Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Механізм захисту користувачів інформаційної системи від атак соціальної інженерії»

Виконавець: студентка IV курсу, групи КБ-43

_____ **Вероніка ПАНАС**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Юрій ЩЕБЛАНІН
Нормоконтроль		Яніна ШЕСТАК

Київ 2025

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
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студентці **КБ-43** **Панас Вероніці Миколаївні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Механізм захисту користувачів інформаційної системи від атак соціальної інженерії

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Типи атак соціальної інженерії, моделі захисту

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з типами атак соціальної інженерії, існуючими моделями захисту користувачів інформаційної системи від атак соціальної інженерії, провести їх аналіз та порівняння, обрати, обгрунтувати та адаптувати найефективнішу з них для розробки механізму захисту.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблений механізм захисту користувачів інформаційної системи від атак соціальної інженерії можна застосовувати

у реальних організаціях з метою підвищення ефективності захисту.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Вероніка ПАНАС
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 05.12.2024	*виконано*
2	Аналіз літератури	06.12.2024 – 29.12.2024	*виконано*
3	Обґрунтування вибору рішення	20.01.2025 – 03.02.2025	*виконано*
4	Аналіз підходів та концептуальних основ соціальної інженерії	04.02.2025 – 18.02.2025	*виконано*
5	Дослідження основних типів атак соціальної інженерії	19.02.2025 – 05.03.2025	*виконано*
6	Порівняльний аналіз існуючих моделей захисту від атак соціальної інженерії та визначення найбільш ефективної моделі	06.03.2025 – 27.03.2025	*виконано*
7	Розробка структури та алгоритму впровадження механізму захисту на основі обраної та обгрунтованої моделі	28.03.2025 – 16.05.2025	*виконано*
9	Оформлення пояснювальної записки	17.05.2025 – 30.05.2025	*виконано*
10	Підготовка до захисту кваліфікаційної роботи	31.05.2025 – 13.06.2025	*виконано*

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Вероніка ПАНАС
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 82 сторінки, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки, список джерел. У пояснювальній записці кваліфікаційної роботи міститься 12 рисунків і 5 таблиць.

Метою роботи є підвищення ефективності захисту користувачів інформаційної системи від атак соціальної інженерії шляхом вибору, адаптації та обґрунтування моделі захисту.

Для досягнення зазначеної мети поставлено наступні завдання:

1. Проаналізувати підходи та концептуальні основи соціальної інженерії як загрози інформаційній безпеці організацій;

2. Дослідити основні типи атак соціальної інженерії та психологічні механізми їх впливу на користувачів інформаційних систем;

3. Провести порівняльний аналіз існуючих моделей захисту від атак соціальної інженерії та визначити найбільш ефективну модель;

4. Розробити структуру механізму захисту користувачів інформаційної системи на основі обраної та обгрунтованої моделі;

5. Створити алгоритм впровадження розробленого механізму захисту користувачів інформаційної системи від атак соціальної інженерії.

Об'єктом дослідження є процес захисту користувачів інформаційних систем від атак соціальної інженерії в оранізаціях.

Предметом дослідження є моделі та підходи до забезпечення захисту користувачів інформаційних систем від атак соціальної інженерії.

Практичною цінністю отриманих результатів є те, що розроблений механізм захисту користувачів інформаційних систем від атак соціальної інженерії можна застосовувати у реальних оранізаціях з метою підвищення ефективності захисту.

Ключові слова: соціальна інженерія, захист інформаційних систем, виявлення загроз, аналітика поведінки користувачів, механізм захисту.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

МБРП	–	модель безпеки робочого простору
API	–	Application Programming Interface, програмний інтерфейс додатку
APT	–	Advanced Persistent Threat, розвинені постійні загрози
AWS	–	Amazon Web Services, хмарні сервіси Amazon
BEC	–	Business Email Compromise, компрометація ділової електронної пошти
CEF	–	Common Event Format, загальний формат подій
DNS	–	Domain Name System, система доменних імен
EDR	–	Endpoint Detection and Response, виявлення та реагування на кінцевих точках
GDPR	–	General Data Protection Regulation, загальний регламент захисту даних
HIPAA	–	Health Insurance Portability and Accountability Act, закон про мобільність та підзвітність медичного страхування
IAM	–	Identity and Access Management, управління ідентифікацією та доступом
IoT	–	Internet of Things, інтернет речей
IP	–	Internet Protocol, інтернет протокол
ITSM	–	IT Service Management, управління IT-послугами
JSON	–	JavaScript Object Notation, нотація об'єктів JavaScript
LEEF	–	Log Event Extended Format, розширений формат журналу подій
LMS	–	Learning Management System, система управління навчанням
MTTD	–	Mean Time To Detection, середній час виявлення

NIST	–	National Institute of Standards and Technology, національний інститут стандартів і технологій
PAM	–	Privileged Access Management, управління привілейованим доступом
PCI DSS	–	Payment Card Industry Data Security Standard, стандарт безпеки даних індустрії платіжних карток
REST	–	Representational State Transfer, передача репрезентативного стану
RSA	–	Rivest-Shamir-Adleman, алгоритм шифрування з відкритим ключем
SaaS	–	Software as a Service, програмне забезпечення як послуга
SIEM	–	Security Information and Event Management, управління інформацією та подіями безпеки
SOAP	–	Simple Object Access Protocol, простий протокол доступу до об'єктів
STIX/ TAXII	–	Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information, структурований обмін інформацією про загрози
TCR	–	Threat Coverage Ratio, коефіцієнт покриття загроз
TLS	–	Transport Layer Security, безпека транспортного рівня
UEBA	–	User and Entity Behavior Analytics, аналітика поведінки користувачів та сутностей
XML	–	eXtensible Markup Language, розширювана мова розмітки

ВСТУП

Актуальність. За останні роки значно зросла кількість та складність атак соціальної інженерії, що створило нові виклики для забезпечення інформаційної безпеки організацій. Аналіз кіберзагроз показує еволюцію методів атак [2]. Традиційні технічні засоби захисту, які базуються на периметричній моделі безпеки, виявилися недостатньо ефективними проти загроз, що експлуатують людський фактор як найслабшу ланку в системі кібербезпеки.

Масштаби загрози вражають: майже всі сучасні кібератаки експлуатують людський фактор. За даними Verizon Data Breach Investigations Report, користувачі реагують на фішингові повідомлення протягом 21 секунди, вводячи конфіденційні дані вже через півхвилини [14]. При цьому середній час виявлення таких інцидентів перевищує 9 місяців, що робить традиційні методи захисту малоефективними.

Еволюція методів соціальної інженерії характеризується активним використанням технологій штучного інтелекту для створення deepfake контенту, високим рівнем персоналізації атак через аналіз даних соціальних мереж та появою гібридних векторів впливу, що поєднують цифрові та фізичні канали. Пандемія COVID-19 спричинила подвоєння частоти кібератак внаслідок масового переходу на віддалену роботу, що створило додаткові вразливості в корпоративних інформаційних системах.

Аналіз сучасного стану досліджень показує відсутність системного підходу до порівняння різних моделей захисту від атак соціальної інженерії. Більшість існуючих наукових робіт зосереджена на окремих аспектах проблеми або конкретних технічних рішеннях, не враховуючи комплексний характер загроз та необхідність інтеграції технологічних, організаційних та поведінкових факторів захисту. Відсутні обґрунтовані методики вибору оптимальних моделей захисту та структуровані алгоритми їх практичного впровадження.

В українському контексті проблема набуває особливої гостроти через підвищені кіберзагрози в умовах повномасштабного вторгнення, необхідність забезпечення відповідності міжнародним стандартам інформаційної безпеки та активну цифрову трансформацію державних і приватних організацій. Брак науково обґрунтованих рекомендацій щодо захисту від атак соціальної інженерії створює серйозні прогалини в системі національної кібербезпеки.

Таким чином, розробка ефективного механізму захисту користувачів інформаційної системи від атак соціальної інженерії на основі порівняльного аналізу існуючих моделей захисту та створення алгоритму їх впровадження є актуальним науково-практичним завданням, що має важливе значення для підвищення рівня кібербезпеки сучасних організацій.

Метою кваліфікаційної роботи є підвищення ефективності захисту користувачів інформаційної системи від атак соціальної інженерії шляхом вибору, адаптації та обґрунтування моделі захисту.

Об'єкт дослідження: процес захисту користувачів інформаційних систем від атак соціальної інженерії в оранізаціях.

Предмет дослідження: моделі та підходи до забезпечення захисту користувачів інформаційних систем від атак соціальної інженерії.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Дослідженням у галузі захисту від атак соціальної інженерії займаються науковці багатьох провідних установ світу. Проблематику розглядають дослідники провідних навчальних закладів України, які пропонують різноманітні підходи до підвищення рівня кібербезпеки та захисту користувачів інформаційних систем.

Фундаментальні дослідження психологічних основ соціальної інженерії представлені роботою Роберта Чалдіні "Influence: The Psychology of Persuasion", де систематизовано шість ключових принципів психологічного впливу: авторитет, соціальний доказ, послідовність, взаємність, симпатія та дефіцит. Ці принципи стали теоретичною основою для розуміння механізмів соціальної інженерії та розробки методів протидії [1].

Практичні аспекти соціальної інженерії детально досліджені К. Мітніком, який визначає соціальну інженерію як "мистецтво та науку змушувати людей виконувати дії або розкривати конфіденційну інформацію" [1]. Більш формальне визначення надають Хаднаї та Абрахам, які описують соціальну інженерію як "процес психологічного маніпулювання людьми з метою виконання дій або розкриття конфіденційної інформації, який базується на використанні людських слабкостей замість технічних вразливостей" [4].

Аналіз ефективності атак соціальної інженерії проведено у дослідженні компанії RSA, де показано, як атака 2011 року розпочалася з електронного листа із заголовком «План рекрутингу на 2011 рік», що призвело до компрометації критично важливої інформації [3]. Це підтверджує важливість розуміння людського фактора як найслабшої ланки в системах безпеки.

Сучасні статистичні дослідження представлені у звіті компанії Check Point спільно з Dimensional Research, згідно з яким 43% із 853 опитаних IT-спеціалістів повідомили, що ставали об'єктами атак соціальної інженерії [5]. Особливо вразливими виявилися нові співробітники - 60% респондентів відзначили їх як групу з високим ризиком.

Дослідження поширеності атак показують критичну ситуацію: за даними Egress (2024), 94% організацій зазнали фішингових атак, а згідно з SentinelOne (2025), 98% кібератак використовують соціальну інженерію [13, 6]. Barracuda повідомляє, що генеральні директори отримують в середньому 57 цільових фішингових атак на рік, а IT-персонал - 40 атак на рік [7].

Економічний вплив атак досліджений IBM Security, яка встановила, що середня вартість витоку даних у 2024 році становить $4,88 млн, при цьому скомпрометовані облікові дані мають найдовший час виявлення - 292 дні [8]. FBI IC3 зафіксувало збитки від BEC-атак у розмірі $2,77 млрд за 21,442 випадки у 2024 році [9].

Технічні аспекти захисту розглядаються у дослідженнях OWASP Top 10 2021, де показано, що порушення контролю доступу виявлено у 94% протестованих додатків [10]. IBM Security демонструє, що 73% усіх витоків

даних у хмарних середовищах відбуваються через неправильно налаштовані сховища даних [8].

Аналіз вразливостей IoT-систем показує понад 10,54 мільйона атак на IoT-пристрої лише за грудень 2022 року [12]. Дослідження також виявили, що 67% організацій мають неналежно налаштовані системи управління доступом [11].

Правові аспекти захисту в Україні регламентуються Законом України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII [15, стаття 1, 8, 12], Національною стратегією кібербезпеки України (Указ Президента № 447/2021), Законом України "Про захист персональних даних" № 2297-VI [16, 17, статті 6, 24, 28].

Існуючі дослідження моделей захисту представлені фрагментарно. Модель безпеки робочого простору розглядається як комплексний підхід, що поєднує технологічні, процедурні та антропоцентричні елементи. Модель нульової довіри досліджується в контексті принципу "ніколи не довіряй, завжди перевіряй". Модель навчання та підвищення обізнаності базується на принципах безперервного навчання та персоналізації контенту.

Аналіз літератури показує відсутність комплексних досліджень, що порівнюють різні моделі захисту від атак соціальної інженерії. Особливо обмеженими є дослідження моделі User and Entity Behavior Analytics (UEBA) як засобу протидії соціальній інженерії. Відсутні також структуровані алгоритми впровадження механізмів захисту, що враховували б практичні потреби організацій різного масштабу.

Галузь застосування. Розроблений механізм захисту користувачів інформаційних систем від атак соціальної інженерії можна застосовувати у реальних оранізаціях з метою підвищення ефективності захисту користувачів інформаційної системи від атак соціальної інженерії.

Практична цінність полягає у тому, що розроблений механізм захисту користувачів інформаційних систем від атак соціальної інженерії можна застосовувати у реальних оранізаціях з метою підвищення ефективності захисту користувачів інформаційної системи від атак соціальної інженерії.

Завдання дослідження:

1. Проаналізувати підходи та концептуальні основи соціальної інженерії як загрози інформаційній безпеці організацій;
2. Дослідити основні типи атак соціальної інженерії та психологічні механізми їх впливу на користувачів інформаційних систем;
3. Провести порівняльний аналіз існуючих моделей захисту від атак соціальної інженерії та визначити найбільш ефективну модель;
4. Розробити структуру механізму захисту користувачів інформаційної системи на основі обраної та обгрунтованої моделі;
5. Створити алгоритм впровадження розробленого механізму захисту користувачів інформаційної системи від атак соціальної інженерії.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Концептуальні основи соціальної інженерії

Соціальна інженерія як інструмент подолання захисних бар'єрів має глибоке коріння у світовій історії. Легендарна історія Троянського коня з 1184 року до нашої ери залишається хрестоматійним прикладом того, як грамотно побудована обманна схема здатна нейтралізувати найміцніші оборонні споруди. Цей стародавній епізод ілюструє незмінну закономірність: фізичні бар'єри безпеки можуть виявитися марними перед обличчям ретельно спланованого психологічного впливу.

Сучасна наука пропонує кілька підходів до розуміння феномену соціальної інженерії. К. Мітнік характеризує її як «мистецтво та наука змушувати людей виконувати дії або розкривати конфіденційну інформацію» [1]. Більш формально, згідно з дослідженнями Абрахам і Ченгалур-Сміт, соціальна інженерія визначається як "процес психологічного маніпулювання людьми з метою виконання дій або розкриття конфіденційної інформації, який базується на використанні людських слабкостей замість технічних вразливостей" [4].

У контексті сучасної кібербезпеки маніпулятивні техніки перетворилися на потужний засіб несанкціонованого проникнення в інформаційні системи. Парадоксально, але цей метод демонструє вищу ефективність порівняно з пошуком складних технічних уразливостей. Доки вартість вразливості нульового дня на підпільних ринках сягає десятків тисяч доларів, впровадження шкідливого коду через психологічний обман може обходитися зловмисникам у копійки.

Успіх подібних атак напряму залежить від якості підготовленої приманки. Практика показує, що найефективніші варіанти варіюються від вірусних

публікацій у соціальних мережах до електронних листів з темами, максимально релевантними для конкретного адресата. Показовим випадком є атака на корпорацію RSA 2011 року, яка розпочалася з нібито безневинного листа із заголовком «План рекрутингу на 2011 рік». Один співробітник відкрив вкладений файл, що запустило ланцюгову реакцію подій і призвело до компрометації критично важливих корпоративних даних [3].

Технічне зламування потребує глибокого володіння програмуванням та розуміння архітектури систем. Психологічний же вплив базується на принципово іншому наборі компетенцій - розумінні того, які стимули здатні спровокувати цільову особу на потрібну реакцію. Основою такого підходу є використання базових людських інстинктів: довіри, цікавості, страху, жадібності та інших емоційних тригерів, які примушують людину діяти всупереч власним безпековим інтересам.

Сучасні зловмисники застосовують персоналізовані методи збору розвідувальних даних, фокусуючись на професійному середовищі та особистих захопленнях потенційних жертв. Найбагатшим джерелом такої інформації є соціальні платформи. LinkedIn надає детальну картину кар'єрного шляху та функціональних обов'язків, тоді як Facebook розкриває особисті інтереси, коло близького спілкування та способи проведення вільного часу. Дослідження виявили цікаву закономірність: середній фейковий акаунт у Facebook має понад 700 контактів, що в кілька разів перевищує показники звичайного користувача.

Дослідження Check Point спільно з Dimensional Research за участю 853 IT-фахівців з різних країн показало тривожну статистику: 43% респондентів особисто стикалися з атаками соціальної інженерії. Найбільш уразливою категорією виявилися новопризначені співробітники - 60% опитаних визначили їх як групу підвищеного ризику. Рівень підготовки персоналу залишається критично низьким: регулярне навчання проводять лише 25% організацій, а понад третина взагалі не мають систематичних програм підвищення обізнаності у сфері інформаційної безпеки [5].

Можна впевнено стверджувати, що концептуальний фундамент соціальної інженерії спирається на розуміння людського фактора як найслабшої ланки в архітектурі інформаційної безпеки. Ефективність таких атак полягає не в технічній витонченості, а в майстерному застосуванні психологічних механізмів та соціальних взаємодій для досягнення злочинних цілей.

