Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)
спеціальність *125 Кібербезпека*
(код і назва спеціальності)
освітній ступень *магістр*
освітньо-наукова програма *Кібербезпека*

на тему: «Методи зменшення поверхні атак в інформаційних системах з урахуванням людського фактору»

Виконавець: студентка ІІ курсу, групи КБм-21

Анастасія ПЕТРЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Іван ПАРХОМЕНКО.	
Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

здобувачки КБм-21 (група) Петренко Анастасії Ігорівни (прізвище, ім'я та по-батькові)

Тема кваліфікаційної роботи: Методи зменшення поверхні атак в інформаційних системах з урахуванням людського фактору

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ
Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № *3* від *20 жовтня 2022 року.* .

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ
Об'єкт досліджень: людський фактор як складова культури безпеки в процесі зменшення поверхні атак

Предмет досліджень: вплив людського фактору на поведінку у кіберпросторі, та технології, методи та засоби підвищення компетентності в питаннях кібербезпеки для зменшити поверхні атак

Мета досліджень: формування фундаментального методу підвищення компетентності в питаннях кібербезпеки для зменшення поверхні атак, які використовують вразливості людського фактору

Вихідні дані для проведення роботи: інциденти безпеки, які стали наслідками людського фактору через призму OWASP Top 10, контролі безпеки, що застосовуються для зниження рівня ризиків, та практичні приклади реалізованих інструментів, методів та кампаній

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна: удосконалено підхід до підвищення обізнаності з кібербезпеки шляхом вивчення впливу людського фактору та поєднання інноваційних підходів, широкого спектру досліджень та практичних рекомендацій; вперше розроблено фундаментальний метод, що пропонує практичний, адаптований та ефективний підхід до підвищення кіберобізнаності для зменшення поверхні атак

Практична цінність: можливість впровадження фундаментального підходу в системах будь-якого масштабу та галузі

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів роботи	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	24.10.2022 – 20.11.2022
Розробка плану для досягнення мети кваліфікаційної роботи	21.11.2022 – 04.12.2022
Аналіз літературних джерел	05.12.2022 – 03.02.2023
Аналіз інцидентів безпеки, пов’язаних з людським фактором	04.02.2023 – 19.02.2023
Узагальнення категорій користувачів в інформаційній безпеці	20.02.2023 – 25.02.2023
Вивчення контролів безпеки, що можуть бути використані для зменшення поверхні атак	26.02.2023 – 08.03.2023
Найменування етапів роботи	**Строки виконання робіт (початок-кінець)**
Розробка фундаментального методу підвищення кіберобізнаності поетапно з рекомендацією технічних рішень	09.03.2023 - 09.04.2023
Обґрунтування специфіки використання методу	10.04.2023 – 14.04.2023
Оформлення пояснювальної записки	15.04.2023 – 10.05.2023
Підготовка до захисту кваліфікаційної роботи	11.05.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект: Зменшення поверхі атак та відповідно збитків, нанесених через численні інциденти безпеки, що були пов’язані з людським фактором

Соціальний ефект: Підвищення кіберобізнаності користувачів завдяки впровадження ефективного та структурованого процесу сучасними методами

7. ДОДАТКОВІ ВИМОГИ

Завдання видав	_____ (підпис)	Іван ПАРХОМЕНКО (прізвище, ініціали)
Завдання прийняла до виконання	_____ (підпис)	Анастасія ПЕТРЕНКО (прізвище, ініціали)

Дата видачі завдання: від 24 жовтня 2022 року.

Термін подання кваліфікаційної роботи до ЕК: 19 травня 2023 року.

УДК. 004.588

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи зменшення поверхні атак в інформаційних системах з урахуванням людського фактору» містить 79 сторінок основного тексту, 1 рисунок, 1 таблицю, 1 додаток, список використаних джерел з 42 найменувань.

Об’єкт дослідження: людський фактор як складова культури безпеки в процесі зменшення поверхні атак.

Мета дослідження: розробка фундаментального підходу процесу підвищення компетентності в питаннях кібербезпеки для зменшення поверхні атак, які використовують вразливості людського фактору.

Методи дослідження: методи наукової абстракції, індукції та дедукції, аналізу, структурування, алгоритмізація та макетування.

В роботі проведено аналіз інцидентів безпеки, пов’язаних з людським фактором, визначено характерні особливості поведінки людини. Запропоновано застосування методів підвищення кіберобізнаності для зменшення поверхні атак.

Актуальність дослідження: Людська помилка є основною причиною порушень кібербезпеки. Традиційні підходи для вирішення наявної проблеми на жаль не завжди справляються з поставленою задачею через ряд причин. Таким чином, потрібен всебічний та спеціалізований підхід.

Практичне значення дослідження полягає у розробці нових та удосконаленні наявних методів зменшення поверхні атак, спричинених людиною.

Наукова новизна дослідження полягає в удосконаленні підходу до підвищення обізнаності з кібербезпеки шляхом вивчення впливу людського фактору та поєднання інноваційних підходів, широкого спектру досліджень та практичних рекомендацій.

Ключові слова: людський фактор, зменшення поверхні атак, кіберобізнаність, інцидент, ризик, аналіз та оцінка загроз.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AWS	**—**	Amazon Web Services
UEBA	**—**	User and Entity Behavior Analytics
SIEM	**—**	Security Information and Event Management System
ENISA	**—**	European Union Agency for CybesSecurity
ECSM	**—**	European Conference on Social Media
OWASP	**—**	Open Web Application Security Project
CERT	**—**	Computer Emergency Response Team
NIST	**—**	National Institute of Standards and Technology
IT	**—**	Інформаційні технології
UEBA	**—**	User Entity and Behavior Analytics

ЗМІСТ

ВСТУП

В умовах постійного розвитку інформаційних технологій, безпека даних, користувачів та систем неодноразово опинялася темою світових обговорень, особливо коли мова йде про інцидент безпеки та компрометацію інформаційних систем. Причини таких подій зазвичай криються в некомпетентній поведінці користувачів, операторів даних. На відміну від технічних вразливостей і системних протоколів, людська сутність, не може бути виправлена належними конфігураціями. Тим самим постає нагальне питання як зменшити поверхню атак, спрямованих на поведінку людину.

Дослідженням особливостей людського фактору в інформаційних системах були висвітлені в наукових працях багатьох вчених, серед яких видатні автори та організації. До таких вчених належать Кевін Мітнік, відомий хакер та автор книги "The Art of Deception", який досліджував соціальний інжиніринг у кібербезпеці. Іншими відомими дослідниками є Брюс Шнайер, автор книги "Secrets and Lies: Digital Security in a Networked World", та Росс Андерсон, який зосередився на аналізі людського фактору в кібербезпеці у своїй книзі "Security Engineering". Також варто відзначити організації, які вносять вагомий внесок у кібербезпеку та вивчення людського фактору, такі як OWASP, SANS Institute, CERT та NIST. В їх дослідженнях та рекомендаціях знаходяться цінні висновки та рекомендації щодо зменшення впливу людського фактору на кібербезпеку.

Люди є центральними фігурами у системі, і найефективнішим способом зменшити ризик людського фактору у кіберпросторі - це зробити людей більш обізнаними у питаннях інформаційної безпеки. Хоча були проведені численні дослідження щодо різних аспектів обізнаності з кібербезпеки, вони залишаються непослідовними та вузько-спеціалізованими, що обмежує їх використання в широких масштабах.

Актуальністю кваліфікаціної роботи, що має практичне значення, є розробка нових та удосконалення наявних методів зменшення поверхні атак, спричинених людським фактором.

Метою кваліфікаційної роботи є зменшення поверхні атак шляхом дослідження людського фактору та методів підвищення кіберобізнаності користувачів.

Для досягнення мети кваліфікаційної роботи поставлені окремі завдання:

- провести аналіз інцидентів порушення безпеки, причиною яких стала людина за категоріями OWASP Top 10;
- встановити причинно-наслідкові зв'язки між ментальністю людини та її поведінкою у кіберпросторі
- узагальнити традиційні підходи до навчання інформаційної безпеки та основні категорії користувачів в інформаційних системах;
- обґрунтувати неефективність наявних методів підвищення кіберобізнаності
- дослідити інструменти, методи та засоби підвищення кіберобізнаності користувачів;
- формалізувати вимоги до процесу підвищення обізнаності у сфері кібербезпеки для зменшення поверхні атак
- запропонувати метод зменшення поверхні атак через призму 5 етапів: дослідження, перевірка, навчання, аналіз, звітність;

Об’єкт дослідження – людський фактор як складова культури безпеки в процесі зменшення поверхні атак.

Предмет дослідження - людські фактори, що впливають на поведінку у кіберпросторі, та технології, методи та засоби підвищення компетентності в питаннях кібербезпеки, що дозволяють зменшити поверхню атак

При вирішенні поставлених завдань у кваліфікаційній роботі використані: методи наукової абстракції, індукції та дедукції, аналізу (при розкритті основних особливостей функціонування, причин виявлених інцидентів); метод максимальної правдоподібності (для обґрунтування принципів безпеки через призму людського

фактору); метод синтезу (при дослідженні окремих технологій, засобів та заходів для побудови ефективного підходу для зменшення поверхні атак).

Методи підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людини, має потенціал для значного впливу на світ кібербезпеки. Зосереджуючись на людському факторі та використовуючи технології, цей підхід усуває основні причини вразливості системи безпеки та дає можливість окремим особам і організаціям побудувати культуру безпеки. Оскільки все більше і більше організацій і окремих людей звертають увагу на складову людини в системі, можна очікувати зміни парадигми в практиках кібербезпеки.

Теоретична і методична значущість отриманих результатів:

– удосконалено підхід до підвищення обізнаності з кібербезпеки шляхом вивчення впливу людського фактору та наявністю індивідуального підходу;

– вперше розроблено концептуальну метод для процесу підвищення обізнаності з кібербезпеки, що пропонує практичний, адаптований та ефективний підхід до підвищення кіберобізнаності для зменшення поверхні атак;

Практична цінність роботи полягає в наступному:

– можливості впровадження фундаментального підходу в системах будь-якого масштабу та галузі;

Запропоновані методи можуть бути покладені в основу створення процесу зменшення поверхні атак, пов’язаних з людський фактором.

Основні наукові положення і результати доповідалися та обговорювалися на V Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2022), VI Міжнародно-науковій конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)» (Київ, 2023).

Окремі аспекти кваліфікаційної роботи були опубліковані за результатами VIII Міжнародно-науковій конференції «Інформаційні технології та впровадження» (IT&I-2021).

РОЗДІЛ 1
ЛЮДСЬКИЙ ФАКТОР В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стан інформаційної безпеки характеризується постійною зміною ландшафту загроз, коли кібератаки стають все більш поширеними, витонченими та різноманітними.

Людський фактор залишається однією з найважливіших та менш контрольованих ланок у системі, оскільки людські помилки та поведінка можуть створювати вразливі місця та сприяти атакам.

Поточна ситуація безпеки у світі в 21 столітті відзначається декількома відмінними характеристиками. Збільшення взаємозв'язку людей, пристроїв і систем створило високо взаємопов'язаний цифровий ландшафт. Цей взаємозв'язок створив нові можливості для співпраці та інновацій, але також створив складні проблеми безпеки.

Однією з помітних особливостей поточного ландшафту безпеки є швидкий темп технологічного прогресу. Нові технології, такі як штучний інтелект, машинне навчання, блокчейн і 5G, змінили різні галузі, але вони також принесли нові ризики безпеці, які необхідно вирішити. Ці ризики включають вразливі місця в нових технологіях, проблеми з конфіденційністю та численні можливості бути використаними зловмисниками.

Крім того, ландшафт загроз, що розвивається, створює серйозні проблеми для безпеки. Зловмисники стали більш досвідченими, використовуючи передові методи та інструменти для здійснення кібератак. Суб'єкти національної держави, організовані злочинні групи та хактивісти постійно атакують критичну інфраструктуру, уряди, підприємства та окремих осіб, що призводить до збільшення ризиків і потенційних наслідків.

Людський фактор відіграє вирішальну роль у загальній безпеці. Людська поведінка, включаючи недбалість, недостатню обізнаність і сприйнятливість до атак соціальної інженерії, може мати глибокий вплив на безпеку. Дії

співробітників, такі як стати жертвою фішингових електронних листів, використання слабких паролів або некоректна обробка конфіденційних даних, можуть наражати організації на значні ризики.

Топ-10 OWASP розкриває інформацію про найпоширеніші вразливості та ризики безпеки в доступній формі. Він служить посібником для розуміння та визначення пріоритетів заходів безпеки. Топ-10 OWASP включає такі вразливості, як ін’єкційні атаки, несправний контроль доступу, неправильні конфігурації безпеки та міжсайтовий сценарій тощо. Усуваючи ці вразливості, організації можуть покращити рівень безпеки та зменшити ймовірність успішних атак.

Підводячи підсумок, можна сказати, що стан безпеки в 21-му столітті характеризується посиленням взаємозв’язків, швидким технологічним прогресом, розвитком ландшафту загроз і критичною роллю людського фактора. Розуміння цих особливостей, викликів і зв’язку з OWASP Top 10 може стати основою для наукових досліджень і скерувати розробку ефективних заходів безпеки та стратегій.

1.1 Інциденти порушення безпеки, пов’язані з людською поведінкою

Ядром будь-якої інформаційної системи є людина, оскільки саме вона визначає захищеність системи в цілому – люди розробили систему і люди ж нею і користуються. Тому не дивно що людська поведінка завжди була в центрі уваги і інтерес буде лише зростати.

Останнім часом були численні історії коли людська поведінка призвела до нанесення збитків компаніям, суспільству та державам в різному вигляді – від фінансових втрат до втрати репутації. Відповідно до списку OWASP Top 10 людина може внести свою лепту в кожну з вразливостей [1].

Зламаний контроль доступу (Broken Access Control): у січні 2018 року хакери проексплуатували сторонній додаток, який мережа готелів Marriott використовувала для надання гостьових послуг. Зловмисники отримали доступ до 5,2 мільйонів записів гостей Marriott. Ці записи включали паспортні дані, контактну

інформацію, стать, дні народження, дані облікового запису лояльності та особисті переваги [2].

Зловмисники скомпрометували облікові дані двох співробітників Marriott, щоб увійти в одну із сторонніх програм мережі готелів. Системи кібербезпеки Marriott протягом двох місяців не помічали підозрілої активності профілів цих співробітників. Завдяки моніторингу сторонніх постачальників і аналітиці поведінки користувачів і суб'єктів, Marriott могла виявити злом до того, як хакери отримали доступ до даних клієнтів.

Marriott Hotels & Resorts заплатила штраф у розмірі 18,4 мільйона фунтів стерлінгів, оскільки компанія не виконала вимог Загального регламенту захисту даних (GDPR).

Витік даних Equifax у 2017 році був значною кібератакою, яка скомпрометувала особисту інформацію 147 мільйонів споживачів, включаючи імена, номери соціального страхування, дати народження та адреси [3]. Атака сталася через вразливість у фреймворку програмного забезпечення з відкритим кодом, який використовував Equifax, що дозволило зловмисникам отримати доступ до систем і даних компанії.

Відповідно до офіційного звіту Комітету Палати представників Конгресу США з нагляду та реформ, причиною злому стали технічні та людські збої. Зокрема, співробітники Equifax не дотримувалися основних протоколів безпеки, таких як виправлення відомої вразливості та забезпечення актуальності їхніх систем. Крім того, IT-відділ компанії не мав належного нагляду за своїми системами, а його команда безпеки не змогла виявити атаку, поки не стало надто пізно.

Capital One зазнала витоку даних у липні 2019 року, який торкнувся понад 100 мільйонів клієнтів у Сполучених Штатах і Канаді. Порушення було спричинене вразливістю у брандмауері веб-додатків, якою скористався колишній співробітник Amazon Web Services (AWS), який був провайдером хмарного хостингу для Capital One.

Колишній співробітник отримав доступ до середовища AWS Capital One і зміг викрасти конфіденційну інформацію про клієнтів, включаючи імена, адреси, кредитні рейтинги та номери соціального страхування [4].

Capital One не зміг належним чином контролювати своє середовище AWS на предмет несанкціонованого доступу та підозрілої активності. Нарешті, порушення виявило недоліки в процесах найму та перевірки даних як для Capital One, так і для AWS, оскільки колишній співробітник мав історію нестабільної поведінки та попередні арешти за злочини, пов’язані з комп’ютером.

У 2020 році Zoom, популярна програма для відеоконференцій, зазнала кількох недоліків у безпеці, зокрема «Zoom-bombing», коли непрохані користувачі приєднувалися до зустрічей і зривали їх, а також спостерігався витік особистої інформації [5].

Ці недоліки безпеки були пов’язані з людськими факторами, такими як користувачі, які публічно ділилися посиланнями на зустрічі, використовували слабкі або взагалі не використовували паролі, а також не розуміли налаштувань конфіденційності програми. У деяких випадках користувачі не дотримувалися найкращих практик безпеки, що полегшувало зловмисникам використання вразливостей у програмі.

Витік даних LinkedIn у 2012 році включав крадіжку облікових даних понад 167 мільйонів користувачів, включаючи адреси електронної пошти та паролі. Порушення було спричинене поєднанням людського фактору та неправильної конфігурації безпеки [6].

