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: “МЕТОДИ УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

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

_____ Марія ЛЯШЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-42

Марія ЛЯШЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Доктор філософії з кібербезпеки 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

Ляшенко Марії Сергіївні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи управління поведінкою персоналу у сфері інформаційної безпеки”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки
(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: *інформаційна безпека підприємства, управління людським фактором в інформаційній безпеці, методи та технології формування культури інформаційної безпеки, управління поведінкою персоналу*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати теоретичні засади управління поведінкою персоналу у сфері інформаційної безпеки.
4.2. Проаналізувати стан управління поведінкою персоналу у сфері інформаційної безпеки в українських організаціях.
4.3. Удосконалити методи управління поведінкою персоналу у сфері інформаційної безпеки шляхом розробки комплексної моделі та надати практичні рекомендації щодо її впровадження

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “5“ 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.	Аналіз теоретичних засад управління поведінкою персоналу у сфері ІБ	08.04.2026	
4.	Дослідження стану управління поведінкою персоналу у сфері ІБ в українських організаціях в умовах воєнного стану та гібридної роботи	15.04.2026	
5.	Розробка комплексної моделі управління поведінкою персоналу та її впровадження	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.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувачка вищої освіти _____ Марія ЛЯШЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО

(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 здобувачка Ляшенко М.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи управління поведінкою персоналу у сфері інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка ЛЯШЕНКО Марія у кваліфікаційній роботі дослідила теоретичні засади управління поведінкою персоналу у сфері інформаційної безпеки, проаналізувала стан застосування методів управління поведінкою персоналу в в умовах воєнного стану та гібридної роботи, виявила основні проблеми їх впровадження, розробила модель комплексного управління поведінкою персоналу та надала практичні рекомендації щодо її впровадження.

Робота демонструє високий рівень теоретичної підготовки та практичних навичок здобувачки. ЛЯШЕНКО Марія проявила самостійність, відповідальність та вміння застосовувати здобуті знання. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки ЛЯШЕНКО Марії на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Ляшенко М.С. 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

здобувачки вищої освіти ЛЯШЕНКО Марії
на тему “Методи управління поведінкою персоналу у сфері інформаційної безпеки”

Актуальність. В умовах воєнного стану та масового переходу українських організацій на гібридну форму роботи людський фактор залишається найвразливішою ланкою системи інформаційної безпеки. Зростання соціально-інженерних атак, використання генеративного ШІ, діпфейків та психологічного виснаження персоналу вимагає переходу від традиційного технічного захисту до комплексного управління поведінкою працівників та формування зрілої культури інформаційної безпеки.

З огляду на це, дослідження методів управління поведінкою персоналу з урахуванням реалій воєнного часу та гібридної роботи має важливе як теоретичне, так і практичне значення для підвищення кіберстійкості українських організацій.

Позитивні сторони.

1. У роботі проведено ґрунтовний теоретичний аналіз сучасних підходів до управління поведінкою персоналу, розглянуто ключові психологічні моделі (TPB, PMT, SCT) та їх застосування у сфері інформаційної безпеки.
2. Розроблено комплексну модель управління поведінкою персоналу, яка інтегрує технічні, організаційні та психологічні інструменти.
3. Робота добре структурована, містить значну кількість аналітичних таблиць, чіткі висновки до кожного розділу. Авторка опрацювала сучасну джерельну базу, зокрема міжнародні звіти

Недоліки.

Доцільно було б посилити емпіричну частину роботи шляхом проведення власного опитування або анкетування працівників українських організацій для підтвердження теоретичних висновків.

Зазначене зауваження має уточнюючий характер і не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ _____
_____ *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню та вдосконаленню методів управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану та гібридної роботи. Робота складається зі вступу, трьох розділів, що містять 11 таблиць і 2 рисунків, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 72 аркушів, з яких 4 аркуші займає список використаних джерел.

Метою роботи є удосконалення методів управління поведінкою персоналу у сфері інформаційної безпеки з урахуванням умов воєнного стану та гібридної форми роботи.

Об'єктом дослідження є процес управління поведінкою персоналу в системі інформаційної безпеки підприємства.

Предмет дослідження – методи та технології управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану та гібридної роботи.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі у роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу, також теоретичне узагальнення та моделювання.

Галузь застосування. Розроблена модель комплексного управління та практичні рекомендації можуть бути використані підприємствами різних форм власності, органами державної влади та організаціями критичної інфраструктури для підвищення ефективності системи інформаційної безпеки шляхом формування зрілої культури безпеки персоналу в умовах воєнних викликів та гібридної організації праці.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ, КУЛЬТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЛЮДСЬКИЙ ФАКТОР, ВОЄННИЙ СТАН, ГІБРИДНА РОБОТА, КОМПЛЕКСНЕ УПРАВЛІННЯ, БЕЗПЕЧНА ПОВЕДІНКА.

ABSTRACT

The qualification thesis is devoted to the study and improvement of methods for managing personnel behavior in the field of information security under martial law and hybrid work conditions. The work consists of an introduction, three chapters containing 11 tables and 2 figures, conclusions and the list of 40 references. The total volume of the work is 72 pages, of which 4 pages are occupied by the list of references.

The purpose of the study *is* to improve the methods of managing personnel behavior in the field of information security, taking into account the conditions of martial law and hybrid work.

The object the study is the process of managing personnel behavior in the enterprise information security system.

The subject of the study is the methods and technologies of managing personnel behavior in the field of information security under martial law and hybrid work conditions.

Research methods. To solve the scientific task, the methods of analysis and synthesis, comparison, classification, systematic approach, as well as theoretical generalization and modeling were used in the work.

Field of application. The developed model of integrated management and practical recommendations can be used by enterprises of various forms of ownership, public authorities, and critical infrastructure organizations to increase the effectiveness of the information security system by forming a mature security culture of personnel in the conditions of wartime challenges and hybrid work organization.

Keywords: INFORMATION SECURITY, PERSONNEL BEHAVIOR MANAGEMENT, INFORMATION SECURITY CULTURE, HUMAN FACTOR, MARTIAL LAW, HYBRID WORK, INTEGRATED MANAGEMENT, SECURE BEHAVIOR.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі кіберзагрози набувають дедалі складніших форм, а людський фактор продовжує залишатися найвразливішою ланкою системи інформаційної безпеки підприємств. Особливо гостро ця проблема проявляється в Україні, де поєднання воєнного стану та масового переходу на гібридну форму роботи суттєво розширило поверхню атаки, посилило психологічне навантаження працівників і призвело до зростання кількості помилок, порушень політики безпеки та успішних соціально-інженерних атак.

Актуальність дослідження полягає в необхідності переходу від традиційного технічного підходу до інформаційної безпеки до комплексного управління поведінкою персоналу з урахуванням специфічних умов воєнного стану та гібридної роботи. Формування зрілої культури інформаційної безпеки через системне поєднання психологічних, організаційних та технічних методів дозволяє не лише знижувати ризики, пов’язані з людським фактором, але й забезпечувати стійкість організацій до сучасних динамічних кіберзагроз у тривалих кризових умовах

З огляду на зазначене, дослідження та удосконалення методів управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану та гібридної роботи є вкрай актуальним науковим і практичним завданням.

Мета роботи полягає в удосконаленні методів управління поведінкою персоналу у сфері інформаційної безпеки з урахуванням умов воєнного стану та гібридної форми роботи.

Об’єкт дослідження **–** процес управління поведінкою персоналу в системі інформаційної безпеки підприємства.

Предмет дослідження – методи та технології управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану та гібридної роботи.

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

1. Проаналізувати теоретичні засади управління поведінкою персоналу у сфері інформаційної безпеки, виявити ключові проблеми, сучасні підходи, компоненти та чинники впливу.

2. Дослідити стан управління поведінкою персоналу в умовах воєнного стану та гібридної роботи, оцінити ефективність застосовуваних методів та виявити основні проблеми їх впровадження.

3. Розробити модель комплексного управління поведінкою персоналу та надати практичні рекомендації щодо її впровадження в умовах воєнного стану та гібридної форми роботи.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі у роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу, також теоретичне узагальнення та моделювання.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу впровадити модель комплексного управління та інші практичні рекомендації, які можуть бути використані підприємствами різних форм власності, органами державної влади та організаціями критичної інфраструктури для підвищення рівня культури інформаційної безпеки персоналу, зниження ризиків, пов’язаних з людським фактором, та підвищення загальної кіберстійкості в умовах воєнних викликів

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

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Проблеми управління поведінкою персоналу та формування культури інформаційної безпеки в організації

Однією з найбільш стійких характеристик сучасного ландшафту кіберзагроз є домінуюча роль людського фактора. За даними Verizon Data Breach Investigations Report (DBIR) 2025 [1], понад 22 000 інцидентів та 12 195 підтверджених витоків даних, людський елемент (помилки, соціальна інженерія або зловмисне використання) брав участь у 60 % усіх порушень безпеки. Цей показник залишається стабільно високим протягом останніх років.

Аналогічні висновки містить Proofpoint Human Factor 2025 [2]: атаки, що базуються на соціальній інженерії, становлять значну частку загроз. Зокрема, чиста соціальна інженерія присутня у 25 % кампаній APT. Зростає використання URL-based phishing (посилання застосовуються в чотири рази частіше, ніж вкладення), smishing, QR-кодів та ClickFix-технік. Окремо зазначається, що складність кіберпростору посилюється саме через людський фактор: працівники стають головною мішенню через розширення поверхні атаки (гібридна робота, використання штучного інтелекту та хмарних сервісів).

Одним із найбільш ефективних механізмів реалізації соціально-інженерних атак є маніпулювання емоційним станом працівника. Зловмисники свідомо використовують базові людські емоції та психологічні тригери, щоб знизити критичне мислення та спонукати до небезпечних дій (перехід за посиланням, відкриття вкладення, розголошення конфіденційної інформації) На рисунку 1.1 наведено основні емоційні важелі, які найчастіше експлуатують кіберзлочинці в сучасних атаках

Діаграма ілюструє п’ять ключових емоційно-психологічних векторів впливу:

- Страх — створення панічного настрою та відчуття неминучої загрози;
- Цікавість — спонукання до пошуку інформації;
- Авторитет — використання статусу керівника чи офіційної установи;
- Нагальність — створення відчуття дефіциту часу;
- Винагорода — спокуса швидкого отримання грошей чи приємного сюрпризу.

Рис. 1.1 Використання емоцій як психологічний інструментарій зловмисника в соціальній інженерії

В Україні ситуація ще гостріша через гібридну війну. За даними Державної служби спеціального зв’язку та захисту інформації (Держспецзв'язку) та CERT-UA [3], у 2024 році було зафіксовано 4315 кіберінцидентів — зростання на 70 % порівняно з 2023 роком. У 2025 році CERT-UA обробила майже 6000 інцидентів. Частка інцидентів, пов’язаних з людським фактором (фішинг, компрометація облікових даних, помилки конфігурації), за оцінками експертів, коливається в межах 55–72 %. Найчастіше під прицілом кібератак стають державні органи, енергетика, телекомунікації, медицина та оборонна сфера.

Особливо небезпечними стали сучасні тенденції 2023–2026 років:

- Масштабне використання генеративного AI (Generative AI) для створення персоналізованих фішингових кампаній;
- Використання діпфейків у голосових та відеодзвінках для компрометації співробітників через пошту (Business Email Compromise);
- Зростання неавторизованого IT та порушень політики через гібридну роботу;
- Втома від постійних тренінгів та когнітивне перевантаження працівників.

Людський фактор залишається не просто «слабкою ланкою», а головним вектором реалізації кіберзагроз. Технічні засоби захисту (фаерволи, антивіруси, мультифакторна автентифікація) часто обходять саме через передбачувану поведінку людини.

Одним із ключових наслідків впливу людського фактора на інформаційну безпеку є значне розширення поверхні атаки організації. Найбільший внесок вносять перехід на гібридну форму роботи (32 %), використання хмарних сервісів (28 %) та впровадження технологій штучного інтелекту (25 %). Таке поєднання факторів суттєво збільшує кількість потенційних векторів атак і ускладнює захист інформації.

Як показано на рисунку 1.2, таке поєднання факторів суттєво збільшує кількість потенційних векторів атак і ускладнює захист інформації.

Рис. 1.2. Основні фактори розширення поверхні атаки в умовах гібридної роботи та цифрової трансформації

Це підтверджує необхідність переходу від переважно технічного підходу до комплексного управління поведінкою персоналу та подальшого формування

зрілої культури інформаційної безпеки, що, у свою чергу, зумовлює застосування комплексних психологічно-організаційних методів.

Для глибокого розуміння сутності досліджуваної проблеми та подальшого аналізу необхідно чітко визначити ключові концептуальні категорії:

1. Під управлінням поведінкою персоналу у сфері інформаційної безпеки розуміється системний, цілеспрямований процес впливу на знання, ставлення, мотивацію, навички та реальну поведінку працівників з метою забезпечення дотримання вимог політики інформаційної безпеки та мінімізації людських ризиків. Воно включає як мотиваційні, так і контрольні механізми, що дозволяють трансформувати бажану поведінку в стійку звичку.

