МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОЦІНЮВАННЯ ВПЛИВУ ЛЮДСЬКОГО ФАКТОРУ НА ЕФЕКТИВНІСТЬ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

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

_____ Ігор Бишук
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Ігор БИШУК
Ім’я, ПРІЗВИЩЕ

Керівник: Діана ПРИМАЧЕНКО
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бишуку Ігорю Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оцінювання впливу людського фактору на ефективність системи управління інформаційною безпекою”,
керівник кваліфікаційної роботи ПРИМАЧЕНКО Діана.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *система управління інформаційною безпекою підприємства, методи оцінювання ризиків та впливу людського фактору, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1 Дослідити теоретичні основи управління інформаційною безпекою.
   4.2 Проаналізувати вплив людського фактору на ефективність системи управління інформаційною безпекою.
   4.3. Вивчити методи оцінювання та мінімізації впливу людського фактору.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження основ управління інформаційною безпекою	08.04.2026	
4.	Аналіз впливу людського фактору на ефективність системи управління інформаційної безпеки	15.04.2026	
5.	Вивчення методів оцінювання та мінімізації впливу людського фактору	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	05.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Ігор БИШУК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Бишук І.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оцінювання впливу людського фактору на ефективність системи управління інформаційною безпекою "

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач БИШУК Ігор у кваліфікаційній роботі дослідив теоретичні основи управління інформаційною безпекою, проаналізував вплив людського фактору на ефективність системи управління інформаційною безпекою, вивчив методи оцінювання та мінімізації впливу людського фактору, розробив практичні рекомендації щодо підвищення обізнаності персоналу.

БИШУК Ігор 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 конференції.

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

Керівник кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бишук І.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Бишука Ігоря
на тему “Оцінювання впливу людського фактору на ефективність системи управління інформаційною безпекою”

Актуальність. Одним із ключових чинників, що впливають на рівень захищеності інформаційних ресурсів, є людський фактор. Незважаючи на постійне вдосконалення технічних і програмних засобів захисту інформації, значна кількість інцидентів інформаційної безпеки виникає саме через помилки працівників, недостатній рівень обізнаності, нехтування правилами безпеки або навмисні дії персоналу. Людський фактор є однією з найбільш складних та непередбачуваних складових системи управління інформаційною безпекою, оскільки безпосередньо впливає на ефективність реалізації політик безпеки, процесів контролю та управління ризиками.

У зв’язку з цим особливої актуальності набуває питання оцінювання впливу людського фактору на ефективність системи управління інформаційною безпекою та розроблення заходів щодо мінімізації пов’язаних із ним ризиків.

Позитивні сторони.

1. У роботі досліджено теоретичні основи систем управління інформаційною безпекою та визначено особливості впливу людського фактору на ефективність їх функціонування.
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, сформульовано обґрунтовані висновки. Основні положення роботи представлено у вигляді таблиць і рисунків.
3. Автор опрацював значну кількість наукових джерел, зокрема сучасні зарубіжні публікації та матеріали з питань інформаційної безпеки, управління ризиками й впливу людського фактору.
4. За результатами дослідження запропоновано рекомендації щодо підвищення ефективності системи управління інформаційною безпекою шляхом зменшення негативного впливу людського фактору та підвищення рівня обізнаності персоналу.

Недоліки.

Доцільно було б приділити більше уваги практичному аналізу сучасних програмних засобів оцінювання ризиків та контролю людського фактору в системах управління інформаційною безпекою.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню впливу людського фактору на ефективність системи управління інформаційною безпекою. Робота складається зі вступу, трьох розділів, що містять 5 рисунків, 1 таблицю, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 75 аркушів, з яких 4 аркуши займають список використаних джерел.

Метою роботи є дослідження впливу людського фактору на ефективність системи управління інформаційною безпекою.

Об'єктом дослідження є система управління інформаційною безпекою підприємства.

Предмет дослідження – вплив людського фактору на ефективність функціонування системи управління інформаційною безпекою.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, оцінювання ризиків, експертної оцінки, а також системний підхід до управління інформаційною безпекою.

Як результат у роботі досліджено основи управління інформаційною безпекою; проаналізовано вплив людського фактору на ефективність системи управління інформаційної безпеки; вивчено методи оцінювання та мінімізації впливу людського фактору, розроблено рекомендації щодо підвищення обізнаності персоналу.

Галузь застосування. Отримані результати можуть бути використані при вдосконаленні системи управління інформаційною безпекою підприємства з урахуванням впливу людського фактору та підвищення її ефективності.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЛЮДСЬКИЙ ФАКТОР, ЕФЕКТИВНІСТЬ СИСТЕМИ БЕЗПЕКИ, ОЦІНЮВАННЯ РИЗИКІВ, ПОВЕДІНКА ПЕРСОНАЛУ.

ABSTRACT

The qualification work is devoted to the study of the impact of the human factor on the effectiveness of the information security management system. The work consists of an introduction, three chapters containing 5 figures, 1 table, conclusions and the list of references containing 40 items. The total volume of the work is 75 pages, of which 4 pages is occupied by the list of references.

The purpose of the study is to investigate the impact of the human factor on the effectiveness of the information security management system.

The object the study is the information security management system of the enterprise.

The subject of the study is the impact of the human factor on the effectiveness of the functioning of the information security management system.

Research methods. In order to solve the above-mentioned scientific task, the methods of analysis and synthesis, comparison, classification, risk assessment, expert evaluation, as well as a systematic approach to information security management were used in the work.

As a result, the study investigates the fundamentals of information security management; analyzes the impact of the human factor on the effectiveness of the information security management system; examines the methods of assessing and minimizing the influence of the human factor, and develops recommendations for increasing personnel awareness.

Field of application. The obtained results can be used in improving the information security management system of the enterprise, taking into account the influence of the human factor and increasing its effectiveness.

Keywords: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, HUMAN FACTOR, SECURITY SYSTEM EFFECTIVENESS, RISK ASSESSMENT, PERSONNEL BEHAVIOR.

ЗМІСТ

ВСТУП

Актуальність теми. Незважаючи на активний розвиток технічних засобів захисту, значна частина інцидентів інформаційної безпеки пов’язана саме з людським фактором, зокрема помилками персоналу, недостатнім рівнем обізнаності або навмисними діями співробітників. Людський фактор залишається одним із найуразливіших елементів системи управління інформаційною безпекою, що безпосередньо впливає на її ефективність.

З огляду на це особливої актуальності набуває дослідження впливу людського фактору на ефективність системи управління інформаційною безпекою та пошук підходів до його оцінювання і мінімізації.

Мета роботи полягає у дослідженні впливу людського фактору на ефективність системи управління інформаційною безпекою.

Об’єкт дослідження – система управління інформаційною безпекою підприємства.

Предмет дослідження – вплив людського фактору на ефективність функціонування системи управління інформаційною безпекою.

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

1. Дослідити теоретичні основи управління інформаційною безпекою.
2. Проаналізувати вплив людського фактору на ефективність системи управління інформаційною безпекою.
3. Вивчити методи оцінювання та мінімізації впливу людського фактору.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, оцінювання ризиків, експертної оцінки, а також системний підхід до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування отриманих результатів дозволить підвищити ефективність системи управління інформаційною безпекою підприємства шляхом врахування впливу людського фактору, а також обґрунтовано застосовувати методи його оцінювання та

мінімізації відповідно до умов діяльності організації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Поняття та складові системи управління інформаційною безпекою

Система управління інформаційною безпекою сьогодні є невід'ємною складовою діяльності будь-якої організації, що працює з інформацією, електронними базами даних, цифровими сервісами або корпоративними мережами. Розвиток інформаційних технологій, поява хмарних платформ, дистанційної роботи та електронного документообігу значно збільшили обсяг інформаційних ресурсів, які потребують постійного захисту. У таких умовах питання інформаційної безпеки вже не обмежується лише встановленням антивірусних програм або паролів. Йдеться про створення цілісної системи управління, здатної контролювати ризики, попереджати витоки даних та забезпечувати стабільне функціонування організації [1].

Таблиця 1.1

Наукові підходи до трактування системи управління інформаційною безпекою

Науковець	Трактування системи управління інформаційною безпекою
В. Цуркан	Система управління інформаційною безпекою розглядається як сукупність взаємопов'язаних організаційних, технічних та управлінських заходів, спрямованих на захист інформаційних ресурсів підприємства
С. Гордієнко	Інформаційна безпека трактується як безперервний динамічний процес адаптації до нових кіберзагроз і ризиків
О. Ананченко	Система управління інформаційною безпекою визначається як система із чіткою організаційною структурою, у межах якої закріплюються функції та відповідальність працівників
В. Хох, Є. Мелешко	Система управління інформаційною безпекою розглядається як інструмент постійного аудиту, контролю та вдосконалення захисту інформації

Продовження таблиці 1.1

Л. Дегтярьова, М. Мірошникова	Система управління інформаційною безпекою трактується як багаторівнева система захисту, що поєднує технічні, організаційні та програмні засоби
В. Поддубний, О. Сєвєрінов	Інформаційна безпека визначається через процес постійного управління вразливостями та усунення слабких місць інформаційної системи

На думку В. Цуркана, система управління інформаційною безпекою являє собою сукупність взаємопов'язаних заходів, процедур, технічних засобів та управлінських рішень, спрямованих на забезпечення захисту інформаційних ресурсів підприємства. Дослідник підкреслює, що ефективність такої системи залежить не лише від технічного оснащення, а й від організації внутрішніх процесів, розподілу відповідальності між працівниками та здатності керівництва оперативно реагувати на загрози [2].

Поняття системи управління інформаційною безпекою трактується як комплексний механізм, у межах якого поєднуються організаційні, правові, кадрові, програмні та технічні елементи [1]. Така система функціонує безперервно й охоплює всі рівні діяльності установи – від стратегічного планування до повсякденних операцій працівників. Її головною метою є не тільки захист інформації від несанкціонованого доступу, а й підтримання цілісності, доступності та достовірності даних [3].

С. Гордієнко зазначає, що інформаційна безпека в сучасних умовах має розглядатися як динамічний процес, а не як статичний набір правил. Це пояснюється постійною зміною характеру кіберзагроз, розвитком шкідливого програмного забезпечення та появою нових способів втручання в інформаційні системи. Відповідно, система управління інформаційною безпекою повинна постійно адаптуватися до нових ризиків та оновлювати механізми захисту [4].

Однією з базових характеристик система управління інформаційною безпекою є її комплексність. Якщо організація використовує лише окремі засоби захисту без єдиного механізму координації, рівень безпеки залишається

недостатнім. Наприклад, навіть сучасне програмне забезпечення не гарантує захисту інформації у випадку, коли персонал не дотримується встановлених правил роботи з даними. Саме тому важливим елементом системи є поєднання технічних та організаційних рішень [5].

Система управління інформаційною безпекою виконує декілька важливих функцій. Передусім вона забезпечує виявлення потенційних загроз. Це можуть бути як зовнішні атаки, так і внутрішні порушення, пов’язані з помилками персоналу або навмисними діями працівників. Наступною функцією є оцінювання ризиків. Організація повинна визначати, які інформаційні ресурси є найбільш цінними та які наслідки може спричинити їх втрата чи пошкодження [6].

Система управління інформаційною безпекою виконує функцію контролю доступу до інформації. Працівники повинні отримувати доступ лише до тих даних, які необхідні їм для виконання службових обов’язків. Такий підхід дозволяє зменшити ризик внутрішніх витоків інформації та зловживань. Важливою складовою також є моніторинг подій безпеки, який дає можливість своєчасно виявляти підозрілу активність у мережі або інформаційній системі [1].

О. Ананченко наголошує, що система управління інформаційною безпекою повинна мати чітко визначену організаційну структуру. У межах цієї структури розподіляються обов’язки між керівниками, адміністраторами систем, фахівцями з кібербезпеки та іншими працівниками. Відсутність такого розподілу часто призводить до ситуацій, коли відповідальність за безпеку інформації фактично не закріплена за конкретними особами [7].

Однією з ключових складових систем управління інформаційною безпекою є політика інформаційної безпеки. Вона містить основні правила та принципи роботи з інформацією в організації. У політиці визначаються вимоги до паролів, порядок використання електронної пошти, правила доступу до внутрішніх ресурсів, процедури резервного копіювання та реагування на інциденти. Наявність чіткої політики дозволяє стандартизувати дії працівників та уникнути хаотичних рішень у критичних ситуаціях [8].

Наступною складовою системи є управління ризиками. Цей процес передбачає виявлення потенційних небезпек, аналіз їхнього впливу та визначення способів мінімізації можливих втрат. У межах управління ризиками організація оцінює вразливості інформаційної системи, рівень ймовірності атак та масштаби можливих наслідків. Важливо, що ризики можуть бути не лише технічними, а й організаційними або кадровими [9].

Особливе значення має кадровий компонент системи управління інформаційною безпекою. Практика показує, що значна частина інцидентів виникає через людський фактор. Причиною можуть бути необережність працівників, використання слабких паролів, відкриття підозрілих файлів або недотримання внутрішніх правил. Саме тому навчання персоналу є необхідною умовою ефективного функціонування системи управління інформаційною безпекою [3].

У багатьох організаціях проводяться регулярні інструктажі та тренінги з інформаційної безпеки. Працівникам пояснюють правила поводження з конфіденційними даними, методи розпізнавання фішингових повідомлень та порядок дій у разі виявлення загроз. Такий підхід дозволяє не лише зменшити кількість помилок, а й сформувати культуру безпечної роботи з інформацією [5].

Важливу роль у системі управління інформаційною безпекою відіграють технічні засоби захисту. До них належать антивірусні програми, міжмережеві екрани, системи виявлення вторгнень, засоби шифрування даних та резервного копіювання. Їхнє використання дозволяє створити багаторівневий захист інформаційної інфраструктури організації. Проте самі по собі технічні засоби не можуть гарантувати абсолютну безпеку без належного управління та контролю [10].

Однією з найважливіших характеристик системи управління інформаційною безпекою є її безперервність. Захист інформації не може бути одноразовою дією або окремим технічним заходом [1]. Будь-яка організація постійно змінюється: оновлюється програмне забезпечення, збільшується кількість користувачів, з’являються нові цифрові сервіси та канали передавання

даних. Усе це створює нові ризики, які потребують постійного контролю. Саме тому система управління інформаційною безпекою функціонує як процес, що передбачає регулярне оцінювання стану безпеки, виявлення недоліків та вдосконалення механізмів захисту [7].

В. Цуркан звертає увагу на те, що ефективність системи управління інформаційною безпекою значною мірою залежить від здатності організації аналізувати власні слабкі місця. У практичній діяльності це означає необхідність постійного тестування інформаційних систем, перевірки рівня захищеності мережі та оцінювання стійкості до зовнішніх і внутрішніх загроз. Без такого аналізу навіть добре організована система з часом втрачає свою ефективність [10].

Суттєвим елементом системи управління інформаційною безпекою є управління інцидентами інформаційної безпеки. Під інцидентом розуміють будь-яку подію, яка може призвести до порушення захисту інформації або нормального функціонування інформаційної системи [11]. Це може бути вірусна атака, спроба несанкціонованого доступу, витік конфіденційних даних, пошкодження баз даних чи блокування роботи серверів. Основне завдання системи управління полягає не лише у запобіганні таким випадкам, а й у швидкому реагуванні на них [5].

