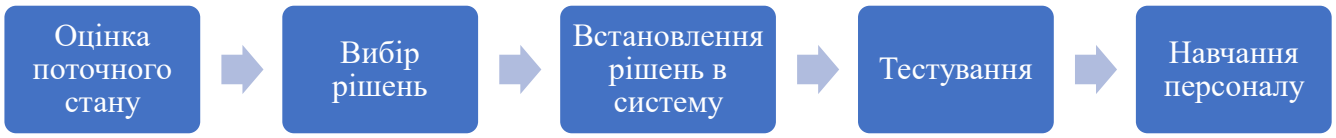

Рис. 3.1. Процес впровадження нових засобів в систему

Сегментація мережі — процес розділення локальної мережі на декілька незалежних сегментів, кожен з яких має свій рівень доступу та захисту, з метою збільшення загальної швидкості обміну даними. Цей підхід дозволяє мінімізувати ризики, пов'язані з несанкціонованим доступом до критичних систем та даних. Впровадження сегментації мережі починається з аналізу поточної мережевої інфраструктури та визначення ключових активів, які потребують підвищеного рівня захисту. Після цього здійснюється розподіл мережі на сегменти. Наприклад, можна виділити окремі сегменти для фінансових даних, виробничих систем, загальнодоступних ресурсів та інших критичних частин мережі. Кожен сегмент мережі ізолюється від інших, що зменшує ризик поширення загроз у випадку успішного вторгнення в одну з частин мережі[39].

Для реалізації сегментації використовуються різні технології, серед яких однією з найпоширеніших є віртуальні локальні мережі (VLAN). VLAN

дозволяє логічно розділити фізичну мережу на окремі віртуальні сегменти, кожен з яких має свій набір правил доступу та безпеки.

Ще однією рекомендацією, яка може підвищити рівень безпеки в організації є партнерство з третіми сторонами. Завдяки їх залученню можна виявити приховані вразливості та отримати незалежні рекомендації щодо їх усунення. В ролі третіх сторін можуть виступати зовнішні аудитори, партнери організації, залучені експерти з інформаційної безпеки.

Крім того, участь у галузевих форумах та обмін досвідом з іншими організаціями є важливою складовою безперервного розвитку системи інформаційної безпеки. На таких заходах фахівці мають можливість ознайомитися з новітніми технологіями та підходами, а також отримати цінну інформацію про реальні випадки атак та способи їх відбиття. Взаємодія з іншими компаніями дозволяє створити спільноту, яка активно обмінюється знаннями та підтримує один одного у боротьбі з кіберзагрозами.

3.2 Моніторинг та оцінка ефективності впроваджених рекомендацій

Найкращі практики для успішного процесу моніторингу та оцінки мають важливе значення для забезпечення успіху будь-якого проекту або програми. Важливо розробити стратегію, яка стане основою для процесу оцінювання, оскільки це допоможе забезпечити досягнення бажаних результатів. Крім того, наявність чітко визначених етапів і процесів має важливе значення для забезпечення ефективного і точного збору всіх даних.

Постійний моніторинг впроваджених рекомендацій передбачає систематичний підхід до відстеження ефективності заходів безпеки з плином часу. Цей процес починається зі встановлення ключових показників ефективності (KPI) та метрик, узгоджених з цілями стратегії безпеки. Використовуючи поєднання автоматизованих інструментів і ручних оцінок, організації збирають відповідні дані про різні аспекти інформаційної безпеки,

включаючи мережевий трафік, системні журнали, дії користувачів і звіти про інциденти[40].

Оцінка ефективності впроваджених рекомендацій - це систематичний процес, спрямований на оцінку впливу заходів з інформаційної безпеки та визначення їх успішності в досягненні бажаних результатів. Цей процес включає кілька ключових кроків для вимірювання ефективності за заздалегідь визначеними критеріями та показниками.

Оцінка починається з визначення чітких цілей і критеріїв для оцінки ефективності заходів інформаційної безпеки. Ці критерії можуть включати такі фактори, як відповідність нормативним вимогам, зменшення кількості інцидентів безпеки, зменшення вразливостей та покращення загального стану безпеки[41].