2. Культура інформаційної безпеки (Information Security Culture) є одним із центральних понять. Згідно з A.D Veiga (2020) [4], культура інформаційної безпеки — це сукупність спільних цінностей, переконань і моделей поведінки працівників, при яких безпека стає невід'ємною частиною організаційної культури. M. Alshaikh (2020) [5], доповнює це визначення, наголошуючи на контекстуалізації поведінки людини для дотримання політики безпеки через регулярну комунікацію, навчання та підвищення обізнаності.

3. Поведінковий ризик (Behavioral Risk) — це потенційна загроза інформаційній безпеці, що виникає внаслідок дій, бездіяльності або помилок людини. Він охоплює як ненавмисні помилки (через незнання чи втомленість), так і свідомі порушення (зловмисні інсайдерські дії). Поведінковий ризик є частиною загального ландшафту ризиків організації і часто стає основним вектором реалізації кіберзагроз, оскільки легко обходить технічні засоби захисту.

4. Дотримання вимог безпеки (Security Compliance) — це ступінь відповідності реальної поведінки працівників встановленим політикам, процедурам, стандартам і нормативним вимогам у сфері інформаційної безпеки. Воно вимірюється не лише формальним виконанням правил, а й рівнем внутрішньої мотивації та усвідомленого ставлення до безпеки. Високий рівень

безпеки свідчить про зрілу культуру ІБ, тоді як низький — про наявність значних поведінкових ризиків

Чітке розмежування цих понять дозволяє перейти від опису проблем до аналізу чинників, що формують поведінку персоналу, та розробки ефективних методів управління. Основні поняття у сфері управління поведінкою персоналу ІБ порівняно в таблиці 1.1.

Таблиця 1.1

Порівняння ключових понять у сфері управління поведінкою персоналу ІБ

Поняття	**Визначення**	**Рівень управління**
Управління поведінкою персоналу	Системний процес впливу на знання, ставлення, мотивацію, навички та реальну поведінку працівників з метою підвищення security compliance	Організаційно-управлінський рівень
Культура інформаційної безпеки	Сукупність спільних цінностей, переконань, норм і моделей поведінки, при яких безпека стає «способом мислення» організації	Організаційний / культурологічний рівень
Поведінковий ризик	Потенційна загроза інформаційній безпеці, що виникає внаслідок дій, бездіяльності або помилок людини	Ризик-орієнтовний рівень
Дотримання вимог безпеки	Ступінь відповідності реальної поведінки працівників встановленим політикам, процедурам і стандартам ІБ	Операційний / поведінковий рівень

Управління поведінкою персоналу у сфері інформаційної безпеки стикається з низкою системних проблем, які суттєво знижують загальну ефективність захисту інформації.

Найпоширенішою проблемою залишається низька обізнаність та недостатні практичні навички працівників. Незважаючи на проведення

регулярних тренінгів, значна частина співробітників не здатна ефективно розпізнавати сучасні загрози.

Другою критично важливою проблемою є відсутність внутрішньої мотивації. Багато працівників сприймають заходи інформаційної безпеки як бюрократичну перешкоду, яка заважає виконанню основних робочих завдань. Безпека розглядається як «обов'язок IT-відділу», а не як спільна відповідальність. У результаті формується формальне ставлення до політик: вимоги виконуються лише під контролем, а в реальних ситуаціях перевага віддається зручності. Це призводить до постійних порушень — від використання слабких паролів до передачі конфіденційних даних через незахищені канали.

Значно ускладнює ситуацію опір організаційним змінам. Впровадження нових політик, інструментів контролю чи посилення вимог часто зустрічає пасивний або активний спротив. Особливо схильні до цього працівники старшого покоління та ті, хто тривалий час працює в організаціях зі слабкою культурою безпеки. Зміни сприймаються не як інвестиція в безпеку, а як додаткове навантаження.

Суттєвого загострення проблем спричинив перехід на гібридну та віддалену форму роботи. Розширення периметра безпеки створило нові вразливості: використання домашніх мереж, особистих пристроїв (BYOD), незахищених Wi-Fi та хмарних сервісів. За даними досліджень 2025 року [6], insider threats у компаніях з гібридною моделлю роботи зросли на 58 %. Працівники частіше застосовують неавторизовані IT програми, ігнорують VPN і пропускають оновлення безпеки, що значно підвищує рівень ризиків.

Окремим небезпечним викликом став вплив сучасних технологій, зокрема генеративного AI та діпфейків. Штучний інтелект дозволяє створювати високоякісні персоналізовані фішингові кампанії, голосові клони керівників та реалістичні відеодзвінки. Працівники все важче відрізняють справжнє від підробленого, що різко підвищує ефективність соціальної інженерії.

Усі зазначені проблеми взаємопов’язані та утворюють замкнене коло: низька мотивація призводить до слабкого дотримання вимог, що, у свою чергу, генерує нові інциденти та посилює опір змінам. Традиційні підходи у вигляді разових тренінгів і технічного контролю вже не дають бажаного ефекту. Тому необхідним є перехід до комплексного, поведінково-орієнтованого управління, яке враховує психологічні особливості працівників, організаційний контекст та сучасні технологічні виклики.

Для систематизації факторів, що зумовлюють проблеми управління поведінкою персоналу у сфері інформаційної безпеки, було проведено їх групування за чотирма основними категоріями.

Шкала оцінки сили впливу має такий зміст:

- Дуже висока — чинники, які мають вирішальний (домінуючий) вплив на виникнення та розвиток проблем управління поведінкою персоналу та цільового рівня безпеки;
- Висока — чинники, що суттєво впливають на поведінку працівників і значною мірою зумовлюють поведінкові ризики;
- Середня–висока — чинники, вплив яких є помітним, але менш визначальним порівняно з попередніми групами, і часто проявляється у поєднанні з іншими факторами.

Результати групування факторів за категоріями та оцінкою сили їхнього впливу наведено в таблиці 1.2.

Таблиця 1.2.

Причини виникнення проблем управління поведінкою персоналу у сфері інформаційної безпеки

Група причин	**Основні фактори**	**Прояви в організаціях**	**Сила впливу**
Індивідуально-психологічні	Когнітивні упередження, психологічна втома	Переоцінка власної захищеності, ігнорування загроз, вибір зручності замість безпеки	Висока

Продовження таблиці 1.2.

Група причин	**Основні фактори**	**Прояви в організаціях**	**Сила впливу**
Організаційні	Слабке лідерство, недостатнє фінансування, відсутність мотивації та покарань, низька інтеграція ІБ у стратегію компанії	Формальне ставлення до політик, сприйняття безпеки як «справи ІТ-відділу»	Дуже висока
Технологічні	Складність інструментів, швидке впровадження нових технологій без оновлення політик	Використання shadow IT, ігнорування оновлень, обхід складних засобів захисту	Висока
Зовнішні	Гібридна війна, цифрова трансформація, швидка еволюція загроз, діпфейки	Зростання персоналізованих атак, розширення поверхні атаки через гібридну роботу	Середня–висока

Як результат організаційні недоліки посилюють психологічні бар’єри, які, у свою чергу, знижують ефективність технологічних заходів. Без усунення цих корінних причин навіть найсучасніші технічні рішення не забезпечать необхідного рівня захисту інформації.

Таким чином, проблеми управління поведінкою персоналу призводять до тяжких наслідків на всіх рівнях діяльності організації:

- Фінансові втрати є найбільш відчутними. За даними IBM Cost of a Data Breach Report 2025 [7], середня вартість одного витоку даних у світі становить 4,44 млн дол. США. У компаніях, де значну роль відіграв людський фактор, витрати часто суттєво перевищують середні значення через тривале розслідування та відновлення.
- Репутаційні наслідки можуть бути ще руйнівнішими. Втрата довіри клієнтів, партнерів та інвесторів призводить до відпливу клієнтів і падіння ринкової вартості компанії. Негативний медійний резонанс від публічних витоків даних триває роками.

- Юридичні наслідки стають дедалі жорсткішими. В Україні керівництво несе персональну відповідальність відповідно до Законів «Про кібербезпеку» та «Про захист інформації в інформаційно-комунікаційних системах». На міжнародному рівні діють GDPR та NIS2, штрафи за якими сягають десятків мільйонів євро.
- Операційні наслідки включають зупинку бізнес-процесів, втрату доступу до критичних систем і значні витрати на відновлення. У державному секторі України такі інциденти безпосередньо впливають на роботу лікарень, шкіл, логістики та державних реєстрів, загрожуючи національній безпеці.
- Стратегічні наслідки проявляються у втраті конкурентних переваг, ускладненні цифрової трансформації та зниженні інвестиційної привабливості. Організації зі слабкою культурою ІБ стають легкою мішенню для конкурентів і державних акторів.

Таким чином, аналіз проблематики людського фактора, ключових понять, основних проблем, їх причин та наслідків переконливо доводить: традиційний технічний підхід до інформаційної безпеки є недостатнім у сучасних умовах. Технічні засоби захисту легко обходять через передбачувану поведінку людини. Тому необхідним є перехід від реактивної стратегії «захисту периметра» до проактивної стратегії управління поведінкою персоналу.

Сильна культура інформаційної безпеки виконує роль «людського firewall» — останньої та найважливішої лінії оборони, яка працює навіть тоді, коли технічні засоби дають збій. Ефективне управління поведінкою персоналу дозволяє не лише підвищити рівень відповідності стандартам безпеки, а й трансформувати працівників із потенційного джерела ризику в активний елемент системи захисту.

Людський фактор залишається головною причиною більшості інцидентів інформаційної безпеки. Існуючі проблеми мають системний, багатофакторний характер і призводять до значних фінансових, репутаційних, юридичних, операційних та стратегічних наслідків. Подолати їх можливо лише за умови

впровадження комплексних психолого-організаційних методів управління поведінкою персоналу та формування зрілої культури інформаційної безпеки.

1.2. Аналіз сучасних підходів до управління поведінкою персоналу в контексті інформаційної безпеки

Однією з ключових особливостей сучасного ландшафту інформаційної безпеки є розуміння того, що технічні засоби захисту, якими б досконалими вони не були, не здатні повністю усунути ризики, що походять від людського фактора. У зв'язку з цим виникає об'єктивна необхідність переходу від переважно технічного підходу до комплексного управління поведінкою працівників як до самостійного та стратегічно важливого напряму забезпечення кіберстійкості організації.

Для цього потрібно провести системний аналіз сучасних теоретичних моделей та практичних підходів до управління поведінкою персоналу в контексті інформаційної безпеки, виявлення їх сильних і слабких сторін, а також визначення місця цих методів у загальній системі управління інформаційною безпекою організації.

Теоретичною основою сучасних досліджень управління поведінкою персоналу в сфері інформаційної безпеки є низка психологічних і соціологічних моделей, адаптованих до контексту кіберзагроз.

Найбільш впливовими серед них залишаються:

1. Теорія запланованої поведінки (TPB) - розроблена I. Ajzen у 1991 році [8], пояснює, що намір людини виконати певну поведінку (у нашому випадку — дотримання вимог ІБ) визначається трьома основними чинниками: ставленням до поведінки, суб'єктивними нормами та сприйнятим поведінковим контролем. У сфері інформаційної безпеки модель TPB широко застосовується для прогнозування наміру працівників дотримуватися політик безпеки.

2. Теорія мотиваційного захисту (PMT) - запропонована R. Rogers у 1975 році та розвинена в 1983-му [9], є найбільш цитованною моделлю в

дослідженнях інформаційної безпеки. Згідно з PMT, захисна поведінка визначається двома основними процесами когнітивної оцінки: оцінкою загрози , що включає сприйняття серйозності загрози та власної вразливості, а також оцінкою копінгу, яка охоплює сприйняту ефективність захисної реакції, само-ефективність та вартість захисних дій. Якщо працівник оцінює загрозу як серйозну, а себе — здатним ефективно їй протидіяти за прийнятних витрат, імовірність здійснення захисної поведінки суттєво зростає. Звіт ZHan et al. (2025) [10] підтверджує високу прогностичну силу моделі PMT у контексті фішингу, дотримання парольної гігієни та використання багатофакторної автентифікації. Модель особливо ефективна для пояснення впливу страхітливих повідомлень, а також для аналізу реакції працівників на сучасні загрози, такі як діпфейки та атаки з використанням генеративного штучного інтелекту

3. Теорія соціального розпізнання (SCT) - Альберта Бандури акцентує увагу на взаємодії особистісних факторів, поведінки та середовища. Ключовим конструктом є само-ефективність — віра людини у власну здатність виконувати захисні дії. У сфері кібербезпеки SCT пояснює, як спостереження за поведінкою колег і керівництва яка в результаті формує культуру безпеки. Дослідження показують, що високий рівень само-ефективності працівників суттєво знижує кількість порушень політики безпеки.

Окрім базових моделей, у дослідженнях застосовуються й інші теоретичні конструкти:

- Модель прийняття технологій (TAM) — пояснює прийняття працівниками нових засобів захисту;
- Теорія стримування (Deterrence Theory) та Загальна теорія стримування (General Deterrence Theory) — акцентують на ролі покарань і санкцій;
- Теорія рутинної діяльності (Routine Activity Theory) — розглядає умови, за яких виникають можливості для порушень.

Більш детальна порівняльна характеристика основних моделей наведена в таблиці 1.3

Таблиця 1.3.