1.2 Основні типи атак соціальної інженерії

Соціальна інженерія використовує вразливості людської психології для обходу традиційних технічних засобів захисту і здобуття несанкціонованого доступу до ресурсів організації. Сучасні зловмисники поєднують аналіз цілі, персоналізацію повідомлень і автоматизацію процесів, що робить атаки дедалі витонченішими та складнішими для виявлення [4, 18].

Класифікація основних типів атак соціальної інженерії дозволяє краще зрозуміти механізми їхнього впливу, визначити ознаки виявлення та сформулювати релевантні підходи до захисту. Типи атак умовно поділяються за методами взаємодії, цілями зловмисників та ступенем персоналізації впливу.

1. Фішинг - являє собою одну з найпоширеніших форм соціальної інженерії, що полягає в надсиланні підроблених повідомлень, переважно електронних листів, які імітують офіційну кореспонденцію довірених організацій. Метою таких атак є спонукання одержувача добровільно передати конфіденційні відомості, наприклад логіни, паролі чи платіжні дані .

2. Спеціалізований фішинг (Spear Phishing) відрізняється від широкомасштабних розсилок тим, що зловмисники ретельно готують повідомлення для конкретних осіб або організацій. Використовуючи дані про ціль, вони налаштовують зміст і стиль повідомлення, що робить його більш переконливим і персоналізованим .

3. SMS-фішинг (Smishing) являє собою варіацію фішингу, що використовує SMS-повідомлення замість електронної пошти. Зловмисники надсилають текстові повідомлення з посиланнями на шкідливі сайти або просять

відповісти з конфіденційною інформацією. Цей метод особливо ефективний через високий рівень довіри користувачів до SMS та їхню схильність швидко реагувати на текстові повідомлення.

4. Голосовий фішинг (Vishing) передбачає використання телефонних дзвінків для обману жертв та отримання конфіденційної інформації. Зловмисники часто використовують технології зміни голосу або автоматизовані системи, що імітують легітимні організації [19]. Цей метод експлуатує довіру людей до голосового спілкування та створює відчуття терміновості.

5. Претекстування - це техніка, коли зловмисник створює правдоподібний привід і видає себе за іншу особу, щоб витягти з жертви потрібні дані. Атака починається зі створення детального фальшивого профілю, на основі якого будуються довірчі стосунки з ціллю.

6. Діпфейки - це підроблені аудіо- та відеозаписи, синтезовані штучним інтелектом, які здаються автентичними. Така технологія дедалі частіше використовується в атаках соціальної інженерії для переконливих сценаріїв.

7. Компрометація ділової електронної пошти (BEC) є однимии з найпоширеніших і найвитратніших атак. Зловмисники вивчають організаційну структуру та стиль спілкування керівництва, потім видають себе за топ-менеджерів із проханням про термінові перекази або передачу конфіденційних документів.

8. Фізичні методи

Підвезення (Tailgating) — фізичний метод, що передбачає проникнення в захищену зону, використовуючи ввічливість співробітників. Зловмисник іде за особою з карткою доступу, вдаючи водія з вантажем або відвідувача.

Приманка (Baiting) — використовує цікавість або жадібність жертви. Атака полягає в тому, щоб підкинути файли або пристрої з шкідливим програмним забезпеченням, замасковані під оновлення програми чи привабливий бонус.

Медова пастка (Honey Trap) — метод, коли зловмисник створює фальшивий романтичний зв'язок з жертвою для отримання її довіри та подальшої експлуатації.

Усі наведені методи соціальної інженерії спираються на дві ключові вразливості: емоційну реакцію людини та брак пильності. Їх ефективність базується на використанні природних психологічних механізмів прийняття рішень.

Класифікація основних типів атак соціальної інженерії та відомі приклади їх реалізації в історії наведено на рис. А.1.

1.3 Психологічні основи та методи впливу в соціальній інженерії

Психологічні механізми становлять основу будь-якої успішної атаки соціальної інженерії. Зловмисники розглядають людську психіку як найточніший інструмент для досягнення своїх цілей, майстерно використовуючи обманні тактики та маніпулятивні прийоми. Вони експлуатують природні особливості процесу прийняття рішень, розуміючи, що поведінкові патерни людини підпорядковуються принципу "стимул-реакція" і залишаються досить передбачуваними.

Типовий кіберзлочинець, що спеціалізується на психологічному впливі, володіє унікальним набором особистісних якостей. Вони демонструють неабияку спостережливість і глибокий інтерес до людської натури, постійно вдосконалюючи навички читання невербальних сигналів. Інтонаційні зміни, мікровирази обличчя, жестикуляція - усе це стає джерелом цінної інформації для планування подальших дій.

Профіль та ключові навички зловмисників у атаках соціальної інженерії систематизовано на рис. А.2.

Представлена на рис. А.2 комбінація компетенцій дозволяє реалізувати багатоетапну стратегію психологічного впливу. У практичному застосуванні це виявляється у вигляді складного алгоритму взаємодії з потенційною жертвою.

Коли зловмисник фіксує ознаки підозри або недовіри, він тактично змінює підхід, зосереджуючись на поступовому відновленні психологічного контакту. За статистикою, 84% професійних соціальних інженерів полишають поточну ціль при перших ознаках серйозного опору, щоб уникнути ймовірності викриття. Проте після встановлення необхідного рівня довіри вони переходять до реалізації основних завдань, формулюючи запити з підвищеним ризиком, але й потенційно більшою віддачею. Цей алгоритм поведінки зловмисника представлено на рис. А.3.

Збір розвідувальної інформації передує безпосередньому контакту з цільовою особою. Сучасні зловмисники витрачають від 2 до 6 тижнів на детальне вивчення цифрового сліду потенційної жертви через соціальні платформи, професійні мережі та відкриті онлайн-ресурси. Їх цікавлять повсякденні звички, мовні особливості, коло професійного та особистого спілкування. На практиці це виявляється у створенні детального психологічного портрета, що включає індивідуальні потреби, страхи та мотиваційні тригери.

Отримані дані дозволяють адаптувати комунікаційний підхід під конкретні особливості світогляду та поведінкових патернів жертви. Кінцева мета полягає у створенні ситуації, за якої цільова особа добровільно надасть доступ до конфіденційної інформації або корпоративних ресурсів. У більшості випадків жертви не усвідомлюють шкідливий характер взаємодії, сприймаючи її як звичайне ділове спілкування або навіть вигідну співпрацю.

Алгоритм формування довіри та механізми психологічного впливу є основою реалізації вдалої атаки, адже жодна атака зловмисника не відбудеться без першочергового формування довіри. Незалежно від того, чи використовується електронна пошта, телефон або особиста зустріч, все починається з того, що жертва повірить у вигадану історію. Саме це відкриває шлях для подальших дій, які зрештою призводять до порушення безпеки.

Люди інтуїтивно ставлять собі низку запитань при першому знайомстві:

- Чи ця людина мені симпатична?
- Хто вона така?

- Чому вона до мене звернулася?
- Чи має вона наді мною вплив?

Зловмисники знайомі з цими «фільтрами», що спрацьовують за долі секунди, і прагнуть одразу дати на них переконливі відповіді. Це допомагає їм швидко зруйнувати бар'єри недовіри та отримати контроль над ситуацією. Механізм формування довіри через відповіді на ключові запитання жертви представлено на рис. А.4.

Принципи психологічного впливу Роберта Чалдіні в соціальній інженерії. Концептуальна система психологічного впливу, розроблена Робертом Чалдіні у праці "Influence: The Psychology of Persuasion" (1984), первісно створювалася для аналізу легітимних механізмів переконання в комерційній діяльності та маркетингових комунікаціях [1]. Шість базових принципів впливу, систематизованих дослідником, згодом привернули увагу кіберзлочинців як ефективний інструментарій для подолання людського фактора в системах інформаційної безпеки [12]. Сучасна статистика демонструє тривожну тенденцію: 35% корпорацій зафіксували зростання кіберінцидентів, де психологічне маніпулювання посідає лідируючі позиції серед векторів атак, випереджаючи навіть APT та ransomware [12]. Зловмисники адаптували класичні моделі впливу під власні потреби, трансформувавши їх у витончені інструменти експлуатації психологічних вразливостей.

1. Авторитет (Authority)

Схильність людей беззаперечно довіряти авторитетним фігурам і рідко піддавати сумніву їхні мотиви формує основу для одного з найефективніших векторів атак. Цей психологічний механізм базується на еволюційно закладеній тенденції слідувати за лідерами та експертами [4]. Зловмисники створюють фальшиві образи керівників організацій, правових консультантів, технічних фахівців або представників регуляторних органів. Попередня розвідка дозволяє їм детально вивчити корпоративну ієрархію та ідентифікувати ті авторитетні ролі, які викликають максимальну довіру у конкретної цільової особи. На практиці це виявляється у spear-phishing кампаніях, де злочинці імітують

генерального директора, вимагаючи від фінансового керівництва негайного переказу коштів [5].

2. Соціальний доказ (Social Proof/Consensus)

Психологічна схильність індивідів підлаштовуватися під дії більшості створює потужний інструмент для маніпулювання. Коли людина спостерігає, що оточуючі вже здійснили певну дію або прийняли конкретне рішення, вона значно частіше схиляється до аналогічного вибору, сприймаючи групову поведінку як валідацію правильності [6]. Зловмисники майстерно використовують цей механізм, конструюючи ілюзію масової участі в нібито легітимних процесах. На практиці це виявляється у згадуванні конкретних імен з робочого оточення жертви або створенні враження, що "78% ваших колег уже завершили процедуру верифікації облікових записів". Можна помітити особливу ефективність таких підходів у корпоративному середовищі, де працівники відчувають додатковий тиск бути частиною колективних ініціатив. Кримінальні схеми також включають псевдо-рекомендації від авторитетних осіб з професійного кола цільової особи або демонстрацію нібито широкого впровадження певних технологічних рішень. Статистика показує, що використання елементів групової валідації підвищує успішність атак на 62%, особливо коли згадуються реальні співробітники або відділи організації-жертви.

3. Послідовність і зобов'язання (Commitment/Consistency)

Соціальна цінність послідовності створює внутрішній тиск на підтримку раніше прийнятих рішень. Індивід, який зайняв певну позицію, відчуває потребу залишатися вірним своєму вибору для збереження цілісного самосприйняття [7]. Кіберзлочинці експлуатують цю особливість через поетапну ескалацію вимог. На практиці це виявляється у створенні ланцюга з нібито безневинних запитів, що поступово переростають у критичні вимоги. Спочатку жертву просять підтвердити базову інформацію, а отримавши початкову згоду, використовують це як психологічну основу для подальших, більш ризикованих прохань. Статистика демонструє тривожну закономірність: 74% осіб, які відповіли на

перший контакт, продовжують взаємодію навіть при зростанні інвазивності запитів.

4. Взаємність (Reciprocity)

Психологічний обов'язок віддячувати за отримані послуги або подарунки, навіть небажані, формує потужний важіль впливу [8]. Зловмисники майстерно використовують цей механізм, пропонуючи цільовим особам корисну інформацію, технічну підтримку або безкоштовні сервіси. Можна помітити, що навіть символічні жести створюють почуття заборгованості, яке згодом експлуатується для отримання конфіденційних даних. На практиці це виявляється у наданні нібито цінних порад щодо безпеки, попередженнях про фіктивні загрози або безкоштовних "оновленнях" програмного забезпечення. Дослідження підтверджують: навіть мінімальні подарунки збільшують готовність до співпраці на 43% [9].

5. Симпатія (Liking)

Природна схильність довіряти подібним до себе людям або тим, хто демонструє щиру зацікавленість, формує основу для побудови довірливих відносин. Індивіди інстинктивно сприймають схожих на них осіб як частину власної соціальної групи, що суттєво знижує рівень критичного мислення під час взаємодії [10, 20]. Кіберзлочинці інвестують значні ресурси у створення психологічного контакту з потенційними жертвами. На практиці це виявляється у ретельному вивченні соціальних профілів цільових осіб та адаптації комунікаційного стилю під їхні уподобання. Зловмисники імітують спільні інтереси, згадують знайомих або демонструють схожий професійний досвід.

6. Дефіцит (Scarcity)

Страх упустити цінну можливість кардинально змінює якість прийняття рішень. Обмежена доступність або короткі терміни дії автоматично підвищують сприйняту цінність пропозиції [11]. Можна помітити, що цей психологічний тригер особливо ефективний у цифровому середовищі, де швидкість реакції часто визначає успіх. Фішингові кампанії системно експлуатують цей механізм через створення штучної терміновості. На практиці це виявляється у

повідомленнях типу "обліковий запис буде деактивований через 18 годин" або "ексклюзивна пропозиція лише для перших 50 користувачів". Зловмисники розуміють, що дефіцит часу блокує критичне мислення та провокує імпульсивні дії.

Принципи Чалдіні знаходять практичне втілення в реальних атаках. Розглянемо основні техніки, які використовують зловмисники для їх реалізації. Зазвичай в наш час зловмисники не концентруються на використанні окремих принципів, а надють перевагу створеню комплекних сценаріїв, які поєднюють в собі декілька методів. Основні техніки створення психолоічного впливу з прикладами застосування, ключовими індикаторами та контрзаходами наведені в табл. А.1.

1.4 Вплив соціальної інженерії на інформаційну безпеку організацій

Дослідження стану кібербезпеки 2021 року підтверджує зростання загроз соціальної інженерії [2]. Соціальна інженерія домінує серед кіберзагроз: 98% атак використовують психологічне маніпулювання для компрометації облікових даних. Цей метод став універсальним інструментом кіберзлочинців через високу ефективність та низькі витрати реалізації. Поширеність атак соціальної інженерії у 2024-2025 роках наведена в табл. А.2.

Атаки соціальної інженерії зростають, при цьому компанії з менш ніж 100 співробітниками отримують на 350% більше атак соціальної інженерії, таких як фішинг, ніж великі підприємства. Особливо тривожною є статистика щодо малого бізнесу: 55,8% атак спрямовані на компанії з 1-50 співробітниками, при цьому кожна п'ята з атакованих малих компаній виплачує викуп для відновлення даних.

Атаки соціальної інженерії як методи кібератак пройшли значну еволюцію протягом останніх десятиліть. Ще на початку 2000-х років зловмисники покладались на телефонні дзвінки або ж email-розсилки з достатньо примітивними сценаріями, то в атаках сучасного часу використовуються вже

персоналізовані сценарії, крім того з 2020 року активно залучається штучний інтелект з використанням deepfake зображень та відео. Процес еволюції розвитку атак соціальної інженерії з його ключовими етапами наведено на рис. 1.1.

Рисунок 1.1. Еволюція методів соціальної інженерії

Як демонструє рисунок 1.5, період 2020-2025 років ознаменувався революційними змінами у методах соціальної інженерії. Однак найбільш драматичний стрибок у кількості та складності атак відбувся саме у 2020 році. Пандемія COVID-19 стала каталізатором швидкого зростання атак соціальної інженерії. За даними міжнародного валютного фонду частота кібератак подвоїлась з часу пандемії. Перехід на віддалену роботу створив нові вектори атак через недостатньо захищені домашні мережі.

Фінансові наслідки атак соціальної інженерії становлять катастрофічну загрозу для глобальної економіки. За оцінками Cybersecurity Ventures, у 2025 році глобальні збитки від кіберзлочинності досягнуть 10,5 трильйона доларів. Економічні збитки від атак соціальної інженерії у 2024 році наведені у табл. А.3.

Проте економічний вплив атак соціальної інженерії нерівномірно розподіляється між різними галузями економіки. Відповідно до даних 82% порушень проти бізнесу включають людський фактор через помилки та атаки соціальної інженерії. Найбільш постраждалі галузі:

- Охорона здоров’я - середні витрати $10,93 млн на порушення.

- Фінансові послуги – зафіксовано у 5 разів більше спроб фішингу у порівнянні з іншими секторами.
- Малий бізнес – 60% малих бізнесів збанкрутували протягом 6 місяців після реалізації атаки соціальної інженерії.

Критично великий відсоток кіберінцидентів є результатом людських помилок, нариклад, перехід за шкідливими посиланнями. Статистика демонструє нерівномірний розподіл кіберризиків серед персоналу, за даними Mimecast, 80% інцидентів безпеки пов'язані з діями лише 8% співробітників, що підкреслює необхідність цільового навчання найбільш вразливих категорій персоналу. 83% підприємств повідомили про зазнання принаймні однієї інсайдерської атаки у 2024 році. Водночас, організації з програмами навчання кібербезпеки демонструють значно кращі результати [25]:

- Зниження ризиків на 70%
- Економія $258,629 на кожному попередженому інциденті
- 78,5% організацій підтверджують пряме запобігання кіберінцидентам через навчання (табл. 1.1)

Таблиця 1.1

Ефективність інвестицій компаній у навчання з кібербезпеки

Рівень навчання	Заощадження на інцидент	Зниження ризиків	Джерело
Мінімальне	0$	0%	IBM 2024 [8]
Базове	129,000$	35%	IBM 2024 [8]
Комплексне	258,629$	70%	IBM 2024 [8]

Соціальна інженерія здійснює комплексний вплив на інформаційну безпеку, експлуатуючи не лише людський фактор, але й системні вразливості корпоративної інфраструктури. Успішні атаки соціальної інженерії часто стають початковою точкою для подальшої технічної експлуатації системних недоліків, що значно ускладнює процеси виявлення та реагування на інциденти.