Для цього в організаціях створюються процедури реагування на інциденти. Вони визначають порядок дій працівників у разі виникнення загрози, способи локалізації проблеми та механізми відновлення роботи системи. Наявність чітких алгоритмів дозволяє мінімізувати негативні наслідки та скоротити час простою інформаційної інфраструктури. Особливо важливо це для банківських установ, медичних закладів, державних органів та підприємств критичної інфраструктури [7].

С. Гордієнко підкреслює, що сучасна система управління інформаційною безпекою повинна ґрунтуватися на принципі прогнозування загроз. Це означає, що організація має не лише реагувати на вже наявні проблеми, а й передбачати можливі ризики ще до момента їх реалізації. Такий підхід передбачає постійний

аналіз нових кіберзагроз, моніторинг діяльності зловмисників та вивчення сучасних методів атак [4].

Важливим напрямом функціонування системи управління інформаційною безпекою є забезпечення конфіденційності інформації. Конфіденційність означає, що доступ до даних мають лише уповноважені особи. Для цього використовуються різні механізми контролю доступу: системи авторизації, багатофакторна автентифікація, електронні ключі, біометричні засоби ідентифікації. Такі інструменти дозволяють знизити ризик несанкціонованого використання інформації [1].

Не менш важливим принципом є цілісність інформації. Йдеться про збереження правильності та незмінності даних під час їх обробки, передавання або зберігання. Порушення цілісності може призвести до спотворення інформації, помилкових управлінських рішень або фінансових втрат. Для захисту цілісності використовують системи резервного копіювання, контроль змін, криптографічні методи та спеціальні механізми перевірки достовірності даних [3].

Третім базовим принципом є доступність інформації. Навіть найбільш захищена система не буде ефективною, якщо працівники не можуть своєчасно отримати необхідні дані. Саме тому система управління інформаційною безпекою повинна забезпечувати стабільну роботу серверів, мережевого обладнання та інформаційних ресурсів. Для цього використовуються резервні канали зв’язку, дублювання обладнання та системи аварійного відновлення [2].

О. Ананченко наголошує, що структура системи управління інформаційною безпекою має враховувати специфіку діяльності організації. Наприклад, у фінансовому секторі основна увага приділяється захисту платіжної інформації та персональних даних клієнтів, тоді як у промисловості важливим стає захист технологічних процесів та виробничих систем. Через це не існує універсальної моделі системи управління інформаційною безпекою, яка однаково підходила б для всіх установ [5].

Окремою складовою системи управління інформаційною безпекою є нормативно-правове забезпечення. Будь-яка організація повинна діяти відповідно до законодавства у сфері захисту інформації та персональних даних. Це стосується як державних нормативних актів, так і внутрішніх документів підприємства. Правова база визначає порядок обробки інформації, відповідальність за порушення вимог безпеки та правила взаємодії між працівниками [10].

У сучасних умовах велике значення має міжнародна стандартизація у сфері інформаційної безпеки. Найбільш відомими є стандарти серії ISO/IEC 27000, які визначають загальні вимоги до побудови систем управління інформаційною безпекою. Їх використання дозволяє організаціям створити єдині правила захисту інформації, забезпечити контроль ризиків та підвищити рівень довіри з боку партнерів і клієнтів [7].

Важливу роль у функціонуванні системи управління інформаційною безпекою відіграє аудит інформаційної безпеки. Він дозволяє оцінити реальний стан захищеності інформаційної системи та виявити проблемні місця. Аудит може проводитися як внутрішніми фахівцями, так і незалежними експертами. Під час перевірки аналізуються технічні засоби захисту, дотримання внутрішніх політик, рівень підготовки персоналу та ефективність реагування на інциденти [11].

В. Хох та Є. Мелешко зазначають, що аудит є важливим інструментом удосконалення системи управління інформаційною безпекою. Його результати дозволяють виявити невідповідності між встановленими вимогами та фактичним станом безпеки. На основі отриманих даних організація може коригувати політику захисту, оновлювати програмне забезпечення або змінювати підходи до управління ризиками [9].

Складовою системи управління інформаційною безпекою також є криптографічний захист інформації. Його головне завдання полягає у забезпеченні конфіденційності даних шляхом їх шифрування. Навіть у разі перехоплення інформації сторонні особи не можуть ознайомитися зі змістом

повідомлення без спеціального ключа доступу. Криптографічні технології широко використовуються в електронному банкінгу, державних інформаційних системах та корпоративних мережах [3].

У сучасних організаціях дедалі більшого значення набуває питання захисту персональних даних. Велика кількість інформації про клієнтів, працівників та партнерів зберігається в електронному вигляді, що підвищує ризик її незаконного використання. Система управління інформаційною безпекою повинна забезпечувати контроль доступу до таких даних, їх захист від копіювання та дотримання вимог конфіденційності [5].

Відповідно, система управління інформаційною безпекою є складною багаторівневою структурою, яка охоплює організаційні, технічні, правові та кадрові елементи. Її ефективність залежить від здатності організації постійно вдосконалювати механізми захисту, аналізувати ризики та адаптуватися до змін інформаційного середовища [11].

У сучасному цифровому середовищі система управління інформаційною безпекою дедалі частіше розглядається не лише як технічний механізм захисту даних, а як важливий елемент загального управління організацією. Інформація перетворилася на один із найцінніших ресурсів підприємства, тому її втрата, пошкодження або незаконне використання можуть призвести до серйозних фінансових, правових та репутаційних наслідків. Саме через це система управління інформаційною безпекою поступово інтегрується в усі управлінські процеси організації [7].

Однією з важливих складових системи управління інформаційною безпекою є система контролю доступу. Її основне призначення полягає у визначенні того, хто саме може працювати з певною інформацією та які дії дозволено виконувати користувачу. Контроль доступу допомагає обмежити коло осіб, які мають право переглядати, змінювати або копіювати інформацію. Такий підхід значно знижує ризик внутрішніх порушень безпеки [1].

На практиці системи контролю доступу реалізуються через паролі, електронні перепустки, біометричну ідентифікацію або багатофакторну

автентифікацію. Останній метод сьогодні вважається одним із найбільш ефективних, оскільки передбачає використання кількох способів підтвердження особи одночасно. Наприклад, користувач може вводити пароль та додатково підтверджувати вхід через мобільний пристрій [5].

Важливим напрямом функціонування системи управління інформаційною безпекою є забезпечення безпеки мережевої інфраструктури. Більшість сучасних організацій використовують локальні мережі, хмарні сервіси та віддалений доступ до інформаційних ресурсів. Це створює додаткові можливості для кіберзлочинців, які намагаються проникнути в систему через мережеві вразливості. Для захисту мережі використовуються міжмережеві екрани, системи фільтрації трафіку, засоби моніторингу активності та спеціальні програми для виявлення вторгнень [10].

Л. Дегтярьова та М. Мірошникова зазначають, що структура системи захисту інформації повинна бути багаторівневою. Це означає, що захист не може обмежуватися лише одним технічним засобом. Наприклад, навіть якщо зловмисник отримає доступ до мережі, він повинен зіткнутися з додатковими бар’єрами у вигляді шифрування даних, систем авторизації та контролю дій користувачів. Багаторівневий підхід значно ускладнює реалізацію кібератак [11].

Окреме місце у структурі системи управління інформаційною безпекою займає резервне копіювання інформації. У процесі роботи організація накопичує значні обсяги даних, втрата яких може паралізувати діяльність підприємства. Причинами втрати можуть бути технічні несправності, помилки персоналу, вірусні атаки або навмисне знищення інформації. Саме тому створення резервних копій є одним із базових інструментів забезпечення безпеки [5].

Резервне копіювання передбачає збереження копій даних на окремих носіях або серверах. У разі пошкодження основної системи інформацію можна швидко відновити. Для підвищення надійності резервні копії часто зберігають у різних місцях, зокрема в хмарних середовищах. Це дозволяє мінімізувати ризик одночасної втрати як основних, так і резервних даних [11].

Важливим компонентом системи управління інформаційною безпекою є управління вразливостями. Вразливістю називають слабке місце в інформаційній системі, яке може бути використане для здійснення атаки. Причиною вразливостей можуть бути помилки програмного забезпечення, неправильне налаштування обладнання або використання застарілих технологій [3].

В. Поддубний та О. Сєвєрінов підкреслюють, що процес управління вразливостями повинен бути постійним. Організація має регулярно перевіряти інформаційні системи, встановлювати оновлення програмного забезпечення та усувати виявлені недоліки. Ігнорування навіть незначних вразливостей може призвести до масштабних інцидентів інформаційної безпеки [12].

Суттєве значення у функціонуванні системи управління інформаційною безпекою має документування процесів безпеки. Усі правила, процедури та інструкції повинні бути офіційно зафіксовані у внутрішніх документах організації. Це дозволяє забезпечити єдине розуміння вимог інформаційної безпеки серед працівників та спрощує контроль за виконанням встановлених правил [7].

Документування охоплює політику безпеки, порядок реагування на інциденти, правила користування інформаційними ресурсами, процедури резервного копіювання та інші аспекти захисту інформації. Особливу роль відіграють посадові інструкції, у яких визначаються обов’язки працівників щодо дотримання вимог безпеки [3].

Однією з важливих складових системи управління інформаційною безпекою є фізичний захист інформаційної інфраструктури. Захист інформації стосується не лише програмного забезпечення, а й приміщень, серверного обладнання, систем зберігання даних та засобів зв’язку. Для цього використовуються системи відеоспостереження, контроль доступу до приміщень, охоронна сигналізація та обмеження фізичного доступу до серверів [5].

Особливої актуальності питання фізичного захисту набуває для організацій, що працюють із критично важливою інформацією. Пошкодження

серверного обладнання або несанкціоноване проникнення до технічних приміщень можуть призвести до втрати інформації та зупинки діяльності підприємства. Саме тому фізична безпека розглядається як невід'ємна частина загальної системи управління інформаційною безпекою [11].

Сучасні умови розвитку інформаційних технологій значно підвищують роль хмарних сервісів у діяльності організацій. Використання хмарних платформ дозволяє зменшити витрати на технічну інфраструктуру та забезпечити швидкий доступ до даних. Водночас це створює нові ризики, пов'язані зі зберіганням інформації на віддалених серверах [1].

У зв'язку з цим система управління інформаційною безпекою повинна враховувати специфіку захисту даних у хмарному середовищі. Організації повинні контролювати рівень захищеності хмарних сервісів, використовувати шифрування даних та обмежувати доступ до конфіденційної інформації. Важливим також є перевірка надійності постачальників хмарних послуг [7].

Ще однією складовою системи управління інформаційною безпекою є безперервний моніторинг стану інформаційної безпеки. Його головна мета полягає у своєчасному виявленні підозрілої активності та попередженні можливих інцидентів. Для цього використовуються спеціальні системи моніторингу, які аналізують події в мережі, фіксують спроби несанкціонованого доступу та повідомляють про потенційні загрози [13].

Ефективність моніторингу залежить від швидкості реагування на виявлені порушення. Якщо організація не здатна оперативно усунути проблему, навіть сучасні системи контролю втрачають свою практичну цінність. Саме тому важливою умовою функціонування системи управління інформаційною безпекою є взаємодія між технічними фахівцями, керівництвом та працівниками організації.

Таким чином, система управління інформаційною безпекою є складним багатокомпонентним механізмом, що поєднує організаційні рішення, технічні засоби, кадрову політику та правове регулювання. Її головне завдання полягає у створенні умов для стабільного та безпечного функціонування інформаційного

середовища організації в умовах постійного розвитку цифрових технологій і зростання кількості кіберзагроз.

1.2 Роль людського фактору в забезпеченні інформаційної безпеки.

Інформаційна безпека зазвичай асоціюється з технічними засобами захисту – програмами, шифруванням, мережевими екранами або складними алгоритмами контролю доступу. Однак на практиці найслабшим і водночас найважливішим елементом усієї системи залишається людина. Саме дії користувачів, адміністраторів, працівників організацій і керівників визначають, наскільки ефективно працюють навіть найдосконаліші технології захисту [1].

Людський фактор в інформаційній безпеці охоплює поведінку, навички, рівень обізнаності та дисципліну всіх осіб, які взаємодіють з інформаційними системами. Йдеться не лише про спеціалістів з кібербезпеки, а про кожного працівника, який має доступ до комп’ютера, електронної пошти чи внутрішніх документів. Будь-яка помилка, необережність або нехтування правилами може створити умови для витоку даних або порушення роботи системи.

Однією з найпоширеніших проблем є людські помилки. Вони можуть бути як випадковими, так і пов’язаними з недостатнім рівнем підготовки. Наприклад, працівник може відкрити шкідливий файл, перейшовши за підозрілим посиланням, або використати слабкий пароль, який легко підібрати. У таких випадках технічні засоби захисту часто виявляються безсилими, оскільки атака відбувається через довіру або неуважність користувача [11].

Рис. 1.1 Людський фактор в забезпеченні інформаційної безпеки

Окрему категорію ризиків становить соціальна інженерія. Це метод впливу на людину з метою отримання конфіденційної інформації або доступу до системи. Зловмисники можуть видавати себе за колег, представників технічної підтримки або керівництва, щоб змусити користувача добровільно надати пароль чи інші дані. У таких ситуаціях саме психологічні фактори відіграють ключову роль, а не технічні вразливості.

Важливо розуміти, що людина в системі інформаційної безпеки є не лише джерелом ризиків, але й основним елементом захисту. Саме користувачі першими можуть виявити підозрілу активність, нестандартну поведінку системи або спроби несанкціонованого доступу. Тому рівень їхньої підготовки безпосередньо впливає на швидкість реагування на потенційні загрози [14].

Ще одним аспектом людського фактора є організаційна культура безпеки. Якщо в установі не сформовано чітких правил роботи з інформацією або працівники не сприймають їх серйозно, навіть найкращі технічні рішення втрачають ефективність. У таких умовах безпека стає формальною вимогою, а не реальним процесом. Навпаки, у середовищі, де працівники розуміють

важливість захисту даних, ризики значно зменшуються.

Суттєвий вплив має також рівень навчання персоналу. Багато інцидентів виникає через те, що працівники не знають базових правил інформаційної безпеки або не вміють розпізнавати загрози. Регулярні інструктажі, тренінги та практичні навчання дозволяють сформувати стійкі навички безпечної роботи з інформацією. Особливо це важливо в умовах постійної появи нових видів атак і технологій зловмисників [11].

Окремо слід виділити проблему надмірних прав доступу. У багатьох організаціях працівникам надається більше можливостей, ніж їм реально потрібно для виконання своїх обов'язків. Це створює додаткові ризики, оскільки у випадку помилки або зловмисних дій шкода може бути значно більшою. Саме тому принцип мінімально необхідних привілеїв є одним із базових у побудові безпечних інформаційних систем.

Людський фактор також проявляється у поведінці керівництва. Якщо управлінці не приділяють достатньої уваги питанням безпеки, не виділяють ресурси на навчання персоналу або оновлення систем захисту, рівень захищеності організації поступово знижується. Навпаки, стратегічний підхід керівництва дозволяє сформувати цілісну систему управління ризиками.