Зловмисники змогли отримати базу даних паролів за допомогою SQL-атаки, яка стала можливою завдяки неправильно налаштованому брандмауеру веб-додатків. Паролі в базі даних зберігалися в несолідному хешованому форматі SHA-1, що полегшувало зловмисникам їх зламати. Людський фактор, залучений до злому, полягав у відсутності складності пароля та повторному використанні паролів для кількох облікових записів, що полегшило зловмисникам доступ до конфіденційної інформації.

Атака на ланцюжок поставок SolarWinds у 2020 році була однією з найбільших і найскладніших кібератак в історії, яка вразила численні організації по всьому світу [7]. Атака була спрямована на SolarWinds, постачальника програмного забезпечення, який надає інструменти керування мережею, і призвела до розповсюдження зловмисного програмного забезпечення серед клієнтів через оновлення програмного забезпечення. Зловмисники змогли скомпрометувати процес оновлення SolarWinds, вставивши шкідливий код у програмне забезпечення, яке потім було розповсюджено серед тисяч організацій, які використовували програмне забезпечення.

З точки зору людського фактору, атака SolarWinds підкреслює важливість пом'якшення внутрішньої загрози та безпеки ланцюга поставок. Зловмисники змогли проникнути в системи SolarWinds і поширити зловмисне програмне забезпечення через низку факторів, включаючи погані методи безпеки, недостатню обізнаність співробітників і неспроможність застосувати відповідні засоби контролю безпеки.

У 2017 році Equifax, одне з найбільших бюро кредитних історій у США, зазнало серйозного витоку даних, що вплинуло на приблизно 143 мільйони споживачів. Порушення було викликано вразливістю в програмному забезпеченні веб-додатків компанії, яка не була виправлена вчасно [8]. Зловмисники змогли використати вразливість і отримати доступ до конфіденційної інформації, включаючи імена, номери соціального страхування, дати народження та адреси.

Взлом Equifax став яскравим прикладом впливу людського фактора на кібербезпеку. Відповідно до офіційного звіту Комітету Палати представників Конгресу США з нагляду та урядової реформи, порушення сталося через «як людську помилку, так і технологічні збої».

У липні 2020 року атака соціальної інженерії була спрямована на кілька відомих облікових записів у Twitter, зокрема на ті, що належать Ілону Маску, Бараку Обамі та Джеффу Безосу. Зловмисникам вдалося опублікувати твіти з проханням підписників надсилати пожертви в біткойнах на певну адресу з

обіцянкою подвоїти свої інвестиції. В результаті атаки на цю адресу було надіслано біткойни на суму понад 100 000 доларів США [9].

Пізніше було встановлено, що атаку здійснила група молодих хакерів, які використовували методи соціальної інженерії, щоб обманом змусити співробітників Twitter надати їм доступ до внутрішніх інструментів і систем. Повідомляється, що хакери зв'язалися з декількома співробітниками Twitter і представилися співробітниками IT-відділу, переконавши їх передати свої облікові дані.

Злом Sony Pictures у 2014 році був значною кібератакою на Sony Pictures Entertainment з боку групи, яка називає себе Вартові миру. Хакери отримали доступ до комп'ютерних систем компанії та викрали величезну кількість даних, включаючи неопубліковані фільми, конфіденційну інформацію про співробітників та електронні листи керівників. Порушення даних пояснюється сукупністю факторів, включаючи недостатнє ведення журналів, слабкі паролі та невиправлене програмне забезпечення [10].

Крім того, команда з кібербезпеки Sony не змогла вчасно виявити вторгнення, а компанії не вистачало достатньої можливості реєстрації, щоб відстежувати пересування зловмисників у своїй мережі. У результаті зловмисники змогли підтримувати доступ до мережі Sony протягом кількох місяців, перш ніж їх викрили.

У 2019 році Capital One зазнала витоку даних через уразливість системи підробки запитів на стороні сервера (SSRF), якою скористався хакер, щоб отримати доступ до особистої інформації понад 100 мільйонів клієнтів. Уразливість була спричинена неправильно налаштованим брандмауером, який дозволив зловмиснику отримати доступ і отримати конфіденційні дані з хмарного сервера Amazon Web Services (AWS) [11].

Згідно зі звітом про розслідування Палати представників Конгресу США, взлом був спричинений нездатністю команди безпеки Capital One належним чином налаштувати та підтримувати брандмауер, а також відсутністю моніторингу та реєстрації мережевого трафіку. У звіті також підкреслюється важливість

впровадження заходів безпеки для запобігання та виявлення атак SSRF, таких як перевірка вхідних даних, обмеження швидкості та сегментація мережі.

Отже, незалежно від контексту атаки, людина прикладає руку більшою чи меншою мірою.

1.2 Аналіз факторів, що впливають на захищеність користувачів в системі

Людський фактор має вирішальне значення у сфері кібербезпеки, і людська поведінка відіграє важливу роль у визначенні загального рівня безпеки. Людські фактори стосуються психологічних, соціальних, культурних та організаційних факторів, які впливають на те, як люди взаємодіють із технологіями та як вони приймають рішення. Ці фактори можуть включати індивідуальні риси особистості, когнітивні упередження, процеси прийняття рішень, соціальні норми, очікування та організаційну культуру [12, с. 35]. Важливо розуміти складну взаємодію цих факторів для розробки ефективних систем кібербезпеки, які можуть пом’якшити ризики, пов’язані з людською помилкою, недбалістю або зловмисною поведінкою.

Люди є невід’ємною частиною ландшафту кібербезпеки, оскільки вони взаємодіють із технологіями, приймають рішення щодо методів безпеки та реагують на потенційні загрози. Їхні знання, ставлення, поведінка та вразливі місця значно впливають на стан безпеки як організацій, так і окремих осіб. Розуміючи ці людські фактори, ми можемо розробити втручання, політику та навчальні програми, спрямовані на корінні причини порушень безпеки.

Людський фактор охоплює широкий спектр аспектів, включаючи сприйняття ризику, процеси прийняття рішень, когнітивні упередження, соціальну динаміку та рівень обізнаності [13, с. 11]. Отримавши розуміння цих факторів, ми можемо визначити вразливі місця та розробити відповідні контрзаходи. Наприклад, розуміння загальних психологічних упереджень, які демонструють люди, таких як надмірна впевненість або схильність віддавати перевагу зручності над безпекою, дозволяє нам розробити втручання, які пом’якшують ці упередження та заохочують більш безпечну поведінку.

Крім того, визнання людського фактора в кібербезпеці дозволяє нам вирішувати такі проблеми, як інсайдерські загрози, атаки соціальної інженерії та недотримання протоколів безпеки. Вивчаючи людські фактори, ми можемо розробити індивідуальні програми підвищення обізнаності про безпеку, покращити навчальні модулі та встановити ефективні процедури реагування на інциденти.

Зрештою, важливість розуміння людського фактору полягає в тому, що сама по собі технологія не може повністю захистити від кіберзагроз. Враховуючи людський фактор, можна створити цілісний підхід до кібербезпеки, який узгоджує технологічні заходи з людською поведінкою, мотиваціями та обмеженнями. Ця інтеграція дає можливість організаціям і окремим особам активно виправляти вразливості, зменшувати поверхню атаки та розвивати культуру обізнаності та стійкості до кібербезпеки. Загалом виділяють різні поведінкові підходу ментальності людини [14, с. 215].

Бажання бути підключеним звідусіль у будь-який час збільшує ризик недовіреного підключення. Постійна потреба людей у підключенні та зручності спонукає їх підключатися до мереж і пристроїв, не беручи до уваги їх безпеку. Така поведінка наражає їх на ризик підключення до ненадійних мереж, таких як загальнодоступні точки доступу Wi-Fi, якими можуть скористатися зловмисники, щоб отримати несанкціонований доступ до їхніх пристроїв або викрасти конфіденційну інформацію.

Люди звикли натискати кнопку «Я приймаю» та отримувати повідомлення, пов’язані з безпекою. Користувачі часто мають звичку швидко приймати умови, не читаючи їх уважно. Вони, як правило, переглядають повідомлення, пов’язані з безпекою, включно з попередженнями чи запитами на дозвіл, не розуміючи повністю наслідків своїх дій. Така поведінка робить їх уразливими до потенційних ризиків безпеці та дозволяє зловмисникам використовувати їх відсутність уваги.

Намір вибрати легкий шлях завжди перемагає безпеку. Зазвичай люди віддають перевагу зручності, а не безпеці. Вони обирають прості у використанні та швидкі рішення, навіть якщо вони менш безпечні. Ця схильність до зручності робить людей більш сприйнятливими до атак соціальної інженерії, використання

слабких паролів або нехтування методами безпеки, які потребують додаткових зусиль.

Бажаність (бажання бути на зв’язку, завантажувати музику, відео, додатки, ділитися) перемагає безпеку. Бажання розваг, соціальних зв’язків і обміну вмістом часто переважує занепокоєння щодо безпеки. Користувачі можуть вдаватися до ризикованої поведінки, наприклад завантажувати файли з ненадійних джерел або ділитися конфіденційною інформацією, не враховуючи потенційні наслідки. Така поведінка робить їх уразливими до різних кіберзагроз.

Фінансові витрати (програмне забезпечення безпеки та витрати на оновлення) не завжди покривають підвищення безпеки. Користувачі можуть неохоче інвестувати в заходи безпеки, такі як антивірусне програмне забезпечення або регулярні оновлення системи, через фінансові обмеження або переконання, що витрати переважають переваги. Це небажання робить їхні пристрої та дані більш сприйнятливими до порушень безпеки та компрометації.

Приваблення негайної та невпевненої поведінки. Люди часто надають перевагу негайним прибуткам або перевагам над потенційними майбутніми ризиками. Це може спонукати їх до небезпечної поведінки, як-от клацання підозрілих посилань або обміну конфіденційною інформацією без належних запобіжних заходів, в обмін на негайне задоволення чи уявну вигоду.

Необхідні зусилля, щоб навчитися користуватися різними інструментами, оновлюватись, входити в систему та запам’ятовувати паролі. Складність і зусилля, необхідні для розуміння та впровадження заходів безпеки, можуть стримувати людей від безпечної поведінки. Необхідність вивчати та дотримуватися найкращих практик, регулярно оновлювати програмне забезпечення, безпечно входити в систему та керувати паролями може розглядатися як обтяжлива та трудомістка справа, що призводить до нехтування основними методами безпеки.

Дефіцит уявної вигоди. Деякі користувачі не можуть усвідомити відчутні переваги безпечної поведінки. Вони можуть не повністю розуміти, як безпечні методи сприяють захисту їхньої конфіденційної інформації, підтримці конфіденційності в Інтернеті або пом’якшенню потенційних кіберзагроз. Ця

відсутність сприйнятої вигоди зменшує їхню мотивацію віддавати пріоритет безпеці.

Відсутність передбачуваного ризику. Користувачі можуть недооцінювати ймовірність або наслідки кібератак або вважати, що їхні особисті дані недостатньо цінні чи важливі, щоб стати ціллю. Таке сприйняття низького ризику призводить до самовдоволення та ігнорування заходів безпеки, що робить їх більш вразливими до різноманітних загроз.

Відсутність уявлення про необхідність змін і відсутність віри в негативні результати, якщо правила не дотримуються. Деякі люди не усвідомлюють або не розуміють необхідності змінити свою поведінку чи дотримуватися правил безпеки. Вони можуть не повністю бачити потенційні наслідки ігнорування методів безпеки, наприклад витоку даних, крадіжки особистих даних, фінансових втрат або шкоди репутації. Цей брак обізнаності перешкоджає їхній мотивації прийняти безпечну поведінку.

Брак знань щодо навичок та інформації про те, як виявити шахрайство. Користувачам може не вистачати необхідних знань і навичок для ідентифікації та виявлення шахрайських дій або оманливих тактик, які використовують кібер-зловмисники. Така недостатня обізнаність збільшує ймовірність стати жертвою шахрайства, спроб фішингу чи інших форм атак соціальної інженерії.

Незнання, якій інформації вірити, коли надаються суперечливі рекомендації. Користувачі можуть зіткнутися з суперечливими порадами чи рекомендаціями щодо найкращих практик кібербезпеки з різних джерел. Відсутність ясності чи довіри до цих джерел може призвести до плутанини та невизначеності щодо того, яку інформацію слід використовувати. Така плутанина збільшує ризик прийняття невпевнених рішень або нехтування важливими заходами безпеки.

Забуття про безпечну поведінку під час активності в кіберпросторі та зосередження на активності в Інтернеті. Коли користувачі поглинені діяльністю в Інтернеті, вони можуть стати менш уважними до практики безпечної поведінки. Їхня зосередженість на поточному завданні або відволікання можуть призвести до

помилок у судженні та нехтування основними методами безпеки, такими як натискання підозрілих посилань або обмін конфіденційною інформацією без належної перевірки.

Перешкода соціального етикету (наприклад, передача паролів або пристроїв на знак довіри). Соціальні норми чи очікування, як-от передача паролів або пристроїв друзям або членам родини на знак довіри чи зручності, можуть підірвати безпеку. Користувачі можуть надавати перевагу підтримці соціальних стосунків або зручності, а не суворим обмеженням безпеки, що робить їх більш сприйнятливими до несанкціонованого доступу або витоку даних.

Неправильні або неповні ментальні підходу. Користувачі можуть мати хибні уявлення або неповне розуміння власної поведінки, ризиків безпеки та моментів, у яких вони вразливі до загроз. Ці неправильні ментальні підходу можуть призвести до неправильного сприйняття безпеки, що призведе до неадекватного захисту та сприйнятливості до атак.

Низький рівень чутливості. Люди, які мають низький рівень чутливості до ризиків безпеці, можуть не повністю усвідомлювати або оцінювати важливість прийняття безпечної поведінки. Їхня недостатня чутливість робить їх більш схильними до участі в ризикованій онлайн-діяльності або нехтування методами безпеки, які інакше могли б захистити їх від потенційних загроз.

Ризик того, що кіберзловмисники використовують страх і загрози, щоб викликати небезпечну поведінку. Кіберзловмисники часто використовують страх і загрози, щоб змусити людей маніпулювати небезпечною поведінкою. Наприклад, фішингові електронні листи або повідомлення можуть викликати відчуття терміновості або страх перед наслідками, спонукаючи користувачів розкривати конфіденційну інформацію або виконувати дії, які ставлять під загрозу їх безпеку.

Переоцінка розуміння загроз. Деякі користувачі можуть переоцінювати свої знання або розуміння загроз кібербезпеці, припускаючи, що вони добре поінформовані та належним чином захищені. Така надмірна самовпевненість може призвести до самовдоволення та помилкового відчуття безпеки, що робить їх більш сприйнятливими до атак соціальної інженерії чи інших форм експлуатації.

Делегування відповідальності за безпеку іншим особам, які вважаються більш обізнаними. Користувачі можуть значною мірою покладатися на зовнішні сторони, такі як IT-відділи або спеціалісти з кібербезпеки, щоб вирішити свої проблеми безпеки. Таке делегування відповідальності може призвести до відсутності особистої відповідальності та зниження почуття власності у підтримці безпечної поведінки, роблячи їх уразливими до потенційних загроз.

Ці додаткові фактори підкреслюють різні психологічні, соціальні та когнітивні аспекти, які сприяють небезпечній поведінці в контексті кібербезпеки. Розуміння цих факторів має вирішальне значення для розробки ефективних стратегій для підвищення обізнаності в кіберпросторі та посилення заходів безпеки.

Досліджені фактори сприяють небезпечній поведінці в контексті кібербезпеки, висвітлюючи проблеми у просуванні ефективної кіберобізнаності та зменшенні поверхні атак, спричинених поведінкою людини.

1.3 Узагальнення категорій користувачів в через призму поведінки

Розуміння індивідуальних рис особистості та того, як вони впливають на поведінку, може допомогти запровадити більш ефективні заходи безпеки. Автори статті «Does personality enhance susceptibility to cyber attacks?» виділяють п’ять типів особистості: любителі гострих відчуттів, недбалі, надто самовпевнені, приголомшені та сумлінні, а також обговорюють, як кожен тип може поводитися таким чином, що може зробити їх вразливими до кібератак або збільшити ризик атаки. У статті також підкреслюється важливість постійного навчання та навчання співробітників, а також впровадження таких заходів, як двофакторна автентифікація та контроль доступу, щоб зменшити ризик успішної атаки [15].

Більшість кібератак вдаються, тому що кіберзлочинцям вдається обійти людський фактор. Візьмемо, наприклад, фішингові атаки. Успішна фішингова атака вимагатиме від жертви несвідомого надання конфіденційної інформації в електронному листуванні. Подібним чином атаки IoT (Інтернет речей)

відбуваються через те, що люди випадково забувають або вирішують не захищати свої пристрої. Загальною темою тут є те, що людська помилка все ще є основним фактором у багатьох випадках кібератак.

Інше дослідження, проведене The Myers-Briggs Company та ESET, показало, що існує кореляція між типом особистості та вразливістю до різних типів кібератак, так само як і існує кореляція між займаною посадою та відповідним шаблоном поведінки [16].

Більшість компаній і людей не усвідомлюють, що знання кібербезпеки охоплює всіх, а не лише IT-спеціалістів. У статті йдеться про те, що вище керівництво може відігравати більшу роль у виявленні вразливостей у своїх командах і впроваджувати системи кібербезпеки з підходом «людина/машина», щоб зменшити людський фактор ризику.

Неодноразово досліджували цей зв’язок, і результати незмінно показують, що індивідуальні відмінності в поведінці людей впливають на те, як люди сприймають кіберзагрози, і на ймовірність їхньої ризикованої поведінки.