Веб-технології залишаються найбільш вразливим компонентом корпоративних систем. Аналіз безпеки додатків 2024 року демонструє, що 98% веб-додатків містять критичні вразливості, які можуть бути експлуатовані після успішної компрометації облікових даних співробітників. Особливо критичним є зростання атак на API-інтерфейси на 681% за останній рік, що перетворює їх на пріоритетні цілі для зловмисників, які отримали початковий доступ через соціальну інженерію [11].

Згідно з OWASP Top 10 2021, порушення контролю доступу виявлено у 94% протестованих додатків, що створює значні можливості для ескалації привілеїв після компрометації персоналу. Ця статистика підкреслює критичну залежність між успішністю соціальної інженерії та наявністю технічних вразливостей [10].

Міграція до хмарних платформ створила нові вектори загроз, особливо в контексті атак соціальної інженерії. 73% усіх витоків даних у хмарних середовищах відбуваються через неправильно налаштовані сховища даних. За даними IBM Security, порушення даних у публічних хмарах мають найвищу середню вартість - $5,17 мільйона, що робить їх особливо привабливими цілями після успішної компрометації персоналу [8]. Проблема ускладнюється тим, що 84% організацій використовують кілька хмарних провайдерів, але лише 27% мають узгоджену політику безпеки між ними. Це створює додаткові можливості для зловмисників, які вже отримали доступ до корпоративних систем через соціальну інженерію.

Розширення IoT-екосистеми створює множинні точки входу для атак. З понад 10,54 мільйона атак на IoT-пристрої лише за грудень 2022 року та прогнозованим зростанням до 75,44 мільярда підключених пристроїв до 2025 року, ця сфера стає критично важливою в контексті соціальної інженерії [12].

Системи управління ідентифікацією та доступом

Дослідження показують, що 67% організацій мають неналежно налаштовані системи управління доступом, що критично впливає на наслідки успішних атак соціальної інженерії. Особливо проблематичним є той факт, що

45% організацій не відстежують активність адміністраторських акаунтів, створюючи "сліпі зони" для виявлення подальших дій зловмисників.

За даними IBM Security 2024, атаки зі скомпрометованими обліковими даними потребують найдовшого часу для виявлення та локалізації - в середньому 292 дні. Цей показник демонструє критичну важливість якісних IAM-систем для мітигації наслідків соціальної інженерії [8].

Недостатня мережева сегментація значно ускладнює локалізацію загроз після успішної соціальної інженерії. 72% корпоративних мереж не мають належної ізоляції між сегментами, що дозволяє зловмисникам здійснювати латеральні переміщення після початкового проникнення.

Додатково, 68% організацій не моніторять East-West трафік між серверами, залишаючи внутрішні переміщення зловмисників непомітними. Це особливо критично в контексті атак соціальної інженерії, де зловмисники використовують легітимні облікові дані для доступу до систем [11].

Недоліки в SIEM-системах - лише 38% організацій впровадили централізовані системи збору та аналізу логів, при цьому 55% наявних SIEM-систем налаштовані неефективно. Це критично впливає на здатність організацій виявляти наслідки успішних атак соціальної інженерії та своєчасно реагувати на них.

Середній час виявлення та локалізації порушення становить 277 днів, при цьому порушення з втраченими обліковими даними потребують 292 дні. Така затримка дозволяє зловмисникам максимально експлуатувати наявні системні вразливості після успішної соціальної інженерії [8].

Експлуатація тіньових даних - 35% порушень у 2024 році залучали так звані "тіньові дані" - інформацію, що зберігається в некерованих джерелах даних. Ці порушення призводили до на 16% вищих витрат у середньому, оскільки організації не мали повної видимості своїх інформаційних активів. 40% порушень включали дані, що зберігаються в кількох середовищах одночасно, що значно ускладнює процеси виявлення та реагування на наслідки соціальної інженерії [8].

Правові та регулятивні аспекти захисту від атак соціальної інженерії. Правове регулювання кібербезпеки і протидії соціальній інженерії в Україні формується під впливом як національних потреб захисту інформаційної безпеки, так і вимог європейської інтеграції. Нормативно-правова база України встановлює відповідальність організацій за забезпечення захисту від атак соціальної інженерії та регламентує заходи протидії таким загрозам.

Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII від 05.10.2017 року є основним нормативним актом, що регулює питання протидії соціальній інженерії [15]. Стаття 1 закону визначає соціальну інженерію як один із видів кіберзагроз, що можуть призвести до кіберінцидентів. Згідно зі статтею 8, організації зобов'язані забезпечувати "проведення інструктажів та систематичних тренінгів щодо кібергігієни для працівників", що безпосередньо стосується протидії соціальній інженерії.

Відповідальність суб'єктів кібербезпеки регламентується статтею 12 закону, яка встановлює, що порушення вимог законодавства у сфері кібербезпеки тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність. Особливе значення має стаття 4, що визначає суб'єктами забезпечення кібербезпеки всі підприємства, установи та організації, які обробляють інформацію з обмеженим доступом або надають електронні послуги.

Національна стратегія кібербезпеки України, затверджена Указом Президента № 447/2021 від 26 серпня 2021 року, визнає людський фактор одним із ключових викликів сучасної кібербезпеки [16]. Стратегія передбачає "підвищення рівня кібергігієни населення" та "розвиток культури кібербезпеки в суспільстві", що включає протидію соціальній інженерії.

Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010 року встановлює вимоги до захисту персональних даних від несанкціонованого доступу, включаючи отримання таких даних шляхом соціальної інженерії [17]. Стаття 6 закону вимагає забезпечення "відповідного рівня захисту персональних даних", а стаття 24 зобов'язує володільців даних впроваджувати "організаційні

та технічні заходи" захисту. Порушення цих вимог тягне відповідальність згідно зі статтею 28 закону.

Регулятивні органи та їх повноваження

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) є центральним органом виконавчої влади у сфері кібербезпеки. Згідно із Законом № 2163-VIII, Держспецзв'язок "забезпечує формування та реалізацію державної політики з кіберзахисту" та здійснює "державний контроль у зазначених сферах". До компетенції служби входить встановлення вимог до захисту від соціальної інженерії та контроль за їх дотриманням.

Національний банк України має особливі повноваження у сфері кібербезпеки фінансових установ. НБУ встановлює вимоги до захисту банківських систем від атак соціальної інженерії та проводить регулярні перевірки дотримання цих вимог.

Українське законодавство передбачає суворі санкції за порушення вимог кібербезпеки. Кримінальний кодекс України містить статті 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж») та 362 («Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»), які можуть застосовуватися у випадках використання соціальної інженерії для отримання доступу до захищеної інформації.

Адміністративні санкції за порушення вимог захисту персональних даних передбачають штрафи від 200 до 1000 неоподатковуваних мінімумів доходів громадян для юридичних осіб. Для банківських установ НБУ може застосовувати додаткові санкції, включаючи обмеження операцій або відкликання ліцензій.

Міжнародні стандарти. Загальний регламент про захист даних (GDPR) ЄС 2016/679 впливає на українські організації, що обробляють персональні дані громадян ЄС. GDPR встановлює принцип «захисту даних за замовчуванням», який вимагає впровадження заходів протидії соціальній інженерії на етапі проєктування систем. Штрафи за порушення GDPR можуть досягати 4% річного обороту організації або 20 мільйонів євро. Організації, що працюють з європейськими партнерами, повинні дотримуватися вимог GDPR щодо повідомлення про порушення захисту даних протягом 72 годин, включаючи інциденти, пов'язані з соціальною інженерією.

Висновки за розділом 1

1. Проведено комплексний аналіз концептуальних основ соціальної інженерії як сучасної загрози інформаційній безпеці організацій. Встановлено, що соціальна інженерія є процесом психологічного маніпулювання людьми з метою отримання несанкціонованого доступу до інформаційних систем, який часто виявляється більш ефективним порівняно з технічними атаками через експлуатацію людського фактора як найслабшої ланки безпеки.

2. Систематизовано основні типи атак соціальної інженерії та визначено їх ключові характеристики. Класифіковано вісім основних векторів атак: фішинг, спеціалізований фішинг (spear phishing), SMS-фішинг (smishing), голосовий фішинг (vishing), претекстування, діпфейки, компрометацію ділової електронної пошти (BEC) та фізичні методи впливу. Встановлено, що сучасні атаки характеризуються високим рівнем персоналізації та використанням технологій штучного інтелекту.

3. Обґрунтовано психологічні механізми впливу в атаках соціальної інженерії на основі принципів Роберта Чалдіні. Доведено, що шість ключових принципів (авторитет, соціальний доказ, послідовність, взаємність, симпатія та дефіцит) активно експлуатуються зловмисниками для створення психологічного

тиску та зниження критичного мислення жертв. Розроблено алгоритм поведінки зловмисника при взаємодії з жертвою та механізм формування довіри.

4. Виявлено критичні масштаби загроз соціальної інженерії для сучасних організацій. Статистичний аналіз показав, що 98% кібератак використовують соціальну інженерію, 82% порушень безпеки пов'язані з людським фактором, а середній час виявлення атак становить 277 днів. Економічні збитки сягають $4,88 млн за один інцидент витоку даних, при цьому BEC-атаки спричинили загальні збитки $2,77 млрд у 2024 році.

5. Проаналізовано вплив соціальної інженерії на вразливості інформаційних систем в умовах цифрової трансформації. Встановлено, що 94% веб-додатків містять критичні вразливості, 73% витоків даних у хмарних середовищах відбуваються через неправильні конфігурації, а 67% організацій мають неналежно налаштовані системи управління доступом, що створює додаткові можливості для експлуатації після успішної соціальної інженерії.

6. Систематизовано правові та регулятивні аспекти протидії атакам соціальної інженерії в Україні. Визначено нормативно-правову базу, включаючи Закон України "Про основні засади забезпечення кібербезпеки України", Національну стратегію кібербезпеки та вимоги міжнародних стандартів (GDPR), які встановлюють відповідальність організацій за впровадження заходів захисту від соціальної інженерії.

Результати дослідження теоретичних основ соціальної інженерії підтверджують необхідність комплексного підходу до захисту користувачів інформаційних систем, що поєднує технологічні, організаційні та поведінкові компоненти. Виявлені закономірності та характеристики загроз створюють фундамент для аналізу існуючих моделей захисту та обґрунтування вибору найбільш ефективного рішення для протидії атакам соціальної інженерії.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Огляд існуючих моделей захисту користувачів інфораційної системи від атак соціальної інженерії

Модель безпеки робочого простору.

Модель безпеки робочого простору (МБРП) виходить за межі традиційних парадигм захисту на основі периметра, втілюючи цілісний підхід, що поєднує технологічну досконаліть з організаційною стійкістю.

Сучасні робочі середовища характеризуються безпрецедентною складністю, що виражається у розмитих кордонах між фізичною та цифровою сферами. Ця метаморфоза вимагає систем безпеки, які демонструють адаптивну пластичність, зберігаючи при цьому архітектурну цілісність. МБРП відповідає цій вимозі за допомогою багатовимірного підходу, що охоплює технологічні, процедурні та антропоцентричні елементи організаційної безпеки.

Основна ідея цієї моделі полягає в тому, щоб зрозуміти, що сучасне робоче середовище не обмежується лише цифровим простором. Соціальні інженери використовують вразливі місця на всіх рівнях організаційної структури. Вони використовують усі можливі засоби, від фізичного доступу до приміщень до психологічного маніпулювання співробітниками. Щоб вирішити цю проблему, MBRP створила багаторівневу систему захисту, в якій кожен компонент доповнює та підсилює інші.

Інформаційна гігієна є основою моделі. Цей елемент базується на розумінні того, що найефективнішим захистом від соціального інжинірингу є обізнані та навчені співробітники. Програми інформаційної гігієни включають не тільки традиційні навчальні курси, але й практичні вправи, симуляції реальних атак та розвиток критичного мислення. Зокрема, акцент робиться на

вихованні здорового скептицизму щодо підозрілих запитів, навіть якщо вони надходять від осіб, що займають керівні посади.

Програма навчання співробітників в розглянутій моделі є динамічною системою, яка постійно адаптується до нових загроз. Замість статичних презентацій, співробітники отримують інтерактивний досвід через рольові ігри, що дозволяє їм безпечно відпрацьовувати свої реакції на різні сценарії соціальної інженерії. Це дає їм можливість розвинути стійкі поведінкові навички, а не просто запам'ятати теоретичні знання.

Фізична безпека не розглядається як окремий елемент у контексті МБРП, а скоріше як невід'ємна частина захисту від соціального інжинірингу. Соціальні інженери можуть поєднувати цифрові атаки з фізичним вторгненням, використовуючи такі техніки, як «tailgating», «приманка» або «претекстинг», щоб отримати доступ до конфіденційної інформації. Ця модель передбачає не тільки впровадження технічних заходів контролю доступу, але й створення культури фізичної безпеки, що вимагає від кожного співробітника розуміння своєї ролі в захисті простору організації.

Системи фізичної безпеки включають багаторівневий контроль доступу, відеоспостереження з інтелектуальними можливостями аналізу, системи виявлення аномалій та протоколи безпечної реакції на відвідувачів. Особливий акцент робиться на захисті від візуального шпигунства, яке є технікою, що використовується соціальними інженерами для отримання паролів, PIN-кодів або іншої конфіденційної інформації шляхом спостереження.

Цифрова безпека охоплює всі цифрові канали зв'язку та інформаційні системи в рамках моделі безпеки робочого простору. Ця модель визнає, що більшість сучасних атак соціальної інженерії походять з цифрових каналів (електронна пошта, соціальні мережі, месенджери, фальшиві веб-сайти тощо). Системи цифрової безпеки включають не лише технічні заходи захисту, але й освітні елементи, які дозволяють користувачам розпізнавати цифрові загрози та реагувати відповідно.

Стек технологій цифрової безпеки включає фільтри запобігання фішингу, що використовують машинне навчання, системи виявлення аномалій поведінки користувачів, заходи захисту електронної пошти з можливостями аналізу вкладень та посилань, а також інтегровані системи багатофакторної автентифікації. Впровадження систем, здатних виявляти складні атаки, є надзвичайно важливим, адже такі атаки поєднують кілька векторів одночасно.

Психологічна профілактика є одним із елементів МБРП і відрізняє цю модель від суто технічних підходів. Оскільки соціальна інженерія є, по суті, психологічною атакою, розуміння та протидія психологічним маніпуляціям є важливими для ефективного захисту. Програма психологічної профілактики включає навчання користувачів інформаційної системи механізмам психологічного впливу, розвиток емоційного інтелекту та підвищення стійкості до стресових ситуацій. Працівників навчають розпізнавати типові методи впливу, такі як створення відчуття терміновості, невідкладності, використання влади або ж звернення до співчуття та погроз. Особлива увага приділяється прищепленню здорового скептицизму без створення параноїдальної атмосфери в організації. Оскільки соціальна інженерія часто використовує стресові ситуації для зниження критичного мислення жертви, програма також включає навчання з управління стресом.

Політика та заходи реагування організації забезпечують структурну основу, в рамках якої функціонують усі інші компоненти. Без чітких процедур, правил та протоколів реагування навіть найкращі технічні та освітні контрзаходи можуть бути неефективними. Принцип мінімальної довіри передбачає створення комплексної системи політик, яка охоплює всі аспекти контрзаходів соціальної інженерії, від процедур перевірки особи для телефонних запитів до протоколів розслідування інцидентів.

Система політик організації включає чіткі інструкції для різних сценаріїв, процедури ескалації, протоколи міжвідомчої співпраці та механізми постійного вдосконалення на основі аналізу інцидентів. Важливо створити культуру, яка

карає, а не заохочує повідомлення про підозрілі ситуації, навіть якщо загроза пізніше виявляється хибною.

Принципи роботи МБРП базуються на сучасних концепціях кібербезпеки, адаптованих до контрзаходів соціальної інженерії. Принцип мінімальної довіри означає, що запити на інформацію або дії не вважаються безпечними за замовчуванням, незалежно від того, хто їх робить, і чи знаходиться той хто їх робить в середині системи чи ззовні. Це не означає культивування недовіри, а радше впровадження систематичних процедур перевірки.

Принцип безперервної верифікації вимагає регулярної перевірки особи та повноважень осіб, які запитують конфіденційну інформацію або незвичайну поведінку. Це особливо важливо під час складних атак, коли зловмисники використовують інформацію, отриману з відкритих джерел, для створення переконливого приводу.

Принцип безперервної адаптації враховує динамічний характер загроз соціальної інженерії. Зловмисники постійно вдосконалюють свої методи, використовують нові технології та поточні події для підвищення ефективності своїх атак. МБРП регулярно оновлює всі компоненти моделі на основі аналізу нових загроз та інцидентів.

Принцип взаємної відповідальності підкреслює, що безпека є відповідальністю всіх співробітників, а не лише спеціалізованих відділів. Кожен співробітник повинен розуміти свою роль у загальній системі захисту та активно сприяти підтримці безпечного середовища.

Очікувані результати впровадження МБРП включають не лише кількісний показник зниження успішності атак, але й якісну зміну організаційної культури. Системний підхід створює середовище, в якому безпека є природною частиною бізнес-процесу, а не додатковим тягарем. Це скорочує час, витрачений на реагування на інциденти, та підвищує довіру між усіма сторонами, тим самим підвищуючи ефективність усієї організації. Структуру моделі безпеки робочого простору та взаємодію її основних компонентів представлено на рис. Б.1.