У сучасних умовах інформаційна безпека вже не може розглядатися як суто технічна сфера. Вона поступово перетворюється на міждисциплінарну область, де поєднуються технології, психологія, організаційне управління та поведінкові науки. Людина стає центральною ланкою цієї системи, оскільки саме через її дії реалізується більшість як загроз, так і механізмів захисту [15].

Однією з ключових причин порушень інформаційної безпеки залишаються помилки персоналу. Вони виникають не як виняток, а як закономірний результат взаємодії людини з технологічно складними системами. Навіть добре налаштована інфраструктура не гарантує захисту, якщо користувачі неправильно виконують базові дії або ігнорують встановлені правила.

Помилки працівників умовно можна поділити на кілька груп. Перша – це неуважність у повсякденній роботі. Сюди належать ситуації, коли користувач

випадково надсилає конфіденційний файл не тому адресату, зберігає дані у відкритому доступі або використовує незахищені носії інформації. Такі дії часто не мають злого наміру, але їхні наслідки можуть бути серйозними, особливо якщо йдеться про фінансові або персональні дані.

Друга група помилок пов’язана з недостатнім рівнем знань. Працівник може не розуміти принципів роботи систем безпеки або не усвідомлювати ризиків, які виникають під час використання певних інструментів. Наприклад, встановлення стороннього програмного забезпечення без перевірки його безпечності може відкрити доступ до системи для шкідливих програм. У таких випадках проблема полягає не в техніці, а в недостатній підготовці користувача.

Третя група – це свідоме порушення правил. Хоча такі випадки трапляються рідше, вони є найбільш небезпечними. Працівник може навмисно передати інформацію конкурентам, використати службовий доступ у власних інтересах або обійти встановлені обмеження. Подібні дії складніше виявити, оскільки вони часто маскуються під звичайну робочу активність [16].

Окрему роль у структурі загроз відіграє соціальна інженерія. Це метод впливу на людину, при якому основна мета полягає не у зламі технічних систем, а у маніпулюванні поведінкою користувача. Зловмисники використовують психологічні прийоми, такі як створення відчуття терміновості, авторитетності або довіри.

Найпоширенішим прикладом є фішингові повідомлення. Працівник отримує електронного листа, який зовні виглядає як офіційне повідомлення від банку, керівництва або сервісної служби. У тексті міститься прохання перейти за посиланням і підтвердити дані або змінити пароль. У результаті користувач самостійно передає свої облікові дані зловмисникам, не підозрюючи про загрозу.

Ще один поширений сценарій соціальної інженерії – телефонні дзвінки від осіб, які представляються співробітниками технічної підтримки. Вони можуть просити надати пароль, встановити певну програму або виконати дії, що нібито необхідні для «усунення проблеми». Насправді ці дії відкривають доступ до системи стороннім особам [17].

Соціальна інженерія особливо небезпечна тим, що вона експлуатує не технічні вразливості, а природні особливості людської поведінки – довіру, бажання допомогти, страх зробити помилку або підпорядкування авторитету. Саме тому навіть досвідчені користувачі можуть стати жертвами таких атак. У відповідь на ці загрози організації формують комплекс організаційних механізмів захисту. Їхня мета полягає у зменшенні впливу людського фактора та створенні умов, за яких імовірність помилки або зловмисних дій мінімізується.

Одним із базових механізмів є регламентування доступу до інформації. Працівники отримують лише ті права, які необхідні для виконання їхніх обов'язків. Такий підхід дозволяє обмежити можливі наслідки помилок або навмисних дій. Наприклад, якщо співробітник бухгалтерії не має доступу до технічних серверів, він не зможе випадково або навмисно вплинути на їхню роботу.

Важливим елементом організаційного захисту є розподіл відповідальності. У межах організації чітко визначається, хто відповідає за інформаційну безпеку, хто контролює виконання правил і хто реагує на інциденти. Відсутність такого розподілу часто призводить до ситуацій, коли порушення залишаються без належної реакції [7].

Ще одним інструментом є регулярне навчання персоналу. Воно спрямоване на формування стійких навичок безпечної роботи з інформацією. Працівникам пояснюють, як розпізнавати підозрілі повідомлення, як поводитися з конфіденційними даними та як діяти у разі виявлення загроз. Важливо, що навчання має бути не одноразовим, а систематичним, оскільки методи атак постійно змінюються.

Окрему роль відіграють внутрішні політики безпеки. Вони визначають правила використання інформаційних ресурсів, порядок доступу до систем, вимоги до паролів та процедури роботи з даними. Такі документи створюють єдині стандарти поведінки для всіх працівників і зменшують простір для довільних рішень [11].

Контроль за дотриманням правил також є важливою складовою організаційного захисту. У багатьох системах використовуються журнали подій, які фіксують усі дії користувачів. Це дозволяє не лише виявляти порушення, а й аналізувати причини їх виникнення. У разі необхідності керівництво може швидко реагувати на інциденти та запобігати їх повторенню.

Відповідно, помилки персоналу та соціальна інженерія є одними з найскладніших викликів у сфері інформаційної безпеки. Вони не завжди піддаються технічному контролю, оскільки пов’язані з поведінкою людини. Саме тому ефективна система захисту повинна поєднувати технічні рішення з організаційними механізмами та постійним навчанням працівників.

У сучасних умовах інформаційної безпеки дедалі більше залежить від того, наскільки організація здатна керувати поведінкою людей, а не лише технічними засобами захисту. Навіть найскладніші системи моніторингу та шифрування не дають очікуваного ефекту, якщо внутрішні процеси побудовані хаотично або працівники не розуміють своєї ролі в загальній системі безпеки [18].

Одним із ключових напрямів зменшення впливу людського фактора є формування стійкої культури безпеки. Йдеться про сукупність норм, звичок і внутрішніх установок, які визначають ставлення працівників до інформаційних ризиків. Якщо в організації безпека сприймається як формальність, правила виконуються вибірково, а контроль ігнорується. Натомість у середовищі з розвиненою культурою безпеки працівники автоматично дотримуються встановлених вимог і критично ставляться до будь-яких підозрілих ситуацій.

Важливим елементом цієї культури є усвідомлення цінності інформації. Працівник має розуміти, що навіть на перший погляд незначні дані можуть мати комерційну або стратегічну важливість. Наприклад, внутрішні службові листи, списки клієнтів або технічна документація можуть бути використані зловмисниками для підготовки атак або конкурентного аналізу [1].

Суттєву роль у зниженні ризиків відіграє система мотивації персоналу. У багатьох випадках працівники не дотримуються правил не через незнання, а через відсутність стимулів. Якщо організація не заохочує відповідальну

поведінку, працівники сприймають вимоги безпеки як додаткове навантаження. Натомість впровадження системи заохочень за дотримання правил або своєчасне повідомлення про інциденти підвищує загальний рівень дисципліни.

Не менш важливим є питання контролю за поведінкою користувачів у цифровому середовищі. Сучасні інформаційні системи дозволяють відстежувати дії працівників: входи в систему, копіювання файлів, відправлення даних або підключення зовнішніх пристроїв. Такий моніторинг не має на меті тотальний контроль, а спрямований на виявлення аномальної поведінки, яка може свідчити про загрозу [19].

Однак ефективність контролю залежить від правильного балансу між безпекою та приватністю. Надмірне спостереження може викликати недовіру серед працівників і знижувати їхню мотивацію. Тому організації повинні чітко пояснювати мету збору даних і забезпечувати прозорість процедур контролю.

Важливим організаційним механізмом є план реагування на інциденти. Він визначає, як саме працівники повинні діяти у випадку виявлення загрози. Чітко прописані алгоритми дозволяють уникнути паніки та неправильних рішень у критичних ситуаціях. Наприклад, у разі виявлення підозрілої активності користувач має знати, до кого звернутися і які дії виконати першочергово.

Окрему увагу слід приділяти сегментації обов’язків. Розподіл функцій між працівниками дозволяє уникнути концентрації надмірних повноважень в одних руках. Це зменшує ризик як помилок, так і навмисних зловживань. Наприклад, особа, яка створює доступи до системи, не повинна одночасно мати повний контроль над їх використанням [20].

У практиці інформаційної безпеки також застосовується принцип «перевірки подвійного контролю». Він передбачає, що критично важливі операції повинні підтверджуватися щонайменше двома незалежними особами. Це особливо актуально для фінансових операцій, зміни системних налаштувань або доступу до конфіденційних баз даних.

Ще одним важливим аспектом є адаптація організації до змін зовнішнього середовища. Кіберзагрози постійно еволюціонують, тому правила безпеки не

можуть залишатися незмінними. Організація повинна регулярно переглядати свої політики, оновлювати інструкції та враховувати нові типи атак. У цьому процесі людський фактор відіграє роль не лише об’єкта захисту, а й джерела інформації про нові ризики [21].

Окремо варто зазначити роль керівництва у забезпеченні інформаційної безпеки. Саме управлінські рішення визначають, наскільки пріоритетною є ця сфера в організації. Якщо керівництво не підтримує впровадження заходів безпеки або не виділяє достатніх ресурсів, будь-які технічні рішення втрачають ефективність. Натомість стратегічний підхід дозволяє інтегрувати безпеку в усі бізнес-процеси [5].

Отже, людський фактор є одночасно найбільш вразливою і найбільш впливовою складовою інформаційної безпеки. Саме через дії людей реалізується більшість загроз, але водночас саме люди забезпечують виявлення, запобігання та реагування на інциденти. Тому ефективна система інформаційної безпеки повинна будуватися не лише на технологіях, а й на розумінні поведінки, мотивації та відповідальності персоналу.

1.3 Основні загрози інформаційній безпеці, пов’язані з людським фактором

Інформаційна безпека дедалі менше залежить лише від технічних засобів захисту і дедалі більше – від поведінки людей. Організації можуть впроваджувати складні системи шифрування, багаторівневі механізми автентифікації та автоматизований моніторинг, однак значна частина інцидентів усе одно виникає через дії або рішення працівників. Це пояснюється тим, що людина залишається найбільш непередбачуваним елементом будь-якої інформаційної системи [22].

Людський фактор у сфері інформаційної безпеки охоплює широкий спектр явищ: від випадкових помилок у роботі до свідомих порушень правил або зовнішнього психологічного впливу. На практиці саме цей фактор формує

найбільшу частку ризиків, оскільки він не завжди піддається технічному контролю і часто залежить від суб’єктивних рішень [23].

Однією з базових загроз є ненавмисні помилки користувачів. Вони виникають у процесі звичайної щоденної роботи з інформаційними системами. Працівник може випадково видалити важливий файл, надіслати конфіденційний документ неправильному адресату або зберегти дані у відкритому доступі. Подібні ситуації часто не мають злого наміру, але їхні наслідки можуть бути критичними для організації.

Причини таких помилок зазвичай пов’язані з перевантаженням інформацією, багатозадачністю або недостатнім досвідом роботи з системами. У сучасних умовах працівники змушені швидко виконувати велику кількість операцій, що підвищує ймовірність випадкових дій. Особливо це проявляється в середовищах, де відсутні чіткі інструкції або стандартизовані процедури [24].

Неправильне використання облікових даних є ще однією суттєвою проблемою. Люди часто використовують прості паролі, повторюють їх на різних сервісах або записують у небезпечних місцях. Це створює можливість для несанкціонованого доступу до інформаційних систем. У багатьох випадках саме слабка дисципліна користувачів стає причиною компрометації корпоративних акаунтів [22].

Рис. 1.2 Основні загрози інформаційній безпеці, пов’язані з людським фактором

Окрему категорію становлять помилки, пов’язані з встановленням або використанням програмного забезпечення. Працівники можуть завантажувати сторонні програми без перевірки їх безпечності або ігнорувати оновлення системи. У результаті це створює додаткові вразливості, які можуть бути використані для проникнення в інформаційну інфраструктуру [25].

Важливою особливістю людського фактора є те, що помилки часто накопичуються. Одна незначна дія може не мати серйозних наслідків, але у поєднанні з іншими недоліками створює умови для масштабного інциденту. Наприклад, поєднання слабкого пароля, відсутності оновлень і необережного відкриття електронного листа може призвести до повного компрометування системи [5].

Наступною великою групою загроз є навмисні дії користувачів, які мають доступ до внутрішніх ресурсів організації. Такі загрози часто називають внутрішніми, оскільки вони походять зсередини системи. На відміну від зовнішніх атак, їх складніше виявити, оскільки дії працівника можуть виглядати

як звичайна робоча активність [23].

Причини таких дій можуть бути різними: особиста вигода, конфлікти в колективі, незадоволення умовами праці або зовнішній тиск. У деяких випадках працівники свідомо передають конфіденційну інформацію конкурентам або використовують службові дані у власних інтересах. Подібні інциденти є особливо небезпечними, оскільки людина вже має легальний доступ до системи [24].

Окремо варто виділити ситуації, коли співробітники обходять встановлені правила безпеки для спрощення своєї роботи. Наприклад, вони можуть вимикати антивірусні програми, використовувати несанкціоновані пристрої або передавати паролі колегам. Хоча такі дії часто не мають злого наміру, вони суттєво підвищують ризик порушення безпеки [25].

Ще однією важливою загрозою є недостатній рівень обізнаності працівників. Багато користувачів не усвідомлюють, наскільки складними можуть бути сучасні атаки. Вони можуть не розпізнавати підроблені повідомлення, не звертати увагу на ознаки фішингу або не розуміти наслідків своїх дій. У результаті навіть проста взаємодія з електронною поштою може стати джерелом серйозної загрози.

Усе це свідчить про те, що людський фактор є не лише допоміжним елементом у системі інформаційної безпеки, а й основним джерелом ризиків. Його особливість полягає у непередбачуваності та залежності від великої кількості психологічних, організаційних і соціальних чинників [23].

Однією з найнебезпечніших форм впливу на інформаційну безпеку є соціальна інженерія. Її особливість полягає в тому, що атака спрямована не на технічні системи, а на людину як найбільш вразливу ланку. У таких випадках зловмисники не намагаються зламати захист напряму, а створюють ситуації, у яких користувач самостійно передає необхідну інформацію або виконує потрібні дії [5].

Соціальна інженерія може набувати різних форм. Найпоширенішою є підробка електронних повідомлень, які виглядають як офіційні листи від банків,

державних установ або внутрішніх служб організації. У тексті зазвичай міститься термінове прохання підтвердити дані, змінити пароль або перейти за посиланням. Людина, яка не має достатнього рівня обізнаності, часто виконує ці дії автоматично, не перевіряючи джерело повідомлення.

Ще одним поширеним варіантом є телефонні дзвінки, під час яких зловмисники представляються співробітниками технічної підтримки або адміністраторами системи. Вони можуть переконувати користувача встановити певне програмне забезпечення або надати доступ до комп'ютера. Основний механізм впливу тут базується на авторитеті та довірі до нібито офіційної особи [24].

Окрему роль відіграють психологічні прийоми тиску. У багатьох випадках створюється відчуття терміновості або загрози, наприклад повідомлення про блокування облікового запису чи можливі фінансові втрати. У такому стані користувач приймає рішення швидко і не завжди раціонально, що підвищує ефективність атаки.

Соціальна інженерія є особливо небезпечною через те, що вона не потребує складних технічних засобів. Достатньо базових знань про поведінку людей, щоб створити сценарій, у якому користувач добровільно порушує правила безпеки. Саме тому цей тип загроз вважається одним із найскладніших для протидії [23].