Одне дослідження, проведене Белдадом і де Фрізом (2010), виявило, що люди, які займаються більш ризикованою поведінкою в Інтернеті, як-от відвідування незахищених веб-сайтів і використання незахищених бездротових мереж, швидше за все недооцінюють ризики, пов’язані з такою поведінкою. Інше дослідження Веліса та Санчеса (2019) виявило, що люди з вищим рівнем ризикованої поведінки в кіберпросторі менш схильні сприймати серйозність кіберзагроз.

Ці результати показують, що індивідуальні відмінності в поведінці людей відіграють вирішальну роль у тому, як люди сприймають кіберзагрози та реагують на них. Він підкреслює важливість урахування людського фактора під час проектування систем інформаційної безпеки та розробки політики кібербезпеки.

Якщо люди покладаються на ці неточності, це може призвести до хибного відчуття безпеки або неусвідомлення потенційних ризиків.

Неточні відповіді також можуть вплинути на сприйняття людиною ризику, що може вплинути на її поведінку. Якщо люди вважають нижчий рівень ризику,

ніж той, який існує насправді, вони можуть не вживати відповідних заходів безпеки, наприклад використовувати надійні паролі, підтримувати своє програмне забезпечення в актуальному стані або бути обережними, натискаючи посилання чи завантажуючи вкладення.

З іншого боку, якщо люди відчувають вищий рівень ризику, ніж той, який існує насправді, вони можуть стати надмірно параноїдальними або тривожними, що може призвести до непотрібних або надмірних заходів безпеки, які можуть заважати їхній продуктивності або повсякденній діяльності.

Люди займають центральне місце в кібербезпеці. Отримавши відповідні навички та інструменти, люди зможуть захистити себе та свої організації від кібератак. Але люди не всі однакові. У кожного з нас своя індивідуальність. І дослідження показують зв’язок між нашими особистостями та нашою поведінкою у сфері безпеки. Якщо особистість впливає на кіберризик, універсальний підхід не є оптимальним. Спеціальний підхід краще обмежить кіберризик.

Поведінкові психологи використовують метод великої п'ятірки, щоб ідентифікувати та зрозуміти особистості. Метод включає п'ять рис особистостей. Це відкритість (openness), сумлінність (conscientiousness), екстраверсія (extraversion), прийняття (agreeableness) і нейротизм (neuroticism); скорочено OCEAN [17].

Усі ці риси є найбільш вираженими серед інших поведінкових проявів. Людина може отримати високий або низький бал для кожної риси. Риси не є ні негативними, ні позитивними. У кожного з них є свої сильні та слабкі сторони.

В таблиці нижче наведено короткий опис, особливості та аспекти, на які варто звернути увагу, якщо ставиться за ціль побудувати міцний фундамент та культуру безпеки .

Таблиця 1.1

OCEAN Велика п’ятірка рис особистості та їх вплив на кібербезпеку та людський фактор

Категорія	Короткий опис	Особливості	Вразливості	Навчальний підхід
Відкритість Openness	Схильність до фантазії та відкритість до нового досвіду	Використовує інноваційні технології та швидко адаптується до змін	Схильність довіряти незнайомим джерелам без перевірки	Заохочуйте критичне мислення та скептицизм щодо інформації в Інтернеті
Сумлінність Conscientiousness	Ступінь організованості, відповідальності та самодисципліни	Дотримується протоколів безпеки та найкращих практик	Може стати надмірно обережним і стійким до впровадження нових технологій	Проведіть комплексне навчання методам безпеки та оновлюйте протоколи
Екстраверія Extraversion	Перевага соціальної взаємодії та отримання енергії з неї	Надійна мережа з'єднань, яку можна використовувати для безпеки	Може надсилати конфіденційну інформацію в соціальних мережах	Пропагуйте безпечне онлайн-спілкування та підкреслюйте налаштування конфіденційності
Привітність Agreeableness	Схильність до співпраці та співчуття до інших	Сприяє позитивній та інклюзивній культурі кібербезпеки	Сприйнятливий до тактик соціальної інженерії, що використовують довіру	Розвивайте знання про методи соціальної інженерії та заохочуйте повідомляти про інциденти
Невротизм Neuroticism	Схильність до переживання негативних емоцій і стресів	Підвищена пильність щодо потенційних загроз	Більша ймовірність потрапити на фішингові шахрайства в умовах підвищеної тривоги	Надайте методики управління стресом і тренінги щодо фішингу

Відкритість означає відкритість досвіду. Люди, які мають високу оцінку відкритості, як правило, схильні до пригод і творчі, активно шукають новий досвід. Вони також відносно вразливі до фішингу. Через цікавість вони можуть виконувати вимоги кіберзлочинців.

Проте відкритість допомагає людям справлятися з несподіваними подразниками. Більш відкриті люди можуть краще помітити щось незвичайне. Це допомагає їм виявляти незвичні або підозрілі електронні листи.

Тим не менш, відкриті люди, швидше за все, кинуть виклик владі. Їхній кіберризик може збільшитися, якщо вони кинуть виклик правилам і нормам.

Совісні люди демонструють високий рівень надійності, організованості та самодисципліни. Вони обережні та методологічні, але прагнуть досягнути. Совісні люди схильні дотримуватись правил і приписів. Вони також більш схильні регулярно оновлювати програмне забезпечення та створювати надійні паролі. Це зменшує кіберризик в цілому.

Проте прагнення до досягнення може збільшити ризик. Сумлінна людина може повірити фішинговому електронному листу, якщо він приносить успіх або допомагає досягти її цілей. Вони можуть повірити в шахрайство миттєво, особливо під тиском.

Екстраверсійна риса особистості описує тих, хто любить товариство інших. Екстраверти оптимістичні, наполегливі, енергійні та теплі. Люди з високим рівнем екстраверсії реагують на нагороди та соціальну увагу. Кіберзлочинці використовують такі характеристики в атаках соціальної інженерії.

Проте готовність екстравертів до спілкування може допомогти створити культуру, орієнтовану на безпеку. Ініціатива повідомляти про порушення сприяє безпеці організації.

Приємні люди довірливі, співчутливі, готові співпрацювати та скромні. Оскільки вони довірливі, дуже приємні люди, швидше за все, піддадуться кібератакам. Фішингові листи з проханням про допомогу користуються особливою популярністю серед приємних людей.

Але приємні люди також дбають про безпеку. Як правило, вони краще виявляють обман. Вони також схильні демонструвати прихильність на робочому місці та високу обізнаність щодо безпеки. Їхня схильність до співпраці заохочує приємних людей повідомляти про кіберзагрози.

Невротизм відноситься до емоційної стабільності. Ті, хто має високий бал за нейротизм, імпульсивні, схильні до стресу та тривоги, сором’язливі та скептичні.

Хоча люди, які часто зображуються в негативному світлі, мають високу оцінку невротизму, можуть бути менш сприйнятливими до фішингу. Вони часто ефективно відрізняють справжні електронні листи від підроблених.

Проте дуже невротичні люди можуть приймати поспішні рішення в стресових ситуаціях. Добре продумане шахрайство може бути ефективним проти людей, які мають високі бали за цю рису.

Цифрові записи (наприклад, Facebook, історія веб-перегляду та пошукові запити) можуть містити конфіденційні дані (наприклад, стать). До них можна легко отримати доступ без згоди людини. Надалі їх можна використовувати в цільовій рекламі. Їх навіть можна використати, щоб залучити більше виборців на виборах. Тому збір даних має бути прозорим. Дійсно, це був урок, засвоєний Cambridge Analytica.

Cambridge Analytica використовувала «психографічне націлювання», використовуючи риси особистості «Великої п’ятірки», щоб надавати індивідуальні повідомлення. Вони збирали дані користувачів Facebook без явної згоди через сторонній додаток [18]. Додаток завантажили 300 тисяч людей. Невідомо їм, завантажувачі в кінцевому підсумку поділилися своїми даними, а також даними своїх друзів, додавши до набору даних, який включав 87 мільйонів людей. Дані про риси особистості були використані під час виборчої кампанії в США 2016 року. Тут учасники кампанії намагалися переконати виборців, адаптуючи меседжі до особистостей.

З тих пір отримані дані було видалено. Але скандал із Cambridge Analytica є нагадуванням про те, наскільки вразливими є люди в цифровому середовищі. Це показує, як легко можна «добувати» інформацію в Інтернеті без згоди або повного розуміння того, чим особа погоджується поділитися.

Хоча можна використовувати «психографічне» профілювання для підвищення обізнаності про кібербезпеку, цей процес має бути прозорим. Люди повинні знати, як використовується, зберігається їхня інформація та як вони можуть змінити дані або повністю видалити їх. Довіра дуже важлива для кібербезпеки.

Тому важливо надавати точну та достовірну інформацію, щоб допомогти людям приймати зважені рішення щодо запобіжних заходів безпеки та сприйняття ризику. Також важливо сприяти розвитку культури безперервного навчання та

вдосконалення, коли людей заохочують бути в курсі останніх загроз кібербезпеці та передового досвіду.

Висновки за розділом 1

Організації в різних галузях і секторах стикаються з цілою низкою загроз, від фішингу та програм-вимагачів до атак на ланцюги поставок і експлойтів нульового дня. У цьому контексті для організацій вкрай важливо прийняти проактивний і цілісний підхід до кібербезпеки, який враховує як технічні, так і людські фактори.

Людська помилка є основною причиною порушень кібербезпеки. У 2021 році він був визнаний відповідальним за 95% цих порушень відповідно до «Звіту IBM Cyber Security Intelligence Index Report» [19]. Це означає, що якби людський фактор був пом’якшений, лише 1 із 20 порушень безпеки мав би місце бути.

Люди грають вирішальну у створенні ефективної системи кібербезпеки організації та формування стійкості, необхідної для захисту від потенційного порушення. Вони знаходяться в авангарді проектування, тестування, впровадження та експлуатації засобів захисту. В той же час, їхні невдачі через злі наміри, недбалість чи незнання, стають джерелом кіберінцидентів.

Зловмисники зосереджуються на пошуку слабкої ланки в захисті фірми – того одного недоліку, що дозволить їм непомітно проникнути у систему – то чому зосереджувати свої зусилля на взломі міжмережевого екрану, коли є ідеальна можливість використати людську природу?

За дослідженням 50 основних зломів даних, неадекватні технологічні рішення сприяли 28 % атак, а решта 72% успішних хакерських зломів пов’язані з збоями в роботі людей і процесів; а саме фішингові електронні листи, шкідливі інсайдери та помилки конфігурації IT. Що ще більш дивно, дослідження IBM показало, що людська помилка була основною причиною 95% порушень кібербезпеки.

Основними типами проблем є помилки, пов’язані з набутими навичками або прийнятими рішеннями. Тому навчання з кібероюбізнаності та практика можуть суттєво змінити кількість порушень кібербезпеки.

РОЗДІЛ 2
ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕННОСТІ ВІД ІНЦИДЕНТІВ БЕЗПЕКИ, ПОВ'ЯЗАНИХ З ПОВЕДІНКОЮ ЛЮДИНОЮ

Вплив людського фактора на кібербезпеку стає дедалі очевиднішим, підкреслюючи критичну потребу звернути увагу на поведінку людей і процеси прийняття рішень з метою підвищення загальної безпеки. У цьому розділі розглянуто фундаментальні концепції та підходи, спрямовані на зменшення впливу людського фактору та пом'якшення ризиків безпеки.

Розуміння ролі людської поведінки в кібербезпеці має вирішальне значення для розробки ефективних стратегій і заходів. Існують різні підходи, які охоплюють як технічні, так і нетехнічні аспекти, починаючи від програм інформування користувачів і освітніх програм до принципів проектування, орієнтованих на користувача, і передових методів автентифікації.

Щоб забезпечити повний огляд, ці підходи згруповані в окремі групи безпеки, кожна з яких спрямована на певні області вразливості. Досліджуючи ці концепції та їхню застосовність у різних групах безпеки, відповідь на питання про те, як ефективно врахувати людський фактор у кібербезпеці та створити безпечне кіберсередовище.

2.1 Кіберпсихологія як міжгалузевий напрям науки про поведінку людини

«Кіберпсихологія» не є загальновизнаним терміном або галуззю дослідження, і немає чіткого визначення. галузь кіберпсихології зростає та стає все більш широко дослідженою, оскільки використання технологій та Інтернету продовжує розширюватися.

Зростає інтерес до розуміння того, як люди взаємодіють із технологіями та як технології впливають на людську поведінку, емоції та прийняття рішень.

Дослідження в цій галузі можуть бути міждисциплінарними, спираючись на психологію, соціологію, інформатику та інші суміжні галузі для вивчення різних аспектів взаємодії людини та технологій.

Однією з основних цілей кіберпсихології є розуміння того, як технології впливають на людську поведінку та розумові процеси, а також зворотного впливу людської поведінки на технологію [20]. Він прагне виявити психологічні чинники, які сприяють залученню людей, прийняттю рішень і досвіду в онлайн-контекстах. Вивчаючи ці фактори, дослідники та практики кіберпсихології прагнуть глибше зрозуміти інтерфейс людини та технологій та його наслідки для різних сфер, включаючи кібербезпеку.

Деякі галузі досліджень у кіберпсихології включають [21]:

- Інтернет-ідентичність: вивчення того, як люди представляють себе в Інтернеті, і чим це відрізняється від їх офлайн-персони.
- Кібербулінг: дослідження причин, наслідків та запобігання кібербулінгу та онлайн-переслідуванням.
- Інтернет-залежність: вивчення психологічних і соціальних наслідків надмірного використання Інтернету та визначення потенційних стратегій лікування.
- Соціальні медіа: аналіз того, як використання соціальних мереж впливає на самооцінку, стосунки та емоційне благополуччя.
- Віртуальна реальність: вивчення психологічного впливу захоплюючих віртуальних середовищ, у тому числі потенціалу залежності та зниження чутливості до насильства.
- Конфіденційність і безпека в Інтернеті: дослідження впливу проблем конфіденційності та безпеки на поведінку в Інтернеті, а також методи підвищення обізнаності про кібербезпеку та зниження ризиків.

Загалом, дослідження в кіберпсихології спрямовані на розуміння складних відносин між людьми та технологіями, а також на розробку стратегій сприяння позитивним результатам і мінімізації негативних наслідків.

Використовуючи кіберхологічні принципи, можна отримати уявлення про основні фактори, які впливають на поведінку людини в кіберпросторі, включаючи процеси прийняття рішень, когнітивні упередження та соціально-психологічну динаміку. Це розуміння може допомогти розробити та реалізувати ефективні заходи для підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людини.

Кіберхологія може надати цінну інформацію про мотивацію, ставлення та поведінку людей щодо кібербезпеки, дозволяючи адаптувати інформаційні кампанії для вирішення конкретних проблем. Застосовуючи кіберхологічні концепції та методології, можна розробити комплексний підхід, заснований на фактах, для покращення практик кібербезпеки, сприяння безпечній поведінці та, зрештою, зниження ризику кіберзагроз.

2.2 Огляд контролів безпеки для зменшення поверхні атак

Засоби керування безпекою можна згрупувати за призначенням. Групуючи засоби контролю відповідно до їхньої мети дій, організації можуть краще зрозуміти, як їхні засоби контролю працюють разом для захисту їхніх активів і ресурсів, і можуть визначити області, де можуть знадобитися додаткові засоби контролю [22].

Запобіжні засоби контролю: ці засоби керування призначені для запобігання виникненню інцидентів безпеки. Приклади включають засоби контролю доступу, брандмауери та шифрування.

Технічні рішення можуть бути ефективними у впровадженні профілактичних заходів, таких як брандмауери, антивірусне програмне забезпечення та шифрування. Однак навчання також необхідне, щоб гарантувати, що співробітники розуміють важливість дотримання політики та процедур безпеки, наприклад, використання надійних паролів і відсутність натискань на підозрілі посилання.

Детективні засоби контролю: ці засоби керування призначені для виявлення інцидентів безпеки або вразливостей, які можуть існувати. Приклади включають системи виявлення вторгнень, перевірки безпеки та сканування вразливостей.

Детективні засоби контролю, такі як аудит безпеки та сканування вразливостей, можуть бути реалізовані за допомогою технічних рішень. Однак навчання співробітників також може відігравати важливу роль у виявленні інцидентів безпеки, таких як розпізнавання фішингових електронних листів або підозрілої активності в мережі.

Коригувальні засоби керування: ці засоби керування призначені для виправлення або пом’якшення наслідків інцидентів безпеки, які сталися. Приклади включають процедури реагування на інциденти, процедури резервного копіювання та відновлення, а також керування виправленнями.

За допомогою технічних рішень можна запровадити коригувальний контроль, наприклад керування виправленнями та процедури реагування на інциденти. Однак навчання співробітників також є важливим для забезпечення швидкої та ефективної обробки інцидентів, а також для того, щоб працівники знали, як повідомляти про інциденти безпеки.

Стримувальні засоби контролю: Ці елементи керування призначені для запобігання потенційним зловмисникам або зловмисникам від спроб порушити безпеку. Приклади включають камери спостереження, попереджувальні банери та видимі патрулі безпеки.

Засоби стримування, такі як видимі патрулі безпеки та попереджувальні банери, як правило, не впроваджуються за допомогою технічних рішень і часто ефективніші в поєднанні з навчанням співробітників для сприяння культурі безпеки.