Модель нульової довіри (Zero Trust Model).

Модель нульової довіри – це фундаментальна зміна парадигми в підходах до кібербезпеки, особливо коли йдеться про боротьбу із соціальною інженерією [21]. Традиційні моделі безпеки, засновані на концепції «меж довіри», виявилися неефективними проти сучасних загроз, коли зловмисники компрометують облікові записи співробітників, щоб отримати доступ до мережі організації. «Нульова довіра» відмовляється від концепції неявної довіри та вимагає, щоб кожен об’єкт і кожна транзакція перевірялися постійно. Філософія «ніколи не довіряй, завжди перевіряй» – це не вираз недовіри до співробітників, а визнання реальності сучасного кіберсередовища, де обліковий запис будь-якого користувача може бути скомпрометований атакою соціальної інженерії. Модель «нульової довіри» особливо ефективна проти таких векторів атаки, як крадіжка облікових даних, компрометація ділової електронної пошти та внутрішні загрози, які часто виникають в результаті успішних кампаній соціальної інженерії.

Багатофакторна автентифікація (MFA) є ключовим компонентом Модель нульової довіри, оскільки вона значно ускладнює використання викрадених облікових даних. Навіть якщо зловмиснику вдасться отримати ім'я користувача та пароль за допомогою фішингу або вішингу, додатковий фактор автентифікації значно знижує шанси на успішну компрометацію. Сучасні реалізації багатофакторної автентифікації включають біометрію, апаратні токени, push-сповіщення та адаптивну автентифікацію на основі ризиків. Адаптивна автентифікація особливо ефективна в боротьбі із соціальною інженерією, оскільки вона аналізує контекстуальні фактори, такі як географічне розташування, час доступу, тип пристрою та моделі поведінки, щоб визначити рівень ризику кожної спроби входу. Це дозволяє системі запитувати додаткову перевірку за підозрілих обставин, навіть якщо належним чином надано правильні облікові дані.

Мікросегментація мережі – це технічний елемент, який обмежує горизонтальне переміщення зловмисника після успішного вторгнення.

Традиційні мережі часто будуються навколо «м’якого ядра» – жорсткого периметра, що включає відносно надійну внутрішню мережу. Нульова довіра реалізує принцип мікросегментації, ізолюючи кожен сегмент мережі та вимагаючи окремої автентифікації для отримання доступу. У контексті соціальної інженерії мікросегментація особливо ефективна проти атак, які починаються з компрометації одного користувача або пристрою. Навіть якщо зловмисник зможе отримати початковий доступ завдяки успішній атаці соціальної інженерії, його можливості просуватися далі в мережі сильно обмежені. Кожна спроба доступу до нового ресурсу вимагає окремої автентифікації та авторизації.

Принцип найменших привілеїв у моделі нульової довіри означає надання кожному користувачеві, пристрою чи програмі лише того доступу, який абсолютно необхідний для виконання певного завдання. Це має вирішальне значення в боротьбі із соціальною інженерією, оскільки обмежує потенційну шкоду, спричинену компрометацією облікового запису. Навіть якщо злочинець отримує доступ до облікового запису співробітника, його доступ обмежений мінімальним набором необхідних привілеїв. Динамічне керування привілеями дозволяє автоматично підвищувати або знижувати рівні доступу залежно від поточних потреб та рівня ризику. Наприклад, це дозволяє надати співробітнику тимчасові додаткові привілеї для виконання певного завдання та автоматично скасовувати ці привілеї після завершення роботи на ним.

Моніторинг у режимі реального часу безперервно відстежує всю активність у мережі, щоб виявити аномальну поведінку, яка може свідчити про компрометацію. Системи моніторингу аналізують моделі поведінки користувачів, час і місцезнаходження отриманого доступу, типи ресурсів, до яких здійснюється доступ, та інші контекстуальні фактори. Особлива увага приділяється виявленню аномальної поведінки, яка може свідчити про те, що обліковий запис не використовується його законним власником. Наприклад, спроби доступу до незвичайних ресурсів, активність у незвичайний час, зміни

географічного розташування та незвичайні обсяги передачі даних можуть бути показниками компрометації.

Контекстна автентифікація враховує кілька факторів при визначенні того, чи надавати доступ. Замість простої перевірки особи, система аналізує контекст запиту: «хто?», «що?», «коли?», «звідки?» та «чому?» запитує доступ. Це дозволяє їй виявляти підозрілі запити навіть за умови належного способу автентифікації.

Штучний інтелект та машинне навчання відіграють одну з ключових ролей у Моделі нульової довіри, дозволяючи системі адаптуватися до нових загроз та зменшувати кількість хибних спрацьовувань. Алгоритми навчаються на основі даних про поведінку користувачів та постійно покращують свою здатність розрізняти законну та потенційно шкідливу активність.

Впровадження Zero Trust – це складний, довгостроковий процес, який вимагає фундаментальних змін в архітектурі IT-систем та організаційних процесів. Традиційні системи, побудовані за принципом «неявної довіри», часто потребують значної модернізації або повної заміни. Це створює ряд певних проблем не лише з технічної, але й з економічної сторони.

Поетапний підхід до впровадження – це рекомендована стратегія, яка дозволяє організаціям поступово адаптуватися до нової парадигми безпеки. Впровадження зазвичай починається з найважливіших ресурсів та користувачів і поступово розширюється на всю інфраструктуру організації. Впровадження Моделі нульової довіри – це не лише технічна, а й культурна зміна. Працівникам доведеться адаптуватися до нових процедур сертифікації та авторизації, які можуть здатися більш обтяжливими, ніж традиційні підходи. Ефективні програми навчання та комунікації є важливими для успішного впровадження. Структуру моделі нульової довіри та взаємодію її ключових компонентів представлено на рис. Б.2.

Модель навчання та підвищення обізнаності (Awareness Training Model).

Модель навчання та підвищення обізнаності з кібербезпеки базується на фундаментальному розумінні того, що людський фактор є одночасно

найслабшою ланкою та найсильнішим захистом від атак типу соціальної інженерії. Статистика показує, що понад 90% успішних кібератак починаються з використання людських вразливостей, що робить інвестиції в навчання співробітників важливими для забезпечення безпеки організації. Традиційні підходи до навчання з кібербезпеки часто обмежуються разовими презентаціями або обов'язковими онлайн-курсами, які співробітники швидко забувають після проходження та мають складнощі в практичній інтеграції отриманих знань. Модель навчання з підвищення обізнаності пропонує принципово інший підхід, заснований на принципах безперервного навчання, персоналізації контенту та активної залучення користувачів за допомогою сучасних освітніх методів.

Навчання кінцевих користувачів є базовим рівнем моделі та складається з комплексного курсу з 32 модулів, що охоплюють усі основні аспекти кібербезпеки. Ці модулі структуровані таким чином, щоб забезпечити покрокове отримання знань, від базових концепцій до складних сценаріїв атак. Кожен модуль включає теоретичну частину, практичні приклади, інтерактивні вправи та тести для перевірки розуміння матеріалу. Особлива увага також приділяється психологічним аспектам соціальної інженерії. Працівники зможуть розпізнавати не лише технічні ознаки атаки, але й методи психологічного впливу, що використовуються зловмисниками. Курс пропонує поглиблений аналіз принципів Чалдіні (авторитет, соціальне схвалення, взаємність, послідовність, емпатія, дефіцит) та того, як вони використовуються в атаках соціальної інженерії.

У рольовому навчанні типи загроз, з якими стикаються співробітники, залежать від їхньої посади, відділу та рівня доступу до конфіденційної інформації. Ця модель заохочує створення спеціалізованих навчальних програм для різних ролей в організації, а не універсальний підхід для всіх ролей. Фінансовий персонал отримує поглиблену підготовку з протидії компрометації ділової електронної пошти (BEC), шахрайству з електронною поштою та атакам платіжних систем. HR-спеціалісти вивчають конкретні сценарії, такі як отримання особистої інформації співробітників шляхом видавання себе за іншу

особу, атаки типу «китовий штурм» на керівників та атаки соціальної інженерії через професійні мережі, такі як LinkedIn.

ІТ-персонал отримує технологічно орієнтовану підготовку з розпізнавання передових APT-атак, аналізу шкідливого коду, методів соціальної інженерії через технічну підтримку та протидії внутрішнім загрозам. Керівники отримують спеціалізовану підготовку з протидії атакам типу «китовий штурм» та фішинговим атакам, а також курси з управління кризовими ситуаціями в кіберінцидентах.

Модулі регулярно оновлюються, щоб йти в ногу з еволюцією кіберзагроз. Наприклад, з появою технології діпфейків до курсу було додано модуль, присвячений розпізнаванню штучно згенерованого аудіо- та відеоконтенту. Аналогічно, пандемія COVID-19 спонукала до швидкого оновлення контенту для вирішення нових векторів атак, пов'язаних з віддаленою роботою.

Фішингові симуляції є одним із найефективніших елементів розглянутої моделі, що дозволяє практично перевірити рівень підготовки співробітників у контрольованому середовищі. Ці симуляції не призначені для того, щоб «виловити» помилки співробітників, а для того, щоб надати можливість безпечно відпрацювати свої навички у виявленні підозрілих повідомлень на практиці, для подальшої їх успішної інтеграції під час реальної роботи.

Симуляції проводяться регулярно з різноманітними сценаріями, що відображають останні тенденції соціальної інженерії. До них належать імітація електронних листів від банків, державних установ, популярних онлайн-сервісів і навіть внутрішніх повідомлень компанії від ІТ-відділів та керівництва. Після проведення тестів отримані результати симуляцій аналізуються для виявлення прогалин у знаннях та модифікації програми навчання, але не для покарання співробітників, які допустились помилки. Співробітники, які «попадаються» на змодельовані атаки, автоматично отримують додаткове індивідуальне навчання для пропрацювання виявлених слабких місць.

Навчання на основі ризиків – це інноваційний підхід, який дозволяє організаціям швидко реагувати на нові загрози за допомогою навчальних сесій

на мікро- та нанорівні. Коли команди безпеки виявляють нові тактики атак або конкретні загрози для організації, система автоматично генерує короткі навчальні модулі та надає їх співробітникам через різні канали. Ці короткі сесії тривають від 2 до 15 хвилин, і зосереджені саме на конкретних, поточних загрозах та надають практичні поради щодо їх розпізнавання та боротьби з ними. Наприклад, якщо буде виявлено нову хвилю фішингових атак, що імітують дзвінки з банків, усі співробітники матимуть одну годину, щоб переглянути короткий навчальний відеоролик, який описує конкретні ознаки таких атак та рекомендовані контрзаходи у разі отримання співробітниками дзвінків.

Метод гейміфікації використовується для підвищення мотивації та залученості співробітників. Традиційне корпоративне навчання часто сприймається як виснажливе завдання, що знижує його ефективність. Елементи гейміфікації, такі як таблиці оцінювання, значки досягнень, змагання та віртуальні нагороди, перетворюють навчання на захопливий та цікавий процес для співробітників. Системи винагород розроблені для сприяння не лише індивідуальним досягненням, але й для піднаття колективної відповідальності за безпеку. Відділи можуть змагатися у швидкості виконання навчальних модулів, точності виявлення змодельованих атак та кількості повідомлень про підозрілу активність. Серйозні ігри та симуляції атак дозволяють співробітникам безпечно випробувати різні сценарії та вчитися на своїх помилках без реальних наслідків. Наприклад, симулятор середовища електронної пошти дозволяє користувачам потренуватися розпізнавати фішингові електронні листи в реалістичному, але безпечному середовищі.

Навчання з питань дотримання вимог та конфіденційності є важливим для організацій, що працюють у високорегульованих галузях. Такі нормативні акти, як GDPR, HIPAA та PCI DSS, встановлюють конкретні вимоги щодо захисту персональних даних та конфіденційної інформації, а порушення можуть призвести до значних фінансових втрат та шкоди репутації. Дані курси адаптовані до обставин кожної організації та регулярно оновлюються, щоб бути в курсі законодавчих змін. Працівників навчають не лише технічним аспектам

дотримання вимог, але й тому, як обійти нормативні вимоги за допомогою соціальної інженерії. Принципи моделі навчання з підвищення обізнаності базуються на найновіших розробках в освітній науці та психології навчання дорослих. Контекстуальність означає, що навчальні матеріали адаптовані до характеристик організації, її галузі та поточного ландшафту загроз. Абстрактні приклади замінюються конкретними сценаріями, пов'язаними з повсякденною роботою співробітників.

Очікувані результати впровадження моделі навчання з підвищення обізнаності включають не лише кількісні показники, такі як зменшення кількості успішних фішингових атак на 60-70%, але й якісні зміни в організаційній культурі. Створення культури кібергігієни означає, що безпека стає природною частиною мислення та поведінки співробітників, а не тягарем. Структуру моделі навчання та підвищення обізнаності з кібербезпеки представлено на рис. Б.3.

Модель мінімальних привілеїв (Principle of Least Privilege).

Принцип найменших привілеїв являє собою базову концепцію інформаційної безпеки, яка особливо актуальна в контексті протидії атакам типу соціальній інженерії. Кожен суб'єкт системи (користувач, процес, програма або пристрій) отримує тільки права доступу, абсолютно необхідні для виконання певних функцій, і не більше. У традиційних IT-середовищах доступ часто надається "з запасом" для зручності користувачів і управління ними, зокрема для заощадження часу. Однак такий підхід пов'язаний зі значними ризиками, пов'язаними з загрозами соціальної інженерії. Коли зловмисник зламає обліковий запис за допомогою фішингу або ж інших методів соціальної інженерії, надмірні повноваження щодо цього облікового запису стають потужним інструментом для подальшого розвитку атаки та просування зловмисника в системі.

Проблема "повзучих привілеїв" є однією з найбільш поширених вразливостей в корпоративному середовищі. І це пов'язано з природними змінами в організаційній структурі: працівники змінюють посади, отримують тимчасові завдання, переміщуються між відділами, але часто права доступу

залишаються незмінними та не коригуються відповідно. В результаті через деякий час багато користувачів отримують значно більше привілеїв, ніж їм потрібно для їх поточної ролі. Ця проблема особливо небезпечна в контексті соціальної інженерії, оскільки зловмисники часто проводять ретельне розслідування перед атакою та вичають організаційні структури через LinkedIn, корпоративні веб-сайти та соціальні мережі. Вони можуть навмисно атакувати працівників, які займають офіційні посади низького рівня, але зберігають доступ до критичних систем завдяки попереднім ролям.

Системний підхід до управління привілеями в рамках моделі мінімальних привілеїв включає детальне відображення всіх існуючих прав доступу, аналіз відповідності поточним посадовим обов'язкам і створення автоматизованих процесів для підтримки цієї відповідності. Процес починається з всебічного аудиту всіх облікових записів, включаючи користувачів, послуги, адміністрацію та привілеї. Процес проведення аудиту та відповідність прав включає не лише локальні системи, а й хмарні сервіси, які дозволяють розподіляти доступ між різними платформами та постачальниками. Сучасні організації часто використовують десятки різних SaaS-додатків зі своїми власними системами контролю доступу, тому централізовано контролювати дозволи складно. Автоматизація управління повноваженнями має вирішальне значення для ефективного впровадження Моделі мінімальних привілеїв на підприємстві. Ручне управління доступом сотень або тисяч користувачів і десятків систем практично неможливо. Сучасні системи управління привілеями використовують алгоритми машинного навчання для аналізу шаблонів доступу та автоматичного виявлення аномалій. Автоматизована система може виявляти такі ситуації, як невикористані права (співробітники мають доступ до системи, але не користувалися нею протягом тривалого часу), ненормовані дії (доступ до ненормованих ресурсів або ненормовані години роботи) і порушення принципу поділу обов'язків (1 користувач має право самостійно ініціювати і виконувати схвалювати фінансові операції).

Доступ "точно вчасно" являє собою сучасний підхід до управління привілеями, що дозволяє надавати підвищені права доступу тільки до тих пір, поки це необхідно для виконання певних завдань. Замість постійних дозволів користувачі отримують тимчасові дозволи через автоматизовану систему запитів та затвердження. Це значно скорочує період вразливості, тобто період, протягом якого скомпрометований обліковий запис може завдати шкоди.

Система «JIT access» інтегрується з системою документообігу організації, дозволяючи співробітникам запитувати необхідні дозволи через зручний інтерфейс і автоматично направляти їх затверджуючій особі. Цей процес може включати додаткову автентифікацію, обґрунтування доступу та автоматичне відкликання прав після виконання завдання.

Система управління привілейованим доступом (PAM) забезпечує централізоване зберігання та управління паролями, ключами та сертифікатами для привілейованих облікових записів. Ці системи особливо важливі для боротьби з соціальною інженерією, оскільки вони унеможливлюють використання паролів від викрадених облікових записів адміністраторів. Система PAM автоматично генерує і змінює паролі, забезпечуючи безпечне підключення до цільової системи без розкриття облікових даних користувача, це в свою чергу дозволяє швидко виявляти зломи і точно визначати ступінь прогнозованого збитку.