Ще однією важливою категорією ризиків є внутрішні загрози, пов'язані з діями співробітників організації. На відміну від зовнішніх атак, вони виникають всередині системи і часто залишаються непоміченими тривалий час. Людина, яка має легальний доступ до ресурсів, може виконувати дії, що формально не виглядають підозрілими, але фактично завдають шкоди безпеці.

Внутрішні загрози можуть мати як свідомий, так і несвідомий характер. У першому випадку працівник навмисно використовує свої повноваження для отримання вигоди або нанесення шкоди організації. Це може бути передача конфіденційної інформації третім особам, копіювання баз даних або зміна службових даних. У другому випадку шкода виникає через необережність або порушення процедур [5].

Особливу складність становить те, що внутрішні загрози важко виявити за допомогою стандартних засобів контролю. Дії співробітника часто виглядають як звичайна робота, тому автоматичні системи моніторингу не завжди можуть визначити аномалії. Це створює потребу в додаткових організаційних механізмах контролю [23].

До внутрішніх загроз також належать конфліктні ситуації в колективі. У разі напружених відносин між працівниками може з'являтися мотив до навмисного порушення правил безпеки. Це може проявлятися у саботажі, приховуванні інформації або навмисному створенні проблем у роботі системи.

Окремо слід розглянути проблему недостатнього контролю за доступом до інформації. У багатьох організаціях співробітники мають ширші права, ніж це необхідно для виконання їхніх обов'язків. Така ситуація збільшує ризик як навмисних, так і випадкових порушень. Чим більше доступів має користувач, тим більший потенційний вплив його дій на систему [22].

Важливою причиною внутрішніх загроз є також відсутність чіткої системи відповідальності. Якщо працівники не розуміють меж своїх повноважень або не усвідомлюють наслідків своїх дій, це призводить до хаотичного використання інформаційних ресурсів. У таких умовах навіть незначні порушення можуть накопичуватися і перетворюватися на серйозні інциденти.

Ще одним суттєвим фактором є психологічний стан працівників. Втома, стрес, перевантаження або професійне вигорання знижують концентрацію уваги і підвищують ймовірність помилок. У такому стані людина частіше ігнорує попередження системи або діє автоматично, не аналізуючи наслідки своїх рішень [17].

Таким чином, людський фактор у сфері інформаційної безпеки охоплює не лише окремі помилки, а цілу систему поведінкових, психологічних та організаційних явищ. Соціальна інженерія, внутрішні загрози та недостатній рівень контролю формують складний комплекс ризиків, який не може бути усунутий лише технічними засобами. Для його зменшення необхідне поєднання організаційних правил, навчання персоналу та постійного моніторингу

поведінки користувачів.

У реальних умовах функціонування організацій значна частина інцидентів інформаційної безпеки виникає не через складні зовнішні атаки, а через повсякденні дії користувачів, які здаються незначними. Саме накопичення дрібних порушень створює середовище, у якому інформаційна система стає вразливою. Це особливо помітно в організаціях, де відсутня усталена дисципліна роботи з даними або контроль за виконанням базових правил [24].

Однією з поширених проблем є використання слабких або повторюваних паролів. Користувачі часто обирають прості комбінації, які легко запам’ятати, або застосовують один і той самий пароль для різних сервісів. Такий підхід суттєво підвищує ризик несанкціонованого доступу, оскільки компрометація одного облікового запису може призвести до доступу до інших систем. У багатьох випадках саме ця поведінкова звичка стає початковою точкою більш серйозних інцидентів.

Ще однією загрозою є нехтування оновленням програмного забезпечення. Працівники або технічні користувачі можуть відкладати встановлення оновлень через незручність або побоювання порушити робочий процес. Однак саме оновлення часто містять виправлення критичних вразливостей, які можуть бути використані для атак. Ігнорування таких оновлень створює приховані ризики, що накопичуються з часом.

Важливу роль відіграє також використання сторонніх пристроїв і носіїв інформації. Підключення невідомих флеш-накопичувачів, зовнішніх дисків або особистих пристроїв до корпоративної мережі може призвести до проникнення шкідливого програмного забезпечення. У багатьох випадках саме такі дії стають каналом для зараження внутрішніх систем, оскільки користувачі не завжди усвідомлюють ризики фізичного носія [6].

Окрему групу становлять загрози, пов’язані з неправильним поводженням з електронною поштою. Працівники можуть відкривати вкладення з невідомих джерел, переходити за підозрілими посиланнями або не перевіряти адресата повідомлення. У результаті зловмисники отримують можливість впровадження

шкідливого коду або збору конфіденційної інформації. Електронна пошта залишається одним із найпоширеніших каналів атак саме через людську неуважність.

Також значний ризик становить неконтрольоване використання хмарних сервісів і зовнішніх платформ для зберігання даних. Працівники можуть завантажувати службові файли на особисті акаунти для зручності доступу, не замислюючись про наслідки. У таких випадках організація втрачає контроль над інформацією, а дані можуть бути доступні стороннім особам або залишатися без належного захисту.

Проблемою є і недостатнє розуміння принципів конфіденційності. У деяких випадках працівники передають інформацію колегам без необхідності або обговорюють службові дані у відкритих каналах комунікації. Такі дії створюють додаткові канали витоку інформації, які важко контролювати технічними засобами [23].

Ще одним важливим аспектом є вплив організаційного середовища на поведінку працівників. Якщо в компанії відсутні чіткі правила або вони не виконуються на практиці, формується відчуття допустимості порушень. У таких умовах навіть базові вимоги безпеки сприймаються як формальність, що суттєво знижує загальний рівень захищеності системи [23].

Окремо слід звернути увагу на проблему перевантаження працівників інформацією та завданнями. Коли людина працює в умовах постійного стресу або дефіциту часу, її здатність до критичного аналізу знижується. Це призводить до автоматичних дій без перевірки деталей, що підвищує ймовірність помилок і порушень.

Важливою складовою людського фактора є також недостатній рівень взаємодії між підрозділами, відповідальними за інформаційну безпеку. Якщо комунікація між технічними спеціалістами, керівництвом і кінцевими користувачами є слабкою, інформація про загрози не доходить вчасно або сприймається неправильно. Це уповільнює реагування на інциденти і знижує ефективність захисних заходів.

Ще одним суттєвим ризиком є відсутність регулярної перевірки дотримання політик безпеки. Навіть добре розроблені правила не мають практичного значення, якщо їх не контролюють. У багатьох організаціях працівники поступово відходять від встановлених процедур, якщо не бачать системного нагляду або наслідків за порушення [26].

Отже, основні загрози, пов’язані з людським фактором, формуються не лише через окремі помилки чи зовнішні атаки, а через комплекс повсякденних дій, звичок і організаційних недоліків. Сукупність цих чинників створює середовище, у якому інформаційна безпека стає нестабільною і залежною від поведінки кожного користувача. Саме тому ефективний захист вимагає не тільки технічних рішень, а й постійної роботи з людьми, їх навчання та формування відповідальної поведінки.

Висновки до розділу 1

У межах розглянутого розділу встановлено, що система управління інформаційною безпекою є складною багаторівневою структурою, яка поєднує організаційні, технічні, правові та кадрові складові. Її функціонування не обмежується використанням окремих засобів захисту, а передбачає комплексну взаємодію всіх елементів інформаційного середовища організації.

З’ясовано, що ключовою метою системи управління інформаційною безпекою є забезпечення конфіденційності, цілісності та доступності інформації, а також мінімізація ризиків, пов’язаних із її обробкою та зберіганням. Досягнення цієї мети можливе лише за умови системного підходу до управління ризиками та постійного вдосконалення механізмів захисту.

Встановлено, що важливим компонентом системи управління інформаційною безпекою є політика інформаційної безпеки, яка визначає основні правила роботи з даними, розподіл відповідальності та порядок реагування на інциденти. Саме вона формує базові стандарти поведінки працівників у цифровому середовищі.

Окрему увагу приділено ролі технічних засобів захисту, таких як системи контролю доступу, шифрування, резервного копіювання та моніторингу. Водночас підкреслено, що технічні рішення не є достатніми без належної організації процесів і підготовки персоналу.

Важливим елементом системи управління інформаційною безпекою є управління ризиками, яке передбачає виявлення загроз, оцінювання їхнього впливу та розробку заходів щодо їх мінімізації. Ефективність цього процесу безпосередньо впливає на загальний рівень захищеності інформаційної системи.

Також встановлено, що людський фактор є одним із ключових елементів системи безпеки. Він одночасно виступає як джерело потенційних загроз, так і як основний ресурс для їх запобігання. Рівень підготовки, обізнаності та дисципліни персоналу значною мірою визначає ефективність усієї системи.

Розділ 2 АНАЛІЗ ВПЛИВУ ЛЮДСЬКОГО ФАКТОРУ НА ЕФЕКТИВНІСТЬ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Методи оцінювання ефективності систем управління інформаційною безпекою

Система управління інформаційною безпекою не може вважатися ефективною лише через наявність технічних засобів захисту або внутрішніх правил роботи з інформацією. Для визначення реального рівня її результативності необхідно постійно проводити оцінювання функціонування всіх елементів системи. Такий процес дозволяє виявити слабкі місця, визначити рівень захищеності інформаційних ресурсів та встановити, наскільки впроваджені заходи відповідають сучасним загрозам [26].

Оцінювання ефективності системи управління інформаційною безпекою є важливою складовою управління безпекою, оскільки інформаційне середовище постійно змінюється. З’являються нові типи атак, удосконалюються методи несанкціонованого доступу, збільшується кількість цифрових сервісів та обсягів даних. У таких умовах навіть система, яка раніше демонструвала високий рівень захисту, може втратити свою надійність. Саме тому оцінювання повинно здійснюватися регулярно, а не лише після виникнення інцидентів.

У практичній діяльності ефективність системи інформаційної безпеки визначають через здатність забезпечувати стабільний захист інформації без порушення роботи організації. Це означає, що система повинна одночасно протидіяти загрозам, підтримувати безперервність роботи інформаційних ресурсів і забезпечувати контроль над доступом до даних [27].

Одним із базових способів оцінювання є аналіз стану захищеності інформаційних ресурсів. У межах цього підходу перевіряється, наскільки ефективно система запобігає витоку, втраті або зміні інформації. Особлива увага приділяється рівню захисту конфіденційних даних, надійності механізмів

автентифікації та стабільності функціонування інформаційної інфраструктури.

Рис. 2.1 Методи оцінювання ефективності систем управління інформаційною безпекою

Для визначення результативності системи часто використовують метод оцінювання за окремими показниками. Такий підхід передбачає аналіз конкретних характеристик безпеки, які дозволяють оцінити стан системи в різних напрямах. Наприклад, можуть враховуватися кількість інцидентів за певний період, швидкість реагування на загрози, час відновлення після збоїв або рівень доступності інформаційних ресурсів.

Важливе місце займає оцінювання рівня ризиків. Його основна мета полягає у визначенні того, наскільки ймовірними є певні загрози та яких наслідків вони можуть завдати організації. У процесі такого аналізу враховуються технічні вразливості, особливості внутрішніх процесів та можливі дії порушників [24].

Ризик-орієнтований підхід дозволяє визначити найбільш критичні напрями захисту. Наприклад, якщо певна інформаційна система містить особливо важливі дані або є ключовою для роботи організації, їй приділяється

підвищена увага під час оцінювання. Це дозволяє раціонально використовувати ресурси та зосереджувати захисні заходи на найбільш уразливих елементах [8].

Суттєвим методом оцінювання ефективності є проведення аудиту інформаційної безпеки. Його зміст полягає у комплексній перевірці всіх складових системи управління безпекою. У процесі аудиту аналізуються технічні засоби захисту, порядок управління доступом, рівень документування процедур, дотримання внутрішніх правил та готовність персоналу до реагування на інциденти [27].

Особливість аудиту полягає в тому, що він дозволяє оцінити не лише технічний стан системи, а й рівень організації процесів управління безпекою. У багатьох випадках саме організаційні недоліки стають причиною порушення захисту інформації навіть за наявності сучасного обладнання.

Для оцінювання також використовують метод аналізу інцидентів. Його суть полягає у вивченні вже наявних випадків порушення безпеки. Організація аналізує причини виникнення інцидентів, швидкість реагування на них та ефективність дій щодо усунення наслідків. Такий підхід дозволяє виявити повторювані проблеми та визначити напрями вдосконалення системи [16].

Окрему роль у процесі оцінювання відіграє перевірка стійкості інформаційної системи до зовнішніх впливів. Для цього можуть проводитися тестування на проникнення, моделювання кібератак або перевірка резервних механізмів відновлення даних. Подібні заходи дозволяють оцінити реальну готовність системи до протидії сучасним загрозам [4].

Сучасні методи оцінювання також враховують людський фактор. Значна частина порушень інформаційної безпеки виникає через помилки персоналу, недотримання правил або недостатній рівень обізнаності працівників. Тому під час оцінювання аналізується рівень підготовки користувачів, їхня здатність розпізнавати загрози та дотримуватися встановлених процедур.

У практиці управління інформаційною безпекою дедалі більшого значення набуває комплексний підхід до оцінювання. Це означає, що система аналізується одночасно з технічної, організаційної, кадрової та економічної точок зору. Лише

поєднання різних методів дозволяє отримати об’єктивне уявлення про реальний рівень ефективності системи управління інформаційною безпекою та визначити напрями її подальшого вдосконалення [4].

Оцінювання ефективності систем управління інформаційною безпекою поступово переходить від формального контролю до безперервного аналізу реального стану захищеності інформаційного середовища. Організації вже не обмежуються одноразовими перевірками або загальними оцінками, оскільки динамічний розвиток цифрових технологій потребує постійного моніторингу рівня безпеки та швидкого реагування на зміни.

Одним із важливих напрямів оцінювання є аналіз результативності захисних заходів. Його мета полягає у визначенні того, наскільки впроваджені механізми безпеки здатні виконувати свої функції у реальних умовах. Для цього організація досліджує, чи забезпечують технічні та організаційні рішення належний рівень контролю доступу, захисту даних та реагування на потенційні загрози [27].

Практичне оцінювання часто базується на системі показників ефективності. До таких показників можуть належати кількість зафіксованих інцидентів, тривалість простоїв інформаційних систем, швидкість усунення наслідків атак, частота порушень політик безпеки або кількість успішно заблокованих спроб несанкціонованого доступу. Аналіз подібних даних дозволяє визначити реальний рівень стабільності системи [16].

Важливе значення має також оцінювання здатності системи адаптуватися до нових загроз. Інформаційна безпека не є статичним процесом, оскільки методи кібератак постійно вдосконалюються. Через це система управління безпекою повинна своєчасно реагувати на появу нових ризиків, оновлювати механізми захисту та змінювати внутрішні процедури відповідно до сучасних умов.

Для визначення рівня адаптивності організації аналізують швидкість оновлення програмного забезпечення, ефективність реагування на нові типи атак та здатність персоналу працювати в умовах змін. Якщо система не може

оперативно пристосовуватися до нових викликів, її загальна ефективність поступово знижується [23].