Порівняння ключових теоретичних моделей управління поведінкою в ІБ

Модель	**Автор / Рік**	**Основні конструкти**	**Застосування в ІБ**	**Сильні сторони**	**Обмеження**
TPB	Ajzen, 1991	Ставлення, суб'єктивні норми, сприйнятий поведінковий контроль	Дотримання політик, парольна гігієна	Простота, висока емпірична валідність	Недооцінює емоції, страх та інтуїтивні реакції
PMT	Rogers, 1983	Оцінка загрози, оцінка копінгу	Фішинг, використання MFA, антивірусна поведінка	Добре пояснює реакцію на загрози та мотивацію захисту	Ігнорує соціальний тиск і організаційний контекст
SCT	Bandura, 1986	Само-ефективність, навчання через спостереження	Формування культури безпеки, навчання через спостереження	Враховує соціальне середовище та формування звичок	Складна для емпіричної перевірки та кількісного вимірювання
TAM	Davis, 1989	Сприйнята корисність, сприйнята легкість використання	Прийняття нових засобів захисту та технологій	Добре працює з технологічними інноваціями	Не враховує загрози та емоційний компонент

Адаптація цих моделей до сфери інформаційної безпеки відбувається через їх інтеграцію. Наприклад, Ifinedo (2012) [11] поєднав TPB і PMT, створивши потужнішу інтегровану модель. Таким чином, теоретичні моделі надають науковий фундамент для розуміння механізмів формування відповідності безпеки

Сучасні підходи до управління поведінкою персоналу у сфері інформаційної безпеки можна класифікувати за домінуючим типом впливу на

чотири основні групи: технічні, організаційні, психологічні та комбіновані. Така класифікація відображає еволюцію поглядів від суто технологічного захисту до комплексного психолого-організаційного управління.

1. Технічні підходи базуються на використанні технологічних інструментів для контролю та корекції поведінки працівників. До них належать системи поведінкової аналітики (аналіз поведінки користувачів), автоматизовані політики доступу (DLP-системи, UEBA), примусова багатофакторна автентифікація (MFA) та інструменти моніторингу (SIEM з AI-модулями).

- Перевагою цих підходів є висока об’єктивність і можливість реагування на інциденти в режимі реального часу (наприклад, виявлення аномального доступу до даних). Однак головним недоліком є те, що вони часто сприймаються працівниками як тотальний контроль, що знижує мотивацію та провокує обхід систем з неавторизованим ІТ. Крім того, технічні рішення не формують внутрішньої культури безпеки, а лише обмежують можливості порушення.

2. Організаційні підходи акцентують увагу на формуванні правил, норм і структур управління. Центральне місце посідають політики інформаційної безпеки, стандарти ISO/IEC 27001:2022 (особливо Annex A.6 «Людські контролі») [12], ролі CISO. Важливими елементами є регулярні аудити відповідності, система мотивації та дисциплінарної відповідальності.

- Ці підходи ефективні для створення єдиного організаційного поля, але часто залишаються формальними: працівники знають правила, проте не завжди їх дотримуються. Дослідження показують, що без підтримки психологічних механізмів організаційні заходи дають лише короткостроковий ефект.

3. Психологічні підходи спрямовані на зміну внутрішніх установок, мотивації та звичок працівників. Найпоширенішими інструментами є програми підвищення обізнаності, гейміфікація, nudge-технології (м’яке підштовхування до безпечної поведінки) та мотиваційні програми.

- Ці методи ґрунтуються на теоріях TPB, PMT та SCT і спрямовані на формування внутрішньої мотивації. Їхня сильна сторона — висока залученість персоналу та довгостроковий ефект. Водночас психологічні підходи вимагають значних ресурсів і регулярного оновлення, оскільки ефект від одноразових тренінгів швидко зникає).

4. Комбіновані (інтегровані) підходи вважаються найбільш перспективними на сьогодні. Вони поєднують технічні, організаційні та психологічні інструменти в єдину систему.

- Прикладом є моделі Рамка культури безпеки [5], які інтегрують лідерство, технології, навчання та постійний моніторинг. Саме комбіновані підходи дозволяють досягти синергетичного ефекту та адаптуватися до сучасних викликів — гібридної роботи, генеративного AI та діпфейк-атак.

Еволюцію підходів до управління поведінкою персоналу можна розглянути на основі цих трьох етапів:

1. Awareness 1.0 (до 2015 р.) — переважно разові тренінги та плакати;
2. Awareness 2.0 (2016–2022) — інтерактивне навчання, симуляції фішингу, базова гейміфікація;
3. Behaviour Management 3.0 (2023–2026) — постійна обізнаність, поведінкова аналітика, AI-персоналізоване навчання, nudge-технології та інтеграція з системами управління ризиками.

Комбіновані підходи поступово витісняють попередні моделі, оскільки лише вони здатні забезпечити стійкий рівень відповідності безпеки в умовах швидкозмінного кіберландшафту.

В результаті класифікація цих підходів демонструє, що найбільш ефективними є інтегровані рішення, які поєднують сильні сторони технічних, організаційних та психологічних методів.

Тенденції 2024–2026 років свідчать про зростання інтересу до впливу AI на поведінку персоналу та застосування поведінкової науки. Водночас залишаються суттєві прогалини в дослідженнях:

- Недостатнє емпіричне вивчення ефективності комбінованих моделей саме в українських організаціях під час воєнного стану;
- Слабке висвітлення впливу гібридної роботи та психологічної втоми працівників на рівень відповідності;
- Обмежена кількість досліджень, які б оцінювали довгостроковий ефект від програм управління поведінкою;
- Фрагментарність вивчення адаптації міжнародних моделей (ISO 27001, NIST) до національного контексту гібридної війни.

Таким чином, міжнародна наукова база є достатньо розвиненою, тоді як українські дослідження потребують подальшого розвитку, особливо в емпіричній площині та з урахуванням воєнних реалій. Виявлені прогалини обґрунтовують необхідність порівняльного аналізу існуючих підходів та адаптації міжнародних підходів до управління поведінкою персоналу з урахуванням українських реалій воєнного стану

1.3. Компоненти та чинники, що впливають на поведінку персоналу у сфері інформаційної безпеки

Поведінка персоналу у сфері інформаційної безпеки є складним, багатокомпонентним явищем. Для ефективного управління необхідно чітко розуміти її структурні елементи. У науковій літературі найбільш поширеним є п’ятикомпонентний підхід, що включає знання, ставлення, навички, мотивацію та звички.

- Знання (awareness) становить когнітивну основу поведінки. Це рівень інформованості працівника про існуючі кіберзагрози, правила політики безпеки, потенційні наслідки порушень та способи захисту інформації. Водночас, згідно з безпековою поведінковою моделлю компанії SoSafe (2025) [13], високий рівень знань сам по собі має обмежений вплив на рівень безпеки, оскільки ефективна поведінка залежить також від контексту, мотивації та інших факторів.

- Ставлення (attitude) відображає емоційну та оціночну позицію працівника щодо інформаційної безпеки. Позитивне ставлення проявляється в сприйнятті заходів безпеки не як перешкоди, а як інвестиції в спільну безпеку. Навпаки, негативне ставлення («безпека — це проблема IT-відділу») є одним з головних бар'єрів дотримання вимог безпеки. Ставлення працівника до цих процесів є ключовим медіатором між знаннями та реальною поведінкою.
- Навички (skills) — це практична здатність працівника виконувати конкретні захисні дії: розпізнавати фішинг, правильно налаштовувати MFA, безпечно працювати з конфіденційними даними, використовувати інструменти захисту. Відмінність між знаннями та навичками критична: працівник може знати теорію, але не вміти застосовувати її в стресовій ситуації (наприклад, під час атаки з використанням діпфейків).
- Мотивація (motivation) є рушійною силою поведінки. Розрізняють внутрішню мотивацію (усвідомлення особистої відповідальності) та зовнішню (система заохочень і покарань). Найефективнішою є саме внутрішня мотивація, коли безпека стає частиною професійної ідентичності працівника. За моделлю da Veiga (2020) [4], мотивація є найважливішим компонентом для переходу від декларативної до реальної compliance.
- Звички (habits) — це автоматична, малоусвідомлена безпечна поведінка, яка формується внаслідок повторення. Коли працівник автоматично перевіряє URL перед переходом за посиланням або завжди блокує екран при виході з робочого місця, можна говорити про сформовану культуру безпеки на рівні звички. Формування звичок є найвищим рівнем зрілості поведінки.

Знання формують ставлення, ставлення впливає на мотивацію, мотивація спонукає до розвитку навичок, а регулярне повторення навичок перетворює їх на звички. Порушення в будь-якому компоненті (наприклад, високі знання при низькій мотивації) призводить до розриву між декларативною та фактичною поведінкою.

Таким чином, усі п'ять компонентів тісно взаємопов'язані та утворюють єдину систему. Ефективне управління поведінкою персоналу повинно впливати

не на один, а на всі компоненти одночасно. Це створює основу для подальшого аналізу чинників, що посилюють або послаблюють кожен із цих компонентів.

Поведінка персоналу у сфері інформаційної безпеки формується під впливом численних чинників, які можна поділити на дві великі групи: внутрішні (індивідуально-психологічні) та зовнішні. Розуміння їхньої природи, сили впливу та взаємодії є необхідною передумовою для розробки ефективних методів управління.

1. Внутрішні (індивідуально-психологічні) чинники походять безпосередньо від особистості працівника і найважче піддаються зовнішньому впливу.

- Серед них ключову роль відіграють особистісні риси (Big Five: добросовісність, емоційна стабільність, відкритість досвіду). Дослідження показують, що високий рівень доброчесності позитивно корелює з дотриманням політик безпеки.
- Когнітивні упередження суттєво спотворюють раціональну оцінку ризиків. Найпоширенішими є:
  - ➢ переоцінка власної захищеності: «зі мною цього не станеться»
  - ➢ пошук підтвердження своїх переконань
  - ➢ втома від прийняття рішень, через яку працівник обирає найпростіший, але небезпечний варіант)
- Само-ефективність (self-efficacy) за Bandura є одним із найсильніших предикторів безпечної поведінки. Працівник з високою само-ефективністю вірить у свою здатність розпізнати фішинг чи правильно налаштувати MFA і, відповідно, частіше виконує захисні дії.
- Віковий (generational) фактор також має суттєвий вплив. Покоління Z і Мілленіали частіше використовують неавторизовані IT програми і легше приймають нові технології, але гірше дотримуються формальних правил. Працівники старшого віку більш схильні до дотримання інструкцій, але повільніше опановують нові інструменти захисту.

2. Зовнішні чинники поділяються на організаційні, технологічні та соціокультурні.

- Організаційні чинники є найбільш керованими з боку керівництва. До них належать корпоративна культура, стиль лідерства, система мотивації та контролю, рівень підтримки з боку топ-менеджменту. Сильна організаційна підтримка може компенсувати слабкі індивідуальні характеристики працівників.
- Технологічні чинники визначають, наскільки інструменти безпеки є зручними у використанні. Якщо інструмент надто складний, працівник обирає зручність замість безпеки. Сучасні AI-системи можуть як полегшувати (автоматичні підказки, персоналізоване навчання), так і ускладнювати ситуацію (збільшення кількості сповіщень і втоми).
- Соціокультурні чинники особливо актуальні для України. Серед них:

➢ вплив воєнного стану (постійний стрес, психологічна втома, зниження уваги);

➢ національні особливості (вищий рівень довіри до «своїх» у порівнянні з формальними правилами);

➢ суспільні норми та культурні цінності.

Для систематизації чинників за рівнем впливу та керованістю сформована таблиця 1.4.

Для систематизації чинників, що впливають на поведінку персоналу у сфері інформаційної безпеки, їх було класифіковано за двома ключовими параметрами: ступенем впливу та рівнем керованості. Такий підхід дозволяє не лише виявити найбільш значущі фактори, але й визначити пріоритети управлінського втручання.

Ступінь впливу відображає силу та стабільність впливу чинника на формування поведінкових ризиків і рівень відповідності безпеки. Оцінка здійснювалася за якісною шкалою:

- Дуже висока — чинники, які мають домінуючий, системоутворюючий вплив на поведінку працівників;

- Висока — чинники, що суттєво впливають на рівень дотримання вимог інформаційної безпеки;
- Середня–висока — чинники, вплив яких є помітним, але проявляється переважно в поєднанні з іншими факторами.

Рівень керованості показує, наскільки організація може впливати на даний чинник через управлінські інструменти. Шкала включає:

- Висока — чинники, які піддаються безпосередньому і відносно швидкому управлінському впливу;
- Середня–висока — чинники, що піддаються впливу, але вимагають значних ресурсів і часу;
- Низька–середня та Низька — чинники, які важко або практично неможливо змінити в короткостроковій перспективі.

Класифікація чинників за ступенем впливу та рівнем керованості наведена в таблиці 1.4.

Таблиця 1.4.