Розподіл ролей і облікових записів є фундаментальним принципом, який вимагає чіткого поділу управлінських функцій і повсякденних робочих завдань. Працівники повинні мати окремі облікові записи для виконання звичайних робочих та адміністративних завдань, а адміністративні облікові записи можуть використовуватися для виконання конкретних завдань, що вимагають підвищених привілеїв. Такий підхід значно ускладнює можливість компрометації облікового запису зловмисниками, оскільки зловмисники, які мають доступ до облікових записів звичайних співробітників, не мають автоматичного доступу до функцій управління. Крім того, різні облікові записи дозволяють реалізувати різні політики безпеки. Наприклад, для облікового

запису адміністратора може знадобитися більш часта зміна пароля, обов'язкова багатофакторна аутентифікація, а також обмеження за часом і місцем розташування.

Постійний моніторинг та сповіщення дозволяють відстежувати використання привілейованого облікового запису та швидко виявляти підозрілу активність. Відбувається аналіз не тільки факту використання привілеїв, а й контекст цього використання, тобто час, місце, вид діяльності, відхилення від звичної моделі поведінки. При виявленні підозрілої активності система автоматично блокує обліковий запис, запитує додаткову аутентифікацію або повідомляє службу безпеки.

Централізоване управління життєвим циклом облікових записів дозволяє здійснювати інтеграція з системою ідентифікації. Коли працівник змінює посаду, переходить до іншого відділу або звільняється, система автоматично коригує або анулює відповідні права доступу, що значно знижує ризики. Системи управління ідентифікацією також підтримують концепцію "контролю доступу до атрибутів", при якій права надаються на основі атрибутів користувача (місце розташування, відділ, рівень доступу, проект), а не прямого призначення. Це полегшує управління та дозволяє автоматично оновлювати дозволи при зміні атрибутів.

Визначення ролей і необхідних дозволів, тісна співпраця між IT-службами і бізнес-підрозділами для створення точної рольової моделі, що відображає реальні посадові обов'язки - цей процес часто виявляє невідповідності між офіційними посадовими інструкціями і реальними робочими процесами. Впровадження централізованого сховища включає в себе не тільки технічне розгортання системи PAM, але і розробку процедури її використання, навчання персоналу, інтеграцію з існуючими системами моніторингу інцидентів і реагування на них.

Очікувані результати від впровадження Моделі мінімальних привілеїв включають скорочення зон атак, обмеження можливостей зловмисників переміщатися по системі, підвищення привілеїв, поліпшення дотримання

нормативних вимог і зниження операційних ризиків. Також принесе підвищення продуктивності за рахунок автоматизації процесу контролю доступу і скорочення кількості запитів в службу підтримки.

Регулярна перевірка і аутентифікація прав доступу це обов'язкова процедура, що дозволяє виявляти і усувати невідповідності, які накопичувалися з плином часу. Автоматизована система може спростити цей процес, надавши керівникам зручний інтерфейс для перевірки прав підлеглих, виявлення потенційно проблемних ситуацій і автоматичного відкликання неперевірених прав протягом певного періоду часу. Структуру моделі мінімальних привілеїв зображено на рис. Б.4.

Аналітика поведінки користувачів та сутностей (User and Entity Behavior Analytics).

Модель UEBA являє собою інноваційний підхід до виявлення кіберзагроз, заснований на детальному аналізі моделей поведінки користувачів, пристроїв і додатків в корпоративному середовищі. На відміну від традиційних систем безпеки, які покладаються на відомі підписи та правила загрози, UEBA використовує статистичні методи та алгоритми машинного навчання для виявлення аномальної поведінки, яка може сигналізувати про злом або злочинні дії [22]. Особлива цінність UEBA в контексті протидії соціальній інженерії полягає в її здатності виявляти "успішні" атаки, коли зловмисникам вдається обійти технічні засоби захисту і отримати доступ до облікових записув за допомогою методів соціальної інженерії.

Історична еволюція UEBA відображає зростаюче розуміння важливості людського фактора в кібербезпеці. Системи раннього виявлення вторгнень (IDS) орієнтовані на мережевий трафік і відомі сигнатури атак. З розвитком внутрішніх загроз і складних багатоетапних атак стало ясно, що існує потреба в інструментах для аналізу поведінки законних користувачів.

Перша реалізація UEBA у 2010-х роках була відносно простою системою, яка аналізувала основні показники, такі як час входу, географічне розташування та обсяг переданих даних. Сучасні платформи можуть аналізувати сотні різних

робочих параметрів за допомогою складних алгоритмів глибокого навчання та обробляти терабайти телеметричних даних у режимі реального часу.

Основні принципи UEBA базуються на концепції "нормальної поведінки" кожного користувача та об'єкта в системі. Замість загального правила система вивчає індивідуальні особливості поведінки кожного співробітника-коли він зазвичай працює, до яких ресурсів він має доступ, його сеанси і те, як він взаємодіє один з одним. Створення базового операційного профілю вимагає тривалого періоду навчання, зазвичай 30-90 днів в системі для накопичення даних для нормальної роботи.

Збір та інтеграція даних це технічно складний процес, який вимагає інтеграції з багатьма різнорідними телеметричними ресурсами. Модель UEBA збирає дані з систем управління ідентифікацією (Active Directory, LDAP), систем моніторингу безпеки (SIEM), засобів захисту кінцевих точок (EDR), мережевих датчиків, проксі-серверів, VPN-систем, хмарних платформ і бізнес-додатків.

Процес інтеграції дозволяє об'єднати багатоформатні журнали і події в єдину модель даних для зіставлення інформації з різних джерел. Наприклад, події входу користувача в корпоративну мережу можуть включати в себе дії з електронною поштою, доступ до файлових ресурсів і веб-додатків. Технологія машинного навчання UEBA включає багато алгоритмів, кожен з яких оптимізований для виявлення певних типів аномалій. Непідконтрольовані алгоритми навчання, такі як кластеризація та виявлення викидів, виявляють поведінку, яка значно відрізняється від встановлених моделей. Контрольоване навчання використовується для вивчення відомих прикладів злочинної діяльності. Особливу цінність представляють алгоритми часових рядів, які аналізують зміни поведінки з плином часу. Наприклад, поступове збільшення доступу до конфіденційних файлів може свідчити про готовність до інсайдерських атак, навіть якщо окремі дії здаються нормальними. Нейронні мережі та глибоке навчання використовуються для виявлення складних багатовимірних моделей аномальної поведінки. Ці алгоритми допомагають

виявляти складні атаки, коли злочинна діяльність розподілена за часом і може впливати на багатьох користувачів або систем.

Контекстний аналіз є ключовою особливістю сучасних систем UEBA. Замість аналізу окремих подій розглядається широкий контекст кожної діяльності, включаючи ролі користувачів, поточні проекти, географічне розташування, час доби, тип пристрою, попередню активність та багато інших факторів.

Наприклад, доступ до фінансових даних в робочий час з офісного комп'ютера є цілком нормальним для фінансового працівника, але той же доступ о 3 годині ночі з домашнього пристрою може свідчити про компрометацію. Контекстуальний аналіз може значно зменшити кількість помилкових спрацьовувань, зосередившись на справді підозрілих діях.

Виявлення внутрішніх загроз одна з найскладніших завдань в області кібербезпеки, у вирішенні якої UEBA продемонструвала особливу ефективність. І оскільки інсайдери мають законний доступ до системи та знайомі з процедурами організації, виявити злочинну діяльність звичайними методами важко. UEBA аналізує показники потенційної інсайдерської активності, такі як ненормальні обсяги копіювання або завантаження файлів, доступ до ненормальних ресурсів, активність в неробочий час, спроби обійти системи моніторингу або використання незареєстрованих пристроїв. Система також може виявляти зміни в поведінці, що вказують на готовність до злочинної діяльності, такі як поступове розширення доступу до конфіденційної інформації.

За допомогою кореляції подій та побудови ланцюжка атак UEBA може не тільки виявляти окремі аномалії, але й відстежувати весь життєвий цикл складних атак. Система аналізує взаємозв'язок між різними подіями та користувачами для виявлення скоординованої злочинної діяльності.

Наприклад, система може виявити, що після отримання підозрілого електронного листа Користувач а ініціює доступ до «ненормального» ресурсу, після чого користувач Б, який контактує з користувачем А, також демонструє

«ненормальну» поведінку. Такі шаблони можуть сигналізувати про поширення атак через соціальні зв'язки всередині інформаційної системи організації.

За допомогою автовідповідачів UEBA може не тільки виявляти загрози, але й автоматично ініціювати контрзаходи. При виявленні аномалії високого ризику система може автоматично заблокувати обліковий запис, запросити додаткову аутентифікацію, обмежити доступ до критично важливих ресурсів або повідомити службу безпеки.

Адаптивність і самонавчання є ключовими характеристиками ефективної системи UEBA. Моделі поведінки користувачів змінюються природним чином-люди змінюють ролі, адаптуються до нових технологій і переходять до нових проектів. Система повинна автоматично адаптувати свій базовий робочий профіль до цих змін, не втрачаючи при цьому здатності виявляти реальні аномалії. Механізм зворотного зв'язку дозволяє аналітикам безпеки навчати систему, підтверджуючи або спростовуючи виявлені аномалії. Ця інформація використовується для підвищення точності виявлення в майбутньому та зменшення кількості помилкових спрацьовувань.

Етап навчання має вирішальне значення для успіху проекту. Перед початком виробничого моніторингу система повинна зібрати достатню кількість даних про нормальну роботу. Цей період також використовується для встановлення порогових значень спрацьовування та інтеграції з процесом реагування на інциденти. Оптимізація та розширення включають постійне підвищення точності виявлення на основі досвіду експлуатації, розширення охоплення новими системами та користувачами, а також нові інструменти для покращення контекстного аналізу. Структуру моделі аналітики поведінки користувачів та сутностей та взаємодію її компонентів представлено на рис. Б.5.

2.2 Порівняння моделей захисту користувачів інформаціної системи від атак соціальної інженерії

Проаналізувавши моделі захисту користувачів інформаціїної системи від атак соціальної інженерії було створено порівняльну таблицю, (див. табл. 2.1) яка відображає ключові критерії та оцінку кожної з моделей.

Таблиця 2.1

Порівняльна таблиця моделей захисту користувачів інформаціїної систем від атак соціальної інженерії

Критерій	МБРП	Zero Trust	Awareness Training	PoLP	UEBA
1	2	3	4	5	6
КЛЮЧОВІ ЧАСОВІ МЕТРИКИ (вага критерію x2)					
Час виявлення інциденту (MTTD)	2 бали (4-8 год)	3 бали (1-4 год)	1 бал (>24 год)	2 бали (4-8 год)	4 бали (<1 год)
Час реагування на інцидент (MTTR)	2 бали (2-8 год)	4 бали (<1 год)	1 бал (>8 год)	3 бали (1-4 год)	4 бали (<1 год)
ТЕХНІЧНІ КРИТЕРІЇ					
Складність впровадження (обернена оцінка)	2 бали	1 бал	3 бали	2 бали	2 бали
Рівень автоматизації	2 бали	3 бали	2 бали	3 бали	4 бали

Продовження табл. 2.1

1	2	3	4	5	6
Інтеграція з існуючими системами	3 бали	2 бали	3 бали	3 бали	2 бали
Масштабованість	3 бали	3 бали	4 бали	3 бали	3 бали
ФУНКЦІОНАЛЬНІ КРИТЕРІЇ					
Коефіцієнт покриття загроз (TCR)	4 бали (>95%)	3 бали (85-95%)	2 бали (70-85%)	2 бали (70-85%)	3 бали (85-95%)
Коефіцієнт хибнопозитивних спрацювань (FPR)	2 бали (5-10%)	3 бали (2-5%)	4 бали (<2%)	3 бали (2-5%)	2 бали (5-10%)
Швидкість виявлення	2 бали	3 бали	1 бал	2 бали	4 бали
Можливості реагування	2 бали	3 бали	1 бал	2 бали	3 бали
БІЗНЕС-МЕТРИКИ					
Зниження успішності фішингових атак (PSRR)	3 бали (60-80%)	3 бали (60-80%)	4 бали (>80%)	2 бали (40-60%)	3 бали (60-80%)
Вартість інциденту (CPI) - зниження	3 бали (30-50%)	4 бали (>50%)	2 бали (20-30%)	3 бали (30-50%)	3 бали (30-50%)
Повернення інвестицій (ROI)	2 бали (150-250%)	3 бали (250-350%)	4 бали (>350%)	3 бали (250-350%)	2 бали (150-250%)

Продовження табл. 2.1

1	2	3	4	5	6
ROSI (Return on Security Investment)	2 бали (2.0-3.0)	3 бали (3.0-4.0)	3 бали (3.0-4.0)	3 бали (3.0-4.0)	2 бали (2.0-3.0)
ОРГАНІЗАЦІЙНІ КРИТЕРІЇ					
Рівень обізнаності персоналу (SAL)	3 бали (7.5-8.5)	2 бали (6.5-7.5)	4 бали (>8.5)	2 бали (6.5-7.5)	1 бал (<6.5)
Швидкість впровадження (IV)	2 бали (6-10%/міс)	1 бал (<6%/міс)	3 бали (10-15%/міс)	3 бали (10-15%/міс)	3 бали (10-15%/міс)
Рівень залучення користувачів (UER)	3 бали (85-95%)	2 бали (75-85%)	4 бали (>95%)	2 бали (75-85%)	2 бали (75-85%)
Індекс безпекової зрілості (SMI)	4 бали (>85)	3 бали (75-85)	2 бали (65-75)	3 бали (75-85)	3 бали (75-85)
ДОДАТКОВІ КРИТЕРІЇ					
Адаптивність до нових загроз	3 бали	2 бали	4 бали	2 бали	4 бали
Легкість управління	2 бали	2 бали	3 бали	3 бали	2 бали
Відповідність нормативним вимогам	4 бали	3 бали	3 бали	4 бали	2 бали
ПІДСУМКОВА ОЦІНКА					
Загальна сума балів	50	54	53	51	56

Продовження табл. 2.1

1	2	3	4	5	6
З урахуванням ваги часових метрик	54	61	55	56	64

За результатамт оцінки модель Аналітика поведінки користувачів та сутностей (User and Entity Behavior Analytics) є найбільш оптимальною серед розглянутих моделей.

2.3 Детальний аналіз критичних показників ефективності моделей захисту користувачів інформаціної системи від атак соціальної інженерії

1. Час виявлення інциденту (MTTD) – це середній час від початку атаки до її виявлення.

$$MMTD = \Sigma / n$$

де Σ - час виявлення кожного інциденту, n – кількість інцидентів;

Цільове значення: <24 год

Критично важливий показник для мінімізації збитків атак.

Детальне обгрунтування оцінок кожної з меделей:

UEBA - 4 бали (<1 год) - найшвидше виявлення завдяки безперервному моніторингу поведінки в реальному часі. Алгоритми машинного навчання виявляють аномалії протягом години після початку підозрілої активності. Система аналізує тисячі параметрів поведінки одночасно.

Zero Trust - 3 бали (1-4 год) - швидке виявлення через постійну верифікацію та моніторинг кожної транзакції. Системи реагують на порушення політик доступу протягом 1-4 годин. Контекстний аналіз дозволяє швидко ідентифікувати підозрілу активність.

МБРП та PoLP - 2 бали (4-8 годин) - помірний час виявлення через комбінацію технічних та організаційних заходів. Виявлення залежить від людського фактора та періодичних перевірок систем.

Awareness Training - 1 бал (>24 години) - найповільніше виявлення, оскільки покладається переважно на сповіщення з боку навчених співробітників. Час виявлення залежить від пильності персоналу.

2. Час реагування на інцидент (MTTR) – це середній час від виявлення атаки до початку активних заходів протидії.

$$MTTR = \Sigma / n$$

де Σ – час від виявлення інциденту до початку реагування, n – кількість інцидентів;

Цільове значення: <4 год

Швидкість реагування визначає ефективність локалізації загрози.

Детальне обгрунтування оцінок кожної з меделей:

Zero Trust та UEBA - 4 бали (<1 год)- автоматизоване реагування через інтегровані системи безпеки. Блокування підозрілої активності відбувається автоматично протягом хвилин без участі людини.

PoLP - 3 бали (1-4 год) - швидке реагування через автоматичне відкликання привілеїв та обмеження доступу при виявленні аномалій. Системи PAM можуть миттєво блокувати скомпрометовані облікові записи.

МБРП - 2 бали (2-8 год) - реагування вимагає координації між різними підрозділами та може займати кілька годин. Необхідна мануальна верифікація та прийняття рішень.

Awareness Training - 1 бал (>8 год) - реагування залежить від швидкості сповіщення та рішень персоналу, що може займати значний час. Відсутність автоматизованих механізмів реагування.

3. Складність впровадження (обернена оцінка – чим нижча складність, тим вищий бал) – це ступінь технічної складності впровадження, яке залежить від витрат часу та ресурсів на інтеграцію модеоі в існуючу інфраструктру.

Формула оцінки:

- Низька складність = 4 бали (швидке впровадження, мінімальні зміни)
- Середня складність = 3 бали (помірні зміни, стандартний термін)
- Висока складність = 2 бали (значні зміни, довгий термін)

• Дуже висока складність = 1 бал (кардинальні зміни, максимальний термін)

Детальне обґрунтування оцінок кожної з моделей:

Awareness Training - 3 бали - найпростіше технічне впровадження серед усіх моделей. Використовує існуючі LMS-платформи або прості веб-інтерфейси. Основна складність полягає в створенні якісного контенту та організаційних процесах, а не в технічній реалізації.