Потім встановлюються показники для кількісної оцінки ефективності засобів контролю безпеки та вимірювання прогресу в досягненні визначених цілей. Ці показники можуть охоплювати різні аспекти інформаційної безпеки, в тому числі час реагування на інциденти, рівень виявлення та усунення інцидентів, рівень дотримання нормативних вимог та обізнаність користувачів[42].

Отже, основний процес моніторингу можна розглянути на Рис. 3.2.

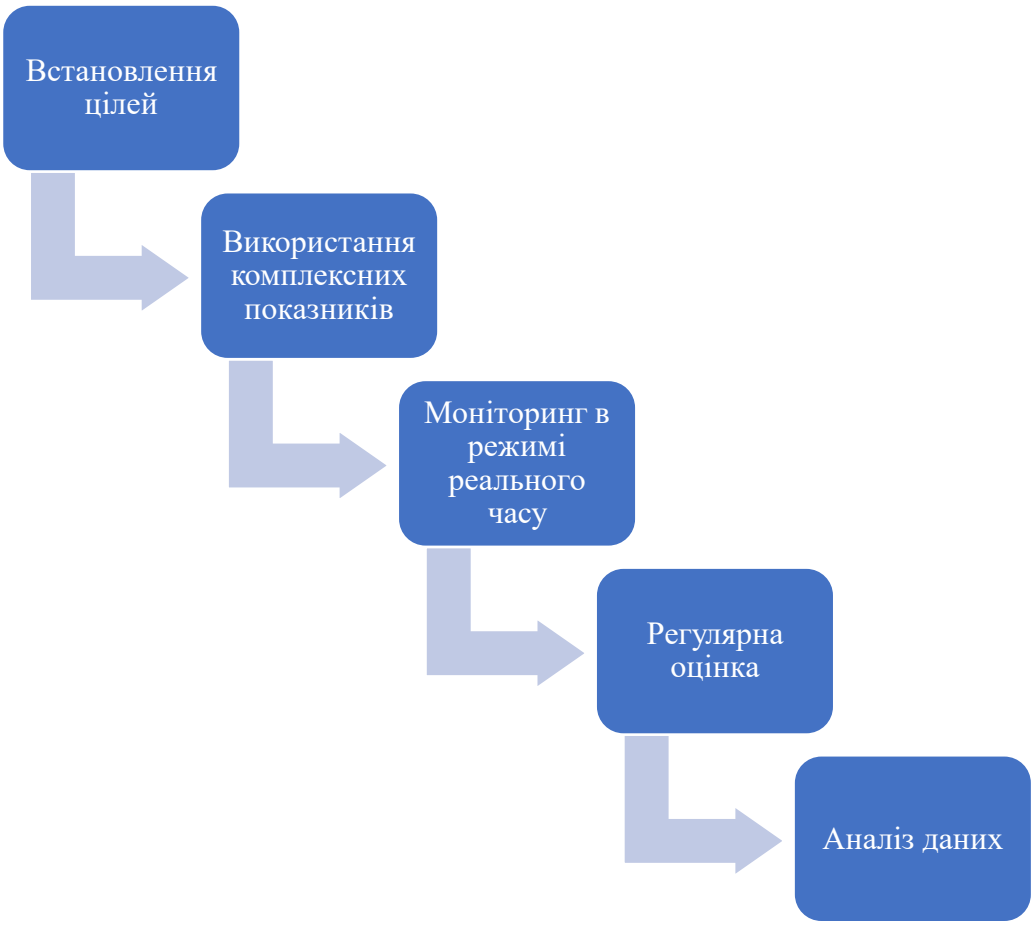

Рис. 3.2. Кращі практики моніторингу впроваджених заходів

Регулярне звітування про стан інформаційної безпеки для керівництва підприємства є важливою складовою ефективної системи контролю. Ці звіти дозволяють керівництву мати наочне уявлення про ступінь виконання запланованих заходів з підвищення безпеки, виявлені ризики та потенційні загрози, а також ефективність впроваджених заходів. Вони також надають можливість вчасно реагувати на виявлені проблеми та приймати обґрунтовані рішення щодо подальших кроків у напрямку забезпечення безпеки інформації[43].

Крім того, відкриті комунікації між відділом інформаційної безпеки та іншими підрозділами підприємства сприяють створенню сприятливого середовища для обміну інформацією щодо загроз та вразливостей. Це дозволяє всім зацікавленим сторонам бути в курсі поточного стану безпеки та вчасно реагувати на виявлені проблеми[44].