Класифікація чинників впливу на поведінку персоналу в ІБ

Група чинників	**Конкретні чинники**	**Ступінь впливу**	**Керованість**	**Приклади прояву**
Внутрішні	Когнітивні упередження, само-ефективність, особистісні риси	Висока	Низька	Упередження оптимізму, втома від прийняття рішень
Організаційні	Лідерство, корпоративна культура, мотивація	Дуже висока	Висока	«Тон зверху», система заохочень та мотивації
Технологічні	Зручність інструментів, AI-підтримка	Висока	Середня–висока	Компроміс «зручність — безпека», поведінкова аналітика
Соціокультурні	Війна, національні норми, generational особливості	Середня–висока	Низька–середня	Психологічна втома, тіньові IT-системи в умовах гібридної роботи

Аналіз таблиці показує, що найсильніший вплив мають організаційні чинники, які водночас є найбільш керованими. Саме тому керівництво організації має ключову роль у формуванні безпечної поведінки. Внутрішні чинники важко змінити напряму, але на них можна опосередковано впливати через зовнішні (навчання, культура, технології).

Таким чином, ефективне управління поведінкою вимагає комплексного врахування всіх груп чинників. Особливу увагу необхідно приділяти організаційним чинникам, оскільки вони здатні суттєво посилювати або послаблювати вплив внутрішніх особливостей працівників.

Висновки до розділу 1

У цьому розділі було розглянуто теоретичні засади управління поведінкою персоналу у сфері інформаційної безпеки. Було визначено та розмежовано основні концептуальні категорії: управління поведінкою персоналу, культура інформаційної безпеки, поведінкові ризики та відповідності безпеки. Виявлено системний характер проблем (низька мотивація, опір змінам, вплив гібридної роботи та сучасних технологій), їх причини (індивідуально-психологічні, організаційні, технологічні та зовнішні) та тяжкі наслідки для організації (фінансові, репутаційні, юридичні, операційні та стратегічні). Зроблено висновок про необхідність переходу від технічного підходу до комплексного психолого-організаційного управління поведінкою персоналу.

За результатами дослідження проведено аналіз сучасних теоретичних моделей та практичних підходів до управління поведінкою. Розглянуто ключові психологічні теорії — Теорії запланованої поведінки (TPB), Теорія мотиваційного захисту (PMT) та Теорія соціального розпізнання (SCT), а також їх адаптацію до сфери інформаційної безпеки. Здійснено класифікацію методів управління на технічні, організаційні, психологічні та комбіновані. Показано, що найбільш перспективними є інтегровані (комбіновані) підходи, які

забезпечують синергетичний ефект. Виявлено прогалини в дослідженнях, зокрема недостатнє вивчення ефективності таких моделей в українських організаціях в умовах воєнного стану.

Окрім цього було розглянуто компоненти поведінки персоналу (знання, ставлення, навички, мотивація, звички) та чинники, що на них впливають. Було встановлено, що найважливішими для формування безпечної поведінки є внутрішня мотивація та звички, а серед чинників найбільший вплив мають організаційні.

Людський фактор вимагає системного, комплексного управління, яке поєднує психологічні, організаційні та технічні інструменти. Сильна культура інформаційної безпеки є ключовим елементом забезпечення кіберстійкості організації в сучасних умовах.

РОЗДІЛ 2. АНАЛІЗ СТАНУ УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Особливості застосування методів управління поведінкою персоналу в умовах воєнного стану та гібридної роботи

Умови воєнного стану та поширення гібридної форми роботи суттєво трансформували контекст, у якому формується поведінка персоналу у сфері інформаційної безпеки. Ці фактори впливають не лише на технічні аспекти захисту, а й на психологічний стан працівників, їхню мотивацію та здатність дотримуватися встановлених правил.

Воєнний стан створює низку психологічних і організаційних викликів, які безпосередньо позначаються на поведінці працівників. Серед них:

- Психологічна втома та хронічний стрес — постійне перебування в стані підвищеної тривоги знижує когнітивні функції, увагу та здатність до прийняття зважених рішень.
- Інформаційне перевантаження — велика кількість повідомлень, попереджень і новин ускладнює виділення дійсно важливих сигналів щодо кіберзагроз.
- Невизначеність і втрата контролю — працівники часто відчувають безсилля, що знижує мотивацію дотримуватися правил, які здаються менш пріоритетними порівняно з фізичною безпекою.
- Зниження рівня довіри та психологічної безпеки — в умовах війни посилюється підозрілість, що може впливати як на повідомлення про інциденти, так і на ставлення до технічних засобів контролю.

Поєднання воєнного стану з гібридною формою роботи створює додаткові ризики:

- Розширення поверхні атаки — працівники використовують домашні мережі, особисті пристрої та незахищені канали зв’язку.

- Зростання тіньового IT — через технічні обмеження та незручності корпоративних рішень працівники частіше вдаються до несанкціонованих сервісів.
- Знижений рівень контролю — керівництво має обмежені можливості безпосередньо спостерігати за дотриманням правил безпеки.
- Проблеми з мотивацією — в умовах гібридної роботи та війни працівники часто сприймають вимоги безпеки як додаткове навантаження, а не як невід'ємну частину професійної діяльності.

Умови воєнного стану та гібридної роботи по-різному впливають на основні компоненти поведінки.

Для наочності вплив воєнного стану та гібридної роботи на ключові компоненти поведінки наведено в таблиці 2.1.

Таблиця 2.1.

Вплив воєнного стану та гібридної роботи на компоненти поведінки персоналу

Компонент поведінки	**Вплив воєнного стану**	**Вплив гібридної роботи**	**Загальний ефект**
Знання	Зниження здатності засвоювати нову інформацію через втому	Фрагментарне проходження навчання	Помірне зниження
Ставлення	Сприйняття безпеки як менш пріоритетної	Формальне ставлення до правил	Значне зниження
Мотивація	Зниження внутрішньої мотивації	Переважання зовнішньої мотивації	Сильне зниження
Навички	Затруднене застосування навичок у стресових ситуаціях	Зниження частоти практичного застосування	Помірне зниження
Звички	Руйнування сформованих звичок	Складність формування нових звичок	Сильне зниження

Найбільшого негативного впливу зазнають мотивація та звички. Це означає, що традиційні методи, орієнтовані лише на підвищення знань, в умовах воєнного стану та гібридної роботи демонструють обмежену ефективність [14].

Натомість зростає значення заходів, спрямованих на підтримку мотивації, спрощення виконання безпечних дій та створення умов для формування стійких звичок.

Разові та формальні програми підвищення обізнаності в умовах воєнного стану показують низьку ефективність. Психологічна втома та інформаційне перевантаження працівників значно знижують здатність засвоювати новий матеріал. Дослідження та практика українських організацій свідчать, що після проведення традиційного тренінгу рівень обізнаності працівників зростає на короткий період (2–4 тижні), після чого повертається до попередніх показників.

Найбільш проблемними є довгі онлайн-тренінги (понад 30–40 хвилин), які працівники часто формально «проглядають» у фоновому режимі. Ефект від разових форматів ще більше знижується через те, що працівники сприймають безпеку як менш пріоритетну тему порівняно з фізичною безпекою та виживанням.

Організаційні заходи, засновані на формальних політиках та системі покарань, в умовах воєнного стану демонструють обмежену ефективність. По-перше, в умовах стресу та невизначеності працівники часто не здатні повністю дотримуватися всіх правил одночасно. По-друге, жорсткі покарання в період війни можуть сприйматися як несправедливі та ще більше знижувати мотивацію.

Дослідження показують, що в українських організаціях у 2023–2025 роках почастішали випадки, коли працівники свідомо порушували політики безпеки, вважаючи їх «надто бюрократичними» в умовах, коли «йдеться про виживання». Це свідчить про необхідність перегляду балансу між контролем та підтримкою персоналу.

Гейміфікація та nudge-технології в умовах воєнного стану показують суперечливі результати [15]. З одного боку, правильно розроблені nudge-механізми (прості нагадування, спливаючі підказки, спрощені сценарії) можуть бути корисними, оскільки не вимагають значних часових витрат від

працівника. З іншого боку, класична гейміфікація (бали, рейтинги, змагання) часто сприймається працівниками як недоречна в умовах війни.

Найбільш ефективними в українських організаціях виявилися спрощені nudge-механізми, які допомагають працівнику швидко прийняти правильне рішення без додаткового когнітивного навантаження (наприклад, чіткі попередження перед надсиланням файлів на зовнішні адреси).

Для оцінки придатності традиційних методів управління поведінкою персоналу в умовах воєнного стану та гібридної роботи було проведено їх порівняльний аналіз. Результати оцінки представлено в таблиці 2.2.

Шкала оцінки рівня ефективності методів має такий зміст:

- Висока — метод демонструє стійкий позитивний ефект навіть в умовах психоемоційного стресу та гібридної організації праці;
- Середня — метод дає помітний, але нестабільний результат, частково втрачає ефективність під впливом воєнних реалій;
- Низька — метод має обмежений або короткостроковий вплив і суттєво втрачає дієвість в поточних умовах.

Шкала оцінки необхідності адаптації відображає ступінь трансформації, якої потребує метод для збереження ефективності:

- Висока — метод потребує суттєвої модифікації або заміни;
- Середня — метод потребує часткової адаптації;
- Низька–середня — метод відносно стійкий і потребує лише незначних коригувань.

Результати оцінки ефективності традиційних методів управління поведінкою персоналу в умовах воєнного стану та необхідності їх адаптації наведено в таблиці 2.2

Таблиця 2.2.

Ефективність традиційних методів управління поведінкою в умовах воєнного стану

Метод	**Рівень ефективності**	**Основні причини зниження/збереження ефективності**	**Необхідність адаптації**
Разові тренінги з обізнаності	Низька	Психологічна втома, інформаційне перевантаження, формальне ставлення	Висока
Організаційні політики та покарання	Низька–середня	Зниження мотивації, сприйняття покарань як несправедливих	Висока
Гейміфікація	Низька–середня	Недоречність змагань в умовах війни	Висока
Nudge-технології	Середня–висока	Не потребують значних зусиль, допомагають у стресових ситуаціях	Низька–середня

В умовах воєнного стану та гібридної роботи традиційні методи управління поведінкою потребують суттєвої адаптації. Не всі підходи, що добре працювали в мирний час, залишаються ефективними. Найбільшої трансформації потребують методи, орієнтовані на тривале навчання та зовнішній контроль.

Найбільшої адаптації потребують:

- Разові та тривалі тренінги з обізнаності — через знижену здатність працівників засвоювати інформацію в умовах стресу.
- Системи жорсткого технічного контролю (DLP, детальний моніторинг) — через ризик зниження довіри та зростання напруги в колективі.
- Системи покарань за порушення політики — можуть посилювати демотивацію та опір.

Натомість методи, що не потребують значних часових витрат і не створюють додаткового тиску (nudge-технології, короткі мікро-навчання, підтримка лідерства), демонструють кращу адаптивність.

Українські організації, які успішно адаптували методи управління поведінкою, найчастіше використовують такі підходи:

- Короткі мікро-тренінги (3–7 хвилин) замість довгих онлайн-курсів. Такі формати краще сприймаються працівниками та дають вищий рівень запам’ятовування.
- Поєднання тем безпеки з психологічною підтримкою — деякі організації включають у програми безпеки елементи управління стресом та інформаційною гігієною.
- Спрощені nudge-механізми — чіткі, лаконічні нагадування та підказки, які не перевантажують працівника.

Важливо, щоб технології не створювали ефекту «тотального контролю», а допомагали працівнику швидко та правильно діяти.

Для наочної демонстрації динаміки ефективності методів управління поведінкою персоналу було проведено порівняльний аналіз їх результативності у довоєнний період (до 2022 року) та в умовах повномасштабного воєнного стану і гібридної роботи (2023–2026 роки). Результати цього порівняння представлено в таблиці 2.3.

Шкала оцінки ефективності методів є якісною та має такий зміст:

- Висока — метод демонструє значний і стабільний позитивний ефект;
- Середня–висока — метод забезпечує помітний результат, але з певними обмеженнями;
- Середня — метод має помірну ефективність;
- Низька–середня — метод показує нестабільний або слабкий результат.

Таблиця 2.3.

Динаміка ефективності методів управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану

Метод	**Ефективність до 2022 року**	**Ефективність у 2023–2026 роках**	**Основні причини зміни**
Разові програми підвищення обізнаності	Висока	Низька–середня	Психологічна втома, знижена увага
Жорсткий технічний контроль	Середня–висока	Низька–середня	Опір, зниження довіри
Система покарань	Середня	Низька	Демотивація в умовах стресу
Nudge-технології	Середня	Висока	Не потребують зусиль, м’який вплив
Короткі мікро-тренінги	Низька	Висока	Краще сприйняття в умовах втоми
Гейміфікація (змагання)	Висока	Низька–середня	Недоречність в умовах війни

Таким чином, в умовах воєнного стану та гібридної роботи пріоритет змістився від методів зовнішнього контролю та разового навчання до методів, що підтримують працівника, спрощують виконання безпечних дій та враховують його психоемоційний стан.

2.2 Огляд та аналіз застосування методів управління поведінкою персоналу в українських організаціях

В українських організаціях у 2024–2025 роках спостерігається нерівномірне впровадження методів управління поведінкою персоналу. Рівень зрілості та системності цих методів суттєво залежить від розміру організації, галузі та рівня цифрової зрілості.

Програми підвищення обізнаності є найбільш поширеним методом в українських організаціях. За оцінками експертів та результатами галузевих спостережень, понад 70–80 % середніх і великих компаній проводять організаційні чи технічні форми навчання з кібербезпеки [16]. Однак домінуючим форматом залишаються разові онлайн-тренінги та формальне ознайомлення з політиками.