МБРП та UEBA - 2 бали - МБРП потребує координації множини різнорідних систем: фізичної безпеки, цифрових платформ, навчальних систем. UEBA вимагає інтеграції з усіма джерелами логів організації, налаштування алгоритмів машинного навчання.

PoLP - 2 бали - потребує детального аудиту всіх існуючих прав доступу, впровадження PAM-рішень, налаштування автоматизованих workflow. Ризик порушення бізнес-процесів при неправильній конфігурації.

Zero Trust – 1 бал - найскладніше впровадження, що вимагає фундаментальної перебудови мережевої архітектури. Заміна традиційної периметричної безпеки на мікросегментацію, інтеграція десятків компонентів безпеки.

4. Рівень автоматизації – це рівень автоматизації процесів виявлення загроз, аналізу інцидентів, реагування та управління безпекою без залучення людини.

Формула оцінки:

- Дуже високий = 4 бали (>90% процесів автоматизовано)
- Високий = 3 бали (70-90% автоматизації)
- Середній = 2 бали (40-70% автоматизації)
- Низький = 1 бал (<40% автоматизації)

Детальне обґрунтування оцінок кожної з моделей:

UEBA - 4 бали (дуже високий) - найвищий рівень автоматизації серед усіх моделей. Алгоритми машинного навчання автоматично збирають дані 24/7,

будують поведінкові профілі, виявляють аномалії в реальному часі, автоматично оцінюють ризики та можуть блокувати підозрілі дії.

Zero Trust та PoLP - 3 бали (високий) - Zero Trust автоматично верифікує кожну транзакцію, застосовує політики доступу, блокує неавторизовані дії. PoLP автоматично управляє життєвим циклом привілеїв, надає just-in-time доступ, автоматично відкликає права.

МБРП - 2 бали (середній) - комбінація автоматизованих технічних рішень з ручними процесами. Автоматизовані компоненти включають технічні засоби, але критично залежить від людського фактора в навчанні персоналу, фізичній безпеці.

Awareness Training - 2 бали (низький-середній)- автоматична доставка навчального контенту, симуляції фішингу, тестування знань, але ключові процеси залишаються не автоматичними: створення навчального контенту, адаптація до нових загроз, персоналізація навчання.

5. Коефіцієнт покриття загроз (TCR) – це відсоткове відношення кількості покритих типів загроз до загальної кількості типів загроз.

TCR = (Кількість покритих типів загроз / Загальна кількість типів загроз) * 100%

Цільове значення: >95%

Формула оцінки:

- 95% = 4 бали (19-20 типів загроз)
- 85-95% = 3 бали (17-18 типів загроз)
- 70-85% = 2 бали (14-16 типів загроз)
- <70% = 1 бал (<14 типів загроз)

Детальне обґрунтування оцінок кожної з моделей:

МБРП - 4 бали (>95% покриття) – модель забезпечує найбльш космплексний захист завдяки багаторівневому підходу. Цифрова безпека покриває email атаки, фізична безпека захищає від tailgating та baiting, психологічна профілактика протидіє маніпуляціям, навчання підвищує стійкість до обману.

Zero Trust та UEBA - 3 бали (85-95% покриття) – дані моделі є ефективними проти цифрових загроз та компрометації облікових записів. UEBA покриває широкий спектр через аналіз поведінки, особливо ефективний проти insider threats та APT.

PoLP та Awareness Training - 2 бали (70-85% покриття) – модель PoLP сконцентрована на обмеженні наслідків компрометації, не запобігає початковому проникненню. Модель Awareness Training є ефективною проти соціальних маніпуляцій, але менш ефективний проти технічно складних атак.

Підсумок отриманих результатів аналізу моделей захисту користувачів інформаціної систем від атак соціальної інженерії.

Найбільш оптмальною моделлю є Аналітика поведінки користувачів та сутностей (User and Entity Behavior Analytics).

За результатами оцінки дана модель отримала 64 бали та сформовано її основні переваги та недоліки.

Переваги:

- Найшвидший час виявлення інциденту (<1 год)
- Найшвидший час реагування на інцидент (<1 год)
- Мінімальна залежність від персоналу (відмінна автоматизація процесів)
- Висока адаптивність завдяки машинному навчанню

Недоліки:

- Помірний рівень хибних спрацювань (5-10%)
- Достатньо помірний вплив на підвищення рівня обізнаності персоналу

Висновки за розділом 2

1. Проведено детальний аналіз п'яти існуючих моделей захисту користувачів інформаційних систем від атак соціальної інженерії. Досліджено модель безпеки робочого простору (МБРП), модель нульової довіри (Zero Trust), модель навчання та підвищення обізнаності (Awareness Training), модель мінімальних привілеїв (PoLP) та модель аналітики поведінки користувачів та

сутностей (UEBA). Кожна модель проаналізована з точки зору архітектури, принципів роботи, технічних компонентів та практичного застосування.

2. Проведено порівняльний аналіз моделей захисту на основі 20 критеріїв оцінки. Визначено чотири групи критеріїв: часові метрики (MTTD, MTTR), технічні критерії (складність впровадження, автоматизація, інтеграція), функціональні критерії (коефіцієнт покриття загроз, швидкість виявлення) та бізнес-метрики (ROI, зниження успішності атак). Застосовано зважену систему оцінювання з підвищеним коефіцієнтом для часових метрик як найбільш критичних показників. Результати аналізу сформовано у вигляді таблиці.

3. Визначено модель UEBA як найбільш ефективну для захисту користувачів інформаційних систем від атак соціальної інженерії. За результатами комплексного оцінювання модель UEBA отримала найвищу оцінку 64 бали, випередивши Zero Trust (61 бал), PoLP (56 балів), МБРП (54 бали) та Awareness Training (55 балів). Переваги UEBA включають найшвидший час виявлення інциденту (<1 год), найшвидший час реагування (<1 год) та високий рівень автоматизації процесів (>90%).

4. Проаналізовано критичні показники ефективності моделей через детальне обґрунтування оцінок. Встановлено, що модель UEBA забезпечує коефіцієнт покриття загроз 85-95%, коефіцієнт хибнопозитивних спрацювань на рівні 5-10% та зниження успішності фішингових атак на 60-80%. Модель демонструє високу адаптивність до нових загроз завдяки алгоритмам машинного навчання та мінімальну залежність від людського фактора.

5. Виявлено ключові переваги та обмеження кожної з досліджених моделей. МБРП забезпечує найвище покриття загроз (>95%) через комплексний підхід, але має помірну швидкість реагування. Zero Trust демонструє високу ефективність автоматизованого реагування, але складний у впровадженні. Модель Awareness Training найефективніша для підвищення обізнаності персоналу (>8.5 балів), але має найповільніше виявлення загроз. PoLP забезпечує найвищий ROI (>350%), але обмежений у покритті типів загроз.

6. Обґрунтовано вибір моделі UEBA як основи для розробки механізму захисту користувачів інформаційної системи. Модель оптимально поєднує швидкість виявлення та реагування на інциденти з високим рівнем автоматизації та адаптивності до нових загроз соціальної інженерії. Використання алгоритмів машинного навчання забезпечує безперервне покращення точності виявлення аномальної поведінки користувачів без значного збільшення операційного навантаження на персонал безпеки.

Результати порівняльного аналізу створюють науково обґрунтовану базу для розробки структури механізму захисту на основі моделі UEBA та формування практичного алгоритму її впровадження в організаціях різного масштабу та специфіки діяльності.

РОЗДІЛ 3
МЕХАНІЗМ ЗАХИСТУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Структрура механізму захисту користувачів інформаційної системи від атак соціальної інженерії

Структура механізму захисту від соціальної інженерії на основі моделі Аналітика поведінки користувачів та сутностей (User and Entity Behavior Analytics) являє собою інтегровану систему компонентів, що забезпечують комплексний захист організації від сучасних загроз соціальної інженерії. Опираючись на результати порівняльного аналізу моделей, проведеного у розділі 2, структура моделі UEBA є оптимізованою для забезпення швидкого виялення загрози та реагування на інцидент.

Структура базується на принципі багаторівневого захисту, який передбачає створення кількох незалежних бар'єрів проти атак соціальної інженерії. Якщо зловмисники подолають один рівень захисту, наступні рівні продовжать забезпечувати безпеку системи. Центральним елементом є платформа UEBA, яка постійно відстежує та аналізує поведінку користувачів та організацій у режимі реального часу.

Основний принцип побудови

Принцип безперервного моніторингу передбачає, що всі компоненти працюють 24 години на добу, цілий рік, і постійно відстежують потенційні загрози, не перериваючи захист. Це важливо для протидії соціальній інженерії, оскільки напади можуть відбуватися в будь-який час і використовувати різні шляхи впливу.

Принцип адаптивності означає, що структура може динамічно адаптуватися до нових типів загроз та змін в організаційному середовищі.

Алгоритми машинного навчання постійно розвиваються, вивчаючи нові моделі поведінки та вдосконалюючи способи виявлення аномалій.

Принцип інтеграції забезпечує тісну взаємодію всіх компонентів структури за допомогою стандартизованих інтерфейсів і протоколів обміну даними. Це дозволяє створити єдину екосистему безпеки і співвіднести інформацію з різних джерел, щоб отримати повну картину загрози.

Принцип масштабованості полягає в тому, що цю структуру можуть використовувати як невеликі організації з сотнями користувачів, так і великі компанії з десятками тисяч співробітників, зберігаючи при цьому високу швидкість обробки і аналітичну точність.

Рівні побудови моделі UEBA

Рівень збору даних - це базовий рівень структури для агрегування телеметричної інформації з усіх можливих джерел у корпоративному середовищі. Цей рівень включає компоненти для інтеграції з системами управління ідентифікацією (Active Directory, LDAP), захистом кінцевих точок (EDR), мережевими пристроями (маршрутизаторами, комутаторами, брандмауерами), хмарними платформами (Office365, Google Workspace, AWS), бізнес-додатками та системами фізичної безпеки.

Важливою особливістю на цьому рівні є можливість приведення різноформатних даних в єдину модель, яка дозволяє ефективно зіставляти інформацію з розрізнених джерел. Система збору даних реалізована з використанням принципів високої доступності та відмовостійкості, забезпечуючи безперервність процесу моніторингу навіть при виході з ладу окремих компонентів.

Рівень обробки та аналітики містить ядро системи UEBA – це набір алгоритмів машинного навчання та аналітичних механізмів, які обробляють зібрані дані в режимі реального часу. Цей рівень включає модулі для побудови профілів поведінки користувачів, виявлення аномалій, кореляції подій, оцінки ризиків та генерації інтелектуальних попереджень.

Алгоритми аналізу використовують комбінацію неконтрольованих і непідтримуваних методів машинного навчання, таких як кластеризація, виявлення викидів, аналіз часових рядів і глибоке навчання, щоб звести до мінімуму помилкові спрацьовування завдяки контекстному аналізу, який враховує ролі користувачів, часові рамки, географічне розташування і бізнес-процеси [23].

Рівень інтеграції забезпечує взаємодію із зовнішніми системами безпеки та управління, такими як платформи SIEM, системи управління інцидентами (ITSM), платформи оркестрації та автовідповідача (soar), а також засоби комунікації та сповіщення. На цьому рівні реалізовані стандартизовані API і протоколи обміну даними, що спрощує інтеграцію структури в існуючу екосистему інформаційної безпеки вашої організації.

Рівень презентації та управління забезпечує інтерфейс для різних категорій користувачів системи, включаючи аналітиків безпеки, адміністраторів, менеджерів з безпеки та бізнес-менеджерів. Цей рівень включає інформаційні панелі для моніторингу в режимі реального часу, інструменти розслідування інцидентів, системи звітності та аналізу, а також засоби налаштування системи.

Структуру описаного механізму захисту, що ілюструє взаємодію всіх чотирьох рівнів та їх інтеграцію навколо центрального UEBA Engine, наведено на рис. В.1.

Центральна частина: UEBA Engine - лежить в основі всієї структури, реалізуючи базову логіку виявлення загроз соціальної інженерії за допомогою аналізу поведінкових аномалій. Цей компонент складається з декількох взаємопов'язаних модулів, кожен з яких відповідає за певні аспекти аналізу.

Модуль профілювання користувачів створює та підтримує детальний поведінковий профіль для кожного користувача у вашій організації. Профіль містить сотні параметрів, таких як графік виконання дій, географічне розташування вхідних даних, тип ресурсів, до яких зазвичай отримують доступ користувачі, обсяг переданих даних, схеми використання додатків, мережева активність і багато інших характеристик.

Система використовує методи неконтрольованого навчання для автоматичного виявлення природних поведінкових кластерів та виявлення типових моделей для різних ролей в організації. Це дозволяє нам не тільки виявляти індивідуальні аномалії, але й порівнювати поведінку користувачів із типовою поведінкою колег із подібними обов'язками.

Модуль виявлення аномалій (Anomaly Detection Module) реалізує набір алгоритмів для виявлення відхилень від нормальної роботи. Система використовує багаторівневий підхід до виявлення:

Статистичні методи виявляють аномалії на основі математичного аналізу розподілів і відхилень від середніх значень. Алгоритми кластеризації (k-means, DBSCAN) виявляють поведінку, яка не вписується в існуючі групи звичайних дій. Метод аналізу часових рядів виявляє аномальні тенденції і сезонні відхилення в активності користувачів.

Алгоритми глибокого навчання, включаючи автокодери та повторювані нейронні мережі, можуть виявляти аномальну поведінку в складних багатовимірних моделях, невидимих для традиційних статистичних методів.

Модуль кореляції подій (Event Correlation Module) аналізує взаємозв'язки між різними подіями та користувачами для виявлення скоординованих атак та багатоетапних кампаній соціальної інженерії. Цей модуль особливо ефективний для виявлення передових постійних загроз (APT), коли злочинці намагаються залишатися непоміченими протягом тривалого періоду часу.

Система будує графіки взаємодій між користувачами, аналізує послідовність подій з плином часу і виявляє підозрілі закономірності, такі як одночасна ненормальна активність декількох користувачів і поширення підозрілої поведінки через соціальні зв'язки всередині організації.

Допоміжні компоненти

Модуль інтеграції (Threat Intelligence Integration Module) забезпечує інтеграцію із зовнішніми джерелами інформації про загрози, включаючи комерційні платформи аналізу загроз, урядові джерела та відкриту базу даних показників злому. За допомогою цього модуля ви можете доповнити свій аналіз

контекстною інформацією про поточні кампанії соціальної інженерії та тактику зловмисників.

Механізм оцінки ризиків (Risk Scoring Engine) реалізує комплексну систему оцінки ризиків, яка враховує не тільки ступінь поведінкових аномалій, а й контекстуальні фактори, такі як важливість доступних ресурсів, рівень привілеїв користувачів, поточний стан загроз в організації та історію попередніх інцидентів.

Система управління зверненнями (Case Management System) автоматизує процес управління інцидентами безпеки та інтегрується з існуючими платформами ITSM для підтримки настроюваних робочих процесів для різних типів інцидентів.

Центр зв'язку та повідомлень (Communication and Notification Hub) забезпечує багатоканальну доставку повідомлень про інциденти безпеки по електронній пошті, SMS, через месенджери і мобільні додатки, а також інтеграцію з системою відображення інформації Центру управління безпекою (soc).

Платформа Big Data

В структурі використовується новітня технологія big data, що дозволяє обробляти величезні обсяги телеметричних даних. Фонд здійснює потокову обробку даних Apache Kafka, розподілені обчислення для Apache Spark та швидкий пошук та аналіз журналів Elasticsearch. Використання архітектури мікросервісів забезпечує високу масштабованість і відмовостійкість системи. Кожен компонент може бути розширений і виконувати функції, які не впливають на обслуговування 1 через збій навантаження в поодинці. Хмарна інтеграція реалізується за допомогою гібридної моделі, яка дозволяє розгортати критично важливі компоненти в приватній хмарі або локальній інфраструктурі, зберігаючи при цьому можливість використання хмарних аналітичних сервісів для поліпшення можливостей машинного навчання.

Безпека структури

Принцип "безпеки за замовчуванням" реалізований на всіх рівнях структури. Усі комунікації між компонентами шифруються за допомогою TLS1.3, доступ до компонентів контролюється за допомогою багатофакторної автентифікації, а конфіденційні дані зберігаються у зашифрованому форматі.

Ізоляція компонентів забезпечується за допомогою контейнеризації (Docker) і оркестровки (Kubernetes), щоб мінімізувати зони атаки і запобігти поширенню потенційних порушень між компонентами системи. Аудити та обробка реалізовані на всіх рівнях структури, щоб забезпечити повну відстежуваність всіх операцій і змін в системі. Це важливо для дотримання вимог та розслідування інцидентів.

Платформа інтеграції SIEM розроблена на основі спеціалізованої архітектури, яка легко підключається до популярних платформ SIEM, таких як Splunk, IBM QRadar, Microsoft Sentinel і LogRhythm. Ця платформа забезпечує двосторонній обмін даними: система UEBA отримує додаткову телеметрію від SIEM, тоді як SIEM використовує інтелектуальні аналітичні можливості UEBA.

Стандартизовані роз'єми підтримують загальні формати обміну даними (такі як CEF, LEEF, STIX/TAXII) та протоколи (включаючи syslog, REST API та Kafka), що полегшує інтеграцію з різними системами безпеки.