Окремим напрямом є оцінювання рівня надійності інформаційної інфраструктури. У межах такого аналізу перевіряється стійкість серверів, мережевого обладнання, систем резервного копіювання та каналів передачі даних. Важливим показником є здатність системи продовжувати роботу навіть у разі виникнення технічних збоїв або зовнішніх атак.

Під час оцінювання надійності враховується не лише кількість технічних несправностей, а й швидкість відновлення роботи системи. Чим менше часу потрібно для повернення до нормального функціонування після інциденту, тим вищим вважається рівень ефективності системи управління інформаційною безпекою [27].

Суттєве місце у процесі оцінювання займає перевірка внутрішніх процедур управління. Організація аналізує, наскільки чітко визначені правила роботи з інформацією, чи існує розподіл відповідальності між працівниками та чи дотримуються встановлені політики безпеки на практиці.

У багатьох випадках саме організаційні недоліки стають причиною порушення захисту інформації. Відсутність чітких інструкцій, несвоєчасне оновлення документації або недостатній контроль за виконанням процедур можуть суттєво знизити ефективність навіть технічно добре захищеної системи [8].

Важливим методом оцінювання є тестування системи безпеки в умовах, наближених до реальних загроз. Для цього можуть проводитися контрольовані перевірки захищеності, моделювання атак або аналіз стійкості до перевантажень. Подібні заходи дозволяють визначити, як система поводиться в критичних ситуаціях і чи здатна вона протидіяти сучасним методам атак [13].

Окрему увагу приділяють оцінюванню роботи персоналу. Людський фактор залишається однією з головних причин порушення інформаційної безпеки, тому рівень підготовки працівників безпосередньо впливає на загальну ефективність системи управління інформаційною безпекою. У процесі

оцінювання перевіряється, чи знають працівники правила безпечної роботи з інформацією, чи можуть вони розпізнавати фішингові повідомлення та як реагують на підозрілі ситуації.

Для цього застосовуються різні методи: тестування знань, практичні тренування, моделювання кібератак та аналіз поведінки користувачів у системі. Такі перевірки дозволяють не лише визначити рівень підготовки персоналу, а й виявити напрями, які потребують додаткового навчання.

Сучасні методи оцінювання також враховують економічний аспект функціонування системи управління інформаційною безпекою. Організація повинна оцінювати, наскільки витрати на захист інформації відповідають отриманому результату. Надмірні витрати на безпеку можуть бути економічно необґрунтованими, тоді як недостатнє фінансування підвищує ризик виникнення інцидентів [6].

У межах економічного аналізу враховуються витрати на технічні засоби захисту, навчання персоналу, аудит системи, оновлення програмного забезпечення та ліквідацію наслідків інцидентів. Отримані результати дозволяють визначити ефективність використання ресурсів у сфері інформаційної безпеки [18].

Отже, сучасні методи оцінювання ефективності систем управління інформаційною безпекою охоплюють широкий спектр напрямів – від технічного стану систем до рівня організації процесів і підготовки персоналу. Їх застосування дозволяє не лише визначити поточний рівень захищеності інформаційного середовища, а й забезпечити постійне вдосконалення всієї системи управління безпекою.

2.2 Аналіз типових помилок персоналу та їх наслідків

Персонал організації є не лише користувачем інформаційних систем, а й одним із ключових елементів загальної системи безпеки. Незважаючи на постійний розвиток технічних засобів захисту, значна частина порушень

інформаційної безпеки виникає саме через помилки працівників. Це пояснюється тим, що людська поведінка є менш передбачуваною, ніж робота автоматизованих систем, а рішення користувачів часто залежать від неуважності, втоми, недостатнього рівня знань або нехтування встановленими правилами [28].

Помилки персоналу в сфері інформаційної безпеки можуть мати як випадковий, так і системний характер. В окремих випадках працівник припускається помилки одноразово через необережність, однак у багатьох організаціях подібні дії стають регулярними через відсутність належного контролю та низький рівень культури безпеки. Саме тому аналіз поведінки персоналу є важливим напрямом забезпечення захищеності інформаційного середовища [29].

Однією з найпоширеніших помилок є використання ненадійних паролів. Працівники часто створюють прості комбінації, які легко запам’ятати, або використовують однакові паролі для різних інформаційних ресурсів. Така практика суттєво спрощує несанкціонований доступ до облікових записів. У разі компрометації одного сервісу зловмисники можуть отримати доступ до інших систем, де використовується той самий пароль.

Проблемою є також зберігання паролів у небезпечних місцях. Працівники можуть записувати їх у блокнотах, текстових файлах або залишати у відкритому доступі на робочому місці. Подібні дії створюють додаткові ризики для конфіденційності інформації, особливо в організаціях із великою кількістю користувачів [30].

Ще однією типовою помилкою є відкриття підозрілих електронних листів та вкладень. Працівники нерідко не перевіряють адресу відправника або зміст повідомлення, особливо якщо лист виглядає офіційно. У результаті користувач може перейти за шкідливим посиланням або завантажити файл, який містить небезпечне програмне забезпечення.

Рис. 2.2 Типові помилки персоналу та їх наслідки

Особливо небезпечними є ситуації, коли працівники реагують на повідомлення, створені методами соціальної інженерії. Зловмисники використовують психологічний вплив, щоб змусити користувача добровільно передати конфіденційні дані або виконати дії, які порушують правила безпеки. Наприклад, працівник може повідомити пароль особі, яка представилася співробітником технічної підтримки, не перевіривши її справжність [28].

Суттєвий ризик створює також нехтування оновленням програмного забезпечення. У багатьох випадках працівники відкладають встановлення оновлень через небажання переривати робочий процес або через недооцінку важливості таких дій. Однак саме оновлення містять виправлення вразливостей, які можуть бути використані для атак. Відсутність актуальних версій програм

значно підвищує ризик компрометації системи.

Поширеною помилкою є використання несанкціонованого програмного забезпечення. Працівники можуть самостійно встановлювати сторонні програми для спрощення роботи або особистих потреб, не погоджуючи це з адміністраторами системи. Подібне програмне забезпечення часто не проходить перевірку безпеки та може містити шкідливі компоненти або приховані механізми збору даних [23].

Окрему групу ризиків становлять помилки, пов’язані з використанням зовнішніх носіїв інформації. Підключення невідомих флеш-накопичувачів або особистих пристроїв до корпоративної мережі може призвести до проникнення шкідливого програмного забезпечення. Працівники не завжди усвідомлюють, що навіть звичайний зовнішній носій може бути джерелом серйозної загрози для всієї інформаційної системи.

Часто порушення безпеки виникають через неправильне поводження з конфіденційною інформацією. Працівники можуть надсилати службові документи через незахищені канали зв’язку, залишати відкритими файли на спільних пристроях або передавати інформацію стороннім особам без належної перевірки. Такі дії можуть спричинити витік даних, фінансові втрати та репутаційні проблеми для організації [31].

Ще однією типовою помилкою є ігнорування внутрішніх політик безпеки. Працівники можуть обходити встановлені обмеження для спрощення власної роботи, використовувати особисті пристрої для службових завдань або вимикати засоби захисту через незручність їх використання. У результаті організація втрачає контроль над інформаційними процесами, а рівень захищеності суттєво знижується.

Важливою причиною багатьох помилок є недостатній рівень підготовки персоналу. Працівники часто не мають необхідних знань щодо сучасних кіберзагроз, не розуміють принципів безпечної роботи з інформацією або не усвідомлюють можливих наслідків своїх дій. Через це навіть базові порушення можуть залишатися непоміченими до моменту виникнення серйозного

інциденту [24].

Суттєвий вплив на поведінку персоналу має також психологічний стан працівників. Втома, перевантаження, стрес або дефіцит часу знижують рівень уважності та здатність аналізувати ризики. У такому стані користувачі частіше приймають необдумані рішення, відкривають підозрілі повідомлення або ігнорують попередження системи безпеки.

Таким чином, типові помилки персоналу в сфері інформаційної безпеки охоплюють широкий спектр дій – від використання слабких паролів до порушення правил роботи з конфіденційною інформацією. Їх особливість полягає в тому, що навіть незначні помилки можуть створювати серйозні ризики для функціонування всієї інформаційної системи. Саме тому аналіз людського фактора є необхідною складовою ефективного управління інформаційною безпекою [32].

Наслідки помилок персоналу в сфері інформаційної безпеки можуть проявлятися на різних рівнях – від локальних технічних збоїв до масштабних порушень роботи всієї організації. Особливість таких інцидентів полягає в тому, що вони часто виникають через звичайні дії користувачів, які на перший погляд не виглядають небезпечними. Саме тому людський фактор залишається одним із найскладніших елементів контролю у сфері захисту інформації [19].

Одним із найпоширеніших наслідків помилок персоналу є витік конфіденційної інформації. Він може виникати через неправильне передавання документів, використання незахищених каналів зв’язку або неналежне зберігання даних. У деяких випадках працівники випадково надсилають службові файли не тим адресатам або залишають відкритий доступ до внутрішніх ресурсів. Такі ситуації створюють ризик потрапляння важливої інформації до сторонніх осіб [33].

Особливо небезпечним є витік персональних даних, фінансової документації або внутрішньої комерційної інформації. Наслідками можуть стати фінансові втрати, юридична відповідальність та погіршення репутації організації. У сучасному цифровому середовищі репутаційні втрати можуть мати

довготривалий характер, оскільки інформація про інциденти швидко поширюється через мережу.

Серйозною проблемою є також зараження інформаційних систем шкідливим програмним забезпеченням. Найчастіше це відбувається через необережні дії працівників: відкриття заражених вкладень, завантаження сторонніх програм або використання небезпечних вебресурсів. У результаті шкідливе програмне забезпечення може порушити роботу системи, викрасти інформацію або заблокувати доступ до даних [6].

Окрему небезпеку становлять програми-вимагачі, які шифрують файли та блокують роботу організації. У багатьох випадках такі інциденти починаються саме з людської помилки – відкриття зараженого повідомлення або переходу за підробленим посиланням. Навіть одна необережна дія користувача може спричинити масштабне порушення роботи всієї інформаційної інфраструктури.

Ще одним наслідком помилок персоналу є порушення безперервності роботи організації. У разі компрометації систем або втрати доступу до інформаційних ресурсів працівники не можуть виконувати свої функції у звичайному режимі. Це призводить до затримок у роботі, фінансових збитків і зниження ефективності діяльності [29].

У деяких випадках порушення безпеки спричиняє втрату або пошкодження інформації. Працівники можуть випадково видалити важливі файли, змінити критичні налаштування системи або некоректно виконати процедури резервного копіювання. Якщо організація не має ефективних механізмів відновлення даних, наслідки таких помилок можуть бути незворотними.

Суттєву небезпеку становить також неналежне управління доступами. Працівники можуть передавати свої облікові дані колегам, використовувати спільні акаунти або залишати відкриті сесії на робочих пристроях. У результаті зростає ризик несанкціонованого доступу до інформаційних ресурсів, а встановити відповідального за певні дії стає складніше [17].

Окремо слід виділити проблему надмірних прав доступу. У багатьох організаціях користувачі мають ширші повноваження, ніж це необхідно для

виконання їхніх обов’язків. У разі помилки або навмисного порушення це дозволяє впливати на значну частину інформаційної системи. Чим більший обсяг доступу має працівник, тим серйознішими можуть бути наслідки його дій.

Важливим наслідком помилок персоналу є зниження довіри до організації. Якщо інформаційні інциденти відбуваються регулярно, партнери та клієнти починають сумніватися у здатності установи забезпечувати належний рівень захисту даних. Це може призвести до втрати клієнтів, скорочення співпраці та погіршення конкурентних позицій [15].

Негативний вплив мають і внутрішні організаційні наслідки. Після серйозних інцидентів організація змушена витрачати ресурси на відновлення систем, проведення перевірок, оновлення механізмів захисту та додаткове навчання персоналу. Такі процеси потребують часу та фінансових витрат, що знижує загальну ефективність діяльності.

Для зменшення кількості помилок персоналу організації впроваджують комплекс профілактичних заходів. Одним із найважливіших є систематичне навчання працівників. Воно повинно охоплювати не лише загальні правила безпеки, а й практичні навички розпізнавання сучасних загроз. Особливу увагу приділяють фішинговим атакам, безпечному використанню електронної пошти та правилам роботи з конфіденційною інформацією [6].

Важливу роль відіграє також формування культури інформаційної безпеки. Працівники повинні сприймати захист інформації не як формальну вимогу, а як невід’ємну частину своєї професійної діяльності. Для цього організації створюють внутрішні політики, проводять інструктажі та підтримують постійний контроль за дотриманням правил [23].

Суттєве значення має автоматизація окремих процесів безпеки. Використання багатофакторної автентифікації, систем моніторингу дій користувачів та автоматичного блокування підозрілої активності дозволяє зменшити вплив людських помилок. Хоча технічні засоби не можуть повністю усунути ризики, вони допомагають мінімізувати наслідки необережних дій персоналу.

Таким чином, типові помилки працівників у сфері інформаційної безпеки можуть спричиняти значні технічні, фінансові та репутаційні наслідки. Їх виникнення пов’язане не лише з недостатнім рівнем знань, а й з організаційними недоліками, психологічними чинниками та відсутністю належного контролю. Саме тому ефективний захист інформації потребує комплексного підходу, який поєднує технічні механізми, навчання персоналу та постійне вдосконалення внутрішніх процедур безпеки.

2.3 Оцінка ризиків, пов’язаних із людським фактором

У сучасному цифровому середовищі людський фактор залишається одним із найбільш нестабільних елементів системи кібербезпеки. Навіть за наявності сучасних технічних засобів захисту значна кількість інцидентів виникає саме через дії користувачів. Помилки працівників, недотримання внутрішніх правил, недостатня обізнаність щодо кіберзагроз або психологічний вплив з боку зловмисників створюють серйозні ризики для інформаційних систем. Саме тому оцінка ризиків, пов’язаних із людським фактором, є важливою складовою управління кібербезпекою [4].

Особливість людського фактора полягає в тому, що поведінка працівників не завжди піддається точному прогнозуванню. Технічні системи працюють за визначеними алгоритмами, тоді як людина може приймати рішення під впливом емоцій, втоми, стресу або дефіциту часу. Через це навіть добре організована система захисту може стати вразливою через необережні дії персоналу [28].

Оцінювання ризиків у сфері людського фактора передбачає визначення ймовірності виникнення помилок або небезпечних дій користувачів, а також аналіз можливих наслідків таких ситуацій. Основна мета цього процесу полягає у виявленні найбільш критичних поведінкових загроз і розробленні заходів щодо їх мінімізації.

Одним із перших етапів оцінювання є визначення потенційних джерел ризику. У більшості випадків до них належать помилки персоналу, недостатній

рівень підготовки, порушення політик безпеки, використання слабких паролів, нехтування правилами роботи з конфіденційною інформацією та необережне поводження з електронною поштою [24].

Суттєву небезпеку становить недостатня обізнаність працівників щодо сучасних кіберзагроз. Працівники можуть не розпізнавати фішингові повідомлення, не перевіряти справжність вебресурсів або відкривати вкладення з невідомих джерел. У результаті організація стає вразливою до шкідливого програмного забезпечення, витоку даних та несанкціонованого доступу до інформаційних ресурсів.