Симуляції фішингових атак та регулярні інтерактивні формати (мікро-навчання, гейміфіковані платформи) використовуються значно рідше — переважно в банках, великих IT-компаніях та іноземних представництвах. У державному секторі та на підприємствах критичної інфраструктури переважає формальний підхід: проведення обов’язкових інструктажів та разових тренінгів без подальшого вимірювання ефекту.

Рівень впровадження технічних засобів контролю поведінки значно варіюється.

- Банки та фінансові установи — найвищий рівень впровадження DLP-систем та елементів UEBA. Багато банків використовують рішення для запобігання витоку даних та моніторингу дій користувачів [17, 18].
- Великі приватні компанії — поступово впроваджують DLP та базовий моніторинг, однак повноцінні UEBA-системи поки що є скоріше винятком.
- Державний сектор та критична інфраструктура — технічний контроль активно розвивається (особливо після 2022 року), однак часто обмежується базовими рішеннями через бюджетні та технічні обмеження.
- Середні та малі підприємства — технічні засоби контролю використовуються рідко, переважно на рівні антивірусного захисту та базових політик доступу.

Організаційні заходи є найбільш формалізованою частиною. Майже всі середні та великі організації мають затверджені політики інформаційної безпеки. Однак на практиці їх виконання часто залишається формальним.

У багатьох компаніях відсутні регулярні аудити відповідності стандартам, а система мотивації та відповідальності за порушення політики або відсутня, або носить декларативний характер. Ролі відповідальних за культуру безпеки впроваджуються переважно в банках та великих технологічних компаніях. У державному секторі акцент робиться на формальному виконанні вимог регуляторів, а не на реальному формуванні поведінки.

Гейміфікація та nudge-технології поки що мають обмежене поширення в українських організаціях. Повноцінні гейміфіковані платформи типу Hoxhunt використовуються переважно в іноземних компаніях та окремих українських банках і великих IT-компаніях [19].

Nudge-технології (м’які підказки в інтерфейсах) впроваджуються точково, найчастіше в рамках DLP-систем або корпоративних месенджерів. У більшості організацій ці методи або відсутні, або знаходяться на початковому етапі впровадження.

Застосування методів управління поведінкою персоналу в українських організаціях суттєво відрізняється залежно від розміру компанії, галузі та рівня цифрової зрілості. Можна виділити 5 основних типів організацій, які демонструють різні моделі впровадження. Для оцінки рівня застосування методів управління поведінкою персоналу в українських організаціях було проведено їх порівняльний аналіз залежно від типу організації. Оцінка здійснювалася за чотирма ключовими параметрами. Результати представлено в таблиці 2.4.

Шкала оцінки рівня застосування методів є якісною та має такий зміст:

- Високий — методи активно та системно впроваджені, використовуються на постійній основі з високим рівнем охоплення персоналу;
- Середній–високий — методи впроваджені в значному обсязі, але мають окремі прогалини в системності чи регулярності;
- Середній — методи застосовуються, але фрагментарно або формально, без достатньої глибини та охоплення;

- Низький–середній — методи використовуються епізодично, з низьким рівнем системності;
- Низький — методи практично відсутні або застосовуються в мінімальному обсязі.

Таблиця 2.4.

Рівень застосування методів управління поведінкою за типами організацій (2024–2025)

Тип організації	**Технічний контроль (DLP/UEBA)**	**Програми з обізнаності**	**Робота з мотивацією та культурою**	**Системність підходу**	**Основні проблеми**
Банки та фінанси	Високий	Високий	Середня	Висока	Формалізм у частині культури
Великі приватні компанії	Середній–високий	Середній–високий	Середня	Середня–висока	Недостатня інтеграція методів
Державний сектор / КІ	Середній	Середній	Низька	Середня	Слабка мотивація, формалізм
ІТ-компанії	Низький–середній	Середній–високий	Середня	Середня	Неавторизоване ІТ, обхід правил
МСП (Малі та середні підприємства)	Низький	Низький–середній	Низька	Низька	Фрагментарність, брак ресурсів

Однією з найслабших сторін української практики є відсутність регулярного вимірювання ефективності методів. Більшість організацій не має чітких KPI щодо рівня відповідності, частоти порушень, результатів симуляцій чи динаміки мотивації персоналу [20].

Навіть у банках, де вимірювання проводиться частіше, воно зазвичай обмежується технічними показниками (кількість блокувань DLP, кількість пройдених тренінгів) і рідко включає якісні метрики (рівень внутрішньої мотивації, реальна зміна поведінки). У державному секторі та МСП регулярне вимірювання ефективності майже відсутнє.

Для оцінки загального стану застосування методів управління поведінкою персоналу в українських організаціях було проаналізовано рівні зрілості цих методів. Результати аналізу представлено в таблиці 2.5.

Поширеність в Україні відображає, наскільки широко той чи інший рівень зрілості представлений серед організацій. Оцінка здійснювалася за якісною шкалою:

- Висока — модель поширена в більшості організацій відповідної категорії;
- Середня — модель зустрічається у значній, але не переважній частині організацій;
- Низька–середня — модель застосовується обмежено, переважно у передових організаціях;
- Дуже низька — модель є винятком і зустрічається лише в поодиноких організаціях.

Таблиця 2.5.

Рівень зрілості застосування методів управління поведінкою в українських організаціях

Рівень зрілості	**Характеристика**	**Приклади організацій**	**Поширеність в Україні**
Фрагментарний	Методи застосовуються точково, без інтеграції та вимірювання результатів	Більшість МСП, частина державних установ	Висока
Базовий	Є регулярні тренінги та базовий технічний контроль, але відсутня інтеграція	Середні компанії, частина держсектору	Середня
Системний	Методи інтегровані (техніка + навчання + політика), проводиться вимірювання	Банки, великі приватні компанії	Низька–середня
Зрілий	Повна інтеграція методів, регулярне вимірювання KPI, робота з культурою	Окремі банки та міжнародні компанії	Дуже низька

У більшості організацій методи управління поведінкою носять формальний характер. Політики безпеки затверджуються, тренінги проводяться, технічні засоби впроваджуються, однак реальна зміна поведінки працівників часто не відбувається. Формальний підхід особливо поширений у державному секторі та на підприємствах, де вимоги до безпеки продиктовані переважно регуляторними нормами, а не внутрішньою потребою організації.

Однією з найсуттєвіших прогалин є недостатня увага до мотивації та формування внутрішньої культури безпеки. Більшість організацій фокусується на зовнішньому контролі (технічні засоби, політики, покарання) і навчанні, але це рідко працює з внутрішніми установками працівників. У результаті навіть при високому рівні знань та наявності технічних засобів контролю працівники часто обирають зручність замість безпеки, коли це не контролюється безпосередньо [21].

Багато організацій продовжують застосовувати методи, розроблені для мирного часу, без достатньої адаптації до умов воєнного стану та гібридної роботи. Разові тренінги, жорсткий технічний контроль та системи покарань часто не враховують психологічний стан працівників, підвищене навантаження та специфіку віддаленої роботи. Це призводить до зниження ефективності методів та зростання формалізму.

У більшості українських організацій відсутня практика регулярного вимірювання ефективності методів управління поведінкою. Навіть там, де проводяться тренінги та впроваджуються технічні засоби, рідко оцінюється реальний вплив на поведінку працівників. Відсутність KPI та метрик відповідності унеможливлює об’єктивну оцінку результатів та своєчасне коригування програм [22].

В Україні досі слабо розвинений обмін практичним досвідом між організаціями щодо управління поведінкою персоналу. Банки та великі компанії рідко діляться успішними кейсами, а державний сектор та МСП часто змушені вирішувати однакові проблеми ізольовано. Це уповільнює поширення ефективних практик та призводить до дублювання помилок [23].

2.3. Оцінка ефективності методів управління поведінкою персоналу та основні проблеми їх впровадження

Оцінка ефективності методів управління поведінкою персоналу в умовах воєнного стану та гібридної форми роботи вимагає спеціально адаптованої системи критеріїв [24]. Традиційні підходи, орієнтовані на стабільне середовище, виявляються недостатніми, оскільки не враховують кумулятивного впливу хронічного психоемоційного стресу, розмиття організаційного периметра та обмежених ресурсів українських організацій.

Для об’єктивного аналізу було відібрано шість ключових критеріїв, які безпосередньо випливають зі специфіки українського контексту та відображають основні виклики сучасного середовища:

1. Адаптивність до психоемоційного стресу — здатність методу зберігати ефективність за умов втоми від прийняття рішеньта вигорання.
2. Вплив на рівень безпеки — ступінь реального (а не декларативного) дотримання політики безпеки.
3. Стійкість до втоми від проходження тренінгів з кібербезпеки — збереження мотиваційного ефекту протягом тривалого часу в умовах інформаційного перевантаження.
4. Ресурсозатратність — фінансові, кадрові та часові витрати на впровадження та підтримку.
5. Масштабованість у гібридному середовищі — можливість ефективного застосування в умовах розпорошеного персоналу та різнорідної технічної інфраструктури.
6. Довгостроковий ефект — здатність формувати стійкі зміни поведінки, а не лише тимчасове підвищення обізнаності.

Вибір саме цих критеріїв зумовлений необхідністю проводити оцінку не в ідеальних умовах, а в реальному контексті гібридної війни. Вони поєднують психологічну реальність воєнного часу (критерії 1 та 3), організаційно-технічні особливості гібридної роботи (критерії 5 та 6) та практичні обмеження

вітчизняних організацій (критерій 4). Такий підхід дозволяє здійснити прагматичну, а не формальну оцінку методів.

Шкала оцінки ефективності за кожним критерієм має такий зміст:

- Висока — метод демонструє стійкий позитивний результат добре адаптується до воєнних реалій та гібридної роботи, забезпечує значне підвищення compliance при відносно низьких витратах [25, 26]
- Середня — метод дає помітний, але нестабільний ефект, частково втрачає дієвість під впливом стресу або гібридних умов і потребує значної підтримки [27])
- Низька — метод має обмежений або короткостроковий вплив , погано адаптується до українських реалій, характеризується високою ресурсозатратністю або швидким згасанням ефекту

Технічні та організаційні методи традиційно становлять основу більшості систем управління інформаційною безпекою в українських організаціях. Однак їхня ефективність у поєднанні хронічного психоемоційного стресу виявляється значно нижчою, ніж у стабільному середовищі.

1. Технічні методи (системи поведінкового аналізу, UEBA, DLP та автоматизований моніторинг) демонструють середню загальну ефективність. Вони забезпечують оперативне виявлення аномальної поведінки та обмеження технічних порушень. Водночас у гібридному середовищі їхня результативність суттєво знижується через технічну фрагментацію інфраструктури (домашні мережі, BYOD, різнорідні пристрої). Крім того, сприйняття таких систем як інструменту тотального контролю посилює опір працівників і провокує поширення несанкціонованого IT. За критеріями адаптивності до стресу та стійкості до стійкості від втоми технічні методи отримують низькі оцінки, оскільки майже не впливають на внутрішню мотивацію.

2. Організаційні методи (формалізація політик, аудити відповідності, системи мотивації та дисциплінарної відповідальності) демонструють низьку ефективність в сучасних українських реаліях. Хоча стандарти ISO/IEC 27001:2022 (Annex A.6) та NIST CSF 2.0 рекомендують потужні організаційні

механізми, їхнє застосування ускладнюється відсутністю фізичної присутності керівництва та ресурсозатратністю регулярних аудитів. У результаті рівень відповідності залишається переважно формальним.

Для порівняльної оцінки ефективності цих двох груп методів проведено їх аналіз за шістьма контекстно-орієнтованими критеріями. Результати представлено в таблиці 2.6.

Шкала оцінки ефективності методів є якісною та має такий зміст:

- Висока — метод демонструє стійкий позитивний результат, добре адаптується до умов воєнного стану та гібридної роботи;
- Середня — метод забезпечує помітний, але нестабільний ефект і частково втрачає дієвість під впливом стресу та гібридних умов;
- Середня–низька / Низька — метод має обмежений або короткостроковий вплив і погано адаптується до українських реалій.

Таблиця 2.6.

Порівняльна оцінка ефективності технічних та організаційних методів за встановленими критеріями

Критерій оцінки	**Технічні методи**	**Організаційні методи**	**Обґрунтування оцінки**
Адаптивність до психоемоційного стресу	Середня	Низька	Технічні методи реагують на поведінку, але не враховують стрес; організаційні — ще менш гнучкі
Вплив на рівень безпеки	Середня	Середня–низька	Дають контроль, але слабко впливають на внутрішню мотивацію
Стійкість до втоми від проходження тренінгів	Висока	Низька	Технічні методи не залежать від мотивації; організаційні швидко втрачають ефект
Ресурсозатратність	Висока	Середня	UEBA та DLP вимагають значних інвестицій і фахівців
Масштабованість у гібридному середовищі	Середня	Низька	Складно забезпечити єдині стандарти на розпорошених робочих місцях

Продовження таблиці 2.6.