Компенсаційні елементи керування: ці засоби керування призначені для компенсації недоліків або вразливості, які не можуть бути повністю усунені іншими засобами керування. Приклади включають компенсаційні елементи керування для слабких паролів або невиправленого програмного забезпечення.

Компенсаційні елементи керування, такі як багатофакторна автентифікація та обмежений доступ до конфіденційних даних, можуть бути реалізовані за допомогою технічних рішень

Навчання та навчання співробітників – це в першу чергу превентивний контроль безпеки, оскільки він спрямований на запобігання інцидентам безпеки шляхом навчання працівників найкращим практикам і інформування їх про потенційні загрози. Однак він також може підтримувати інші засоби контролю безпеки, такі як детективний або компенсаційний контроль, допомагаючи співробітникам розпізнавати інциденти безпеки та повідомляти про них або компенсуючи недоліки технічних або фізичних засобів контролю.

Засоби контролю безпеки відіграють вирішальну роль у зменшенні поверхні атаки та покращенні загальної безпеки систем і мереж. Ці засоби контролю охоплюють ряд превентивних, коригувальних, детективних, стримуючих і компенсаційних заходів [23, с. 212].

Запобіжні засоби контролю призначені для проактивного запобігання інцидентам безпеки шляхом впровадження заходів, які обмежують вразливі місця та несанкціонований доступ. Коригувальний контроль зосереджений на вирішенні інцидентів і мінімізації впливу атаки. Детективні засоби контролю забезпечують моніторинг у реальному часі та сповіщення, щоб ідентифікувати події безпеки та реагувати на них. Засоби стримування відлякують потенційних зловмисників, збільшуючи ризики та витрати, пов’язані з атакою. Компенсаційні засоби контролю пропонують альтернативні заходи для підтримки безпеки, коли основні засоби контролю неефективні або недоступні. Застосовуючи комбінацію цих елементів керування безпекою, організації можуть створити багатошаровий підхід захисту, який допомагає мінімізувати вразливі місця, виявляти загрози та реагувати на них, стримувати потенційні атаки та компенсувати обмеження. Організаціям важливо ефективно впроваджувати ці засоби контролю, регулярно оцінювати їх ефективність і постійно адаптувати свої заходи безпеки для вирішення нових загроз і нових ризиків.

2.3 Microsoft Azure Sentinel – інструмент для аналітики поведінки

Microsoft Azure Sentinel — це хмарний інструмент керування інформацією про безпеку та подіями (SIEM), який використовує аналіз поведінки користувачів і суб’єктів (UEBA) для пом’якшення впливу людського фактора на кібербезпеку [24]. Аналізуючи поведінку користувачів і об’єктів, Azure Sentinel може виявляти ненормальну активність і сповіщати команди безпеки про потенційні загрози. Це допомагає організаціям швидко виявляти інциденти безпеки та реагувати на них, зменшуючи вплив людських помилок на стан безпеки.

Однією з ключових особливостей Azure Sentinel є його можливості аналізу поведінки користувачів і суб’єктів (UEBA) [25]. UEBA допомагає організаціям виявляти та реагувати на загрози безпеці, пов’язані з поведінкою користувачів або організацій, як-от інсайдерські загрози, скомпрометовані облікові записи та аномальна активність користувачів. UEBA використовує алгоритми машинного навчання, щоб встановити базову лінію нормальної поведінки для користувачів і організацій, а потім виявляє відхилення від цієї базової лінії, які можуть вказувати на загрозу безпеці.

UEBA може впливати на ризик людського фактора, допомагаючи виявляти потенційні загрози безпеці, пов’язані з поведінкою людей. Наприклад, якщо обліковий запис працівника зламано та використовується для доступу до конфіденційних даних, UEBA може виявити ненормальну поведінку користувача, наприклад доступ до даних у неробочий час або доступ до даних, до яких користувач зазвичай не має доступу. Це може допомогти організаціям виявляти й реагувати на можливі порушення даних, які можуть бути спричинені людською помилкою або зловмисною діяльністю [26].

UEBA також може допомогти організаціям виявити внутрішні загрози, наприклад, співробітників, які можуть навмисно чи ненавмисно спричиняти порушення безпеки. Відстежуючи підходу поведінки користувачів і виявляючи аномалії, UEBA може допомогти організаціям виявити потенційні внутрішні загрози та вжити відповідних заходів для зменшення ризику.

Загалом, можливості UEBA Azure Sentinel можуть допомогти організаціям покращити рівень безпеки, виявляючи загрози безпеці, пов’язані з поведінкою людей, і реагуючи на них. Це може допомогти організаціям зменшити ризик витоку даних та інших інцидентів безпеки, які можуть бути спричинені людською помилкою або зловмисною діяльністю

2.4 Підвищення обізнаності користувачів на прикладі кампанії покращення безпекової поведінки, проведеної ENISA в європейському просторі

Місяць безпеки Агентства Європейського Союзу з кібербезпеки (ENISA) – це щорічна кампанія, спрямована на підвищення обізнаності про загрози кібербезпеці та просування найкращих практик безпеки в Інтернеті [27]. Кампанія проводиться щороку в жовтні та включає серію заходів, заходів і ресурсів, щоб допомогти окремим особам і організаціям покращити свою кібербезпеку.

Основні цілі Місяця безпеки ENISA – підвищити обізнаність про загрози кібербезпеці та популяризувати належні практики кібербезпеки серед окремих осіб, організацій та урядів по всій Європі. За допомогою кампанії ENISA прагне надати практичні поради та вказівки з таких тем, як безпека паролів, фішинг, соціальна інженерія та безпечні покупки в Інтернеті.

Одним із ключових досягнень Місяця безпеки ENISA є його здатність охопити широку аудиторію та підвищити обізнаність про загрози кібербезпеці на європейському рівні [28]. Кампанія залучає широкий спектр зацікавлених сторін, включаючи національні органи влади, галузеві асоціації та неурядові організації, що допомагає забезпечити скоординований підхід до обізнаності з кібербезпеки.

Місяць безпеки ENISA також має деякі унікальні особливості, які відрізняють його від інших кампаній з підвищення обізнаності про кібербезпеку. Наприклад, кампанія підтримується рядом ресурсів, включаючи інформаційні бюлетені, відео та онлайн-вікторини, які допомагають зробити освіту з кібербезпеки цікавою та доступною. Кампанія також включає різноманітні заходи та заходи, такі як конференції та семінари з кібербезпеки, які надають можливість

окремим особам і організаціям вчитися в експертів з кібербезпеки та ділитися передовим досвідом.

Загалом Місяць безпеки ENISA є важливою ініціативою для підвищення обізнаності про кібербезпеку в Європі. Підвищуючи обізнаність про загрози кібербезпеці та просуваючи найкращі практики, кампанія може допомогти окремим особам і організаціям залишатися в безпеці в Інтернеті та зменшити ризик кібербезпеки.

За даними ENISA, кількість країн-учасниць ECSM зросла з 7 у 2012 році до 27 у 2022 році. У 2022 році в Європі було організовано понад 2400 подій і заходів, які охопили понад 7 мільйонів людей [29].

Крім того, опитування, проведене ENISA у 2022 році, показало, що 79% респондентів почуваються більш обізнаними про ризики кібербезпеки та те, як захистити себе після участі в заходах ECSM. Крім того, 83% респондентів повідомили, що вжили принаймні одну дію для покращення своєї кібербезпеки в результаті кампанії [29].

Ці статистичні дані свідчать про те, що ECSM досяг успіху в підвищенні обізнаності про ризики кібербезпеки та просуванні найкращих практик безпеки в Інтернеті по всій Європі.

2.5 Порівняльна характеристика підходів

Профілактичні контрзаходи спрямовані на запобігання інцидентам безпеки шляхом впровадження заходів, які обмежують або контролюють доступ до ресурсів. Наприклад, вимагати від користувачів використовувати надійні паролі або запроваджувати брандмауери для запобігання несанкціонованому доступу до мереж. Профілактичні контрзаходи ефективні для зниження ймовірності інцидентів безпеки, але вони можуть бути менш ефективними, якщо зловмисник може їх обійти.

Детективні контрзаходи спрямовані на виявлення інцидентів безпеки, які сталися. Цей тип контрзаходів включає моніторинг і журналювання дій у системі

чи мережі, а також використання систем виявлення вторгнень для виявлення ненормальної поведінки. Детективні контрзаходи є ефективними для виявлення інцидентів безпеки, але вони можуть не запобігти виникненню інциденту.

Коригувальні контрзаходи спрямовані на відновлення нормальної функціональності системи після інциденту безпеки. Цей тип контрзаходів включає такі дії, як відновлення з резервної копії або перенастроювання систем для видалення шкідливого програмного забезпечення. Коригувальні контрзаходи ефективні для пом’якшення впливу інциденту безпеки, але вони можуть не запобігти виникненню інциденту.

Стримувальні контрзаходи спрямовані на те, щоб перешкодити зловмисникам намагатися порушити заходи безпеки. Цей тип контрзаходів включає впровадження видимих заходів безпеки, таких як камери спостереження або попереджувальні знаки. Стримувальні контрзаходи ефективні для стримування менш досвідчених зловмисників, але вони можуть бути неефективними проти більш рішучих зловмисників.

Компенсаційні контрзаходи мають на меті компенсувати недоліки в інших засобах безпеки. Цей тип контрзаходів включає такі заходи, як впровадження додаткових засобів контролю для пом’якшення ризиків, пов’язаних із слабшими засобами контролю. Компенсаційні контрзаходи є ефективними для зниження ризику, пов’язаного зі слабкішими засобами контролю, але вони можуть не усунути основні вразливості, які створили потребу в компенсуючих засобах контролю.

Таким чином, кожен тип протидії безпеки має свої особливості, тонкощі та ефективність. Ефективність контрзаходу залежатиме від конкретної загрози безпеці, яка розглядається, а також середовища, в якому воно реалізується. Комплексна стратегія безпеки повинна включати комбінацію різних типів контрзаходів для забезпечення багаторівневого підходу до безпеки [30].

Висновки за розділом 2

Для ефективної кібербезпеки важливі як технічні рішення, так і навчання та навчання співробітників.

Технічні рішення, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення вторгнень, необхідні для захисту від відомих загроз, а також для виявлення потенційних інцидентів безпеки та реагування на них. Ці рішення можуть допомогти автоматизувати процеси безпеки, зменшити ризик людської помилки та забезпечити базовий рівень захисту для систем і даних організації.

З іншого боку, освіта та навчання працівників є критично важливими для створення культури безпеки в організації. Навчання користувачів найкращим практикам, наприклад тому, як створювати надійні паролі, як розпізнавати фішингові електронні листи та повідомляти про них, а також як безпечно обробляти конфіденційну інформацію, може допомогти зменшити ризик людської помилки та запобігти інцидентам безпеки до їх виникнення. Крім того, освіта та навчання співробітників можуть допомогти переконатися, що співробітники обізнані про останні загрози та готові належним чином реагувати у випадку інциденту безпеки.

Зрештою, найефективнішим підходом до кібербезпеки є поєднання технічних рішень і навчання та навчання співробітників. Технічні рішення забезпечують необхідну базову лінію захисту, але вони не можуть усунути всі ризики безпеки. Навчання та тренінги співробітників можуть допомогти зменшити ризик людської помилки та забезпечити, щоб співробітники були обізнані про останні загрози та найкращі практики. Поєднуючи технічні рішення з освітою та навчанням співробітників, організації можуть створити комплексну стратегію кібербезпеки, яка ефективно протидіє широкому спектру ризиків безпеки.

РОЗДІЛ 3
ПРОПОЗИЦІЯ КОНЦЕНТУАЛЬНОГО ПІДХОДУ ПІДВИЩЕННЯ КІБЕРОБІЗНАНОСТІ ДЛЯ ЗМЕНШЕННЯ ПОВЕРХНІ АТАК

Сфера кібербезпеки давно визнала значний вплив людського фактора на інциденти безпеки та вразливі місця.

Традиційні підходи до вирішення проблеми людського фактору часто спиралися на загальні програми навчання обізнаності та політики, які показали обмежену ефективність. Ці підходи, як правило, не враховують індивідуальні відмінності, різноманітність поведінки та розвиток ландшафту загроз, які формують взаємодію людини з технологіями. У результаті організації продовжують стикатися з проблемами, пов’язаними зі зменшенням площі атак, викликаних поведінкою людей.

Попередні дослідження підкреслюють, що лише однією програмою підвищення компетентності чи одним технічним рішенням не вдасться ефективно зменшити поверхню атак. Підхід має бути комплексний та перш за все орієнтованим на результат: замало ознайомити користувачів, заходи мають довгострокову мету – підняти культуру безпеки та захисту інформації на новий рівень, щоб це було в інтересах самого користувача.

Щоб усунути ці обмеження, потрібен всебічний та спеціалізований підхід, який виходить за рамки менталітету «одного розміру для всіх». Такий підхід має враховувати складну взаємодію між людською поведінкою, організаційною культурою та технологією. Він має використовувати інноваційні стратегії, передові технології та практики, що ґрунтуються на фактах, щоб підвищити обізнаність у кіберпросторі та зменшити площу атаки людини.

Враховуючи багатоаспектну перспективу та включаючи постійну оцінку та вдосконалення, ця метод прагне запропонувати більш ефективне та комплексне рішення для зменшення поверхні атаки людини.

3.1 Вхідні дані та постановка завдання

У першому розділі було визначено 15+ поведінкових тверджень, що зазвичай стають на перешкоді підвищенню компетентності. З іншого боку наявні рішення часто створені чисто «для відмітки» і не виконують покладені на них надії.

Загальні навчальні програми можуть не враховувати індивідуальні стилі навчання, посадові ролі та специфічні ризики безпеки, пов’язані з організацією. Це може призвести до відсутності взаємодії та збереження важливої інформації [30, с. 351].

Часто навчальні програми з кіберобізнаності обмежуються кількома годинами або днем, чого може бути недостатньо для охоплення всіх відповідних тем або забезпечення тривалого утримання. Співробітники можуть забути важливу інформацію незабаром після закінчення навчання [31].

Традиційні навчальні програми можуть занадто покладатися на пасивні методи навчання, такі як презентації та відео PowerPoint, які можуть бути нудними та неефективними для залучення аудиторії.

Кібербезпека полягає не лише в дотриманні правил і процедур, але й у розвитку культури безпеки, коли співробітники мають право виявляти підозрілу діяльність і повідомляти про неї. Стандартні навчальні програми можуть не сприяти розвитку такої культури [32].

Традиційні навчальні програми не можуть ефективно імітувати реальні сценарії кібербезпеки, такі як фішингові атаки або тактики соціальної інженерії. Це може призвести до того, що співробітники будуть погано підготовлені розпізнавати реальні загрози безпеці та реагувати на них.

Багато організацій не вимірюють ефективність своїх навчальних програм з кібербезпеки. Без регулярних оцінок важко визначити ефективність навчання та визначити сфери, які потребують покращення.

Загалом, незважаючи на те, що навчальні програми кіберобізнаності можуть бути ефективними для зменшення людського фактору, вони мають бути адаптовані

до потреб організації та окремої цільової аудиторії або індивіда, а також регулярно оцінювати ефективність.

Додатковим не менш важливим чинником є врахування висунутих вимог до подібних рішень. На основі досліджених ресурсів було виділено 15 тверджень, які мають бути реалізовані, щоб вважати пропозицію рентабельною та актуальною [33].

- Визначити конкретні кіберзагрози, з якими стикається організація, включаючи найпоширеніші методи атак, мотивацію зловмисників і найбільш вразливі області IT-інфраструктури організації.
- Розробити чітку та стислу політику та вказівки, які окреслюють очікування організації щодо поведінки співробітників і надають вказівки щодо того, як реагувати на потенційні кіберзагрози.
- Забезпечити регулярне та постійне навчання з кібербезпеки для всіх співробітників, включаючи базові практики кібергігієни, такі як надійні паролі, попередження про фішинг і безпечні звички перегляду.
- Проводити періодичне оцінювання для вимірювання знань співробітників і виявлення прогалин, які необхідно усунути шляхом додаткового навчання або інших заходів.
- Розробити комплексний план реагування на інциденти, у якому описано кроки, яких необхідно вжити у разі кібератаки, включаючи процедури звітування про інциденти, ізоляції постраждалих систем і відновлення нормальної роботи.
- Впровадити засоби технічного контролю, такі як брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення, щоб захистити мережу та дані організації від зовнішніх загроз.
- Впровадити засоби контролю доступу та механізми автентифікації, наприклад двофакторну автентифікацію, щоб запобігти несанкціонованому доступу до конфіденційних даних і систем.
- Регулярне тестування та оновлення засобів кібербезпеки організації, щоб переконатися, що вони залишаються ефективними проти нових і нових загроз.

- Розвиток культуру обізнаності та відповідальності щодо кібербезпеки в усій організації, а старше керівництво задасть тон решті персоналу.
- Заохочування співробітників повідомляти про потенційні інциденти з безпекою або вразливості та надання механізм для анонімних дій, якщо це необхідно.
- Забезпечення постійного спілкування та оновлення інформації про стан кібербезпеки організації та будь-які виявлені нові загрози чи вразливості.
- Встановлення партнерських стосунків та співпраця з іншими організаціями, державними установами та експертами з кібербезпеки, щоб обмінюватися інформацією та досвідом і бути в курсі останніх загроз і найкращих практик.
- Регулярний перегляд та оновлення політик та процедури кібербезпеки організації, щоб переконатися, що вони залишаються актуальними та ефективними.
- Розроблення плану повідомлень у кризових ситуаціях, щоб співробітники, клієнти та інші зацікавлені сторони були поінформовані та в курсі подій у разі великого кіберінциденту.
- Переконання, що всі сторонні постачальники та партнери, які мають доступ до мережі та даних організації, дотримуються тих самих політик і стандартів кібербезпеки, що й внутрішній персонал.