Окрім того, відкриті комунікації сприяють залученню працівників різних підрозділів до процесу забезпечення безпеки інформації. Це стимулює взаємодію між різними відділами та сприяє обміну кращими практиками та ідеями щодо підвищення безпеки інформації. Такий підхід сприяє побудові єдиної команди, яка працює над спільною метою - забезпечення безпеки інформації на підприємстві[45].

Отже, постійно оцінюючи ефективність впроваджених стратегій, компанії можуть виявити сильні та слабкі сторони, а також сфери, які потребують вдосконалення у сфері безпеки. Такий проактивний підхід дозволяє своєчасно виявляти та пом'якшувати нові загрози, захищаючи критичні активи та дані.

Висновок до розділу 3

Отже, постійний моніторинг та оцінка відіграють ключову роль у підтримці надійних заходів інформаційної безпеки в організаціях. Регулярно оцінюючи ефективність впроваджених рекомендацій, компанії можуть виявити сильні та слабкі сторони, що дозволить їм відповідно адаптувати та вдосконалити свої практики безпеки. Організаціям важливо усвідомлювати, що ландшафт загроз постійно змінюється, а отже, їхні заходи безпеки повинні розвиватися разом з ним. Дані, отримані в процесі моніторингу та оцінки, надають безцінну інформацію для прийняття рішень, що дозволяє організаціям випереджати нові загрози та вразливості.

Надалі організаціям рекомендується визначати пріоритетність постійного моніторингу та оцінки як невід'ємних компонентів своєї стратегії інформаційної безпеки. Це передбачає створення структури для регулярних оцінок, використання передових інструментів і технологій для збору та аналізу даних, а також сприяння відкритим каналам комунікації між підрозділами. Крім того, організаціям слід розглянути можливість інвестування в ініціативи з навчання та розвитку, щоб гарантувати, що співробітники залишатимуться поінформованими та пильними щодо нових загроз безпеці.

Застосовуючи проактивний підхід до моніторингу та оцінки, організації можуть посилити свою стійкість до кіберзагроз та ефективно захищати конфіденційну інформацію. Саме завдяки постійній пильності та адаптації компанії можуть підтримувати сильну позицію безпеки в сучасному цифровому ландшафті, що постійно змінюється.

ВИСНОВКИ

У ході аналізу управління інформаційною безпекою на підприємствах виявлено, що інформаційна безпека є критичною складовою для забезпечення стабільності та успішної діяльності підприємства. Внутрішні та зовнішні загрози, які можуть здійснювати вплив на інформаційну безпеку, включають в себе широкий спектр факторів, від технічних вразливостей і системних помилок до кібератак, шпигунства та соціально-інженерних атак.

Внутрішні загрози зазвичай випливають з недосконалої культури безпеки серед персоналу, недостатньої уваги до політик та процедур безпеки, а також недбалості або зловживання привілеями. З іншого боку, зовнішні загрози можуть включати кіберзлочинців, хакерів, зловмисників, які намагаються отримати несанкціонований доступ до систем, крадуть чутливі дані, або впливають на інфраструктуру підприємства через різноманітні технологічні вразливості.

Аналіз засобів та методів захисту інформації показав, що сучасні технології створюють широкий спектр можливостей для захисту інформації на підприємствах. Це включає в себе застосування шифрування даних, розвиток протоколів безпеки, впровадження систем виявлення та запобігання вторгненням, а також розробку багатошарових стратегій захисту, які враховують як технічні, так і організаційні аспекти безпеки.

Проте ефективність цих засобів захисту залежить від їх правильного впровадження та постійного оновлення відповідно до змінних умов та загроз. Ретельна оцінка рівня вразливості та потенційних загроз інформаційній безпеці, а також методи оцінки ефективності засобів захисту, є необхідними етапами у процесі забезпечення інформаційної безпеки на підприємстві.