Критерій оцінки	**Технічні методи**	**Організаційні методи**	**Обґрунтування оцінки**
Довгостроковий ефект	Середня	Низька	Не формують стійкої культури безпеки без психологічної складової

Порівняльний аналіз свідчить, що технічні методи, попри забезпечення певного рівня контролю та оперативного реагування на аномалії, неспроможні самостійно формувати зрілу культуру інформаційної безпеки. Їхня ефективність суттєво обмежується в умовах воєнного стресу через брак впливу на внутрішню мотивацію працівників. Організаційні методи, у свою чергу, залишаються надмірно жорсткими та формальними, що знижує їхню адаптивність до психологічно виснаженого та розрізненого гібридного середовища. Спільною слабкістю обох груп є домінування зовнішнього контролю над формуванням внутрішньої мотивації та стійких поведінкових звичок. Зважаючи на це, технічні та організаційні методи в умовах воєнного стану та гібридної роботи демонструють лише обмежену ефективність і потребують суттєвого доповнення психологічними та інтегративними інструментами [28].

На противагу цьому, комбіновані (інтегровані) методи демонструють найвищу загальну ефективність. Вони не зводяться до простого поєднання інструментів, а створюють синергетичний ефект: дані behavioral analytics використовуються для персоналізації психологічних втручань, а організаційні політики підкріплюються механізмами внутрішньої мотивації. Саме інтегровані моделі найкраще функціонують у складних, динамічних і ресурсообмежених середовищах, характерних для українських організацій. У воєнно-гібридних умовах такі підходи дозволяють динамічно адаптувати інтенсивність втручань залежно від рівня стресу працівника, що суттєво підвищує їхню стійкість.

Якщо психологічні методи, хоч і впливають на ставлення та мотивацію, залишаються вразливими до воєнного стресу та швидко втрачають ефективність, то комбіновані підходи компенсують ці слабкості за рахунок інтеграції. Вони дозволяють перетворювати дані технічного моніторингу на персоналізовані психологічні втручання, а організаційні вимоги — на внутрішньо мотивовану поведінку. Саме така синергія робить їх найбільш стійкими в умовах української реальності, де жоден окремий тип методів не здатен забезпечити необхідний рівень кіберстійкості.

Незважаючи на теоретичну обґрунтованість різних методів управління поведінкою персоналу, їхнє практичне впровадження в українських організаціях стикається з системними бар'єрами, які суттєво знижують загальну ефективність [29]. Умови воєнного стану та гібридної роботи не лише створюють нові виклики, але й посилюють уже існуючі структурні проблеми, перетворюючи окремі перешкоди на взаємопов'язану систему обмежень.

Для систематизації основних бар'єрів впровадження методів управління поведінкою персоналу в українських організаціях було виділено п'ять ключових груп бар'єрів. Оцінка рівня впливу кожного бар'єру здійснювалася з урахуванням його здатності обмежувати ефективність методів в умовах воєнного стану та гібридної роботи. Результати систематизації основних бар'єрів та оцінки рівня їхнього впливу наведено в таблиці 2.7.

Шкала оцінки рівня впливу має такий зміст:

- Критичний — бар'єр блокує або радикально знижує ефективність більшості методів, роблячи їхнє успішне застосування практично неможливим без його усунення;
- Високий — бар'єр суттєво обмежує результативність методів, вимагаючи значних додаткових зусиль для подолання;
- Середній — бар'єр створює помітні труднощі, але може бути частково подоланий наявними ресурсами та інструментами.

Таблиця 2.7

Основні бар’єри впровадження методів управління поведінкою персоналу в українських організаціях

Бар’єр	**Опис прояву в умовах воєнного стану та гібридної роботи**	**Рівень впливу**	**Обґрунтування**
Фінансовий	Обмежене фінансування сучасних платформ (AI, поведінкова аналітика, персоналізоване навчання)	Критичний	Більшість організацій, особливо державного сектору, не можуть дозволити собі необхідні технології
Організаційний	Слабка інтеграція ІБ у загальну стратегію, відсутність «тону зверху», формалізм політик	Високий	Гібридна робота послаблює контроль і лідерство, що критично в умовах війни
Психологічний	Хронічний стрес працівників, стійкість до зміне, низька мотивація через вигорання	Критичний	Працівники пріоритизують фізичну безпеку, що блокує сприйняття програм обізнаності
Кадровий	Дефіцит фахівців	Високий	Відсутність спеціалістів, здатних інтегрувати психологічні та технічні методи
Нормативний	Недосконалість національних стандартів щодо адаптації до воєнних реалій	Середній	Існуючі нормативні вимоги (ISO 27001, Закони України) недостатньо враховують гібридну війну

Проблеми носять яскраво виражений системний характер і утворюють замкнене коло. Фінансовий бар’єр обмежує можливість впровадження сучасних комбінованих рішень, що посилює кадровий дефіцит. Відсутність кваліфікованих фахівців, у свою чергу, призводить до формального застосування організаційних методів і низької якості психологічних програм. Психологічний бар’єр (хронічна втома персоналу) знижує сприйнятливість до будь-яких ініціатив, а слабке організаційне лідерство не дозволяє подолати цей опір. У результаті навіть потенційно ефективні комбіновані методи впроваджуються фрагментарно і не дають очікуваного результату.

Основна проблема впровадження методів управління поведінкою персоналу в Україні полягає не в браку теоретичних підходів, а в системній невідповідності наявних інструментів реальним умовам воєнного стану та гібридної роботи [30]. Бар'єри взаємно посилюються, створюючи ситуацію, коли навіть найкращі міжнародні практики при перенесенні на вітчизняну площину, втрачають значну частину своєї ефективності. Це вимагає не локальних покращень окремих методів, а комплексної трансформації підходу до управління людським фактором — переходу від розрізнених ініціатив до стратегічно інтегрованої системи, що враховує обмежені ресурси та психоемоційну реальність працівників.

Проведена порівняльна оцінка ефективності методів управління поведінкою персоналу дозволяє зробити кілька ключових узагальнень щодо їхньої придатності для українських організацій в умовах воєнного стану та гібридної роботи:

1. По-перше, технічні та організаційні методи, хоча й залишаються необхідними елементами системи захисту, демонструють обмежену ефективність. Вони добре справляються з функціями контролю та стандартизації, але виявляються малоефективними в умовах психоемоційного виснаження працівників і розмиття організаційних кордонів. Їхня основна слабкість полягає в переважанні зовнішнього примусу над внутрішньою мотивацією, що в українських реаліях призводить до формального compliance.

2. По-друге, психологічні методи мають значний потенціал впливу на ставлення та мотивацію персоналу, проте їхня самостійна ефективність суттєво знижується через високу вразливість до втоми та хронічного стресу. Вони потребують постійної підтримки іншими інструментами.

3. По-третє, комбіновані методи є єдиною групою, яка демонструє високу загальну ефективність та стійкість до українських умов. Саме інтеграція технічного моніторингу, організаційних механізмів і психологічних інструментів дозволяє компенсувати слабкі сторони окремих підходів і

створювати синергетичний ефект, що особливо важливо в умовах обмежених ресурсів і динамічного ризикового середовища.

В умовах воєнного стану та гібридної роботи жоден окремий тип методів не забезпечує стійкого підвищення рівня безпеки. Ефективність управління поведінкою персоналу визначається не силою найсучаснішого інструменту, а якістю інтеграції різних підходів об’єднаних у єдину, адаптивну систему, яка враховує психологічну реальність працівників і організаційні обмеження.

Подолання виявлених бар’єрів та максимальне використання потенціалу комбінованих рішень вимагає не лише вдосконалення існуючих методів, але й розробки комплексної моделі управління поведінкою персоналу, адаптованої до українських реалій.

Висновки до розділу 2

У цьому розділі було проведено детальний аналіз стану управління поведінкою персоналу у сфері інформаційної безпеки в умовах воєнного стану та гібридної форми роботи.

Проаналізовано особливості застосування методів управління поведінкою персоналу в умовах воєнного стану та гібридної форми роботи. Встановлено, що поєднання хронічного психо-емоційного стресу, втоми від прийняття рішень та розмиття організаційного периметра створює синергетичний негативний ефект, який суттєво знижує результативність традиційних методів. Порівняльний аналіз показав чітке зміщення пріоритетів: від разових програм обізнаності, жорсткого контролю та систем покарань до підтримуючих підходів, зокрема nudge-технологій і коротких мікро-тренінгів.

За результатами огляду застосуваних методів за типами організацій виявлено значну нерівномірність та переважно фрагментарний характер їхнього впровадження. Найвищий рівень зрілості спостерігається в банках та великих приватних компаніях, тоді як державний сектор, підприємства критичної інфраструктури та МСП характеризуються формальним підходом, слабкою

інтеграцією методів і майже повною відсутністю системного вимірювання ефективності.

На основі шести контекстно-орієнтованих критеріїв проведено оцінку основних груп методів. За результатами досліджено, що технічні та організаційні методи мають обмежену ефективність, психологічні — значний потенціал при низькій стійкості, а комбіновані (інтегровані) методи є єдиною групою, яка забезпечує високу загальну ефективність та адаптивність в українських умовах.

У результаті дослідження було встановлено, що жоден окремий тип методів не здатен забезпечити стійке підвищення кіберстійкості. Ефективність управління поведінкою персоналу визначається якістю інтеграції різних підходів в єдину адаптивну систему.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ МЕТОДІВ УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Модель комплексного управління поведінкою персоналу в системі інформаційної безпеки

Фрагментарне застосування окремих груп методів управління поведінкою персоналу є недостатнім для забезпечення необхідного рівня кіберстійкості українських організацій в умовах воєнного стану та гібридної роботи.

Фрагментарний підхід, який домінує в більшості українських організацій, має системні недоліки. Він не враховує синергетичного ефекту воєнного стресу та гібридної роботи: психологічне виснаження посилює вразливість до соціальної інженерії, створює додаткові можливості для реалізації цих вразливостей. Окремі методи не компенсують слабкі сторони один одного, що призводить до ситуацій, коли технічний контроль існує паралельно зі слабкою мотивацією, а організаційні політики — без реального впливу на ставлення працівників. Окрім цього, фрагментарність унеможливлює динамічну адаптацію системи до змін рівня стресу та робочого контексту, що особливо критично в умовах непередбачуваності воєнного часу.

Необхідність переходу до комплексної моделі обґрунтовується як теоретичними, так і практичними передумовами. та Georgiadou et al. (2022) [31] підкреслює, що ефективна культура інформаційної безпеки виникає лише за умови інтеграції технологічних, організаційних та психологічних елементів у єдину систему. Також доповнюють цей висновок фрагментарні підходи, які не здатні формувати стійку організаційну культуру, особливо в умовах високої невизначеності. В сучасному середовищі ландшафт кібербезпеки вимагає саме комплексного, інтегрованого управління поведінкою, а не розрізнених ініціатив.

На основі проведеного аналізу визначено три фундаментальні принципи побудови моделі комплексного управління поведінкою персоналу:

1. Інтегративність — поєднання технічних, організаційних та психологічних інструментів у єдину цілісну систему, де кожен елемент взаємно посилює інші. Такий підхід дозволяє компенсувати слабкі сторони окремих методів і створювати синергетичний ефект.

2. Контекстна адаптивність — здатність моделі динамічно реагувати на зміни рівня психоемоційного навантаження працівників, типу робочого середовища (офісне чи віддалене) та актуальних кіберзагроз. Цей принцип є особливо критичним для українських організацій в умовах швидкозмінного воєнно-гібридного середовища.

3. Орієнтація на кіберстійкість — формування не лише короткострокової обізнаності, а й психологічної стійкості працівників до кіберзагроз. Модель спрямована на розвиток здатності персоналу зберігати безпечну поведінку навіть за умов високого стресу та когнітивного виснаження.

Запропоновані принципи не є простою комбінацією існуючих методів, а являють собою якісно новий рівень управління людським фактором. Вони враховують обмеження фрагментарних підходів і максимально адаптовані до специфіки воєнного стану та гібридної форми роботи в Україні, дозволяючи перейти від реактивного реагування на інциденти до проактивного формування стійкої культури інформаційної безпеки.

Запропонована модель комплексного управління поведінкою персоналу побудована на чотирирівневій архітектурі, яка забезпечує системну інтеграцію технічних, організаційних, психологічних та інтегративних елементів. На відміну від традиційних фрагментарних підходів, вона ґрунтується на принципі взаємного посилення компонентів, що дозволяє моделі ефективно функціонувати в умовах поєднання воєнних ризиків і гібридної організації праці [32].

1. Технічний блок забезпечує об’єктивний моніторинг і автоматизований контроль поведінки працівників. Він включає системи поведінкової аналітики UEBA, DLP-системи та адаптивні політики доступу. У

воєнно-гібридних умовах головною функцією блоку є раннє виявлення аномалій та генерація даних для персоналізації інших рівнів моделі. Відмінною особливістю є перехід від тотального контролю до контекстного аналізу (наприклад, врахування часу повітряних тривог, зміни локації чи інтенсивності роботи). Саме такий підхід дозволяє технічним системам еволюціонувати від репресивної до підтримуючої ролі.

2. Організаційний блок охоплює політики безпеки, розподіл ролей і відповідальності, систему мотивації, аудити відповідності та лідерство керівництва. У запропонованій моделі організаційні елементи стають гнучкішими: політики враховують сценарії гібридної роботи та воєнних ризиків, а система мотивації поєднує матеріальні й нематеріальні стимули з урахуванням психоемоційного стану працівників.