Під час оцінювання ризиків важливо враховувати психологічні аспекти поведінки користувачів. Зловмисники часто використовують методи соціальної інженерії, які базуються на маніпулюванні людською довірою, страхом або поспіхом. Працівник може виконати небезпечну дію не через технічну необізнаність, а через психологічний тиск або переконливу імітацію офіційного повідомлення [20].

Особливу увагу приділяють оцінюванню ризиків, пов’язаних із внутрішніми загрозами. Йдеться не лише про навмисні дії працівників, а й про випадкові порушення безпеки. Наприклад, користувач може ненавмисно надати доступ до службової інформації стороннім особам або залишити відкритими важливі документи у спільному середовищі [21].

Оцінювання внутрішніх ризиків ускладнюється тим, що працівники вже мають доступ до інформаційної системи та знають особливості її функціонування. Через це навіть незначна помилка користувача може мати серйозні наслідки для організації. Саме тому під час оцінювання враховується рівень доступу працівників до критичних ресурсів та можливість зловживання такими повноваженнями.

Важливим напрямом оцінювання є аналіз поведінкових моделей персоналу. Організація повинна визначати, які дії працівників найчастіше призводять до порушення безпеки. Для цього можуть використовуватися журнали подій, результати тестувань, аналіз інцидентів та моніторинг активності

користувачів [17].

Наприклад, якщо виявляється, що працівники регулярно ігнорують оновлення програмного забезпечення або використовують однакові паролі для різних систем, це свідчить про підвищений рівень поведінкового ризику. Подібні результати дозволяють організації своєчасно змінювати внутрішні процедури та посилювати контроль за дотриманням правил безпеки.

Суттєве значення має оцінювання рівня підготовки персоналу. Працівники повинні не лише знати основні правила безпеки, а й уміти застосовувати їх у практичних ситуаціях. Через це в багатьох організаціях проводяться тестування знань, навчальні тренування та моделювання кіберінцидентів [34].

Одним із найефективніших способів оцінювання є імітація фішингових атак. Працівникам надсилаються тестові повідомлення, які зовні нагадують справжні шахрайські листи. Аналіз реакції користувачів дозволяє визначити рівень їхньої готовності до протидії соціальній інженерії та виявити найбільш уразливі групи персоналу.

Під час оцінювання ризиків важливо враховувати вплив організаційного середовища. Відсутність чітких інструкцій, перевантаження працівників, недостатня комунікація між підрозділами або слабкий контроль за дотриманням політик безпеки значно підвищують ймовірність помилок. У таких умовах навіть кваліфікований персонал може допускати небезпечні дії.

Окрему роль відіграє рівень культури кібербезпеки в організації. Якщо працівники сприймають вимоги безпеки як формальність або перешкоду для роботи, ризик порушень суттєво зростає. Натомість організації, де захист інформації є частиною щоденної професійної діяльності, демонструють значно нижчий рівень інцидентів, пов’язаних із людським фактором [23].

Сучасні підходи до оцінювання ризиків дедалі частіше поєднують технічний та поведінковий аналіз. Організації використовують автоматизовані системи моніторингу, які дозволяють виявляти підозрілу активність користувачів, незвичні спроби доступу або порушення внутрішніх правил. Такий підхід дає можливість своєчасно реагувати на потенційні загрози та запобігати

розвитку інцидентів [12].

Ефективне оцінювання ризиків, пов’язаних із людським фактором, потребує не лише визначення потенційних загроз, а й глибокого аналізу умов, у яких працює персонал. Людські помилки рідко виникають без причини. Найчастіше вони є результатом поєднання декількох чинників: недостатньої підготовки, перевантаження працівників, складності внутрішніх процедур або відсутності чіткої організації роботи з інформацією. Саме тому сучасний підхід до оцінювання ризиків передбачає аналіз не тільки поведінки окремих користувачів, а й усього організаційного середовища [15].

Одним із важливих напрямів є оцінювання ймовірності виникнення помилок персоналу. Для цього організації аналізують попередні інциденти, статистику порушень безпеки та особливості роботи різних категорій працівників. Наприклад, співробітники, які мають постійний доступ до великої кількості інформації або працюють у режимі високого навантаження, частіше допускають помилки через втому та втрату концентрації.

Важливу роль відіграє оцінювання рівня доступу користувачів до інформаційних ресурсів. Чим ширші повноваження має працівник, тим більшими можуть бути наслідки його помилок. Через це в системах кібербезпеки активно застосовується принцип мінімально необхідного доступу. Його сутність полягає в тому, що працівник отримує лише ті права, які потрібні для виконання його посадових обов’язків [15].

Під час оцінювання ризиків аналізується також рівень контролю за діями користувачів. Якщо організація не здійснює моніторинг активності працівників, виявити порушення або підозрілу поведінку стає значно складніше. Сучасні системи контролю дозволяють фіксувати спроби несанкціонованого доступу, копіювання даних, зміну налаштувань або інші дії, які можуть свідчити про підвищений ризик [20].

Окрему увагу приділяють оцінюванню ризиків, пов’язаних із дистанційною роботою. Використання домашніх мереж, особистих пристроїв та віддаленого доступу суттєво збільшує кількість потенційних вразливостей.

Працівники можуть підключатися до корпоративних систем через незахищені мережі або використовувати пристрої, які не відповідають вимогам безпеки.

У таких умовах організації повинні оцінювати не лише технічний рівень захисту, а й поведінку користувачів поза межами офісного середовища. Наприклад, важливо визначити, чи дотримуються працівники правил зберігання службової інформації, чи використовують багатофакторну автентифікацію та наскільки уважно ставляться до підозрілих повідомлень.

Суттєве значення має оцінювання стійкості персоналу до соціальної інженерії. Зловмисники активно використовують методи психологічного впливу для отримання конфіденційної інформації або доступу до систем. Найчастіше вони створюють ситуації, які викликають у користувачів довіру, страх або відчуття терміновості [21].

Для перевірки рівня стійкості працівників проводяться спеціальні тестування та навчальні сценарії. Організація може моделювати фішингові атаки, телефонні дзвінки від імені технічної підтримки або підроблені службові повідомлення. Результати таких перевірок дозволяють визначити, які категорії персоналу є найбільш уразливими до психологічних маніпуляцій.

Важливим елементом оцінювання є визначення потенційних наслідків людських помилок. Організація повинна розуміти, які втрати можуть виникнути в разі порушення безпеки. Наслідки можуть бути фінансовими, технічними, репутаційними або правовими. Наприклад, витік персональних даних може призвести не лише до фінансових збитків, а й до юридичної відповідальності та втрати довіри клієнтів [15].

Під час оцінювання часто використовується поділ ризиків за рівнем критичності. Низький рівень ризику передбачає незначний вплив на роботу організації, середній – локальні порушення, а високий – серйозні інциденти, які можуть вплинути на функціонування всієї інформаційної системи. Такий підхід дозволяє визначити пріоритетність заходів захисту.

Сучасні методи оцінювання дедалі частіше використовують автоматизовані інструменти аналізу поведінки користувачів. Спеціалізовані

системи можуть виявляти нетипову активність працівників, наприклад масове копіювання файлів, підключення з незвичних місць або спроби доступу до ресурсів, які не пов’язані з посадовими обов’язками користувача [12].

Такі технології дозволяють своєчасно виявляти потенційні загрози ще до виникнення серйозного інциденту. Водночас автоматизований контроль не повинен повністю замінювати організаційні заходи, оскільки ефективність кібербезпеки значною мірою залежить від рівня відповідальності самих працівників.

Суттєву роль у зниженні ризиків відіграє навчання персоналу. Регулярні тренінги, інструктажі та практичні заняття дозволяють формувати навички безпечної роботи з інформацією. Особливо важливо, щоб навчання мало практичний характер і враховувало реальні сценарії загроз, з якими працівники можуть зіткнутися у своїй діяльності [1].

Оцінювання ефективності навчання також є важливою складовою управління ризиками. Організація повинна визначати, наскільки добре працівники засвоюють правила безпеки та чи здатні вони застосовувати отримані знання на практиці. Для цього використовуються тестування, перевірки знань та аналіз поведінки персоналу після проведення навчальних заходів.

Таким чином, оцінка ризиків, пов’язаних із людським фактором у кібербезпеці, охоплює широкий спектр напрямів – від аналізу поведінки користувачів до визначення організаційних недоліків та прогнозування можливих наслідків інцидентів. Її головна мета полягає не лише у виявленні проблем, а й у створенні умов, за яких ймовірність помилок персоналу та пов’язаних із ними загроз буде максимально знижена.

Висновки до розділу 2

У межах розглянутого розділу встановлено, що людський фактор є одним із визначальних елементів у забезпеченні ефективності системи управління інформаційною безпекою. Незважаючи на високий рівень розвитку технічних

засобів захисту, саме дії персоналу часто стають причиною виникнення інцидентів, що впливають на стан інформаційної безпеки організації.

Проведений аналіз показав, що вплив людського фактору має комплексний характер і проявляється на різних рівнях функціонування інформаційних систем. Він охоплює як випадкові помилки користувачів, так і свідомі порушення встановлених правил безпеки. До найбільш поширених проявів належать використання слабких паролів, необережне поводження з конфіденційною інформацією, відкриття шкідливих вкладень та ігнорування внутрішніх політик безпеки. Встановлено, що значна частина інцидентів інформаційної безпеки виникає внаслідок недостатнього рівня обізнаності персоналу щодо сучасних кіберзагроз. Працівники не завжди здатні своєчасно розпізнати методи соціальної інженерії або оцінити ризики своїх дій, що підвищує вразливість організації до зовнішніх атак.

Окремо визначено, що важливу роль у формуванні рівня безпеки відіграє організаційне середовище. Відсутність чітких інструкцій, недостатній контроль за дотриманням політик безпеки та перевантаження працівників можуть суттєво збільшувати ймовірність помилок. Таким чином, ефективність системи управління інформаційною безпекою залежить не лише від технічних рішень, а й від якості управлінських процесів.

У ході дослідження також встановлено, що людський фактор може виступати як джерелом загроз, так і елементом їх запобігання. Рівень підготовки персоналу, його дисциплінованість та розуміння принципів інформаційної безпеки безпосередньо впливають на загальну стійкість системи до кіберризиків.

Розділ 3 ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ІБ З УРАХУВАННЯМ ЛЮДСЬКОГО ФАКТОРУ

3.1 Методи мінімізації впливу людського фактору

Людський фактор залишається одним із найменш передбачуваних елементів у системі інформаційної безпеки, оскільки поведінка користувачів залежить від великої кількості змінних. Помилки працівників, необережні дії або недостатня обізнаність часто стають причиною інцидентів, які технічно захищені системи не можуть попередити самостійно. Саме тому мінімізація впливу людського фактору розглядається як окремий напрям управління кібербезпекою. Його мета полягає не у виключенні людини з процесів, а у зниженні ймовірності помилкових або ризикованих дій. Для цього застосовується комплекс організаційних, технічних і поведінкових заходів [35].

Одним із базових методів є систематичне навчання персоналу та підвищення рівня обізнаності щодо кіберзагроз. Працівники повинні розуміти, як працюють сучасні атаки, зокрема фішинг, соціальна інженерія та шкідливе програмне забезпечення. Навчальні програми зазвичай включають практичні приклади, моделювання інцидентів та регулярні перевірки знань. Такий підхід дозволяє формувати у працівників навички розпізнавання небезпечних ситуацій. З часом це зменшує кількість випадкових помилок у повсякденній роботі [36].

Важливим інструментом є проведення симуляцій атак, які імітують реальні загрози. Найчастіше використовуються фішингові тестування, коли працівникам надсилаються спеціально підготовлені повідомлення. Аналіз реакції користувачів дозволяє оцінити рівень їхньої готовності до реальних інцидентів. Якщо працівник переходить за підозрілим посиланням або вводить облікові дані, це свідчить про необхідність додаткового навчання. Такий метод є ефективним, оскільки дозволяє виявити слабкі місця без реальних наслідків для системи [37].

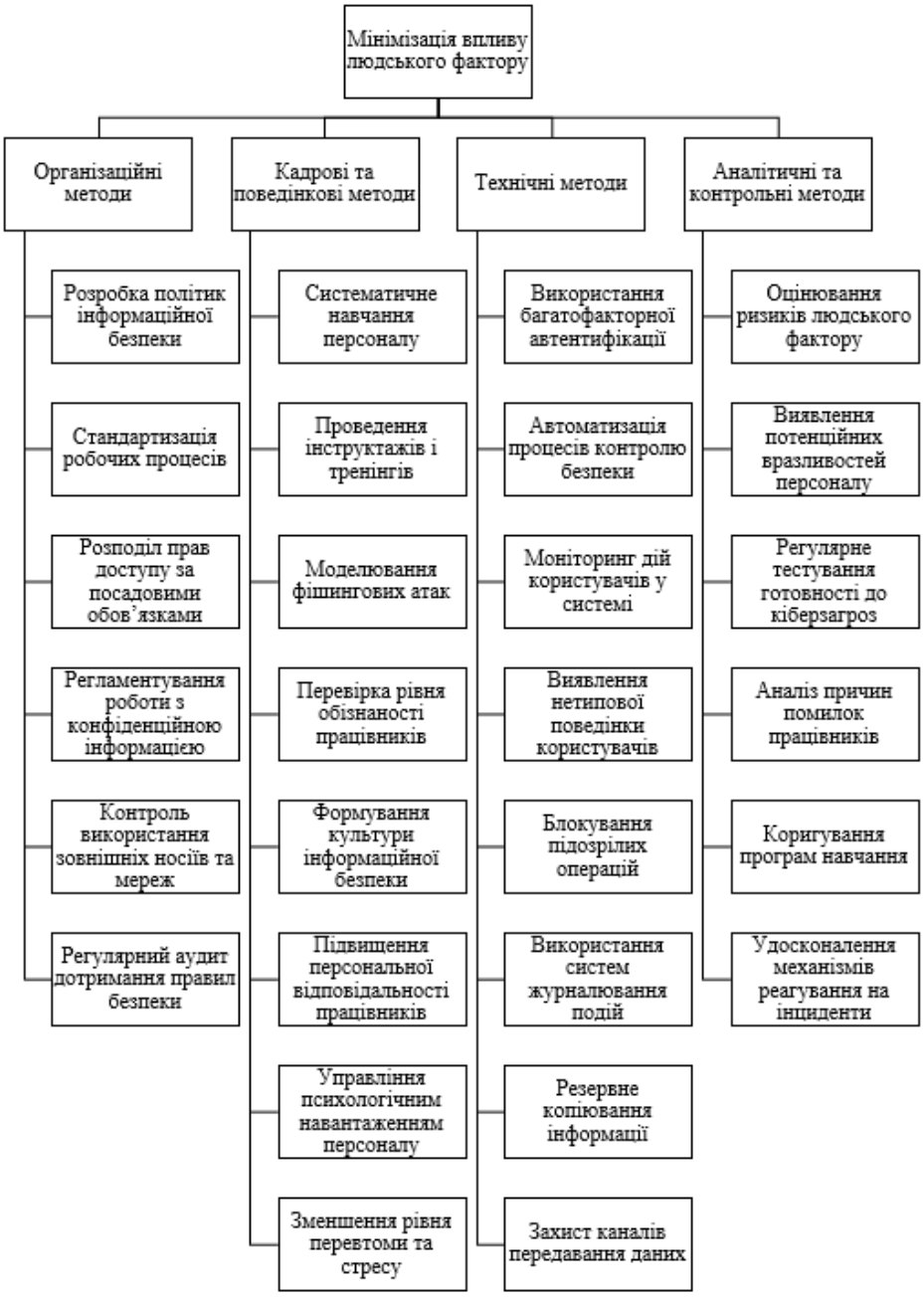

Рис. 3.1 Комплексна система мінімізації впливу людського фактору в інформаційній безпеці

Суттєву роль у зменшенні впливу людського фактору відіграє впровадження чітких політик інформаційної безпеки. Вони визначають правила роботи з даними, вимоги до паролів, порядок доступу до ресурсів та поведінку користувачів у різних ситуаціях. Чітко структуровані політики зменшують кількість невизначених дій і допомагають працівникам орієнтуватися у складних ситуаціях. Однак ефективність таких документів залежить від того, наскільки вони реально застосовуються на практиці, а не лише формально існують [35].