Щоб усунути ці обмеження, потрібен всебічний та спеціалізований підхід, який виходить за рамки менталітету «універсальний підхід». Такий підхід має враховувати складну взаємодію між людською поведінкою, організаційною культурою та технологією. Він має використовувати інноваційні стратегії, передові технології та практики, що ґрунтуються на фактах, щоб підвищити обізнаність у кіберпросторі та зменшити поверхню атак.

Таким чином завданням даної роботи є пропозиція масштабованого фундаментального підходу до підвищення кіберобізнаності користувачів для зменшення поверхні атак, яка включає крім самого процесу навчання процеси, що мають забезпечити ефективність та прозорість вжитих заходів.

3.2 Опис процесів для формування фундаментального підходу

Фундаментальний метод орієнтований на підвищення кіберобізнаності в будь-якому масштабі та розроблентй для вирішення проблеми людського фактора в кібербезпеці. Метод складається з п’яти окремих фаз, кожна з яких є важливою для її загальної ефективності.

Перший етап методу – етап визначення. Цей етап передбачає визначення базової лінії кіберобізнаності користувачів. Цього можна досягти, проаналізувавши організаційну політику, інструкції та позицію, або вибравши із запропонованих варіантів, включаючи низький, середній або високий рівень безпеки. Фаза визначення служить вимогою до підходу та встановлює стандарт для решти фаз.

Другий етап – етап оцінки. На цьому етапі за допомогою різних інструментів оцінюється рівень відповідності підходу вимогам. Отримані результати висвітлюють сфери, в яких користувачі вже обізнані з кібернетичними засобами, і теми, які потрібно вивчити далі, щоб покращити свої загальні знання. На цьому етапі також визначаються будь-які потенційні прогалини, які, можливо, потрібно буде усунути під час етапу навчання.

Третій етап – план навчання для підвищення компетенції в кіберобізнаності. Цей етап підходу включає різні навчальні методики, такі як ігри, лекції, відео та регулярний обмін новинами та статтями, які мають відношення до користувачів. Метою цього етапу є зменшення будь-яких прогалин, виявлених під час етапу оцінювання, і підвищення рівня знань і розуміння користувачами кібербезпеки.

Четверта фаза – це фаза аналізу, на якій аналізуються результати плану навчання, щоб визначити, чи були усунені прогалини, виявлені під час фази оцінювання, і чи покращилася загальна кіберобізнаність користувачів. Цей етап має важливе значення для визначення ефективності плану навчання та чи потрібні будь-які коригування.

Останнім етапом є етап звітності, на якому оцінюється загальна ефективність підходу. Результати етапів оцінки та аналізу порівнюються, щоб оцінити ефективність плану навчання, і визначаються будь-які області, які потребують подальшого вдосконалення. Звітування про ефективність підходу має

вирішальне значення для визначення її успіху та внесення будь-яких необхідних коригувань для майбутніх ітерацій.

Процес зображений на рисунку нижче.

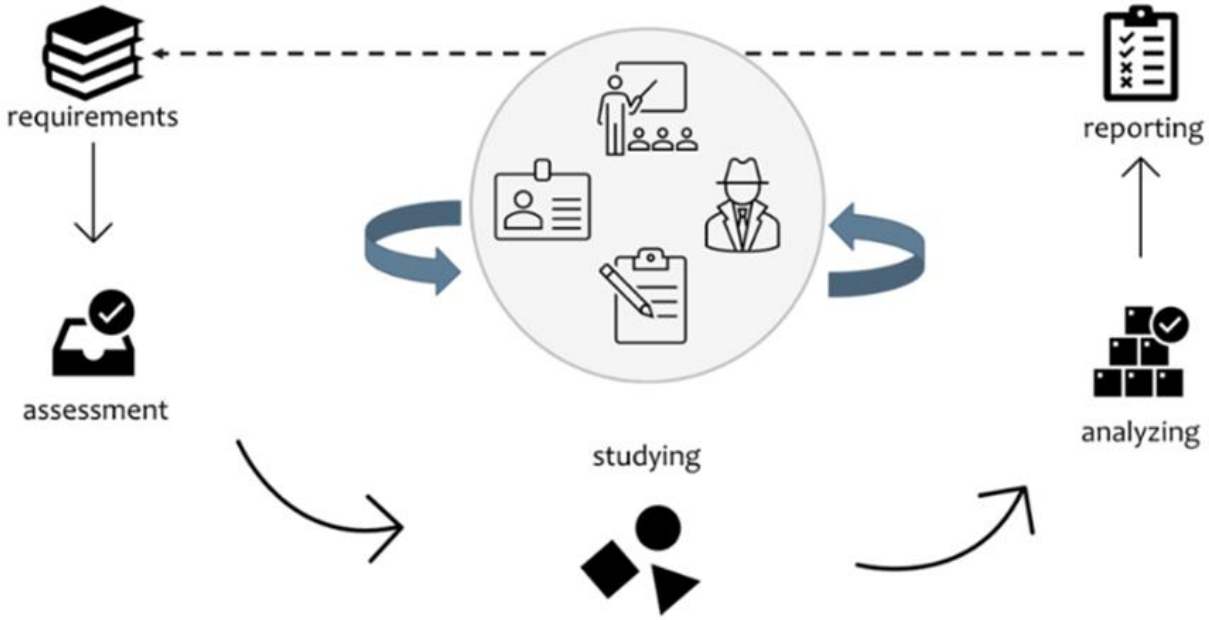

Рисунок 3.1 – Етапи фундаментального підходу з взаємозв’язками

Підсумовуючи, п’ять етапів запропонованої фундаментального підходу є важливими для підвищення кіберобізнаності в будь-якому масштабі.

Встановлюючи базову лінію для кіберобізнаності, оцінюючи відповідність, забезпечуючи навчання, аналізуючи результати та звітуючи про загальну ефективність, організації можуть зменшити свій ризик кібератак, спричинених людською помилкою.

Метод адаптується до будь-якої організації та може використовуватися для вдосконалення знань про кібербезпеку на всіх рівнях організації.

3.2.1 Етап дослідження нормативної бази для визначення вимог

Безсумнівно, вимоги є відправною точкою для кожного процесу. Як хтось сказав: «Не має значення, скільки у вас ресурсів, якщо ви не вмієте ними користуватися, цього ніколи не буде достатньо» [34].

Організації повинні знати свої прогалини та вразливі місця, щоб залатати правильну діру. Який сенс, якщо вони закривають двері, поки вікна ще відкриті? Визначити ці вимоги можна двома способами: просто вибрати потрібний рівень безпеки або пройти швидкий тест (для особистого використання) або як відповідь на проведену оцінку (аудит) на рівні організації.

Цей етап ставить на меті встановити базовий рівень кіберобізнаності користувача та визначити бажаний рівень безпеки, що може бути досягнуто декількома способами :

- Аналіз політики – перегляд організаційної політики, інструкції та стандарти, пов’язані з кібербезпекою. Визначити відповідні політики та виділіть ключові вимоги, яких повинні дотримуватися користувачі. Цей аналіз допомагає встановити основу для бажаного рівня безпеки.
- Оцінка ризику – проведення комплексну оцінку ризиків, щоб визначити потенційні загрози та вразливі місця. Оцінка впливу і ймовірності кожного ризику та визначення пріоритетів відповідно до них. Ця оцінка допомагає визначити необхідний рівень безпеки та керувати визначенням політики.
- Рамки відповідності – аналіз встановлених систем відповідності, таких як ISO 27001 або NIST Cybersecurity Framework. Ці рамки містять вказівки та найкращі практики для організацій, щоб визначити свою безпеку. Використання відповідних елементів керування та вимоги з цих структур допоможе встановити очікувану (бажану) поведінку користувачів.
- Інтерв'ю із зацікавленими сторонами - спілкування з ключовими зацікавленими сторонами, включаючи вище керівництво, IT-персонал і співробітників, щоб зрозуміти їхні погляди на кібербезпеку та їхні очікування щодо

бажаного рівня безпеки. Проведення співбесід чи опитування, щоб зібрати їхні ідеї, проблеми та вимоги.

- Індустріальні показники – дослідження галузевих контрольних показників та стандартів, характерні для сектору організації. Ці тести дають змогу зрозуміти методи кібербезпеки, прийняті подібними організаціями. Порівнення поточного стану організації з цими контрольними показниками, щоб визначити цільовий рівень безпеки.
- Консультація спеціаліста – звернення за порадою до експертів з кібербезпеки, консультантів або зовнішніх аудиторів, які мають досвід оцінки стану кібербезпеки. Їхній досвід може надати цінну інформацію та рекомендації щодо визначення бажаного рівня безпеки.
- Аналіз прогалин – проведення аналізу розбіжностей між поточною практикою кібербезпеки та бажаним рівнем безпеки. Визначення сфери, де організація потребує вдосконалення. Цей аналіз допомагає визначити конкретні цілі та завдання кампанії з підвищення обізнаності в кіберпросторі.
- Вхід управління - співпраця з керівництвом і особами, які приймають рішення, щоб зрозуміти їхні стратегічні цілі, пріоритети та толерантність до ризику.
- Галузеві правила - розгляд будь-яких конкретних галузевих норм або вимоги дотримання, яких має дотримуватися організація. Переконатися, що визначений рівень безпеки відповідає цим нормам, щоб уникнути будь-яких юридичних проблем або проблем з відповідністю.
- Внутрішня комунікація – встановлення ефективних каналів зв’язку всередині організації для поширення інформації про бажаний рівень безпеки та його обґрунтування. Проведення інформаційних сесії, семінарів або зустрічей в мерії, щоб залучити співробітників і отримати їхній внесок.

Варто пам’ятати, що конкретні способи, інструменти та заходи, які використовуються на етапі визначення, можуть відрізнятися залежно від контексту, галузі та розміру організації. Важливо пристосувати підхід до потреб і цілей організації.

Можна використати декілька технічних рішень для покращення бажаного результату встановлення бажаної поведінки для кіберобізнаності користувачів, такі як [35]:

- Інструменти керування політикою безпеки: ці інструменти допомагають аналізувати та визначати організаційні політики, інструкції та рівні безпеки. Вони забезпечують централізовану платформу для керування, перегляду та оновлення політик безпеки, забезпечуючи відповідність найкращим галузевим практикам і нормативним вимогам.
- Інструменти оцінки ризиків і відповідності: ці інструменти допомагають оцінити поточний стан безпеки в організації та виявити будь-які прогалини або вразливі місця. Вони дають уявлення про потенційні ризики та допомагають у визначенні необхідних заходів безпеки та контролю.
- Інструменти керування конфігурацією безпеки: ці інструменти дозволяють організаціям визначати та застосовувати стандарти безпечної конфігурації для своїх систем і програм. Вони допомагають переконатися, що технологічна інфраструктура організації налаштована правильно та відповідає бажаним вимогам безпеки.
- Структури та стандарти безпеки: використання встановлених структур безпеки, таких як NIST Cybersecurity Framework або ISO 27001, може забезпечити структурований підхід до визначення вимог безпеки. Ці рамки пропонують рекомендації, елементи керування та найкращі практики, які організації можуть прийняти та налаштувати відповідно до своїх конкретних потреб.
- Платформи для підвищення обізнаності та навчання у сфері безпеки: ці платформи пропонують рішення для створення та надання співробітникам інформації про безпеку та навчальних матеріалів. Вони надають інтерактивні модулі, відео, вікторини та функції відстеження прогресу, щоб покращити знання користувачів і залучити їх.
- Інструменти класифікації та захисту даних: ці інструменти допомагають у категоризації та класифікації конфіденційних даних на основі їх важливості та рівня ризику. Вони допомагають у визначенні заходів захисту даних,

таких як шифрування, контроль доступу та запобігання втраті даних, щоб забезпечити конфіденційність і цілісність конфіденційної інформації.

Ці технічні рішення сприяють етапу визначення, надаючи ефективні та ефективні способи оцінки, аналізу та визначення бажаних вимог безпеки та базового рівня для кіберобізнаності користувачів. Вони допомагають організаціям створити міцну основу для своїх зусиль у сфері кібербезпеки та узгодити свою технологічну інфраструктуру з бажаними цілями безпеки.

3.2.2 Етап перевірки на відповідність вимог

Після визначення початкового та бажаного рівнів обізнаності про кібербезпеку має сенс визначити звички людини та знайти кращий спосіб навчання. Підготувавши скелет навчального шляху, його можна адаптувати до чиїхось характеристик і мати можливість запропонувати те, що має значення та забезпечить очікуваний результат.

Основною метою даного етапу є оцінка рівня відповідності визначеним вимогам та визначити напрями для вдосконалення. Якими способами це може бути досягнуто:

- Аудити безпеки – проведення комплексних перевірок безпеки, щоб оцінити дотримання організацією визначених вимог безпеки. Ці аудити можуть проводитися всередині компанії або залучати зовнішніх аудиторів, які спеціалізуються на оцінці кібербезпеки.
- Сканування вразливостей - використання автоматизовані інструменти сканування вразливостей, щоб виявити потенційні вразливості безпеки в системах, мережах і програмах організації. Це допомагає визначити конкретні області, які потребують уваги та вдосконалення.
- Тестування на проникнення – виконання вправи з контрольованого тестування на проникнення, щоб імітувати атаки в реальному світі та оцінити здатність організації виявляти такі загрози та реагувати на них. Це допомагає

виявити слабкі місця в інфраструктурі та програмах, якими можуть скористатися зловмисники.

- Опитування обізнаності користувачів – проведення опитування або анкетування, щоб отримати відгуки від співробітників щодо їхнього розуміння найкращих практик кібербезпеки та їх відповідності визначеним вимогам. Це дає уявлення про рівень обізнаності та визначає сфери, де необхідне додаткове навчання чи освіта.
- Аналіз інцидентів безпеки - аналіз попередніх інциденти та порушення безпеки, щоб виявити закономірності, основні причини та області вразливості. Це допомагає зрозуміти прогалини в поточному стані безпеки та вжити профілактичних заходів для їх усунення.
- Оцінка відповідності - оцінка відповідності організації відповідним галузевим нормам, стандартам і структурам. Це включає оцінку того, чи відповідають запроваджені заходи безпеки вимогам, викладеним у цих правилах.
- Моніторинг поведінки користувачів – впровадження інструментів та методів моніторингу поведінки користувачів для відстеження та аналізу дій користувачів у мережі та системах організації. Це може допомогти виявити будь-яку ризиковану поведінку чи порушення правил, які можуть свідчити про необхідність додаткового навчання чи підвищення обізнаності.
- Показники безпеки та KPI – визначення та відстеження ключових показники безпеки та ключові показники ефективності (KPI), які відповідають визначеним вимогам безпеки. Ці показники можуть надати кількісно визначені дані про стан безпеки організації та допомогти оцінити прогрес з часом.
- Оцінка реагування на інцидент безпеки – оцінка ефективності можливостей реагування на інциденти організації щодо виявлення, реагування на інциденти безпеки та пом’якшення їх попередження. Це включає оцінку процедур реагування на інциденти, координацію між командами, а також швидкість і ефективність вирішення інцидентів.
- Зовнішній бенчмаркінг - порівняння практики кібербезпеки та ефективності організації з галузевими тестами, найкращими практиками та

аналогічними організаціями. Це допомагає отримати уявлення про сфери, де організація може відставати, і визначити можливості для вдосконалення.

Важливо вибирати та адаптувати методи оцінки на основі розміру організації, її складності та вимог галузі. Результати етапу оцінювання дадуть цінну інформацію, яка допоможе розробити плани навчання та вдосконалення на наступних етапах фундаментального підходу.

На етапі оцінки можна використати декілька технічних рішень для покращення бажаного результату оцінки відповідності вимогам підходу та визначення областей для вдосконалення. Ось кілька прикладів [36]:

1. Інструменти оцінки вразливості: ці інструменти сканують системи та мережі, щоб виявити потенційні вразливості та слабкі місця безпеки. Вони дають уявлення про поточний стан безпеки та допомагають визначити пріоритетні сфери, які потребують уваги та виправлення.

2. Інструменти тестування на проникнення. Інструменти тестування на проникнення імітують реальні атаки для виявлення вразливостей, якими можуть скористатися зловмисники. Вони допомагають виявити слабкі місця в системах, програмах і мережах і надають рекомендації щодо посилення засобів захисту.

3. Інструменти керування інцидентами та подіями безпеки (SIEM): Інструменти SIEM збирають і аналізують дані журналу з різних джерел для виявлення інцидентів безпеки та аномалій. Вони забезпечують видимість подій безпеки, допомагають у виявленні потенційних загроз або невідповідності політикам безпеки, а також полегшують реагування на інциденти та судово-медичні розслідування.

4. Інструменти аналітики поведінки користувачів (UBA): інструменти UBA відстежують дії користувачів, аналізують підходу поведінки та виявляють аномалії, які можуть вказувати на внутрішні загрози або скомпрометовані облікові записи. Вони допомагають ідентифікувати користувачів, яким може знадобитися додаткове навчання або розслідування через ризиковану поведінку або потенційні інциденти безпеки.