Щодо підвищення ефективності захисту інформації, важливою є розробка та впровадження рекомендацій, спрямованих на збільшення рівня захисту. Це може включати удосконалення політик безпеки, підвищення рівня свідомості персоналу, розвиток та вдосконалення технічних засобів захисту, а також

впровадження процедур реагування на інциденти та планування контингентних заходів. Постійний моніторинг та оцінка ефективності впроваджених заходів дозволяють вчасно виявляти та усувати вразливості, а також адаптувати заходи захисту до нових умов та загроз, які постійно змінюються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. № 56. URL: https://doi.org/10.32782/2524-0072/2023-56-118

2. Економічне обгрунтування управління інформаційною безпекою підприємства. І. М. Сотник та ін. 2017. URL: http://essuir.sumdu.edu.ua/handle/123456789/54491

3. Маковський І. Ю. Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві. *Економіка, управління та адміністрування*. 2020. № 1(91). С. 38–42. URL: https://doi.org/10.26642/ema-2020-1(91)-38-42

4. Медвідь В. Ю., Правдивець О. М., Кривчун Р. Ю. Теоретико-методичні засади формування системи управління інформаційною безпекою підприємства. *Agrosvit*. 2023. № 1. С. 24–30. URL: https://doi.org/10.32702/2306-6792.2023.1.24

5. Батечко О., Цимбаленко Н. В. Інформаційна безпека підприємства. 2016. URL: https://er.knutd.edu.ua/handle/123456789/4464

6. Інформаційна безпека - одна з основних складових успішного бізнесу сучасного підприємства / В. І. Мазур та ін. *Ukrainian information security research journal*. 2007. Т. 9, № 3(34). URL: https://doi.org/10.18372/2410-7840.9.4156

7. Ананченко О. Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. *Сучасний захист інформації*. 2016. № 1. С. 79–83.

8. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49

9. Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. *Ukrainian information security research journal*. 2022. Т. 23, № 4. С. 200–211. URL: https://doi.org/10.18372/2410-7840.23.16766

10. Алгоритми прогнозування вразливостей та загроз інформаційної безпеки на основі тематичних інтернет-ресурсів. Є. Майор та ін. *Measuring and computing devices in technological processes*. 2023. № 4. С. 49–56. URL: https://doi.org/10.31891/2219-9365-2023-76-6

11. Information and analytical forecasting systems information security vulnerabilities and threats. S. V. Lienkov et al. *Collection of scientific works of the military institute of kyiv national taras shevchenko university*. 2023. No. 79. P. 114–127. URL: https://doi.org/10.17721/2519-481x/2023/79-11

12. Савеленко О. К. Формалізація рівня загроз інформаційної безпеки підприємства : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/3001

13. Кан Н. І. Моніторинг загроз інформаційної безпеки підприємства з використанням інформаційних технологій : магістерська робота. 2020. URL: https://dspace.znu.edu.ua/jspui/handle/12345/4716

14. Леськів Г., Гобела В., Лесик Н. Характеристика основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. *Економіка та суспільство*. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-8

15. Aseeva L. A. Analysis of the main components of danger in the construction of information security system of the enterprise. *Modern information security*. 2019. No. 2. URL: https://doi.org/10.31673/2409-7292.2019.024246

16. Овчаренко М. Центр оперативного управління інформаційною безпекою. *Advanced discoveries of modern science: experience, approaches and innovations*. 2021. URL: https://doi.org/10.36074/logos-09.04.2021.v1.49

17. Безштанько В. Цикл впровадження системи управління інформаційною безпекою. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 123–126.

18. Наконечний В. С. Стан розвитку управління інформаційною безпекою в світовій практиці та її вплив на економічний розвиток України. *Сучасний захист інформації*. 2015. № 4. С. 10–15.

19. Цуркан В. В. Метод синтезування структури систем управління інформаційною безпекою. *Ukrainian scientific journal of information security*. 2023. Т. 26, № 2. С. 116–122. URL: https://doi.org/10.18372/2225-5036.26.14966

20. Аналіз біометричних засобів захисту інформації. С. П. Козирев та ін. *Ukrainian information security research journal*. 2010. Т. 12, № 4 (49). URL: https://doi.org/10.18372/2410-7840.12.1973

21. Тертишник В. М. Система технічного захисту інформації на підприємстві : thesis. 2021. URL: http://ir.stu.cn.ua/123456789/22665

22. Шепета О. В., Тугарова О. К. Основні вимоги до створення служби захисту інформації на підприємстві. Прикарпатський юридичний вісник. 2020. № 3(32). С. 74–77. URL: https://doi.org/10.32837/pyuv.v0i3(32).607

23. Поліщук А. В. Дослідження методів і засобів захисту інформації в корпоративних мережах. 2013. URL: http://elartu.tntu.edu.ua/handle/123456789/2677

24. Молодецька-Гринчук К. В. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня. *Системи обробки інформації*. 2017. № 5(151). С. 122–129. URL: https://doi.org/10.30748/soi.2017.151.16

25. Hryk Y. V., Hrynokh N. Y., Selmenska Z. M. Analysis of modern methods and means of protection of labelling and packaging products based on identification and authentication. *Book qualilogy*. 2022. Vol. 2, no. 42. P. 54–66. URL: https://doi.org/10.32403/2411-3611-2022-2-42-54-66

26. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об"єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.

27. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. *Automation of*

technological and business processes. 2017. Т. 9, № 2. URL: https://doi.org/10.15673/atbp.v9i2.560

28. Невойт Я. В. Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці : автореф. дис. канд. техн. наук. Київ, 2015. 22 с.

29. Зуєв О. В., Хмелько Ю. М., Чирков Д. В. Критерій оцінки якості функціонування засобів захисту інформації. *Ukrainian information security research journal*. 2001. Т. 3, № 1(6). URL: https://doi.org/10.18372/2410-7840.3.4615

30. Cherneha V. M., Katsalap V. O., Voitko O. V. Методика оцінки загроз інформаційній безпеці україни у воєнній сфері. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. Т. 1, № 31. С. 149–154. URL: https://doi.org/10.33099/2311-7249/2018-31-1-149-154

31. Морозюк О. О. Інноваційні методи оцінки ефективності використання основних засобів: краща практика. *Реформування фінансово-економічної системи країни в контексті міжнародного співробітництва*. 2023. URL: https://doi.org/10.36059/978-966-397-336-4-38

32. Хамула С. В. Оцінка ефективності застосування технічних засобів захисту інформації. *Ukrainian information security research journal*. 2003. Т. 5, № 4(17). URL: https://doi.org/10.18372/2410-7840.5.4192

33. Мірошник М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах. *Інформаційно-керуючі системи на залізничному транспорті.* 2015. № 4. URL: https://doi.org/10.18664/ikszt.v0i4.53936

34. Чубаєвський В. І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації. *Efektyvna ekonomika*. 2022. № 11. URL: https://doi.org/10.32702/2307-2105.2022.11.20

35. Аналіз біометричних засобів захисту інформації. С. П. Козирев та ін. *Ukrainian information security research journal*. 2010. Т. 12, № 4 (49). URL: https://doi.org/10.18372/2410-7840.12.1973

36. Павленко Л. І. Шляхи комплексного визначення ефективності захисту інформації. *Актуальні проблеми міжнародних відносин*. 2006. Вип. 64, ч. 1. С. 97–102.

37. Суслов А. П., Suslov A. Розробка заходів щодо підвищення ефективності діяльності на підприємстві в умовах ринку : магістерська робота. 2020. URL: https://dspace.znu.edu.ua/jspui/handle/12345/2335

38. Оптимізація вибору засобів захисту інформації за допомогою генетичного алгоритму. V. Lakhno та ін. *Technical sciences and technologies*. 2021. № 3(25). С. 138–149. URL: https://doi.org/10.25140/2411-5363-2021-3(25)-138-149

39. Шумейко В. М. Технологічна сегментація . 2011. URL: http://essuir.sumdu.edu.ua/handle/123456789/28486

40. Василюк В. Об"єкти захисту інформації. Методи та засоби захисту інформації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 88–95.

41. Власюк С. Особливості захисту інформації в бізнесі. *Схід*. 2009. № 3 (94). С. 29–32.

42. Павлов І. М., Бірюков В. О. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації. *Ukrainian information security research journal*. 2011. Т. 13, № 2 (51). URL: https://doi.org/10.18372/2410-7840.13.2004

43. Єгоров Ф. І., Тискіна Є. О., Хорошко В. О. Задачі захисту інформації. *Ukrainian information security research journal*. 2009. Т. 11, № 1(42). URL: https://doi.org/10.18372/2410-7840.11.5368

44. Резніченко В. А. Дослідження методів захисту інформації в телекомунікаційних мережах : thesis. 2014. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/2978

45. Янчук Т. В. Значення сучасних технологій захисту інформації. *Акредитація освітніх програм економічного блоку в умовах війни*. 2022. URL: https://doi.org/10.36059/978-966-397-259-6-23