Окремим напрямом є контроль доступу до інформаційних ресурсів. Використання принципу мінімально необхідних прав дозволяє обмежити потенційний вплив помилок окремого працівника. Якщо користувач має доступ лише до тих даних, які потрібні для виконання його обов'язків, наслідки можливих помилок значно зменшуються. Додатково застосовуються багатофакторна автентифікація та системи ідентифікації, які ускладнюють несанкціонований доступ навіть у випадку компрометації пароля.

Важливим елементом є формування культури інформаційної безпеки в організації. Це означає, що працівники сприймають вимоги безпеки не як обмеження, а як частину робочого процесу. У такому середовищі зменшується кількість свідомих порушень і підвищується відповідальність за власні дії. Формування культури безпеки відбувається поступово через навчання, внутрішню комунікацію та приклади керівництва. Без цього навіть технічно досконалі системи залишаються вразливими до людських помилок [38].

Одним із ефективних способів зниження впливу людського фактору є автоматизація процесів безпеки. Сучасні системи здатні самостійно виявляти підозрілу активність користувачів, блокувати небезпечні дії або попереджати про можливі загрози. Це зменшує залежність від людської уваги, яка може знижуватися через втому або перевантаження. Автоматизовані засоби контролю особливо ефективні у великих організаціях, де кількість користувачів ускладнює ручний моніторинг. Вони дозволяють швидко реагувати на відхилення від нормальної поведінки [36].

Суттєве значення має впровадження систем моніторингу дій користувачів. Такі системи фіксують операції з файлами, доступ до ресурсів, спроби входу та інші дії в інформаційній системі. Аналіз цих даних дозволяє виявляти нетипову поведінку, яка може свідчити про помилки або потенційні загрози. Наприклад, масове копіювання файлів або доступ до незвичних ресурсів може бути ознакою порушення безпеки. Своєчасне виявлення таких ситуацій дозволяє запобігти серйозним інцидентам [36].

Важливим методом є управління навантаженням персоналу. Перевтома та

стрес є одними з основних причин людських помилок у сфері інформаційної безпеки. Коли працівник працює в умовах високого тиску або обмеженого часу, зростає ймовірність необережних дій. Організаційні заходи, спрямовані на рівномірний розподіл завдань та оптимізацію робочих процесів, дозволяють зменшити ці ризики. Таким чином, покращення умов праці безпосередньо впливає на рівень безпеки [33].

Окрему роль відіграє контроль використання зовнішніх пристроїв і незахищених мереж. Працівники часто підключаються до корпоративних систем через публічні або домашні мережі, які не мають достатнього рівня захисту. Це створює додаткові можливості для перехоплення даних або атак. Обмеження доступу з ненадійних мереж та використання захищених каналів зв’язку дозволяє суттєво знизити такі ризики. Аналогічно контролюється використання зовнішніх носіїв інформації.

Важливим напрямом є регулярне тестування рівня готовності персоналу до кіберзагроз. Такі перевірки можуть включати як теоретичні тести, так і практичні сценарії. Результати дозволяють оцінити, наскільки ефективно працівники застосовують отримані знання. Якщо виявляються слабкі місця, організація може оперативно скоригувати навчальні програми. Це забезпечує постійне вдосконалення рівня обізнаності персоналу [35].

Суттєвим елементом мінімізації ризиків є стандартизація робочих процесів. Чітко визначені алгоритми виконання завдань зменшують кількість довільних рішень, які можуть призвести до помилок. Коли працівник діє за встановленою процедурою, ймовірність відхилень від безпечної поведінки значно знижується. Стандартизація також спрощує контроль і дозволяє швидше виявляти порушення [36].

Таким чином, мінімізація впливу людського фактору базується на поєднанні технічних, організаційних і поведінкових заходів. Їх ефективність залежить від системності впровадження та постійного вдосконалення з урахуванням змін у кіберзагрозах і поведінці користувачів.

3.2 Розробка рекомендацій щодо підвищення обізнаності персоналу

Рівень обізнаності персоналу у сфері інформаційної безпеки безпосередньо впливає на стійкість організації до кіберзагроз. У багатьох випадках саме дії користувачів стають початковою точкою інцидентів, які згодом призводять до витоку даних або порушення роботи систем. Тому формування системи рекомендацій щодо підвищення обізнаності не є допоміжним заходом, а виступає ключовим елементом загальної стратегії кіберзахисту. Ефективна система навчання повинна враховувати як технічні аспекти безпеки, так і поведінкові особливості працівників. Лише комплексний підхід дозволяє зменшити кількість помилок і підвищити рівень захищеності інформаційного середовища [38].

Одним із базових напрямів є впровадження регулярного та безперервного навчання персоналу. Одноразові інструктажі не забезпечують довготривалого ефекту, оскільки рівень знань поступово знижується без практичного закріплення. Тому навчальні програми повинні бути системними та повторюваними, із поступовим ускладненням матеріалу. Важливо, щоб працівники отримували не лише теоретичні знання, а й практичні навички розпізнавання загроз. Це дозволяє формувати стійку модель безпечної поведінки у повсякденній роботі.

Суттєвим елементом є використання інтерактивних методів навчання. Замість пасивного сприйняття інформації працівники повинні брати участь у практичних завданнях, які імітують реальні кіберзагрози. Такий підхід дозволяє краще засвоювати матеріал і швидше реагувати на потенційно небезпечні ситуації. Наприклад, моделювання фішингових повідомлень дає можливість оцінити, як користувачі поводяться в умовах, наближених до реальних атак. Результати таких перевірок використовуються для подальшого коригування навчальних програм [30].

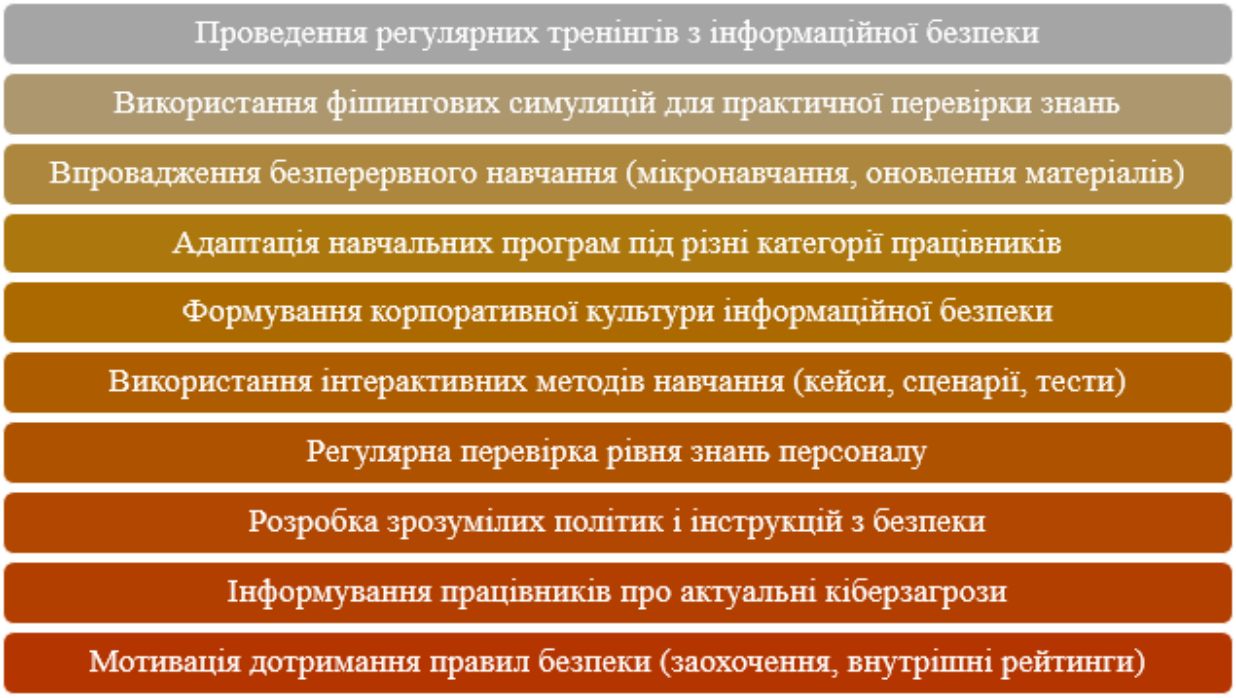

Рис. 3.2 Рекомендації щодо підвищення обізнаності персоналу

Окрему роль відіграє впровадження персоналізованого підходу до навчання. Різні категорії працівників мають різний рівень доступу до інформаційних систем і виконують різні функції, тому їхні ризики також відрізняються. Відповідно, навчальні матеріали повинні враховувати специфіку роботи кожної групи користувачів. Наприклад, співробітники, які працюють із фінансовими даними, потребують більш глибокого розуміння ризиків витоку інформації, тоді як технічний персонал повинен краще орієнтуватися в питаннях конфігурації систем безпеки [31].

Важливим напрямом є формування стійкої культури інформаційної безпеки в організації. Обізнаність персоналу не повинна обмежуватися знанням правил, а має переходити у щоденну практику їх застосування. Це досягається через постійну комунікацію, приклади правильного поводження з інформацією та підтримку з боку керівництва. Якщо керівні працівники демонструють відповідальне ставлення до безпеки, це формує відповідну модель поведінки у всьому колективі [37].

Суттєвим елементом є використання коротких і зрозумілих навчальних матеріалів. Перевантаження складною технічною інформацією може знижувати

ефективність навчання, особливо серед працівників без технічної підготовки. Тому важливо подавати інформацію у доступній формі, використовуючи приклади з реальної практики, візуальні матеріали та сценарії типових загроз. Це підвищує рівень сприйняття та сприяє кращому засвоєнню знань [30].

Окремо слід враховувати необхідність регулярного оновлення навчальних програм. Кіберзагрози постійно змінюються, з'являються нові методи атак і способи соціальної інженерії. Якщо навчальні матеріали не оновлюються, вони швидко втрачають актуальність. Тому система підвищення обізнаності повинна бути гнучкою та адаптивною до сучасних умов.

Одним із ключових напрямів підвищення обізнаності персоналу є впровадження практичних симуляцій кіберінцидентів. Такі заходи дозволяють перевірити, як працівники реагують на потенційні загрози в умовах, максимально наближених до реальних. Найчастіше використовуються фішингові симуляції, підроблені повідомлення або тестові сценарії соціальної інженерії. Важливо, щоб такі перевірки не мали карального характеру, а використовувалися як інструмент навчання. Аналіз результатів дозволяє визначити слабкі місця та сформувати індивідуальні рекомендації для працівників [38].

Суттєву роль відіграє впровадження системи постійного контролю знань. Обізнаність персоналу не є статичною характеристикою, тому вона потребує регулярного оновлення та перевірки. Періодичні тестування дозволяють оцінити рівень засвоєння матеріалу та виявити прогалини у знаннях. У разі необхідності працівникам надаються додаткові навчальні матеріали або проводяться повторні інструктажі. Такий підхід забезпечує безперервний процес навчання.

Важливим елементом є використання мотиваційних механізмів. Працівники частіше дотримуються правил безпеки, якщо розуміють їх значення та бачать позитивні результати своєї поведінки. У деяких організаціях застосовуються системи заохочення за дотримання правил інформаційної безпеки або успішне проходження навчальних програм. Це сприяє формуванню відповідального ставлення до захисту інформації [30].

Окрему увагу слід приділяти зниженню впливу людського фактора через спрощення процедур безпеки. Надмірно складні або незручні правила часто призводять до їх ігнорування. Якщо працівникам складно виконувати вимоги безпеки, вони можуть шукати обхідні шляхи, що підвищує ризики. Тому важливо знаходити баланс між рівнем захисту та зручністю використання інформаційних систем.

Суттєвим напрямом є розвиток навичок критичного мислення у працівників. Обізнаність у сфері кібербезпеки передбачає не лише знання правил, а й здатність аналізувати ситуації та приймати обґрунтовані рішення. Працівники повинні вміти ставити під сумнів підозрілі повідомлення, перевіряти джерела інформації та не діяти імпульсивно. Це особливо важливо у випадках, пов’язаних із соціальною інженерією [31].

Важливою рекомендацією є інтеграція навчання з повсякденною роботою. Якщо навчальні заходи відокремлені від реальних процесів, їх ефективність знижується. Тому доцільно впроваджувати короткі навчальні нагадування, інформаційні повідомлення або мікронавчання безпосередньо в робочому середовищі. Це дозволяє постійно підтримувати рівень обізнаності без значного відволікання від основних обов’язків.

Значну роль відіграє також підтримка з боку керівництва. Якщо керівники демонструють особисту залученість до питань інформаційної безпеки, це підвищує загальний рівень відповідальності в організації. Важливо, щоб дотримання правил безпеки було частиною корпоративної культури, а не формальною вимогою [30].

Отже, розробка рекомендацій щодо підвищення обізнаності персоналу передбачає комплексний підхід, який поєднує навчання, практичні тренування, мотиваційні механізми та організаційні заходи. Лише системна реалізація цих елементів дозволяє суттєво знизити ризики, пов’язані з людським фактором, і підвищити загальний рівень інформаційної безпеки організації.

3.3 Впровадження сучасних підходів до управління інформаційною безпекою

Управління інформаційною безпекою поступово переходить від реактивної моделі до проактивної, коли основна увага приділяється не лише реагуванню на інциденти, а й їх запобіганню. Це зумовлено стрімким зростанням кількості кіберзагроз, ускладненням інформаційних систем та розширенням цифрового середовища організацій. У таких умовах традиційні підходи, які базуються на періодичних перевірках і формальних процедурах, уже не забезпечують достатнього рівня захисту. Тому виникає потреба у впровадженні сучасних моделей управління, які є більш гнучкими, адаптивними та інтегрованими в бізнес-процеси.

Одним із ключових сучасних підходів є ризик-орієнтоване управління інформаційною безпекою. Його сутність полягає у визначенні найбільш критичних загроз та концентрації ресурсів на їх мінімізації. Такий підхід дозволяє організації не розпорошувати зусилля на всі можливі ризики, а зосереджуватися на тих, які можуть завдати найбільшої шкоди. У межах цього підходу здійснюється постійний аналіз вразливостей, оцінка ймовірності інцидентів та потенційних наслідків для бізнес-процесів.