5. Платформи тестування безпеки: ці платформи імітують фішингові атаки, сценарії соціальної інженерії або інші форми тестів безпеки, орієнтованих на користувача. Вони оцінюють ефективність навчальних програм безпеки та надають показники сприйнятливості користувачів до різних типів атак.

6. Рішення для управління відповідністю: ці рішення автоматизують процес оцінки та моніторингу відповідності нормативним вимогам, галузевим стандартам і внутрішнім політикам. Вони надають механізми для відстеження та звітування про статус відповідності, виявлення прогалин і впровадження коригувальних дій.

Ці технічні рішення сприяють етапу оцінки, надаючи автоматизовані та комплексні засоби для оцінки відповідності вимогам безпеки, виявлення вразливостей і вимірювання обізнаності та поведінки користувачів. Вони дають змогу організаціям отримати точне уявлення про стан безпеки, визначити пріоритетність заходів з усунення несправностей і постійно покращувати загальну стійкість кібербезпеки.

3.2.3 Етап покращення компетентності

Третя фаза фундаментального підходу зосереджена на плані навчання для підвищення компетенції в кіберобізнаності.

Під час цього етапу використовуються різні методи та інструменти для навчання людей найкращим практикам і поведінці у сфері кібербезпеки. Навчальні сесії, семінари, модулі електронного навчання та інтерактивне моделювання можна проводити, щоб покращити знання та навички, пов’язані з кіберзагрозами, безпечними онлайн-практиками та важливістю захисту конфіденційної інформації [37].

Крім того, план навчання може включати регулярний обмін відповідними новинними статтями, тематичними дослідженнями та інформаційними ресурсами, щоб тримати людей в курсі нових кіберзагроз і тенденцій.

Мета цього етапу полягає в тому, щоб усунути прогалини в кіберобізнаності та надати людям необхідні знання та навички для прийняття обґрунтованих рішень і вжиття відповідних заходів для зменшення ризиків у їхній цифровій діяльності.

Пропонуючи комплексні та захоплюючі навчальні програми, організації можуть ефективно підвищувати кіберобізнаність серед людей, зменшуючи ймовірність інцидентів безпеки, пов’язаних з людьми, і, зрештою, сприяючи створенню більш безпечного кіберсередовища. Освітня частина складається з кількох методів:

Навчальні курси. Найпопулярнішим рішенням вважається навчання. Те, що таке навчання, може бути цінним лише тоді, коли працівник чітко розуміє зміст і знає, що він знатиме після проходження курсу.

Перевірки та тести. Загальновідомий факт, що люди схильні забувати те, чого вони навчилися. Єдиний спосіб - регулярна перевірка вивченого матеріалу, який можна отримати з тренінгів і курсів завдяки індивідуальним особливостям

Імітація атак. Для чіткого розуміння і засвоєння теорії недостатньо. Такий досвід можна отримати лише практикою. Коли люди намагаються щось зробити самі, вирішити проблему, відбити атаку, вони були мішенню, вони це запам'ятають краще. Використовуючи автоматизований підхід, можна переконатися, що люди отримують відповідний контент для атаки щодо їх діяльності, як це роблять справжні хакери. Оцінка виконується шляхом імітації атак і методів людського фактора, які використовують зловмисники для визначення ефективності політики безпеки організації, заходів безпеки та програм навчання. Наприклад, фішингова атака здійснюється шляхом масової розсилки електронних листів, які виглядають так, ніби вони надіслані від імені популярних брендів, постачальників послуг або людей, відомих адресатам. Він відстежує всіх одержувачів електронної пошти, які відкривали електронний лист, клацали посилання, відкривали вкладення та вводили своє ім’я користувача та пароль на підробленому веб-сайті. Детальна статистика дозволить отримати як загальну картину компанії, так і визначити коригувальні дії в індивідуальному порядку

Щоденні рекомендації та дайджест. Щоденне отримання невеликих порад про те, як підвищити безпеку, дайджест останніх новин і оголошень допомагає людям бути в курсі поточних тенденцій і ситуацій у світі, тому що все змінюється, і слідувати застарілим посібникам – ненайкращий підхід.

На етапі планування навчання підходу можна використовувати різні способи, інструменти та заходи для покращення кіберобізнаності та компетентності людей. Ось кілька прикладів [38]:

- Програми навчання - розробка комплексних навчальних програм, які охоплюють різні аспекти кібербезпеки, включно з передовими методами, безпечними звичками перегляду, безпечним зв’язком, керуванням паролями, обізнаністю щодо соціальної інженерії та процедурами реагування на інциденти. Ці програми можна проводити за допомогою особистих семінарів, онлайн-курсів або комбінації обох.
- Гейміфікація – такі методи зроблять навчання більш захоплюючим та інтерактивним. Це може включати створення викликів кібербезпеки, вікторин, симуляцій або навіть включення елементів змагання, щоб мотивувати учасників і покращити їхній досвід навчання.
- Симуляції фішингу - регулярні симуляції фішингу можуть навчити людей виявляти фішингові електронні листи та ефективно реагувати на них. Ці симуляції передбачають надсилання фіктивних фішингових електронних листів для оцінки вразливості користувачів і надання негайного зворотного зв’язку та навчання тому, як не стати жертвою таких атак.
- Рольове навчання - адаптування програми навчання до конкретних ролей в організації зумовлено тим фактом, що різні особи можуть мати різні обов’язки щодо кібербезпеки. Наприклад, керівникам може знадобитися навчання з конфіденційності даних і управління, тоді як IT-персонал може потребувати додаткової технічної підготовки щодо конфігурації безпечної мережі або методів безпечного кодування.
- Інформаційні матеріали – розробка та розповсюдження навчальних матеріалів, такі як інфографіка, плакати, інформаційні бюлетені або відеоуроки,

щоб підкріпити найкращі практики кібербезпеки та надавати постійні нагадування людям. Цими матеріалами можна ділитися через внутрішні канали зв'язку, такі як електронна пошта, інтранет або цифрові вивіски.

- Імітаційні вправи з нападу – проведення занять з симуляцією атак, як-от тренування з червоною командою або настільні вправи, щоб імітувати кібератаки в реальному світі та перевіряти можливості реагування організації. Ці вправи допомагають людям зрозуміти вплив інцидентів безпеки, покращити процедури реагування на інциденти та визначити сфери, які потребують покращення.
- Постійне навчання та підвищення кваліфікації - застосування підходу до безперервного навчання, який включає періодичні курси підвищення кваліфікації, оновлення щодо нових загроз і вразливостей, а також постійне спілкування з питань кібербезпеки. Це гарантує, що люди залишаються в курсі та пильними у своїх кібер-практиках.
- Співпраця та обмін знаннями - заохочення співпраці та обміну знаннями між співробітниками, створюючи форуми, дискусійні групи або онлайн-платформи, де вони можуть ділитися досвідом, ставити запитання та вчитися на думках і досвіді один одного.
- Чемпіони з безпеки - визначення лідерів з підвищення обізнаності про безпеку в організації та надання їм повноваження, які можуть виступати в якості послів кібербезпеки, просувати ініціативи з підвищення обізнаності та надавати підтримку та вказівки своїм колегам.
- Показники та оцінка - встановлення показників та механізмів оцінки для вимірювання ефективності навчальних програм. Це може включати оцінювання до та після навчання, опитування зі зворотним зв'язком або відстеження інцидентів безпеки, пов'язаних із людськими помилками, щоб оцінити вплив навчання на покращення кіберобізнаності та зменшення поверхні атаки.

Важливо не забувати налаштовувати навчальний план відповідно до конкретних потреб організації, враховувати різні стилі навчання та включати відгуки та уроки, отримані з попередніх навчальних ініціатив.

Мета полягає в тому, щоб створити привабливу та ефективну навчальну програму, яка надає людям необхідні знання та навички для пом’якшення ризиків кібербезпеки.

На етапі навчання можна використовувати різні технічні рішення для покращення бажаного результату покращення кіберобізнаності серед користувачів. Ось кілька прикладів [39]:

1. Системи управління навчанням (LMS): платформи LMS забезпечують централізований центр для доставки та керування навчальним контентом. Вони пропонують такі функції, як створення курсу, відстеження прогресу, оцінювання та звітування. LMS полегшують організацію та адміністрування навчальних програм, спрощуючи відстеження участі користувачів і моніторинг їх прогресу.

2. Платформи гейміфікації: Інструменти гейміфікації вводять ігрові елементи в навчальні програми, щоб залучити користувачів і покращити їхній досвід навчання. Ці платформи використовують бали, значки, таблиці лідерів і винагороди, щоб мотивувати користувачів брати активну участь і вдосконалювати свої навички інформаційної обізнаності.

3. Симулятори фішингу. Симулятори фішингу імітують реальні фішингові атаки та доставляють користувачам імітаційні фішингові електронні листи. Вони допомагають підвищити обізнаність про загрози фішингу та навчать користувачів, як розпізнавати спроби фішингу та відповідним чином реагувати на них. Симулятори фішингу надають миттєвий зворотний зв’язок користувачам і відстежують їхні відповіді з метою оцінки та навчання.

4. Навчальні модулі з питань безпеки: Існують різні онлайн-платформи, які пропонують готові навчальні модулі з питань безпеки, які охоплюють такі теми, як захист паролів, соціальна інженерія, захист даних і безпечний перегляд. Ці модулі можна налаштувати відповідно до конкретних потреб організації та надати користувачам за допомогою плану навчання.

5. Віртуальні навчальні середовища: Віртуальні навчальні середовища забезпечують імітацію практичного навчання для користувачів. Вони дозволяють користувачам практикувати та застосовувати свої навички кібербезпеки в

контрольованому та безпечному середовищі. Віртуальні навчальні середовища можуть імітувати реальні сценарії, такі як реагування на кібератаку або розслідування інциденту безпеки.

6. Платформи мікронавчання: Платформи мікронавчання пропонують короткі, цілеспрямовані навчальні модулі, які легко використовувати та засвоювати. Ці модулі, як правило, охоплюють конкретні теми чи концепції, і до них можна отримати доступ за вимогою. Платформи мікронавчання сприяють безперервному навчанню, надаючи невеликий, легкодоступний вміст, з яким користувачі можуть працювати у своєму власному темпі.

Ці технічні рішення покращують фазу навчання, забезпечуючи інтерактивне, захоплююче та персоналізоване навчання для користувачів. Вони полегшують доставку навчального контенту, сприяють активній участі користувачів і дозволяють організаціям відстежувати й оцінювати ефективність своїх навчальних програм.

3.2.4 Етап аналізу проведеної роботи

Етап аналізу фундаментального підходу відіграє вирішальну роль в оцінці ефективності кампанії з підвищення обізнаності в кіберпросторі та оцінці покращення кіберкомпетентності окремих осіб. Цей етап зосереджений на зборі та аналізі даних, щоб отримати уявлення про вплив програми навчання та прийняти обґрунтовані рішення щодо постійного вдосконалення.

Цілі етапу аналізу включають:

- Оцінка ефективності навчання:

Основною метою є оцінка ефективності навчальної програми щодо підвищення обізнаності учасників у кіберпросторі та зменшення поверхні атак, спричинених поведінкою людей. Це включає в себе аналіз різних точок даних, таких як оцінювання до і після навчання, опитування та відгуки, щоб виміряти рівень знань і навичок, набутих учасниками.

- Визначення сильних і слабких сторін:

Аналізуючи дані, зібрані під час навчальної програми, фаза аналізу спрямована на визначення сильних і слабких сторін кампанії. Це допомагає визначити сфери, де навчальна програма була успішною щодо вирішення людських факторів, і сфери, які потребують подальшого вдосконалення або уваги.

- Вимірювання покращення:

На етапі аналізу намагається виміряти ступінь покращення кіберкомпетентності учасників порівняно з базовим рівнем, встановленим на етапі визначення. Це включає порівняння оцінок до та після навчання, оцінку показників ефективності та відстеження ключових показників ефективності (KPI), пов’язаних з інцидентами безпеки або відповідністю політикам.

- Виявлення прогалин і проблем:

Аналіз даних допомагає виявити будь-які постійні прогалини або проблеми в обізнаності та поведінці учасників у кібернетичному просторі. Це дозволяє визначити конкретні області, де люди все ще можуть проявляти вразливість або важко дотримуватися найкращих практик безпеки. Ці відомості можуть стати основою для цільових заходів або коригування програми навчання.

- Збір і використання відгуків:

Етап аналізу має на меті зібрати відгуки та пропозиції від учасників щодо їх досвіду роботи з навчальною програмою. Цей зворотний зв’язок може надати цінну інформацію про ефективність кампанії, визначити сфери, які потрібно покращити, і внести зміни для посилення загального впливу програми.

- Прийняття рішень для постійного вдосконалення:

Етап аналізу підтримує прийняття рішень на основі даних для постійного вдосконалення інформаційної кампанії з інформаційної безпеки. Він надає необхідну інформацію для вдосконалення стратегій навчання, коригування змісту та впровадження цільових втручань для усунення виявлених слабких місць або проблем. Результати аналізу спрямовують постійне вдосконалення програми, щоб забезпечити її відповідність та ефективність.

Досягнувши цих цілей, фаза аналізу сприяє загальному успіху інформаційної кампанії. На цьому етапі надано науково обґрунтовану інформацію

та рекомендації щодо вдосконалення програми навчання, урахування людського фактору та зменшення поверхні атаки, спричиненої людською поведінкою.

Вищеперераховані цілі можуть бути досягнути наступними способами для оцінки ефективність кіберпросвітницької кампанії та оцінити покращення кіберкомпетентності окремих осіб. Ось кілька прикладів:

- Опитування та анкетування – розробка та проведенян опитування або анкети для збору відгуків від учасників щодо їхнього сприйняття навчальної програми, їхнього розуміння концепцій кібербезпеки та їхньої впевненості у застосуванні безпечних методів. Ці опитування можуть допомогти визначити сфери покращення та зібрати якісні дані для аналізу.
- Попереднє та післяоцінювання - проведення оцінювання до та після навчання, щоб оцінити знання та навички учасників до та після програми навчання. Це може включати тести, практичні вправи або зметодовані сценарії для оцінки рівня вдосконалення їхньої кіберкомпетентності.
- Моніторинг інцидентів та звітність - впровадження системи для відстеження та моніторингу інцидентів безпеки, пов’язаних із людським фактором, таких як спроби фішингу, інциденти соціальної інженерії або порушення політики. Аналізуйте звіти про інциденти, щоб визначити тенденції, загальні вразливі місця або області, де потрібне додаткове навчання чи посилення.
- Аналіз даних – аналіз даних, зібраних під час навчальної програми, як-от показники завершення навчання, продуктивність в оцінюванні або рейтинги відгуків, щоб визначити підходу, тенденції та області успіху чи покращення. Це може включати методи кількісного аналізу, такі як статистичний аналіз, щоб отримати розуміння з даних.
- Аналітика поведінки користувачів – використання інструментів аналізу поведінки користувачів, щоб відстежувати та аналізувати поведінку людей у реальному часі. Ці інструменти можуть допомогти виявити аномальну діяльність, відхилення від встановлених політик безпеки або потенційні ознаки зламаних облікових записів. Аналіз поведінки користувачів може дати цінну інформацію про сфери, які потребують додаткової уваги або цілеспрямованого втручання.

- Фокус-групи та інтерв'ю - створення фокус-групи або інтерв’ю з вибіркою учасників, щоб зібрати більш глибокі відгуки та зрозуміти їхній досвід роботи з програмою навчання. Ці якісні дані можуть надати цінні перспективи щодо ефективності кампанії та визначити конкретні проблеми чи успіхи.
- Порівняльний аналіз - порівняння результатів та даних, зібраних на етапі оцінки, з базовою лінією, встановленою на етапі визначення. Це порівняння може допомогти виміряти ступінь покращення, виявити прогалини, які все ще існують, і оцінити загальний вплив програми навчання на зменшення поверхні атаки, викликаної поведінкою людини.
- Ключові показники ефективності (KPI) – визначення відповідних ключових показники ефективності, які відповідають цілям інформаційної інформаційної кампанії. Ці ключові показники ефективності можуть включати такі показники, як час реакції на інцидент, частота інцидентів, дотримання користувачами політик безпеки або зменшення кількості інцидентів безпеки, пов’язаних із людськими помилками. Регулярно відстежуйте та аналізуйте ці KPI, щоб оцінити ефективність кампанії.
- Відгуки та пропозиції - заохочення учасників надавати відгуки та пропозиції щодо вдосконалення протягом усієї навчальної програми. Це можна зробити за допомогою опитувань, форм зворотного зв’язку або спеціальних каналів зв’язку. Аналіз цього відгуку допоможе визначити області, де можна внести коригування або вдосконалення для подальшого підвищення ефективності кампанії.
- Постійне вдосконалення – використання результатів аналізу, щоб інформувати про постійне вдосконалення інформаційної кампанії щодо кіберобізнаності. Визначення отриманих уроків, найкращі практики та області для вдосконалення, щоб гарантувати, що навчальна програма розвиватиметься та залишатиметься ефективною у вирішенні мінливих ландшафтів кіберзагроз та людських факторів.

Використовуючи ці методи аналізу та вимірювання, можна отримати корисну інформацію, оцінити вплив програми навчання та прийняти обґрунтовані

рішення щодо постійного вдосконалення та вдосконалення інформаційної кампанії з інформаційної безпеки.