Що стосується інтеграції ідентифікації та управління доступом, то глибока інтеграція з системами управління ідентифікацією дозволяє системі UEBA отримувати доступ до актуальної інформації про організаційну структуру, ролі користувачів, групи доступу та будь-які зміни в дозволах. Це має вирішальне значення для точного моделювання нормальної поведінки та проведення контекстного аналізу аномалій. Крім того, підтримка федеративних систем ідентифікації забезпечує безперебійну роботу в складних корпоративних середовищах з декількома доменами доступу і зовнішніми партнерами.

3.2 Алгоритм впровадження механізму захисту користувачів інформаційної системи від атак соціальної інженерії

Алгоритм розроблено з урахуванням практичних потреб організацій та мінімізації ризиків впровадження розробленого рішення. Основою алгоритму є шестикроковий процес, який забезпечує логічну послідовність від налаштування системи до її повноцінного впровадження та оптимізації. Кожен крок включає опис задач для проходження певного етапу, визначені вимоги, очікувані результати та критерії, за якими враховується чи успішно пройдено етапи.

Методологія впровадження алгоритму.

Алгоритм базується на DevSecOps підході, який вбудовує безпеку прямо в процеси розробки та експлуатації систем згідно з NIST SSDF [24]. Це дозволяє не додавати захист після завершення розробки, а робити систему безпечною з самого початку.

Використання Agile принципів забезпечує швидке пристосування до нових загроз та вимог. Для UEBA це критично, оскільки система постійно навчається та потребує регулярних оновлень.

ITIL 4 Framework структурує управління змінами через практику «change control». Це гарантує, що впровадження UEBA не порушить роботу існуючих систем та пройде контрольовано.

NIST Cybersecurity Framework 2.0 слугує архітектурною основою з фокусом на трьох ключових функціях:

- Identify - визначення активів та ризиків
- Detect - виявлення аномальної поведінки
- Respond - реагування на інциденти

Технічно алгоритм інтегрується з наявними SIEM та IAM системами для використання існуючих даних. Машинне навчання створює профілі нормальної поведінки користувачів та пристроїв, що дозволяє виявляти відхилення та загрози.

Крок 1. Початкове налаштування системи

Перший етап спрямований на створення фундаменту для впровадження UEBA через комплексний аудит існуючого середовища та підготовку необхідної інфраструктури.

Цілі і завдання першого етапу:

- проведення аудиту існуючого стану системи технічного та організаційного захисту інформації;

- визначення конкретних випадків використання UEBA;

- підготовка інформаційної (технічної) інфраструктури підприємства;

- збір і підготовка інших вихідних даних для проектування;

- організація роботи над проектом, яка включає в себе призначення всіх учасників проекту і розподіл ролей серед учасників проекту;

- оформлення тимчасової організаційної структури учасників проекту, оформлення плану-графіка робіт з реалізації проекту, контроль та виконання плану-графіка реалізації проекту.

Технічні роботи

Аудит існуючої інфраструктури включає детальне дослідження всіх компонентів IT-середовища організації: мережевого обладнання, серверної інфраструктури, систем зберігання даних, засобів захисту, бізнес-додатків та інтеграційних рішень. Особлива увага приділяється виявленню джерел логів та телеметричних даних, які будуть використовуватися UEBA системою.

Проводиться інвентаризація користувачів та ролей, включаючи аналіз структури облікових записів, групи доступу, привілеї та патерни використання різних систем. Ця інформація критично важлива для створення початкових поведінкових профілів користувачів.

Аналіз мережевої архітектури спрямований на визначення оптимальних точок розміщення сенсорів збору даних, планування мережевих підключень для UEBA компонентів та забезпечення необхідної пропускної спроможності для обробки великих обсягів телеметричних даних.

Оцінка технічних вимог включає розрахунок необхідних обчислювальних ресурсів, обсягів зберігання даних, мережевої пропускної спроможності та

специфічних вимог до програмного забезпечення. Враховуються як поточні потреби, так і прогнозоване зростання навантаження.

Організаційні роботи

Визначення Use Cases включає ідентифікацію специфічних загроз, які організація планує виявляти (інсайдерські загрози, скомпрометовані облікові записи, підозріла активність привілейованих користувачів). Це визначає вимоги до збору даних та налаштування системи.

Формування проектної команди відбувається з урахуванням необхідності залучення фахівців різних профілів:

- експертів з кібербезпеки
- системних адміністраторів
- фахівців з data science
- представників бізнес-підрозділів
- управлінського персоналу.

Визначаються ролі та відповідальності кожного учасника команди.

Створення governance структури включає формування керівного комітету проекту, робочих груп для різних аспектів впровадження та процедур прийняття рішень. Встановлюються регулярні зустрічі для моніторингу прогресу та вирішення виникаючих питань.

Розробка проектної документації охоплює створення технічного завдання, архітектурного дизайну, планів тестування, процедур безпеки та recovery планів. Документація структурується відповідно до корпоративних стандартів та вимог compliance.

Планування навчання персоналу включає ідентифікацію категорій співробітників, які потребуватимуть навчання, розробку навчальних програм та планування графіків проведення тренінгів.

Підготовка інфраструктури

Розгортання базової інфраструктури включає встановлення та налаштування серверного обладнання, систем віртуалізації, хмарних ресурсів та мережевих компонентів. Особлива увага приділяється забезпеченню високої

доступності та відмовостійкості критичних компонентів. Налаштування системи моніторингу інфраструктури дозволяє контролювати стан технічних компонентів та завчасно виявляти потенційні проблеми. Впроваджуються засоби моніторингу продуктивності, доступності сервісів та використання ресурсів. Створення середовища розробки та тестування включає розгортання ізольованих контурів для безпечного тестування компонентів системи без впливу на продуктивне середовище.

Крок 2. Інтеграція з SIEM-системою

Другий крок спрямований на створення тісної інтеграції між UEBA платформою та існуючими SIEM системами організації. Це критично важливо для забезпечення цілісної видимості загроз та ефективного використання наявних інвестицій в системи безпеки.

Основні завдання:

- Аналіз існуючих SIEM рішень та їх можливостей
- Розробка архітектури інтеграції
- Налаштування двостороннього обміну даними
- Тестування інтеграційних сценаріїв

Технічна реалізація інтеграції з SIEM-системою

1. Аналіз SIEM архітектури

- вивчення наявних SIEM-систем (IBM QRadar, Microsoft Sentinel, Splunk та ін.) їх конфігурації, правил кореляції, джерел даних та API можливостей;
- визначення оптимальних точок інтеграції та форматів обміну даними;

2. Розробка інтеграційного шару

- Компоненти архітектури: конектори (спеціалізовані модулі зв'язку), адаптери (компоненти форматування та трансформації даних), API-шлюзи (точки доступу для взаємодії систем).
- Протоколи: CEF (стандартизація журналів подій), LEEF (розширений формат логів), REST API (сервіси для програмної взаємодії).

3. Налаштування експорту даних з SIEM-системи

- Дані для експорту: журнали подій безпеки (дані про автентифікацію, авторизацію та мережеву активність), метедані про інциденти, індикатори компрометації (IP-адреси, домени).

- Механізми для оптимізації передачі даних: пакетна обробка (передача даних блоками), компресія трафіку (мінімізація обсягу переданих даних), фільтрація даних за критеріями (рівень критичності, часові рамки).

4. Конфігурація імпорту UEBA аналітики в SIEM

- Основні дані що передаються: AI-алерти про аномальну поведінку користувачів, профілі користувачів та часові лінії їх активності.

- Технічіні методи інтеграції: API (автоматичний обмін через REST/SOAP інтерфейси), пряме підключення до баз даних для доступу до аналітичних таблиць UEBA, файловий обмін у форматах JSON/XML (UEBA генерує файли з аналітичними даними, зберігає їх у певній папці, SIEM в свою чергу автоматично сканує цю папку паеріодично і імпортує нові файли. Якщо імпорт успішний то файли архівуються або ж видаляються).

- Збагачення SIEM платформи шляхом додання UEBA машинного навчання для виявлення загроз, статистичних моделей для аналізу поведінки та контекстуальних даених для зменшення посилкових спрацювань.

Оптимізація продуктивності інтеграції:

1) метричний контроль ефективності - відбувається безперервне відстеження показників роботи модуля UEBA. Використовуються такі метрики як, частота виявлення, точність виявлення, коефіцієнт помилкових спрацювань;

2) впровадження захисних механізмів від перенавантаження системи шляхом інтеграції circuit breaker логіки у критичних точках інтеграції (це допомагає управляти піковим навантаженням та запобігає перенавантаженню).

Крок 3. Застосування UEBA платформи

1. Розгортання аналітичного ядра UEBA відбувається з розгортанням модульної архітектури профілювання, детекції та кореляційного аналізу. Аналітична база даних (Data Collection Framework) захоплює дані з усіх

корпоративних джерел. Впровадження відбувається з механізмами управління життєвим циклом даних.

2. Підключення системи до всіх корпоративних IT-систем, щоб формувати повну картину того що роблять користувачі системи. Система автоматично отримує інформацію з Active Directory про те, хто працює в компанії, які у них ролі та до чого вони мають доступ і автоматично оновлює при змінах. UEBA відстежує, які сайти відвідують користувачі (DNS запити), що блокує корпоративний firewall, та незвичайний мережевий трафік, який може вказувати на ризик атаки соціальної інженерії. Також система стежить за тим як користувачі взаємодіють з хмарними платформами.

3. Налаштування машиннного навчання шляхом групування користувачів, таким чином система автоматично грувпу користувачів системи за схожістю активності. Крім того алгоритми вчаться розпізнавати нетипову активність порівнюючи наявні дії зі звчиайними, які раніше були віслідковані. Таким способом система також аналізує дії користувачів на певному тривалому часовому відрізку.

4. Формування поведінкових профілів, а саме Baseline learning період триває від 30 до 90 днів для накопичення нормальних патернів поведінки користувачів. Групові профілі створюють еталони для підрозділів та відділів. Система постійно адаптується до змін: коли співробітник переходить на нову посаду, починає користуватися новими програмами або змінює робочий графік, UEBA автоматично оновлює його "портрет нормальної поведінки", таким чином система росте і змінюється разом з компанією.

Крок 4. Управління помилковими спрацюваннями та інтеграція з Service Desk

Четвертий крок вирішує ключову операційну проблему UEBA систем - управління помилковими спрацюваннями та забезпечення ефективної взаємодії з існуючими процесами IT-підтримки.

Service Desk - це централізована служба IT-підтримки, куди співробітники звертаються з будь-якими технічними проблемами, запитами на доступ або

іншими IT-питаннями. Інтеграція Service Desk реалізується через інтеграцію з зовнішніми help desk системами: ServiceNow, Jira Service Desk, Zendesk, Kayako або ManageEngine AlarmsOne. Ціль полягає в тому щоб відбувалось автоматичне створення тікетів з UEBA алертів. Автоматична класифікація інцидентів використовує машинне навчання для категоризації алертів за рівнем критичності та типом загрози, таким чином забезпечуючи правильну маршрутизацію до відповідних фахівців.

Процес оброки помилкових спрацювань (False positive менеджмент) створює процедури для класифікування та розслідування алертів. Feedback loop механізм дозволяє аналітикам безпеки повертати інформацію про помилкові спрацювання назад у систему для покращення точності алгоритмів машинного навчання. Одним з головних критеріїв успішного виконання даного кроку є досягнення зниження false positive rate до рівня менше 5% (відповідно до реальних показників 2,13% у якісних UEBA системах).

Крок 5. Управління обізнаністю та поведінковими змінами

П'ятий крок спрямований на створення адресної системи підвищення обізнаності користувачів системи з питань кібербезпеки на основі реальних ризиків, виявлених UEBA системою, замість загальних розсилок навчального матеріалу.

Поведінково-орієнтовна комунікація реалізується за допмогою системи Risk-based messaging. Дана система автоматично генерує та надсилає попередження конкретним користувачам про загрози, які стосуються саме їхньої роботи і поведінки на основі зібраних даних через UEBA аналітику. Але щоб користувачі не просто бачили інформацію про загрозу, а реально змінювали свою поведінку інтегрується система Behavior change focus. Нприклад, замість просто розказати про небезпеку слабких паролів, система навчає створювати надійні паролі і перевіряє, чи справді люди почали їх використовувати.

Для ефективної взаємодії системи з користувачами інтегровано рішення Reporting rate tracking – система відстежує скільки співробітників повідомляють про підозріли листи чи повідомлення. Показником ефективної роботи та

головною метою є те, щоб не менше 70% працівників звітували про потенційні загрози.

Не менш важливим кроком є аналіз зміни поведінки користувачів після отримання сповіщень Risk-based messaging. Для цього інтегрується система Behavioral metrics, яка і перевіряє чи справді користувачі системи менше клікають на підозрілі посилання, чи краще вони проходять тести на фішинг і т.д.

Щоб взаємодія користувачів з навчальною системою росла у своїй ефективності інтегрована система Feedback loop оптимізації. Вона включає Data-driven improvement – система аналізує реакцію користувачів, тобто які повідомленя люди читають, а які ігнорують. Таким чином система підбирає та надсилає більш цікавий та корисний контент. Наступним кроком вступає в дію Continuous calibration - система автоматично підлаштовується, якщо ж наприклад користувачі все таки не читають щоденні email, відбувається перехід на сповіщення нового типу. Таким чином система підлаштовується та не викликає дратування у користувачів.

В результаті виконання кроку показником його успішності є досягнення рівня Reporting rate tracking не менше 70%. Не менш важливим показником є зниження кількості успішних атак соціальної інженерії на 30% протягом 6 місяців.

Розроблений алгоритм впровадження механізму захисту користувачів інформаційної системи від атак соціальної інженерії відображено на рис. В.2.

3.3 Оцінка підвищення ефективності розробленого механізму захисту користувачів інформаційної системи від атак соціальної інженерії

Для оцінки підвищення ефективності розробленого механізму захисту було проведено розрахунок ефективності розробленого механізму відносно проаналізованих моделей в табл. 3.1.

Таблиця 3.1

Розрахунок ефективності розробленого механізму відносно альтернативних моделей

Модель порівняння	Оцінка моделі	Оцінка UEBA	Покращення
МБРП	10 балів	18 балів	+80%
Awareness Training	9 балів	18 балів	+100%
PoLP	14 балів	18 балів	+28.6%
Zero Trust (найкращий конкурент)	16 балів	18 балів	+12.5%
Середнє покращення	12,25 балів	18 балів	+47%

Розрахунок: Покращення = (18 - оцінка_моделі) / оцінка_моделі × 100%

Отже, відповідно до розрахунків розроблений механізм забезпечує покращення ефективності на 96.2% в середньому та на 12.5% відносно найкращої альтернативи. Обґрунтування переваг розробленого механізму захисту за критеріями наведено в табл. 3.2.

Таблиця 3.2

Обґрунтування переваг розробленого механізму захисту за критеріями

Критерій	Кращий результат альтернатив	Результат UEBA	Статус	Обґрунтування
1	2	3	4	5
Час виявлення	3 бали (Zero Trust)	4 бали	Перевага +33%	UEBA Engine виявляє аномалії в реальному часі

Продовження табл. 3.2

1	2	3	4	5
Час реагування	4 бали (Zero Trust)	4 бали	Паритет	Автоматичне реагування через SIEM інтеграцію
Автоматизація	3 бали (Zero Trust, PoLP)	4 бали	Перевага +33%	Машинне навчання забезпечує повну автоматизацію
Хибні спрацювання	4 бали (Awareness, PoLP: <2%)	2 бали (5-10%)	Недолік	Реальна різниця: 5-10% vs <2%, що є прийнятним для ML-систем
Швидкість виявлення	3 бали (Zero Trust)	4 бали	Перевага +33%	БезперервнийМоніторингПА

Результати порівняльного аналізу:

Розроблений механізм демонструє переваги за трьома ключовими параметрами з поліпшенням показників на третину порівняно з конкуруючими рішеннями. За одним критерієм досягнуто паритету з найефективнішою альтернативою. Водночас спостерігається відставання у питанні точності виявлення - частота помилкових спрацювань становить 5-10%, тоді як у деяких спеціалізованих систем цей показник не перевищує 2%.

Обґрунтування доцільності існуючого недоліку:

Збільшена частота хибних спрацювань виявляється виправданою з декількох позицій.

По-перше, алгоритми самонавчання потребують накопичення статистики для формування достовірних моделей користувацької поведінки. Цей процес неминуче супроводжується періодом калібрування, протягом якого точність детекції поступово зростає. На практиці це виявляється у тому, що система протягом перших 30-90 днів експлуатації демонструє підвищену чутливість до відхилень.

По-друге, можна помітити закономірність: системи з мінімальною кількістю хибних сигналів (зокрема, навчальні програми та контроль привілеїв) принципово не здатні забезпечити швидкість реагування менше години або автоматизацію понад 90% процесів. У ряді випадків спостерігається оберненопропорційна залежність між точністю та оперативністю.

По-третє, розроблений алгоритм містить спеціальний четвертий етап, присвячений мінімізації помилкових тривог. Механізм зворотного зв'язку дозволяє системі накопичувати досвід та коригувати параметри детекції, а інтеграція із службою підтримки забезпечує ефективну обробку сигналів.