Важливою складовою сучасного управління є інтеграція інформаційної безпеки в загальну систему корпоративного управління. Безпека більше не розглядається як окрема технічна функція, а стає частиною стратегічного планування організації. Це означає, що питання захисту інформації враховуються при прийнятті управлінських рішень, розробці нових продуктів і впровадженні цифрових технологій. Така інтеграція дозволяє забезпечити узгодженість між бізнес-цілями та вимогами безпеки [39].

Сучасні підходи також передбачають активне використання автоматизації та інтелектуальних систем моніторингу. Вони дозволяють в режимі реального часу аналізувати поведінку користувачів, виявляти аномалії та реагувати на потенційні загрози до моменту їх реалізації. Автоматизовані системи значно

підвищують швидкість реагування на інциденти та зменшують залежність від людського фактора, який часто є джерелом помилок [38].

Окрему роль відіграє концепція безперервного моніторингу безпеки. На відміну від періодичних перевірок, цей підхід передбачає постійне відстеження стану інформаційних систем. Це дозволяє своєчасно виявляти підозрілі дії, зміни в конфігураціях або спроби несанкціонованого доступу. Безперервний моніторинг є особливо важливим у складних розподілених системах, де ризики можуть виникати в будь-який момент.

Сучасне управління інформаційною безпекою також активно використовує підхід нульової довіри. Його основна ідея полягає в тому, що жоден користувач або пристрій не вважається автоматично безпечним, навіть якщо він знаходиться всередині корпоративної мережі. Кожна спроба доступу до ресурсів потребує перевірки та підтвердження. Це дозволяє суттєво зменшити ризики внутрішніх загроз та компрометації облікових записів [40].

Важливим напрямом є розвиток культури інформаційної безпеки в організації. Сучасні підходи передбачають, що ефективний захист неможливий без активної участі персоналу. Працівники повинні не лише дотримуватися правил, а й усвідомлювати їх значення. Формування такої культури відбувається через навчання, внутрішню комунікацію та залучення керівництва до процесів безпеки. Це дозволяє створити середовище, у якому безпечна поведінка стає нормою.

Суттєве значення має впровадження гнучких моделей управління безпекою, які можуть швидко адаптуватися до змін у зовнішньому середовищі. Кіберзагрози постійно еволюціонують, тому статичні підходи втрачають ефективність. Гнучкі моделі дозволяють оперативно оновлювати політики безпеки, змінювати конфігурації систем і впроваджувати нові засоби захисту без значних затримок.

Сучасні підходи також передбачають активне використання аналітики даних для прогнозування загроз. Аналіз великих обсягів інформації дозволяє виявляти приховані закономірності та передбачати потенційні інциденти. Це дає

можливість переходити від реактивного реагування до превентивного захисту, коли загроза нейтралізується ще до її реалізації [39].

Окрему увагу приділяють управлінню інцидентами інформаційної безпеки. Сучасні системи передбачають чіткі процедури виявлення, аналізу та ліквідації наслідків інцидентів. Важливо, щоб організація не лише реагувала на події, а й аналізувала їх причини для запобігання повторенню. Це дозволяє постійно вдосконалювати систему безпеки та підвищувати її ефективність.

Отже, впровадження сучасних підходів до управління інформаційною безпекою є необхідною умовою забезпечення стабільної роботи організацій у цифровому середовищі. Поєднання ризик-орієнтованого управління, автоматизації, безперервного моніторингу, нульової довіри та розвитку культури безпеки дозволяє створити комплексну систему захисту, яка здатна ефективно протидіяти сучасним кіберзагрозам і забезпечувати стійкість інформаційної інфраструктури.

Висновки до розділу 3

У процесі дослідження встановлено, що підвищення ефективності системи управління інформаційною безпекою неможливе без комплексного врахування людського фактору. Саме поведінка персоналу, рівень його обізнаності та дотримання внутрішніх правил значною мірою визначають рівень захищеності інформаційного середовища організації. Навіть за наявності сучасних технічних засобів захисту помилки працівників можуть створювати критичні вразливості та сприяти реалізації кіберзагроз.

У ході аналізу визначено, що одним із ключових напрямів підвищення ефективності системи управління інформаційною безпекою є розвиток системного навчання персоналу. Регулярні тренінги, практичні заняття, моделювання кіберінцидентів та перевірка знань дозволяють формувати у працівників навички безпечної роботи з інформацією та підвищують їх здатність протидіяти сучасним кіберзагрозам.

Важливу роль відіграє формування культури інформаційної безпеки в організації. Доведено, що ефективний захист інформаційних ресурсів залежить не лише від формального виконання інструкцій, а й від рівня відповідальності персоналу та усвідомлення важливості дотримання правил безпеки. Позитивний вплив має створення середовища, у якому безпечна поведінка є невід'ємною частиною щоденної професійної діяльності.

У роботі обґрунтовано необхідність удосконалення організаційних механізмів захисту. Встановлено, що чіткі політики інформаційної безпеки, контроль доступу до ресурсів, розмежування повноважень і постійний моніторинг дій користувачів дозволяють суттєво знизити ризики, пов'язані з людським фактором. Водночас надмірно складні процедури можуть зменшувати ефективність системи, тому важливим є забезпечення балансу між рівнем захисту та зручністю використання інформаційних систем.

Дослідження також показало ефективність сучасних технічних рішень, спрямованих на мінімізацію впливу людських помилок. Використання автоматизованих систем моніторингу, багатофакторної автентифікації, засобів виявлення аномальної активності та принципу мінімально необхідного доступу дозволяє своєчасно виявляти потенційні загрози та обмежувати наслідки помилкових дій користувачів.

Окремо встановлено, що важливим напрямом удосконалення системи управління інформаційною безпекою є впровадження ризик-орієнтованого підходу. Це дозволяє організації визначати найбільш критичні поведінкові ризики, прогнозувати можливі наслідки інцидентів і спрямовувати ресурси на захист найбільш уразливих елементів інформаційної інфраструктури.

Отже, підвищення ефективності системи управління інформаційною безпекою потребує комплексного поєднання організаційних, технічних та освітніх заходів. Лише системний підхід до управління людським фактором дозволяє забезпечити стабільний рівень інформаційної безпеки, знизити кількість інцидентів та підвищити стійкість організації до сучасних кіберзагроз.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що людський фактор є одним із ключових чинників, які впливають на ефективність системи управління інформаційною безпекою. Незважаючи на постійний розвиток технічних засобів захисту, значна частина інцидентів інформаційної безпеки виникає саме через помилки персоналу, недостатній рівень обізнаності користувачів або порушення встановлених правил роботи з інформацією.

У ході роботи було визначено, що людський фактор має комплексний характер і проявляється як у випадкових діях працівників, так і у свідомому нехтуванні вимогами безпеки. До найбільш поширених проблем належать використання слабких паролів, відкриття фішингових повідомлень, порушення політик доступу, необережне поводження з конфіденційними даними та використання незахищених пристроїв і мереж. Подібні дії створюють сприятливі умови для реалізації кіберзагроз і можуть призводити до значних фінансових, технічних та репутаційних втрат.

Дослідження показало, що ефективність системи управління інформаційною безпекою значною мірою залежить не лише від рівня технічного захисту, а й від організаційних умов функціонування системи. Відсутність чітких внутрішніх процедур, недостатній контроль, перевантаження працівників та низький рівень культури безпеки суттєво підвищують ризик виникнення інцидентів. У зв’язку з цим важливого значення набуває формування системного підходу до управління поведінковими ризиками.

У роботі було проаналізовано основні методи оцінювання впливу людського фактору, серед яких ризик-орієнтований підхід, аудит інформаційної безпеки, статистичний аналіз інцидентів, тестування персоналу та моніторинг поведінки користувачів. Встановлено, що найбільш ефективними є комплексні методи, які поєднують технічний контроль із оцінюванням рівня підготовки працівників та аналізом організаційного середовища.

Окрему увагу приділено методам мінімізації впливу людського фактору. Визначено, що зниження поведінкових ризиків можливе за умови системного навчання персоналу, впровадження політик безпеки, використання фішингових симуляцій, автоматизації контролю та розвитку корпоративної культури інформаційної безпеки. Важливим аспектом є також постійне оновлення навчальних програм відповідно до сучасних кіберзагроз.

У процесі дослідження обґрунтовано необхідність впровадження сучасних підходів до управління інформаційною безпекою, які базуються на безперервному моніторингу, принципі нульової довіри, ризик-орієнтованому управлінні та інтеграції безпеки в загальну систему корпоративного управління. Такі підходи дозволяють підвищити адаптивність системи безпеки та забезпечити більш ефективний захист інформаційних ресурсів.

Узагальнюючи вищенаведене, забезпечення ефективного функціонування системи управління інформаційною безпекою неможливе без урахування впливу людського фактору. Саме комплексне поєднання технічних, організаційних та освітніх заходів дозволяє знизити рівень поведінкових ризиків, підвищити відповідальність персоналу та забезпечити стабільний рівень захищеності інформаційного середовища організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zhmurko O. Social engineering as a cybersecurity threat: Prevention and protection methods. *Security Pedagogy*. 2024. Vol. 9, № 1. P. 37–42.

2. Цуркан В. Метод аналізування вимог до систем управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*. 2020. № 1(9). С. 149–158.

3. Moh P., Yang A., Malkin N., Mazurek M. L. Understanding how people share passwords. *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 2024. P. 219–237.

4. Гордієнко С. Особливості функціонування системи управління інформаційною безпекою. *Інформаційна безпека людини, суспільства, держави.* 2025. № 1(38). С. 72–82.

5. Ананченко О. Методика оцінки ефективності забезпечення інформаційної безпеки освітньої інформаційної системи. *Кібербезпека: освіта, наука, техніка.* 2023. № 1(21). С. 297–308.

6. Богданович В. Ю., Грищук Р. В., Левченко О. В. Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2017. № 4(74). С. 6–23.

7. Ананченко О. Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/536

8. Петренко К. М. Удосконалена система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України. Труди університету. 2022. № 5(174). С. 180–186.

9. Khokh V. D., Meleshko E. V., Smirnov O. A. Дослідження методів аудиту систем управління інформаційною безпекою. URL: https://journals.nupp.edu.ua/sunz/uk/article/view/628 (дата звернення:

28.05.2026).

10. Цуркан В. Метод функціонального аналізування систем управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*. 2020. № 4(8). С. 192–201.

11. Degtyareva L., Miroshnykova M., Voloshko S. Аналіз структури системи захисту інформації. DOI: https://doi.org/10.26906/SUNZ.2019.2.078

12. Poddubnyi V., Sievierinov O., Pustomelnik O. Менеджмент вразливостей як складова частина політики безпеки ITC. DOI: https://doi.org/10.26906/SUNZ.2020.4.055

13. Стратегія інформаційної безпеки України: Указ Президента України від 28 груд. 2021 р. № 685/2021.

14. Yakymenko Yu. M., Rabchun D. I., Zaporozhchenko M. M. The role of social engineering in data leakage issues and organizational aspects of protecting corporate environments from phishing attacks via email. *Cybersecurity: Education, Science, Technique*. 2021. Vol. 1(13). P. 6–15.

15. Перегуда С. П. Методика оцінювання ефективності системи інформаційної безпеки Міністерства оборони України. *Інформація та соціум*. 2023. С. 49–51.

16. Інформаційна безпека організації: аналіз, оцінка, управління ризиками: навч. посіб. / уклад. М. О. Іванов. Одеса: ОНПУ, 2019. 156 с.

17. Воронін Д. В. Ризик-орієнтований підхід в управлінні інформаційною безпекою: міжнародні стандарти та український досвід. *Інформаційні технології та захист інформації*. 2020. № 4(20). С. 77–85.

18. Оцінювання ризиків інформаційної безпеки підприємства: методологічні аспекти: кол. моногр. / за заг. ред. Л. П. Дунаєвої. Київ: Вид-во КНЕУ, 2020. 248 с.

19. Kras A. Human factor and security management. *Problems of Computer Science, Software Modeling, and Security of Digital Systems*. 2025. P. 123–125.

20. Dzhalladova I. A.-k., Kaminskyi O. Ye. Socio-psychological resilience of cybersecurity systems. *Modern Information Technologies in the Sphere of Security*

and Defense. 2025. Vol. 53(2). P. 43–50.

21. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації: навч. посіб. Харків: ХНЕУ, 2013. 364 с.

22. Андріяш В. Управління інформаційною безпекою: навч. посіб. Київ: НАУ, 2018. 324 с.

23. Захист інформації та кібербезпека: посібник для студентів / уклад. В. М. Герасименко. Київ: КПІ ім. Ігоря Сікорського, 2021. 285 с.

24. Кібербезпека в Україні: ризики, загрози, пріоритети: аналітичний звіт / за ред. І. В. Петрова. Київ: Центр Разумкова, 2022. 112 с.

25. Романюк А. Управління ризиками інформаційних технологій: монографія. Львів: Тріада плюс, 2020. 392 с.

26. Khan S., Kabanov I., Hua Y., Madnick S. A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*. 2022. Vol. 26(1). P. 1–29.

27. Богданович В. Ю., Грищук Р. В., Левченко О. В. Метод та методика оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Труди університету*. 2018. № 1(146). С. 10–18.

28. Войтко О. В. Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. № 3(49). С. 97–99.

29. Кирило П. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. Т. 45, № 3. С. 97–100.

30. Клименко О. А. Методи оцінки ризиків інформаційної безпеки підприємства. *Вісник НАУ*. 2018. № 3. С. 34–41.

31. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни. *Стратегічні пріоритети*. 2015. № 4(37). С. 83–90.

32. Бурак М. В. Інформаційна безпека як складова національної безпеки

України. *Економічна та інформаційна безпека: проблеми та перспективи: матеріали Всеукр. наук.-практ. конф*. 2017. С. 21–24.

33. Шевчук В. В., Гончаренко М. Ю. Методики проведення ризик-аналізу інформаційних систем. *Кібербезпека та захист інформації*. 2021. № 2(8). С. 56–65.

34. Дробот О. В. Інформаційні ризики та методи їх аналізу: навч. посіб. Київ: Талком, 2019. 340 с.

35. Kashkanova A. A. Socio-technical approach as a way to improve the security environment in urban transport systems. *Bulletin of Vinnytsia Polytechnic Institute*. 2025. № 4. P. 170–178.

36. Косевцов В. О., Телелим В. М., Лобанов А. А. До питання оцінювання ефективності функціонування системи забезпечення ВБД. Наука і оборона. 2010. № 3. С. 8–12.

37. Oniushchenko S. V., Hlushko A. D. Analytical dimension of cybersecurity in Ukraine under increasing challenges and threats. *Economy and Region*. 2022. Vol. 1(84). P. 13–20.

38. Shevchenko S., Zhdanova Yu., Skladannyi P., Boiko S. Insiders and insider information: Essence, threats, activities, and legal responsibility. *Cybersecurity: Education, Science, Technique*. 2022. Vol. 3(15). P. 175–185.

39. Краснова М. В. Основи оцінки ризиків інформаційної безпеки: навч. посіб. Київ: Алерта, 2020. 216 с.

40. Управління ризиками інформаційної безпеки: метод. рек. / авт.-уклад. О. І. Петренко, В. І. Кузнєцов. Харків: ХНУРЕ, 2021. 98 с.