На етапі аналізу фундаментального підходу можна використовувати різні технічні рішення для покращення бажаного результату оцінки ефективності навчання та оцінки покращення кіберкомпетентності користувачів. Ось кілька прикладів [40]:

1. Аналітика систем управління навчанням (LMS): платформи LMS часто надають функції аналітики та звітності, які дозволяють відстежувати й аналізувати дані користувачів. Ви можете використовувати цю аналітику, щоб оцінити залученість користувачів, відсоток проходження, результати тестів і загальний прогрес. Аналіз цих даних може допомогти визначити тенденції, сильні сторони та області для вдосконалення програми навчання.

2. Інструменти оцінювання: Існують спеціалізовані інструменти для оцінювання та оцінки кіберкомпетентності користувачів. Ці інструменти можуть включати вікторини, тести та моделювання, які вимірюють знання, навички та здатність приймати рішення щодо кібербезпеки користувачів. Результати цих оцінок можна використовувати для оцінки ефективності програми навчання та виявлення будь-яких прогалин або областей, які потребують додаткової уваги.

3. Системи керування інцидентами та подіями безпеки (SIEM): системи SIEM збирають та аналізують журнали безпеки та дані про події з різних джерел в IT-інфраструктурі організації. Аналізуючи журнали безпеки та події, організації можуть отримати уявлення про потенційні інциденти безпеки, аномалії та вразливості. Цей аналіз може допомогти виявити будь-які недоліки безпеки або помилки конфігурації, які можуть вплинути на загальний стан безпеки.

4. Інструменти аналізу поведінки користувачів (UBA): інструменти UBA відстежують та аналізують поведінку користувачів у мережі та системах організації. Вони можуть виявляти та сповіщати про незвичайні або підозрілі дії користувача, які можуть вказувати на потенційні загрози безпеці або несанкціонований доступ. Аналіз поведінки користувачів може надати уявлення

про будь-яку ризиковану або невідповідну поведінку, яку потрібно вирішити за допомогою додаткового навчання або застосування політики.

5. Інструменти опитування та зворотного зв’язку: Опитування та інструменти зворотного зв’язку можна використовувати для збору якісних даних від користувачів щодо їхнього сприйняття навчальної програми, її ефективності та їхньої загальної кіберобізнаності. Ці інструменти можуть допомогти збирати відгуки користувачів, визначати сфери вдосконалення та збирати пропозиції щодо майбутніх навчальних ініціатив.

Використовуючи ці технічні рішення на етапі аналізу, можна отримати дані та інформацію, щоб оцінити ефективність програми навчання, виміряти вдосконалення користувачів, визначити області, на які потрібно звернути увагу, і прийняти обґрунтовані рішення для підвищення загальної кіберобізнаності та зменшення атак поверхні, викликаної поведінкою людини.

3.2.5 Етап підготовки звітності та перевірки ефективності

Етап звітності фундаментального підходу є критично важливим кроком у загальному процесі підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людей.

Цей етап передбачає аналіз і представлення даних, зібраних під час етапів оцінки та аналізу, для оцінки ефективності кампанії з підвищення обізнаності в кіберпросторі та повідомлення результатів відповідним зацікавленим сторонам.

Під час цього етапу порівнюються та аналізуються дані та інформація, зібрані на етапі оцінки та аналізу. Мета полягає в тому, щоб виміряти прогрес і успіх плану навчання в покращенні кіберкомпетентності та зменшенні поверхні атак, спричинених поведінкою людини. Звітність включає створення вичерпних звітів, які висвітлюють ключові показники, такі як рівень відповідності вимогам підходу, відсоток покращення кіберобізнаності та визначення будь-яких прогалин або областей, які потребують подальшого вдосконалення.

Ці звіти є цінним відгуком для зацікавлених сторін, дозволяючи їм оцінити вплив кампанії та прийняти обґрунтовані рішення щодо майбутніх стратегій та інвестицій у кібербезпеку. Крім того, етап звітування може передбачати представлення результатів відповідним особам, командам або керівництву, наголошуючи на важливості постійних зусиль для підтримки та підвищення кіберобізнаності. Надаючи прозорі та змістовні звіти, організації можуть постійно оцінювати ефективність своїх ініціатив з підвищення обізнаності в кіберпросторі та постійно покращувати загальну безпеку.

Цілі етапу звітності включають:

- Оцінка ефективності кампанії:

Основна мета — оцінити загальну ефективність кампанії з підвищення обізнаності в кіберпросторі на основі даних і висновків, отриманих на етапі аналізу. Це включає вимірювання впливу кампанії на підвищення кіберкомпетентності учасників, зменшення вразливості та пом’якшення ризиків безпеці, пов’язаних із людським фактором.

- Презентація ключових висновків:

Етап звітування має на меті представити ключові висновки, отримані в результаті аналізу даних, у чіткій та стислій формі. Це включає підсумовування спостережених покращень, визначення областей успіху та висвітлення будь-яких постійних проблем або прогалин, які потребують уваги.

- Візуалізація даних:

Етап звітності передбачає створення візуальних зображень, таких як діаграми, графіки та інфографіка, щоб покращити розуміння та інтерпретацію даних. Візуалізація може допомогти зацікавленим сторонам легше сприймати складну інформацію та полегшити процеси прийняття рішень.

- Зв'язок із зацікавленими сторонами:

Важливою метою етапу звітування є ефективне інформування відповідних зацікавлених сторін про результати інформаційно-просвітницької кампанії. Це стосується керівництва, осіб, які приймають рішення, та інших осіб або команд, які беруть участь у плануванні та реалізації кампанії. Чітке та стисле

звітування допомагає зацікавленим сторонам зрозуміти вплив кампанії та інформує процеси прийняття майбутніх рішень.

- Рекомендації до дій:

На основі результатів фази аналізу етап звітування має на меті надати дієві рекомендації щодо подальшого покращення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людей. Ці рекомендації можуть включати коригування стратегій навчання, цільові втручання, вдосконалення політики або технологічні заходи для усунення виявлених слабких місць і проблем.

- Планування постійного вдосконалення:

Етап звітування сприяє плануванню постійного вдосконалення інформаційної кампанії з інформаційної безпеки. Це допомагає зацікавленим сторонам визначити сфери, де потрібні подальші дії, встановити цілі для майбутніх ініціатив і визначити стратегії для підвищення ефективності та впливу кампанії.

Досягнувши цих цілей, фаза звітування гарантує, що результати інформаційної кампанії в кібернетичному середовищі передаються ефективно, інформуються зацікавлені сторони та вживаються дієві кроки для постійного вдосконалення. Етап звітування є життєво важливим компонентом загального успіху кампанії, забезпечуючи чітке розуміння її впливу та інформування про майбутні процеси прийняття рішень.

На етапі звітності фундаментального підходу можна використовувати різні способи, інструменти та заходи для ефективного передачі результатів кампанії з підвищення обізнаності в кіберпросторі та оцінки її ефективності. Ось кілька прикладів [41]:

- Письмові звіти – підготовка вичерпних письмових звітів, які підсумовують ключові висновки, ідеї та рекомендації кампанії. Ці звіти можуть містити детальний аналіз, візуалізацію даних і дієві пропозиції щодо покращення.
- Резюме – створення стислих підсумків, у яких висвітлюються найважливіші висновки та рекомендації для осіб, які приймають рішення, і вищого керівництва, яким може знадобитися огляд високого рівня впливу кампанії.

- Візуалізація даних - діаграми, графіки та інфографіка для представлення складної інформації у візуально привабливому та легко зрозумілому форматі. Візуалізації можуть допомогти зацікавленим сторонам швидко осягнути ключові ідеї та полегшити ефективне прийняття рішень.
- Презентації – залучення ключових зацікавлених сторін, таких як команди менеджменту, керівники відділів або спонсори проекту, щоб продемонструвати досягнення кампанії, виклики та запропоновані дії. Інтерактивні презентації можуть стимулювати взаємодію та дискусії.
- Метрики та ключові показники ефективності (KPI) – розроблення спеціальних показників та ключові показники ефективності для вимірювання впливу кампанії та її ефективності в підвищенні кіберобізнаності та зменшенні поверхні атак, спричинених поведінкою людей. Включення цих показників у звіти забезпечить кількісну оцінку успіху кампанії.
- Порівняльний аналіз - порівняння результатів та показників поточної кампанії з попередніми кампаніями або галузевими тестами, щоб надати контекст і оцінити прогрес. Цей порівняльний аналіз може допомогти визначити сфери покращення та виміряти ефективність реалізованих стратегій.
- Опитування зацікавлених сторін або відгуки – збір відгуків від зацікавлених сторін, залучених до кампанії, таких як учасники, інструктори та менеджери, за допомогою опитувань або інтерв'ю. Ці якісні дані можуть надати цінну інформацію та перспективи щодо ефективності кампанії та визначити сфери, які потрібно покращити.
- Аналіз витрат і прибутків:

Проведіть аналіз витрат і прибутків, щоб оцінити фінансові інвестиції, зроблені в кампанію з підвищення обізнаності про кіберпростір, і порівняння із отриманими вигодами з точки зору зниження ризиків, покращення стану безпеки та потенційної економії коштів від пом'якшених інцидентів.

- Дійсні рекомендації – надання чітких та дієвих рекомендації на основі аналізу результатів кампанії. Ці рекомендації мають усунути виявлені слабкі

сторони, прогалини та області для вдосконалення, а також запропонувати практичні кроки для покращення майбутніх ініціатив з кіберобізнаності.

- План постійного вдосконалення – розробка детального плану постійного вдосконалення на основі висновків і рекомендацій етапу звітності. Окреслення конкретних дій, часових рамок, обов'язків та показників успіху, щоб гарантувати, що знання, отримані в ході кампанії, будуть перетворені на постійні вдосконалення.

На етапі звітності фундаментального підходу можна використовувати різні технічні рішення для покращення бажаного результату оцінки ефективності етапу вивчення та створення вичерпних звітів. Ось кілька прикладів [42]:

1. Інструменти візуалізації даних: використовуйте інструменти візуалізації даних для створення візуально привабливих і легких для розуміння звітів. Ці інструменти можуть допомогти представити складні набори даних у формі діаграм, графіків і інформаційних панелей, дозволяючи краще розуміти та інтерпретувати результати.

2. Інструменти бізнес-аналітики (BI): Інструменти BI дозволяють видобувати, трансформувати та візуалізувати дані з різних джерел. Вони можуть бути використані для аналізу даних, зібраних на етапах оцінювання та аналізу, надаючи уявлення про ефективність програми навчання та прогрес, досягнутий користувачами у вдосконаленні своєї кіберкомпетентності.

3. Шаблони звітів і інформаційні панелі: розробляйте індивідуальні шаблони звітів і інформаційні панелі відповідно до вимог

організації. Ці шаблони можуть надати стандартизований формат для представлення ключових показників, показників ефективності та іншої відповідної інформації, полегшуючи порівняння результатів і відстеження прогресу з часом.

4. Інструменти автоматизованого звітування: запровадьте інструменти автоматизованого звітування, які можуть генерувати регулярні звіти на основі попередньо визначених критеріїв. Ці інструменти можуть заощадити час і зусилля, автоматично збираючи та аналізуючи зібрані дані, створюючи звіти через

визначені проміжки часу та розповсюджуючи їх серед відповідних зацікавлених сторін.

5. Інтеграція з системами управління інформацією про безпеку та подіями (SIEM): інтегруйте свій процес звітування з системами SIEM, щоб включити дані про події безпеки та інциденти у звіти. Ця інтеграція може забезпечити цілісне уявлення про стан безпеки організації, пов’язуючи вплив програми навчання з подіями та інцидентами безпеки в реальному світі.

6. Платформи для співпраці та обміну: використовуйте платформи для співпраці та обміну, щоб розповсюджувати звіти та результати ключовим зацікавленим сторонам. Ці платформи забезпечують безперебійне спілкування, полегшують обговорення та спільне прийняття рішень на основі інформації, отриманої зі звітів.

Запропоновані технічні рішення можуть підвищити ефективність оцінювання ефективності етапу навчання, створювати вичерпні звіти, які висвітлюють прогрес і вплив програми навчання, і надавати цінну інформацію для подальшого вдосконалення підвищення кіберобізнаності та зменшення поверхні атаки, викликаної поведінкою людини.

Використовуючи ці способи, інструменти та заходи на етапі звітування, ви можете ефективно повідомити результати інформаційної кампанії про кіберобізнаність, поінформувати зацікавлених сторін і стимулювати постійне вдосконалення підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людей.

3.3 Специфіка використання запропонованого підходу

Запропонований метод підвищення кіберобізнаності пропонує кілька переваг, зокрема:

- Систематичний підхід: метод пропонує структурований і систематичний підхід до підвищення кіберобізнаності, який можна впровадити в будь-якому масштабі. Розбиваючи процес на окремі фази, це допомагає гарантувати, що всі необхідні кроки виконано та ніщо не пропущено.
- Можливість налаштування: метод можна налаштувати відповідно до конкретних потреб організації чи групи. Етап визначення дозволяє розробити політику, яка відображає унікальні вимоги та ризики, з якими стикається організація.
- Оцінка: метод включає фазу аналізу та звітності, яка допомагає оцінити ефективність плану навчання та визначити області для вдосконалення. Це дозволяє постійно вдосконалювати метод і гарантує, що організація залишається в курсі останніх загроз і найкращих практик.
- Постійне вдосконалення: метод заохочує постійне вдосконалення з постійним оцінюванням і навчанням, щоб переконатися, що люди з часом зберігають високий рівень кіберобізнаності. Це може допомогти зменшити ризик кіберзагроз і забезпечити готовність організації реагувати на будь-які потенційні порушення.
- Цілісний підхід: метод використовує комплексний підхід, зосереджуючись на людському факторі та використовуючи технологію для зменшення поверхні атаки, спричиненої людською поведінкою. Цей цілісний підхід забезпечує врахування як технічних, так і людських аспектів, що веде до більш ефективної стратегії кібербезпеки.
- Цільова бажана поведінка: етап визначення підходу встановлює базову лінію для кіберобізнаності користувачів. Об’єктивно визначаючи рівень обізнаності з питань кібербезпеки, організації можуть краще розуміти прогалини

та відповідним чином адаптувати свої навчальні зусилля, забезпечуючи більш цілеспрямований та ефективний підхід.

- Комплексна оцінка. Етап оцінки дає змогу зрозуміти, чи відповідають користувачі вимогам щодо кібербезпеки, і визначає сфери, які потрібно вдосконалити. Використовуючи різні інструменти оцінювання, організації отримують повне розуміння рівня кіберобізнаності користувачів, що дозволяє їм усунути конкретні прогалини в знаннях і вразливості.
- Різноманітні методи навчання: етап навчання підходу включає різні методи навчання, такі як ігри, лекції, відео та регулярний обмін новинами та статтями. Ця різноманітність підходів до навчання забезпечує залучення та враховує різні стилі навчання, роблячи навчання більш ефективним і результативним.
- Результати, що піддаються кількісному вимірюванню: запропонований підхід включає фазу звітності, яка порівнює результати оцінки та аналізу для розрахунку ефективності фази навчання. Це кількісне вимірювання прогресу надає відчутні докази впливу інформаційної кампанії з кібербезпеки, дозволяючи організаціям продемонструвати цінність своїх зусиль.
- Безперервний моніторинг: включаючи журнал безпеки та моніторинг, метод забезпечує постійну видимість поведінки користувачів у сфері кібербезпеки. Цей моніторинг допомагає виявити будь-які недоліки або відхилення від бажаних практик безпеки, дозволяючи вчасно вжити коригувальні дії та мінімізувати потенційні ризики.
- Зменшення ризику: розглядаючи людський фактор, запропонований підхід зменшує поверхню атаки, спричинену людською поведінкою. Підвищуючи кіберобізнаність користувачів і зменшуючи вразливі місця, організації можуть зменшити ризик успішних кібератак і витоку даних.
- Масштабованість: концептуальну метод можна реалізувати в будь-якому масштабі, що робить її придатною для організацій різного розміру та галузей. Незалежно від того, чи це малий бізнес, чи велике підприємство, метод

може бути адаптована та ефективно застосована, забезпечуючи послідовну обізнаність про кібербезпеку та зниження ризиків.

Ці переваги підкреслюють сильні сторони та унікальні особливості фундаментального підходу, що робить її цінним підходом для підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людей.

Загалом, метод пропонує практичний, адаптований та ефективний підхід до підвищення кіберобізнаності в будь-якому масштабі.

Висновки за розділом 3

Фази фундаментального підходу можна описати як послідовний процес, який будується один на одному для створення комплексного та ефективного підходу до підвищення кіберобізнаності та зменшення поверхні атак, спричинених поведінкою людей. Ось як пов’язані між собою фази:

На першому етапі встановлюється фундамент шляхом визначення базової лінії кіберобізнаності користувачів і встановлення вимог до підходу. Цей етап передбачає аналіз організаційної політики, інструкцій і рівнів безпеки для визначення бажаного рівня безпеки. Результати цього етапу забезпечують чітке розуміння цілей і очікувань щодо кібербезпеки.

Етап оцінювання слідує за етапом визначення та включає оцінку поточного стану кіберобізнаності серед користувачів. Щоб оцінити, чи дотримуються користувачі встановлені вимоги, і визначити сфери, які потребують покращення, використовуються різні інструменти та заходи. Результати оцінювання дають змогу зрозуміти наявні прогалини та допомагають визначити пріоритети для плану навчання.