3. Психологічний блок спрямований на формування ставлення, мотивації та психологічної стійкості працівників. Він включає персоналізовані мікро-навчання, nudge-технології, елементи гейміфікації та інтеграцію з програмами психологічної підтримки. В умовах воєнного стану особливого значення набуває розвиток resilience — здатності персоналу зберігати безпечну поведінку навіть за високого рівня стресу.

4. Інтегративний блок є центральним елементом моделі та забезпечує взаємодію всіх трьох попередніх блоків. Він включає:

- єдину платформу збору та аналізу даних;
- алгоритми динамічної персоналізації втручань;
- систему моніторингу ефективності в реальному часі;
- механізми зворотного зв’язку.

Саме цей блок генерує синергетичний ефект: дані технічного моніторингу використовуються для персоналізованих психологічних втручань, а результати психологічних програм впливають на коригування організаційних політик [33].

Основна цінність моделі полягає не в простому сумуванні компонентів, а в їхньому взаємному посиленні. Технічний блок надає об’єктивні дані, організаційний — структуру та відповідальність, психологічний — внутрішню

мотивацію, а інтегративний — забезпечує динамічну адаптацію всієї системи. Такий підхід дозволяє компенсувати ключові недоліки фрагментарних методів.

Модель враховує специфіку українського контексту завдяки механізмам адаптації до обмежених ресурсів, високої динаміки загроз і психологічного навантаження. Вона не вимагає радикальної заміни існуючих систем, а пропонує еволюційний шлях їх інтеграції [34].

Запропонована чотирирівнева модель є цілісною системою, орієнтованою на формування стійкої культури інформаційної безпеки в умовах воєнного стану та гібридної роботи. Вона демонструє вищу адаптивність завдяки трьом ключовим механізмам:

1. По-перше, інтегративний блок забезпечує постійний зворотний зв’язок між технічними даними та психологічними втручаннями. Якщо традиційні підходи застосовують методи статично, то модель динамічно адаптує інтенсивність навчання залежно від поточного рівня стресу працівник.

2. По-друге, модель передбачає модульну архітектуру, яка дозволяє організаціям впроваджувати її поступово — починаючи з критичних компонентів і масштабучись відповідно до наявних ресурсів. Це особливо важливо для українських організацій критичної інфраструктури, де повне оновлення систем часто неможливе через обмежене фінансування.

3. По-третє, акцент на resilience як наскрізному принципі дозволяє моделі не лише реагувати на порушення, але й розвивати стійкість працівників до майбутніх загроз. Дослідження доводять, що саме розвиток психологічної стійкості є одним із найефективніших способів протидії впливу воєнного стресу на поведінку в сфері кібербезпеки.

Запропонована модель комплексного управління поведінкою персоналу може бути ефективно впроваджена в українських організаціях лише за умови чіткого алгоритму реалізації, який враховує обмежені ресурси, специфіку воєнного стану та гібридну організацію праці. Модель не вимагає повної заміни існуючих систем, а передбачає еволюційне інтегрування компонентів у поточну систему інформаційної безпеки [35].

Практичні механізми реалізації моделі демонструють її високу застосовність в українських умовах. На відміну від дорогих європейських рішень, модель побудована за принципом максимальної ресурсоефективності та поетапності, що дозволяє навіть організаціям з обмеженим бюджетом досягати значного покращення культури безпеки. Головна перевага полягає в балансі між контролем і підтримкою, що особливо важливо в умовах воєнного стресу.

Незважаючи на значні переваги запропонованої моделі комплексного управління поведінкою персоналу, її практичне застосування в українських умовах має ряд об'єктивних обмежень, які необхідно чітко усвідомлювати для успішної реалізації [36]. Аналіз цих обмежень дозволяє не лише уникнути переоцінки можливостей моделі, але й визначити перспективні напрями її вдосконалення. Основні обмеження моделі включають:

1. Ресурсні обмеження

- Модель вимагає певного рівня технічної інфраструктури (системи поведінки користувачів, платформи для персоналізованого навчання) та кваліфікованих фахівців, здатних інтегрувати технічний, організаційний і психологічний блоки. Для багатьох організацій державного сектору та малого бізнесу початкові інвестиції можуть бути суттєвими. Навіть у розвинених країнах ресурсні бар'єри стають головним стримуючим фактором при впровадженні комплексних human-centric моделей.

2. Організаційні обмеження

- Успішність моделі значною мірою залежить від зрілості організаційної культури та підтримки вищого керівництва. У багатьох українських компаніях спостерігається слабке залучення топ-менеджменту до питань інформаційної безпеки, що призводить до формального впровадження. Без реагування на зміни вищого керівництва інтегративний блок моделі не зможе працювати ефективно.

3. Культурні та психологічні обмеження

- У воєнних умовах працівники можуть сприймати навіть адаптивні психологічні втручання як додаткове навантаження [37]. Існує ризик опору

змінам, особливо серед старшого покоління працівників та в організаціях з низьким рівнем довіри до керівництва. Культурна несумісність є однією з головних причин невдач при впровадженні комплексних моделей культури безпеки.

4. Методологічні обмеження

- Модель ще не пройшла широкого емпіричного тестування в українських умовах, тому її ефективність базується переважно на синтезі міжнародного досвіду. Це створює певний ризик при масштабуванні.

Обмеження запропонованої моделі не зменшують її цінності, а навпаки — підкреслюють необхідність реалістичного підходу до впровадження. Модель не є універсальним рішенням, яке автоматично вирішує всі проблеми, але створює системну основу для переходу від фрагментарних зусиль до стратегічного управління людським фактором. Її подальше вдосконалення та емпірична валідація в українських організаціях дозволять суттєво підвищити ефективність системи інформаційної безпеки в умовах тривалої гібридної війни.

Модель повністю відповідає українським реаліям. Вона враховує хронічний психоемоційний стрес працівників, обмежені фінансові та кадрові ресурси більшості організацій, розмиття організаційного периметра через гібридну роботу та високий рівень динаміки кіберзагроз. Модульна структура та орієнтація на ресурсоефективність дозволяють впроваджувати її поетапно — від пілотних проєктів у критичній інфраструктурі до масштабування в державному та приватному секторах. Особливо цінним є акцент на розвитку кіберстійкості персоналу, що є критичним фактором стійкості в умовах тривалої гібридної війни.

Науково-практичний внесок моделі полягає в переході від розрізнених методів до цілісної системи управління людським фактором, адаптованої до специфіки національного контексту. Модель не претендує на універсальність, але створює надійну концептуальну основу для підвищення ефективності системи інформаційної безпеки українських організацій.

Модель комплексного управління поведінкою персоналу є важливим кроком у формуванні сучасної, контекстно-адаптованої культури інформаційної безпеки

3.2 Практичні рекомендації щодо впровадження комплексного підходу до управління поведінкою персоналу

Впровадження комплексного підходу до управління поведінкою персоналу в умовах воєнного стану та гібридної роботи вимагає чіткої, поетапної стратегії. Поетапність є оптимальним підходом для українських організацій, оскільки дозволяє мінімізувати ризики, розподілити обмежені ресурси в часі, отримати швидкі видимі результати на пілотних ділянках та скоригувати модель до реальних умов організації. Різке повне впровадження могло б призвести до опору персоналу, перевантаження IT та HR-служб і витрачання критичних ресурсів [38].

Запропонована стратегія передбачає чотири етапи впровадження.

Етап 1. Оцінка зрілості культури інформаційної безпеки (1–1,5 місяця)

На початковому етапі впровадження комплексної моделі управління поведінкою персоналу проводиться рунтовна діагностика поточного стану культури інформаційної безпеки в організації. Цей етап є фундаментом усього подальшого процесу, оскільки без об’єктивного розуміння вихідного рівня зрілості культури безпеки, існуючих бар’єрів та реальних ризиків будь-які подальші заходи можуть мати формальний характер або бути недостатньо ефективними. Така оцінка дозволяє виявити сильні та слабкі сторони існуючої системи, ступінь впливу воєнного стану та гібридної роботи на поведінку працівників, а також визначити пріоритетні напрями втручання. Ключові дії включають:

- Аудит існуючих методів управління поведінкою персоналу;
- Опитування та фокус-групи з працівниками для виявлення основних бар’єрів (стресу, втому від прийняття рішень, ставлення до безпеки);

- Визначення пріоритетних ризиків, пов’язаних з гібридною роботою та воєнними загрозами.

Очікуваний результат: сформований звіт про поточний стан та дорожня карта впровадження. На цьому етапі пріоритетом має бути залучення топ-менеджменту, оскільки без їхньої явної підтримки подальші етапи матимуть формальний характер.

Етап 2. Впровадження моделі (2–3 місяці)

Після завершення діагностики та розробки дорожньої карти починається практична апробація запропонованої комплексної моделі. Пілотне впровадження є ключовим перехідним етапом, який дозволяє перевірити працездатність моделі в реальних умовах організації, виявити потенційні проблеми та ризики до початку повномасштабного впровадження.

На цьому етапі модель запускається в обмеженому масштабі — в одному-двох ключових підрозділах (наприклад, у ІТ-відділі або департаменті критичної інфраструктури). Такий підхід дає можливість мінімізувати ризики для всієї організації, швидко отримати практичні результати, зібрати якісний зворотний зв’язок від працівників та внести необхідні коригування в модель ще до масштабування. Ключові дії включають:

- Запуск технічного блоку (UEBA/DLP з базовою персоналізацією);
- Оновлення організаційних політик під гібридний формат;
- Запуск психологічного блоку (мікро-тренінги, nudge-кампанії).

Очікуваний результат: вимірюване покращення відповідності у пілотних підрозділах, збір зворотного зв’язку від працівників. Впровадження моделі необхідно проводити в підрозділах з найвищим рівнем кіберризику, щоб швидко продемонструвати керівництву практичну цінність моделі та отримати додаткову підтримку.

Етап 3. Масштабування (3–5 місяців)

Після успішного завершення пілотного впровадження та отримання підтверджених позитивних результатів відбувається перехід до масштабування

моделі. На цьому етапі вже є накопичений досвід під час впровадження комплексної моделі, відпрацьовані процеси та виявлені особливості впровадження поширюються на всю організацію.

Масштабування є критичним етапом, оскільки саме на ньому перевіряється здатність запропонованої комплексної моделі працювати в реальних умовах великої кількості працівників з різними категоріями зайнятості (офісні, віддалені, польові), рівнями доступу до інформації та ступенем психоемоційного навантаження. Успішне масштабування дозволяє перейти від локального покращення до системної трансформації культури інформаційної безпеки організації в цілому.

Ключові дії включають:

- Адаптацію моделі для різних категорій працівників (офісні, віддалені, польові);
- Навчання внутрішніх тренерів та HR-спеціалістів;
- Інтеграція всіх блоків моделі в єдину систему моніторингу.

Очікуваний результат: охоплення моделлю не менше 70–80 % персоналу, стабільне підвищення ключових показників безпеки. Масштабування варто проводити поступово за підрозділами, а не одночасно, щоб уникнути перевантаження підтримуючих служб.

Етап 4. Моніторинг, оцінка та постійне вдосконалення (системно, починаючи з 6-го місяця)

Завершальним і водночас безперервним етапом впровадження комплексної моделі управління поведінкою персоналу є створення ефективної системи моніторингу, оцінки та постійного вдосконалення. Якщо попередні етапи спрямовані на запуск і поширення моделі, то цей етап забезпечує її довгострокову життєздатність та адаптивність до динамічних умов воєнного стану, гібридної роботи та еволюції кіберзагроз.

На цьому етапі формується постійно діючий механізм регулярної оцінки ефективності моделі, який дозволяє не лише фіксувати досягнуті результати, але й оперативно виявляти нові виклики, коригувати підходи та підтримувати

високу актуальність усіх компонентів моделі. Без системного моніторингу навіть найуспішніше впровадження з часом може втратити ефективність через зміну рівня загроз, психоемоційного стану колективу чи появи нових технологій [39]. Ключові дії включають:

- Щоквартальний аналіз ключових метрик;
- Збір зворотного зв’язку від працівників;
- Коригування компонентів моделі залежно від зміни рівня загроз та психоемоційного стану колективу.

Очікуваний результат: перетворення моделі на постійно діючу, самовдосконалювану систему управління культурою безпеки.

Технічний блок становить фундамент запропонованої комплексної моделі, оскільки забезпечує об’єктивний моніторинг поведінки працівників та автоматизований захист інформації. Однак у воєнно-гібридному середовищі його впровадження виходить далеко за межі суто технічних завдань і вимагає глибокого аналізу балансу між ефективністю контролю та рівнем довіри персоналу. Надмірний контроль може посилити психологічний опір і спровокувати зростання неавторизованого IT, тоді як недостатній — призвести до неприйнятного підвищення ризиків. Технічний блок повинен еволюціонувати від традиційної репресивної функції до контекстно-орієнтованої підтримуючої ролі.

Практичні кроки впровадження технічного блоку включають:

1. Аудит та вибір інструментів

Ефективність технічного блоку значною мірою залежить від правильного вибору інструментів, що відповідають наявній інфраструктурі та рівню цифрової зрілості організації. Рекомендується проводити комплексний аудит з урахуванням сумісності, масштабованості та ресурсних обмежень. Пріоритетними рішеннями є:

- Microsoft Defender for Endpoint + Microsoft Purview (DLP) — для організацій, що використовують екосистему Microsoft 365;

- Google Workspace Security + BeyondCorp Enterprise — для компаній на платформі Google;
- Open-source інструменти (Elastic SIEM, Wazuh, Osquery) — для організацій з обмеженим бюджетом.