На основі результатів оцінювання фаза плану навчання зосереджена на розробці та впровадженні навчальних програм для усунення виявлених прогалин у кіберобізнаності. Для покращення знань і поведінки користувачів використовуються різні методи навчання, такі як лекції, ігри, відео та регулярний обмін інформацією. Цей етап має на меті покращити навички кібербезпеки,

популяризувати найкращі практики та сприяти розвитку культури обізнаності щодо безпеки.

На етапі аналізу оцінюється ефективність плану навчання та вимірюється вплив на кіберкомпетентність. Це передбачає оцінку того, чи були усунені виявлені прогалини та чи покращилися обізнаність і поведінка користувачів. Цей етап може включати оцінювання, опитування та відгуки учасників, щоб оцінити результати тренінгу та виявити будь-які недоліки, що залишилися.

На етапі звітування порівнюються результати, отримані на етапі оцінювання та етапі аналізу. Він зосереджений на вимірюванні ефективності плану навчання та його впливу на зменшення поверхні атаки. Результати повідомляються через вичерпні звіти, резюме, презентації та візуалізацію даних. Етап звітування дає зацікавленим сторонам чітке уявлення про ефективність кампанії, висвітлює області успіху та надає дієві рекомендації щодо подальших покращень.

Ці фази взаємопов'язані і доповнюють одна одну. Ідеї, отримані на одній фазі, інформують про наступні фази. На етапі оцінки визначаються прогалини, які потім усуваються на етапі планування навчання. На етапі аналізу оцінюється ефективність навчання, а на етапі звітування повідомляються результати та рекомендації щодо майбутніх дій. Цей послідовний процес забезпечує систематичний підхід до підвищення кіберобізнаності та зменшення площі атаки, зосереджуючись на людському факторі та використовуючи технології як механізм.

Загалом метод пропонує більш гнучкий, орієнтований на співробітників і орієнтований на результати підхід до кіберобізнаності та безпеки, що робить її привабливою для багатьох організацій.

ВИСНОВКИ

Проактивний і спільний підхід до кібербезпеки, який залучає всіх зацікавлених сторін і враховує як технічні, так і людські фактори, може допомогти організаціям зменшити поверхню атак і підвищити стійкість до кіберзагроз.

Це дослідження показало, що різні особистості мають різний набір сильних і слабких сторін, кожна з яких має різні результати в кібератаці. Чи може реалізація більш персоналізованої політики кібербезпеки, яка обслуговує кожного працівника, допомогти пом’якшити атаки? Це може, а може і ні. Однак, допомагаючи співробітникам зрозуміти свої сліпі зони, вони можуть бути більш підготовленими та усвідомлювати потенційні атаки.

У кваліфікаційній роботі розв’язано актуальне питання стосовно зменшення поверхні атак, враховуючи особливості людського фактору, що більшою мірою і є вхідною точкою для атаки. У ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено огляд виявлених інцидентів безпеки, причиною яких стала людина за категоріями OWASP Top 10. Узагальнено типові категорії користувачів, які зазвичай є частиною кіберпростору. З огляду на проведений аналіз, потрібно враховувати особливості кожної категорії для більш ефективного підходу.

2. Встановлено причинно-наслідкові зв'язки між ментальністю людини та її поведінкою у кіберпросторі, що дає змогу зробити висновок, що запропоновані методи мають бути зосереджені саме на цьому аспекті людського фактору.

3. Обґрунтовано неефективність існуючих методів підвищення кіберобізнаності більшою мірою через їх обмежену увагу до індивідуальних стилів навчання, недостатню тривалість та утримання, пасивність методів, відсутність розвитку культури безпеки та імітації реальних загроз, а також відсутність систематичних оцінок ефективності навчання та виявлення областей для поліпшення.

4. Досліджено інструменти, методи та засоби підвищення кіберобізнаності користувачів для зменшення поверхі атак. Всі розглянуті пропозиції самі по собі є чудовим інструментом що вирішує конкретну проблему. Тільки об’єднання та правильна комбінація інструментів, методів та засобів може гарантувати результат.

5. Формалізовано вимоги до процесу підвищення обізнаності у сфері кібербезпеки для зменшення поверхні атак. Було виявлено, що метод повинен враховувати: індивідуальні стилі навчання, специфічні ризики безпеки, ефективні методи навчання, підтримку культури безпеки та реалістичні сценарії кібербезпеки.

6. Запропоновано метод зменшення поверхні атак через призму 5 етапів: дослідження, перевірка, навчання, аналіз, звітність. Запропонований метод відрізняється своєю науковою новизною та практичною значущістю, оскільки поєднує широкий спектр інноваційних підходів та методик для підвищення кіберобізнаності. Цей метод базується на вивченні індивідуальних стилів навчання, враховує специфічні ризики безпеки та пропонує ефективні методи навчання, підтримку культури безпеки та реалістичні сценарії кібербезпеки. Інтегративний підхід та акцент на практичному застосуванні робить метод інноваційним та значущим для вирішення актуальних проблем кібербезпеки.

Процес виконання даної роботи охоплював детальне дослідження інструментів, методів та засобів підвищення кіберобізнаності, вивчення різних аспектів людського фактору у кібербезпеці та розробку підходу для зменшення поверхні атак.

Результати цього дослідження відкривають нові горизонти для ефективного забезпечення кібербезпеки, сприяючи зростанню свідомості користувачів та зниженню вразливостей систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OWASP Top Ten | OWASP Foundation [Електронний ресурс] // OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. — Режим доступу: https://owasp.org/www-project-top-ten/

2. Nichols S. Marriott: Good news. Hackers only took 383 million booking records ... and 5.3m unencrypted passport numbers [Електронний ресурс] / Shaun Nichols // The Register: Enterprise Technology News and Analysis. — Режим доступу: https://www.theregister.com/2019/01/04/marriott_stolen_passport_numbers/

3. Fruhlinger J. Equifax data breach FAQ: What happened, who was affected, what was the impact? [Електронний ресурс] / Josh Fruhlinger // CSO Online. — Режим доступу: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

4. Avery D. Today Is the Last Day to File a Claim in Capital One's $190 Million Data Breach Settlement [Електронний ресурс] / Dan Avery // CNET. — Режим доступу: https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/

5. Krenz N. An Analysis of the 2020 Zoom Breach | CSA [Електронний ресурс] / Nicole Krenz // Home | CSA. — Режим доступу: https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach/

6. Correa C. LinkedIn Data Breach 2012 Case Study [Електронний ресурс] / Cecy Correa // cecy-dev. — Режим доступу: https://www.cecy.dev/blog/linkedin-2012-breach-case-study

7. Kerner S. O. S. M. SolarWinds hack explained: Everything you need to know [Електронний ресурс] / Saheed Oladimeji Sean Michael Kerner // WhatIs.com. — Режим доступу: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

8. Security Magazine [Електронний ресурс] // Security Magazine | The business magazine for security executives. — Режим доступу:

https://www.securitymagazine.com/articles/93282-lessons-learned-from-the-equifax-data-breach

9. Conger K. Florida Teenager Is Charged as ‘Mastermind’ of Twitter Hack (Published 2020) [Електронний ресурс] / Kate Conger, Nathaniel Popper // The New York Times. — Режим доступу: https://www.nytimes.com/2020/07/31/technology/twitter-hack-arrest.html

10. Siegel T. Five Years Later, Who Really Hacked Sony? [Електронний ресурс] / Tatiana Siegel // The Hollywood Reporter. — Режим доступу: https://www.hollywoodreporter.com/movies/movie-features/five-years-who-hacked-sony-1257591/

11. Walikar R. An SSRF, privileged AWS keys and the Capital One breach [Електронний ресурс] / Riyaz Walikar // Medium. — Режим доступу: https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af

12. Renaud K. Human-centred cyber security [Електронний ресурс] / Karen Renaud, Stephen Flowerday // Journal of Information Security and Applications. — 2017. — Т. 34. — С. 1. — Режим доступу: https://doi.org/10.1016/j.jisa.2017.05.007

13. Kearney P. Security: The Human Factor / Paul Kearney. — Ely : IT Governance Pub., 2010. — 60 с

14. Ergen A. Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters [Електронний ресурс] / Ahu Ergen, Ahmet Naci Ünal, Mehmet Sıtkı Saygili // Academic Journal of Interdisciplinary Studies. — 2021. — Т. 10, № 4. — С. 210. — Режим доступу: https://doi.org/10.36941/ajis-2021-0111

15. Does personality enhance susceptibility to cyber attacks? / Inka Karppinen [та ін.]. — Britain : Cybsafe, 2021. — 17 с.

16. Myers-Briggs Company. Cyberchology The Human Element. Building Resilient Teams with Cybersecurity Understanding [Електронний ресурс] / Myers-Briggs Company, ESET. — [Б. м.] : ESET, 2020. — 13 с. — Режим доступу: https://www.eset.com/fileadmin/ESET/UK/Documents/PDFs/Cyberchology_ESET_Myers-Briggs_Report2020.pdf

17. The Human Factor in Cyber Attacks: Which Personality Are You? - Pragma - Securing Your Digital Future [Електронний ресурс] // Pragma - Securing Your Digital Future. — Режим доступу: https://www.pragmastrategy.com/news/the-human-factor-in-cyber-attacks-which-personality-are-you/

18. Hern A. Cambridge Analytica: how did it turn clicks into votes? [Електронний ресурс] / Alex Hern // the Guardian. — Режим доступу: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

19. Ramlo S. The human factor: assessing individuals' perceptions related to cybersecurity [Електронний ресурс] / Susan Ramlo, John B. Nicholas // Information & Computer Security. — 2021. — Т. 29, № 2. — С. 350—364. — Режим доступу: https://doi.org/10.1108/ics-04-2020-0052

20. ESET · Digital Security Guide [Електронний ресурс] // ESET · Digital Security Guide. — Режим доступу: https://digitalsecurityguide.eset.com/en-uk/cyberchology-the-human-element-of-cybersecurity

21. Calif S. Cyberchology: The Human Element, finds a remedy in holistic cybersecurity strategies that consider personality, particularly during stressful times — The Myers-Briggs Company [Електронний ресурс] / Sunnyvale Calif // The Myers-Briggs Company — Personality Assessment Inventory & Professional Development. MBTI Assessment, MBTI Instrument, MBTI tool, FIRO Instrument, SII, Strong Assessment, CPI tool, CPI Assessment, CPI instrument, TKI assessment, Leadership Development, Career Management. — Режим доступу: https://asia.themyersbriggs.com/about-us/news-updates/press-centre/cyberchology-the-human-element-finds-a-remedy-in-holistic-cybersecurity-strategies-that-consider-personality-particularly-during-stressful-times/

22. Breier J. On Selecting Critical Security Controls [Електронний ресурс] / Jakub Breier, Ladislav Hudec // 2013 Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg, Germany, 2—6 верес. 2013 р. — [Б. м.], 2013. — Режим доступу: https://doi.org/10.1109/ares.2013.77

23. Viegas V. IT Security Controls: A Guide to Corporate Standards and Frameworks / Virgilio Viegas, Oben Kuyucu. — [Б. м.] : Apress L. P., 2022.

24. What is Microsoft Sentinel? [Електронний ресурс] // Microsoft Learn: Build skills that open doors in your career. — Режим доступу: https://learn.microsoft.com/en-us/azure/sentinel/overview

25. What is User Entity and Behavior Analytics (UEBA)? | Fortinet [Електронний ресурс] // Fortinet. — Режим доступу: https://www.fortinet.com/resources/cyberglossary/what-is-ueba

26. 1st R. K. Industrial Engineering & Human Factor Engineering / Rai Kailash 1st. — [Б. м.] : INSC International Publisher (IIP), 2021.

27. European Cybersecurity Month [Електронний ресурс] // ENISA. — Режим доступу: https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month

28. Cybersecurity Month campaign reduces Cyber Incidents [Електронний ресурс] // ENISA. — Режим доступу: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-month-campaign-reduces-cyber-incidents

29. ENISA. ECSM 2022 CAMPAIGN REPORT [Електронний ресурс] / ENISA. — [Б. м.] : ENISA, 2023. — 24 с. — Режим доступу: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2022-campaign-report

30. Trcek D. Security Models: Refocusing on the Human Factor [Електронний ресурс] / Denis Trcek // Computer. — 2006. — Т. 39, № 11. — С. 103—104. — Режим доступу: https://doi.org/10.1109/mc.2006.399

31. Oggel P. The Human Factor in Cybersecurity Breaches - Cybersecurity Insiders [Електронний ресурс] / Peter Oggel // Cybersecurity Insiders. — Режим доступу: https://www.cybersecurity-insiders.com/the-human-factor-in-cybersecurity-breaches/

32. Teal T. The Human Side of Management [Електронний ресурс] / Thomas Teal // Harvard Business Review. — Режим доступу: https://hbr.org/1996/11/the-human-side-of-management

33. Sánchez-Gordón M. Security as Culture [Електронний ресурс] / Mary Sánchez-Gordón, Ricardo Colomo-Palacios // ICSE '20: 42nd International Conference on Software Engineering, Seoul Republic of Korea. — New York, NY, USA, 2020. — Режим доступу: https://doi.org/10.1145/3387940.3392233

34. It doesn’t matter how many resources you have. If you don’t know how to use them, it | Popular inspirational quotes at EmilysQuotes [Електронний ресурс] // Popular inspirational quotes at EmilysQuotes. — Режим доступу: https://emilysquotes.com/it-doesnt-matter-how-many-resources-you-have-if-you-dont-know-how-to-use-them-it/

35. Applying Human Factors Research Tools for ITS [Електронний ресурс] / John L. Campbell [та ін.] // 1997 SAE Future Transportation Technology Conference and Exposition. — 400 Commonwealth Drive, Warrendale, PA, United States, 1997. — Режим доступу: https://doi.org/10.4271/972670

36. Shi H.-z. Analysis of Web Security Comprehensive Evaluation Tools [Електронний ресурс] / Hui-zhong Shi, Bo Chen, Ling Yu // 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 24—25 квіт. 2010 р. — [Б. м.], 2010. — Режим доступу: https://doi.org/10.1109/nswctc.2010.72

37. Gozon F. Z. Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment [Електронний ресурс] / Fanni Zsuzsanna Gozon, Daniel Vaczi, Edit Toth-Laufer // 2021 IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 16—18 верес. 2021 р. — [Б. м.], 2021. — Режим доступу: https://doi.org/10.1109/sisy52375.2021.9582520

38. Comberti L. Human Skills Assessment as a Support to Human Factor Management [Електронний ресурс] / Lorenzo Comberti, Micaela Demichela, Maria Chiara Leva // Proceedings of the 29th European Safety and Reliability Conference (ESREL), 1—5 листоп. 2020 р. — Singapore, 2020. — Режим доступу: https://doi.org/10.3850/978-981-14-8593-0_3914-cd

39. Schaefer D. Training plan evolution based on training models [Електронний ресурс] / David Schaefer, Alexander Asteroth, Melanie Ludwig // 2015 International Symposium on Innovations in Intelligent SysTems and Applications (INISTA), Madrid,

Spain, 2—4 верес. 2015 р. — [Б. м.], 2015. — Режим доступу: https://doi.org/10.1109/inista.2015.7276739

40. Embedding Cybersecurity Into Design Education: Increasing Designers' Awareness of Cybersecurity Throughout the Design Process [Електронний ресурс] / Euiyoung Kim [та ін.] // ASME 2019 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Anaheim, California, USA, 18—21 серп. 2019 р. — [Б. м.], 2019. — Режим доступу: https://doi.org/10.1115/detc2019-97720

41. Improved Grid Security Posture through Multi-factor Authentication [Електронний ресурс] / Victor Hazlewood [та ін.] // 2011 12th IEEE/ACM International Conference on Grid Computing (GRID), Lyon, France, 21—23 верес. 2011 р. — [Б. м.], 2011. — Режим доступу: https://doi.org/10.1109/grid.2011.41

42. Montasari R. Gauging the effectiveness of computer misuse act in dealing with cybercrimes [Електронний ресурс] / Reza Montasari, Pekka Peltola, Victoria Carpenter // 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, United Kingdom, 13—14 черв. 2016 р. — [Б. м.], 2016. — Режим доступу: https://doi.org/10.1109/cybersecpods.2016.7502346

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

- Petrenko Anastasiia THE ELIMINATION OF HUMAN FACTOR AND ITS EFFECTS IN CORRUPTING SECURITY / Natalia Lukova-Chuiko, Volodymyr Nakonechnyi, Anastasiia Petrenko, Anna Kyrylenko // VIII International conference “Information Technology and Implementation”, December 1-3, 2021
- Petrenko Anastasiia MISCONFIGURATIONS IN FIREWALLS AS A RESULT OF HUMAN FACTOR / Natalia Lukova-Chuiko, Ivan Parkhomenko, Anna Kyrylenko, Anastasiia Petrenko // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27-28 October 2022 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – K.: PPC "Kyiv University", 2022. – 159 pages (30-32 pages)
- Petrenko Anastasiia STRATEGIES TO REDUCE THE IMPACT OF HUMAN FACTOR ON CYBER RESILIENCE / Ivan Parkhomenko, Anna Kyrylenko, Anastasiia Petrenko // “Problems of Cybersecurity of Information and Telecommunication Systems” (PCSITS): Collection of reports and abstracts; Kyiv city, 27 April 2023 year; Taras Shevchenko National University of Kyiv / Editorial board.: V.V. Il′chenko, Dr. Phys.-Math. Sc., Prof., (Head); and others. – K.: PPC "Kyiv University", 2023. – 166 pages (78-80 pages)