2. Адаптація до гібридної роботи та BYOD

У гібридному середовищі традиційний моніторинг стає контрпродуктивним. Більш ефективним є перехід до контекстного аналізу ризиків, який враховує специфіку робочого середовища. Ключовими заходами є:

- Впровадження Conditional Access на основі оцінки ризику (зокрема, додаткової автентифікації при підключенні з ненадійних мереж);
- Налаштування UEBA-модулів з урахуванням індивідуальних патернів поведінки працівника (час роботи, геолокація, типові обсяги даних);
- Використання Mobile Device Management (MDM) рішень (Microsoft Intune, Google Endpoint Management) з мінімальним втручанням в особисті дані.

3. Мінімізація опору працівників

Технічний контроль часто сприймається як прояв недовіри, що особливо гостро проявляється в умовах хронічного стресу. Для подолання цього бар'єру необхідне поєднання прозорості та позитивного підкріплення:

- Проведення відкритих комунікацій щодо цілей і меж моніторингу;
- Використання анонімного режиму на початкових етапах тестування UEBA;
- Запровадження системи позитивного підкріплення (автоматичні повідомлення з подякою, бали в мотиваційній системі).

4. Інтеграція з іншими блоками моделі

Найважливішою умовою ефективності технічного блоку є його тісна інтеграція з організаційним рівнями. Дані з UEBA та DLP повинні автоматично передаватися до інтегративного блоку для формування персоналізованих психологічних втручань (наприклад, працівнику з частими аномаліями автоматично пропонується цільовий мікро-тренінг).

Організаційний блок виконує роль сполучної ланки комплексної моделі, забезпечуючи нормативну базу, розподіл відповідальності та системну підтримку технічних і психологічних заходів [40]. У воєнно-гібридних умовах традиційні організаційні інструменти (жорсткі політики, планові аудити) часто втрачають ефективність через відсутність постійного фізичного контролю та високий рівень психоемоційного стресу працівників. Тому ключовим завданням є модернізація цього блоку — перехід від формального регулювання до динамічного, гнучкого та контекстно-орієнтованого організаційного супроводу.

Практичні напрями оновлення організаційного блоку:

1. Оновлення політик інформаційної безпеки

Політики повинні стати менш жорсткими та більш адаптивними до реальних умов:

- Ввести сценарні політики для різних режимів роботи (офіс, віддалена робота, робота під час повітряних тривог);
- Передбачити допустимі винятки в умовах воєнного стану (наприклад, тимчасове використання особистих пристроїв з обов’язковим звітом);
- Перейти від статичних документів до динамічних, з оновленням не рідше одного разу на 6 місяців або після суттєвої зміни рівня загроз.

2. Посилення «тону зверху»

У воєнних умовах роль керівництва стає визначальною для формування культури безпеки:

- Керівники всіх рівнів повинні регулярно (не рідше одного разу на місяць) публічно демонструвати прихильність до політики безпеки;
- Запровадити практику, коли керівники першими проходять нові навчальні модулі та звітують про результати;
- Включити показники дотримання культури безпеки в KPI топ-менеджменту.

3. Модернізація системи мотивації та відповідальності

Традиційна система покарань у стресових умовах малоефективна. Рекомендується:

- Запровадити позитивну мотиваційну систему (бонусні бали, внутрішні рейтинги, публічне визнання);
- Перейти до прогресивної шкали відповідальності (замість жорстких санкцій — повторне навчання та індивідуальний план корекції);
- Інтегрувати показники безпеки в щорічну оцінку персоналу (performance review).

4. Адаптація системи аудитів та контролю

Аудити повинні стати більш аналітичними та ризико-орієнтованими:

- Перейти до цільових аудитів, частота яких залежить від рівня ризику підрозділу;
- Використовувати дані технічного блоку для фокусованих перевірок замість тотальних;
- Проводити аудити культури безпеки (опитування, фокус-групи) не рідше двох разів на рік.

Ефективність комплексної моделі управління поведінкою персоналу визначається не лише якістю окремих блоків, а насамперед якістю їхньої взаємодії. Без надійних механізмів інтеграції та постійного моніторингу модель ризикує залишитися набором розрізнених інструментів. Тому інтегративний блок є центральним елементом, який забезпечує єдність системи.

Висновки до розділу 3

У розділі здійснено удосконалення методів управління поведінкою персоналу у сфері інформаційної безпеки шляхом розробки комплексної моделі та формування практичних рекомендацій щодо її впровадження.

Запропонована чотирирівнева модель комплексного управління поведінкою персоналу (технічний, організаційний, психологічний та інтегративний блоки) базується на принципах інтегративності, контекстної

адаптивності та орієнтації на кіберстійкість і враховує специфіку воєнного стану та гібридної форми роботи. Відмінною особливістю моделі є забезпечення синергетичного ефекту між різними типами інструментів, що дозволяє компенсувати недоліки фрагментарних підходів і динамічно адаптуватися до змін психоемоційного стану працівників та рівня кіберзагроз.

Запропонована модель та рекомендації становлять комплексне, адаптоване до українських реалій рішення, спрямоване на підвищення ефективності управління людським фактором в системі інформаційної безпеки. Це створює майбутню практичну основу для підвищення кіберстійкості організацій у складних сучасних умовах.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставлену мету, яка полягала в удосконаленні методів управління поведінкою персоналу у сфері інформаційної безпеки з урахуванням умов воєнного стану та гібридної форми роботи.

Проаналізовано теоретичні засади управління поведінкою персоналу у сфері інформаційної безпеки. Визначено та розмежовано ключові концептуальні категорії (управління поведінкою персоналу, культура інформаційної безпеки, поведінковий ризик, дотримання вимог безпеки). Виявлено системні проблеми, їхні причини та наслідки. Розглянуто сучасні психологічні моделі (TPB, PMT, SCT) та інші теоретичні підходи, проведено класифікацію методів управління на технічні, організаційні, психологічні та комбіновані, встановлено перевагу останніх як найбільш перспективних.

Проаналізовано стан управління поведінкою персоналу у сфері інформаційної безпеки в українських організаціях в умовах воєнного стану та гібридної роботи. Встановлено, що поєднання хронічного психоемоційного стресу, інформаційного перевантаження та розмиття організаційного периметра суттєво знижує ефективність традиційних методів. Виявлено значну нерівномірність та переважно фрагментарний, формальний характер їхнього впровадження залежно від типу організації. На основі шести контекстно-орієнтованих критеріїв проведено оцінку ефективності різних груп методів і підтверджено перевагу комбінованих (інтегрованих) підходів.

Удосконалено методи управління поведінкою персоналу шляхом розробки комплексної чотирирівневої моделі (технічний, організаційний, психологічний та інтегративний блоки), яка базується на принципах інтегративності, контекстної адаптивності та орієнтації на кіберстійкість. Розроблено практичні рекомендації щодо поетапного впровадження моделі в українських організаціях з урахуванням обмежених ресурсів, воєнних реалій та специфіки гібридної роботи.

Практичне значення одержаних результатів полягає в тому, що розроблена модель та рекомендації можуть бути використані підприємствами різних форм власності, органами державної влади та організаціями критичної інфраструктури для підвищення рівня культури інформаційної безпеки, зниження ризиків, пов’язаних з людським фактором, та підвищення загальної кіберстійкості в умовах тривалих кризових викликів.

Результати дослідження створюють науково-практичну основу для переходу від фрагментарних заходів до системного, інтегрованого управління людським фактором як ключовим елементом забезпечення інформаційної безпеки сучасних організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verizon: 60% of breaches involve human error / Mimecast. URL: https://www.mimecast.com/blog/verizon-60-of-breaches-involve-human-error/.

2. The Human Factor 2025: Vol. 1 Social Engineering / Proofpoint. URL: https://www.proofpoint.com/us/resources/threat-reports/human-factor-social-engineering.

3. Державна служба спеціального зв'язку та захисту інформації України. URL:https://cip.gov.ua/en/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37.

4. Da Veiga A. Defining organisational information security culture – Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404820300018.

5. Alshaikh M. Information security culture and the human factor. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404820302765.

6. Remote Work's Dark Secret 2025 / Insider Risk. URL: https://www.insiderisk.io/research/remote-work-dark-secret-2025.

7. Cost of a Data Breach Report 2025 / IBM. URL: https://www.ibm.com/reports/data-breach.

8. Rogers R. W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation // Journal of Experimental Social Psychology. – 1991. URL: https://www.sciencedirect.com/science/article/abs/pii/074959789190020T.

9. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation // ResearchGate. URL: https://www.researchgate.net/publication/229068371_Cognitive_and_physiological_processes_in_fear_appeals_and_attitude_change_A_revised_theory_of_protection_motivation.

10. Protection Motivation Theory // PMC. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12589003/.

11. Information security culture assessment // Computers & Security. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404811001337.

12. ISO 27001 Annex A 6: People Controls / DataGuard. URL: https://www.dataguard.com/iso-27001/annex-a/6-people-controls/.

13. How to Create a Security Culture: The Behavioural Security Model / SoSafe.URL: https://sosafe-awareness.com/blog/how-to-create-a-security-culture-the-behavioural-security-model/.

14. Public Administration Review. URL: https://onlinelibrary.wiley.com/doi/10.1111/puar.13895.

15. Application of the Nudge Theory for Improving Information Security Awareness Campaigns / ISACA. – 2023. URL: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/application-of-the-nudge-theory-for-improving-information-security-awareness-campaigns.

16. Security Awareness Report / SANS Institute. URL: https://www.sans.org/for-organizations/workforce/resources/security-awareness-report.

17. Звіт про реалізацію Стратегії розвитку фінансового сектору України на кінець 2025 року / Національний банк України. URL: https://bank.gov.ua/en/news/all/zvit-z-realizatsiyi-strategiyi-rozvitku-finansovogo-sektoru-ukrayini-na-kinets-2025-roku.

18. Updated Cybersecurity Requirements for Non-Bank Financial Institutions / Deloitte Ukraine. URL: https://www.deloitte.com/ua/en/services/tax/perspectives/updated-cybersecurity-requirements-for-non-bank-financial-institutions.html.

19. Gamified Cyber Security Training / Hoxhunt. URL: https://hoxhunt.com/blog/gamified-cyber-security-training.

20. Security Culture Maturity Model / KnowBe4. URL: https://www.knowbe4.com/resources/whitepapers/security-culture-maturity-model.

21. 2025 Security Awareness and Training Report / Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2025-security-awareness-and-training.pdf.

22. Cybersecurity Culture in 2026: Building Resilience Beyond Compliance / AwareGO. URL: https://awarego.com/cybersecurity-culture-in-2026-building-resilience-beyond-compliance/.

23. Taylor & Francis Online. – 2025. URL: https://www.tandfonline.com/doi/full/10.1080/23738871.2025.2451256.

24. Cybersecurity Metrics That Matter: Measuring Behavior, Engagement & Motivation / Living Security. URL: https://www.livingsecurity.com/blog/cybersecurity-metrics-that-matter-measuring-behavior-engagement-motivation.

25. Journal of Information Systems Education. – 2020. URL: https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1845583.

26. Emerald Insight. URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2023-0116/full/html.

27. Development of a Conceptual Model for Assessing Personal Information Security Culture // JPIS. – 2026. URL: https://jpis.az/uploads/article/en/2026_1/DEVELOPMENT_OF_A_CONCEPTUAL_MODEL_FOR_ASSESSING_PERSONAL_INFORMATION_SECURITY_CULTURE.pdf.

28. Springer Link. URL: https://link.springer.com/article/10.1007/s10207-025-01032-0.

29. Monograph / ARMG Publishing. – 2025. URL: https://armgpublishing.com/wp-content/uploads/2025/11/monograph-3-2025.pdf.

30. ScienceDirect. URL: https://www.sciencedirect.com/science/article/pii/S2444569X25000459.

31. Journal of Information Systems Education. – 2020. URL: https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1845583.

32. Adaptive Security. URL: https://www.adaptivesecurity.com/blog/human-centric-security.

33. The Human Factor in Information Security / ISACA. – 2019. URL: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security.

34. Cybersecurity Culture / MIT CAMS. URL: https://cams.mit.edu/wp-content/uploads/Cybersecurity-Culture-HICSS-MISQE.pdf.

35. Wartime Ukraine Offers Global Lessons on the Future of Cyber Resilience / Atlantic Council. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/wartime-ukraine-offers-global-lessons-on-the-future-of-cyber-resilience/.

36. Computers & Security. URL: https://www.sciencedirect.com/science/article/pii/S0167404824005091.

37. JYU. URL: https://jyx.jyu.fi/jyx/Record/jyx_123456789_92716.

38. Heliyon. URL: https://www.sciencedirect.com/science/article/pii/S2405844021006253.

39. An Interdisciplinary Understanding of The Human Factor of Cybersecurity / ODU. – 2025. URL: https://sites.wp.odu.edu/epres010/wp-content/uploads/sites/30561/2025/04/annotated-An20Interdisciplinary20Understanding20of20The20Human20Factor20of20Cybersecurity20-20FINAL.docx.pdf.

40. Human Factors in Cybersecurity / UpGuard. URL: https://www.upguard.com/blog/human-factors-in-cybersecurity.