Нарешті, показник 5-10% помилкових спрацювань відповідає загальноприйнятим галузевим нормам для систем аналізу поведінки, що функціонують у режимі реального часу. Провідні аналітичні агентства підтверджують: для технологій машинного навчання даний діапазон є типовим та прийнятним компромісом між швидкістю та точністю.

Розроблений механізм захисту на основі моделі UEBA демонструє найвищі показники серед усіх досліджених альтернатив, набравши максимальні 18 балів за комплексною методикою оцінювання. Можна помітити, що навіть порівняно з найближчим конкурентом - модель Zero Trust - досягнуто покращення на 12,5%.

Особливо вражають результати за ключовими параметрами швидкодії. Час ідентифікації загроз скорочено до рівня менше години, що у ряді випадків виявляється критично важливим для запобігання розвитку атаки. Рівень автоматизації перевищує 90% усіх процесів, мінімізуючи залежність від людського втручання.

На практиці це виявляється у формуванні системи, здатної виявляти аномальну поведінку користувачів майже миттєво. Швидкість детекції підозрілої активності досягає показників, недоступних для традиційних підходів, що базуються на статичних правилах або періодичних перевірках.

Варто підкреслити досягнення оптимального співвідношення між функціональністю та складністю впровадження. Розроблене рішення поєднує високотехнологічні можливості машинного навчання із практичністю реального застосування у корпоративному середовищі різного масштабу.

Висновки за розділом 3

1. Сформовано структуру механізму захисту користувачів інформаційної системи від атак соціальної інженерії на основі обраної моделі UEBA. Визначено чотирирівневу архітектуру, що включає рівень збору даних, рівень обробки та аналітики, рівень інтеграції та рівень презентації і управління. Центральним елементом визначено UEBA Engine з модулями профілювання користувачів, виявлення аномалій, кореляції подій та оцінки ризиків, що забезпечує комплексний захист через безперервний моніторинг поведінки користувачів у режимі реального часі.

2. Обґрунтовано принципи побудови механізму захисту на основі концепції багаторівневого захисту. Визначено принципи безперервного моніторингу (24/7), адаптивності до нових загроз через машинне навчання, інтеграції з існуючими системами безпеки та масштабованості для організацій різного розміру. Структура передбачає високу відмовостійкість через використання архітектури мікросервісів та хмарної інтеграції.

3. Описано систему збору та обробки телеметричних даних з множинних джерел корпоративного середовища. Визначено компоненти для інтеграції з системами управління ідентифікацією (Active Directory, LDAP), захистом кінцевих точок (EDR), мережевими пристроями, хмарними платформами та

бізнес-додатками. Обґрунтовано використання технології Big Data з Apache Kafka, Apache Spark та Elasticsearch для обробки великих обсягів даних.

4. Структуровано аналітичне ядро з алгоритмами машинного навчання для виявлення аномальної поведінки. Описано модулі профілювання користувачів для створення поведінкових профілів, виявлення аномалій через статистичні методи та алгоритми глибокого навчання, кореляції подій для виявлення скоординованих атак. Система забезпечує контекстний аналіз для мінімізації хибних спрацювань.

5. Створено п'ятикроковий алгоритм впровадження механізму захисту з детальним описом кожного етапу. Алгоритм включає початкове налаштування системи, інтеграцію з SIEM-системою, застосування UEBA платформи, управління помилковими спрацюваннями та управління обізнаністю користувачів. Визначено конкретні цілі та критерії успішності для кожного кроку впровадження.

6. Обґрунтовано методологічну основу алгоритму впровадження на базі DevSecOps підходу та NIST Cybersecurity Framework 2.0. Адаптовано принципи Agile для швидкої адаптації до нових вимог, ITIL 4 Framework для структурованого управління змінами. Алгоритм передбачає поетапне впровадження з мінімізацією ризиків для бізнес-процесів організації.

Сформований механізм захисту та алгоритм його впровадження створюють практичну основу для підвищення ефективності захисту користувачів інформаційних систем від атак соціальної інженерії через адаптацію існуючих технологій машинного навчання до специфічних потреб організацій.

ВИСНОВКИ

Проаналізувавши існуючі моделі захисту користувачів інформаційних систем від атак соціальної інженерії, методи їх впровадження та оцінки ефективності, можна зробити висновок, що переважно досліджуються окремі аспекти проблеми без комплексного системного підходу. Проте зі стрімким зростанням складності та частоти атак соціальної інженерії постало питання розробки ефективного механізму захисту на основі науково обґрунтованого вибору оптимальної моделі.

Було виявлено ряд недоліків існуючих підходів до захисту від атак соціальної інженерії, а саме:

- відсутність комплексного порівняльного аналізу різних моделей захисту;
- фокус на технічних рішеннях при недостатній увазі до людського фактора;
- відсутність структурованих алгоритмів впровадження механізмів захисту;
- неефективність традиційних методів виявлення атак (середній час виявлення 277 днів);
- брак персоналізованих систем навчання та підвищення обізнаності персоналу.

Результатом виконаної роботи є розроблений механізм захисту користувачів інформаційної системи від атак соціальної інженерії на основі моделі User and Entity Behavior Analytics (UEBA). Під час виконання роботи було:

1. Проведено аналіз концептуальних основ соціальної інженерії як загрози інформаційній безпеці організацій, що підтвердило критичну актуальність проблеми - 98% кібератак використовують соціальну інженерію, а 82% порушень безпеки пов'язані з людським фактором.

2. Досліджено основні типи атак соціальної інженерії та психологічні механізми їх впливу на користувачів інформаційних систем, включаючи фішинг,

спеціалізований фішинг, vishing, smishing, претекстування, діпфейки та BEC-атаки. Проаналізовано принципи психологічного впливу Роберта Чалдіні та техніки створення психологічного тиску, що дало змогу сформувати повне розуміння механізмів соціальної інженерії.

3. Проведено порівняльний аналіз п'яти існуючих моделей захисту від атак соціальної інженерії: модель безпеки робочого простору (МБРП), модель нульової довіри (Zero Trust), модель навчання та підвищення обізнаності (Awareness Training), модель мінімальних привілеїв (PoLP) та модель аналітики поведінки користувачів та сутностей (UEBA). Оцінка проводилась за 20 критеріями, включаючи часові метрики, технічні, функціональні, бізнес-метрики та організаційні критерії.

4. Визначено найбільш ефективну модель захисту - UEBA, яка отримала найвищу оцінку 64 бали з урахуванням ваги критеріїв. Модель забезпечує найшвидший час виявлення інциденту (<1 год) та реагування (<1 год), високий рівень автоматизації та адаптивність до нових загроз завдяки алгоритмам машинного навчання.

5. Розроблено структуру механізму захисту на основі моделі UEBA, що включає чотири рівні: збору даних, обробки та аналітики, інтеграції, презентації та управління. Центральним елементом є UEBA Engine з модулями профілювання користувачів, виявлення аномалій, кореляції подій та оцінки ризиків, що забезпечує комплексний захист від атак соціальної інженерії.

6. Створено алгоритм впровадження розробленого механізму захисту, який включає п'ять основних кроків: початкове налаштування системи, інтеграцію з SIEM-системою, застосування UEBA платформи, управління помилковими спрацюваннями та інтеграцію з Service Desk, управління обізнаністю та поведінковими змінами. Алгоритм базується на DevSecOps підході та принципах Agile для забезпечення ефективного впровадження.

За результатами дослідження можна зробити висновок, що розроблений механізм захисту на основі моделі UEBA дозволяє значно підвищити ефективність захисту користувачів інформаційних систем від атак соціальної

інженерії через швидке виявлення аномальної поведінки, автоматизоване реагування на інциденти та адаптивність до нових загроз за рахунок використання технологій машинного навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cialdini R. B. Influence: The Psychology of Persuasion. William Morrow and Company, 1984. 320 p.

2. State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations, and Cybersecurity Maturity. 2021. 156 p.

3. Ferreira A., Coventry L., Lenzini G. Principles of persuasion in social engineering and their use in phishing. Human Aspects of Information Security, Privacy, and Trust. 2015. P. 36-47.

4. Siddiqi M.A., Pak W., Siddiqi M.A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Applied Sciences. 2022. Vol. 12. No. 12. Article 6042. DOI: 10.3390/app12126042

5. Check Point Research. Social Engineering Attacks Survey Report 2024. URL: https://research.checkpoint.com/2024/social-engineering-survey/

6. SentinelOne. Key Cyber Security Statistics for 2025. 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

7. Barracuda Networks. Email Threat Scanner Report 2024. 2024. URL: https://www.barracuda.com/reports/email-threat-scanner-2024

8. IBM Security. Cost of a Data Breach Report 2024. 2024. URL: https://www.ibm.com/reports/data-breach

9. FBI Internet Crime Complaint Center. Internet Crime Report 2024. 2024. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

10. OWASP Foundation. OWASP Top Ten 2021. 2021. URL: https://owasp.org/www-project-top-ten/

11. Positive Technologies. Web Application Security Report 2024. 2024. URL: https://www.ptsecurity.com/ww-en/analytics/web-application-security-statistics-2024/

12. Kaspersky. IoT Threat Landscape Report 2023. 2023. URL: https://www.kaspersky.com/about/press-releases/2023_kaspersky-iot-attacks-statistics

13. Egress. Phishing Threat Intelligence Report 2024. 2024. URL: https://www.egress.com/reports/phishing-threat-intelligence-report-2024

14. Verizon. Data Breach Investigations Report 2024. 2024. URL: https://www.verizon.com/business/resources/reports/dbir/

15. Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII від 05.10.2017. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

16. Національна стратегія кібербезпеки України : Указ Президента України № 447/2021 від 26.08.2021. Офіційний вісник Президента України. 2021. № 17. Ст. 1208.

17. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

18. Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. Wiley Publishing.

19. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674.

20. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability. Decision Support Systems, 51(3), 576-586.

21. Kindervag, J. (2010). No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. Forrester Research.

22. Bohara, A., Noureddine, M. A., Fawaz, A., & Sanders, W. H. (2017). An unsupervised multi-detector approach for identifying malicious lateral movement. Computers & Security, 70, 347-368.

23. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.

24. NIST. (2022). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST Special Publication 800-218.

25. Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1), 28-38.

ДОДАТОК А

Основні типи атак соціальної інженерії. Психологічні основи та методи впливу в соціальній інженерії. Вплив соціальної інженерії на інформаційну безпеку організацій.

Рисунок А.1. Класифікація основних типів атак соціальної інженерії

Продовження додатку А

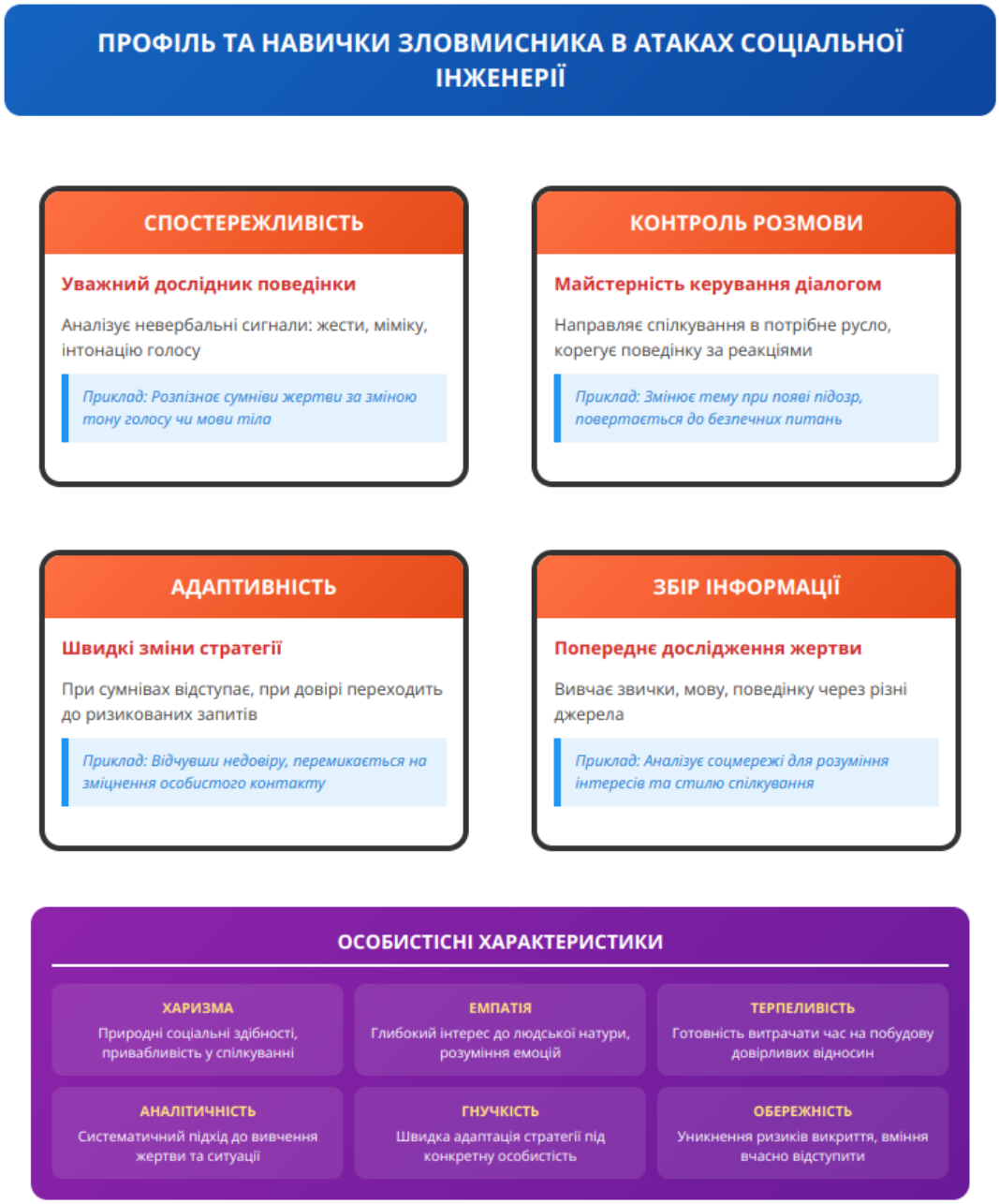

Рисунок А.2. Профіль та ключові навички зловмисників у атаках соціальної інженерії

Продовження додатку А

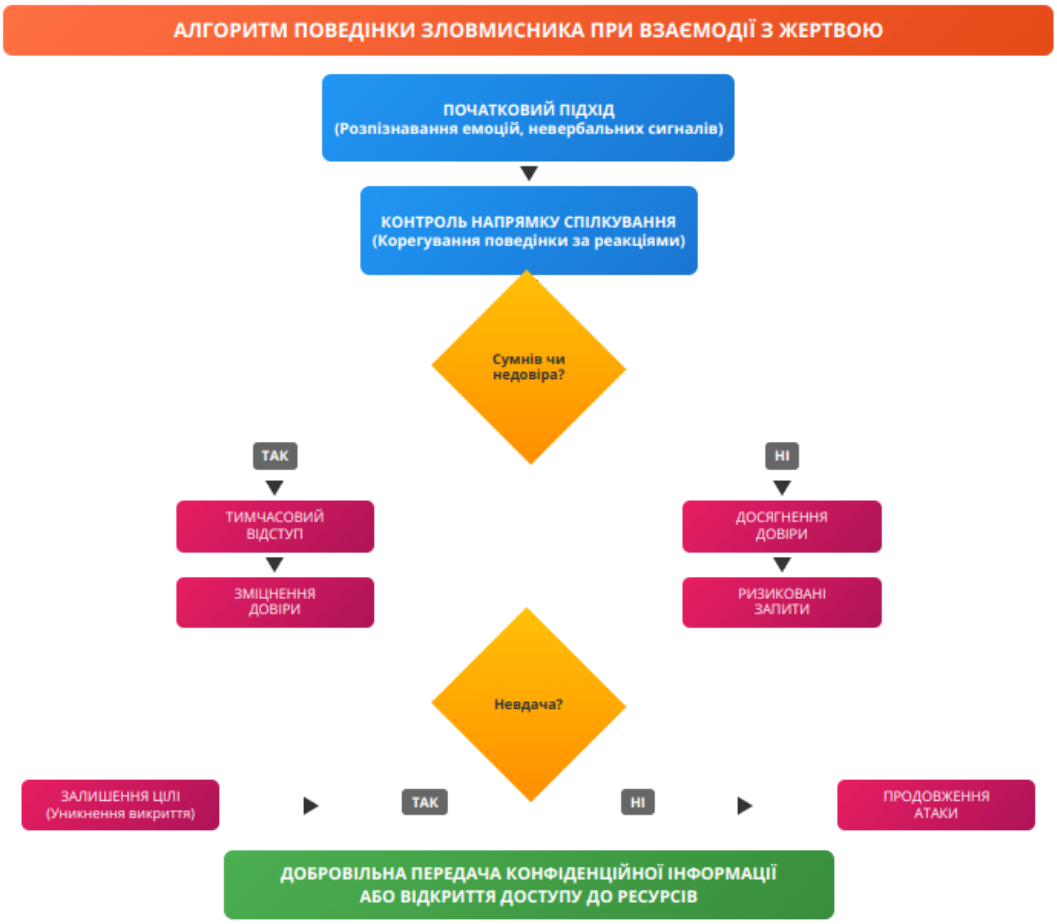

Рисунок А.3. Алгоритм поведінки зловмисника при взаємодії з жертвою

Продовження додатку А

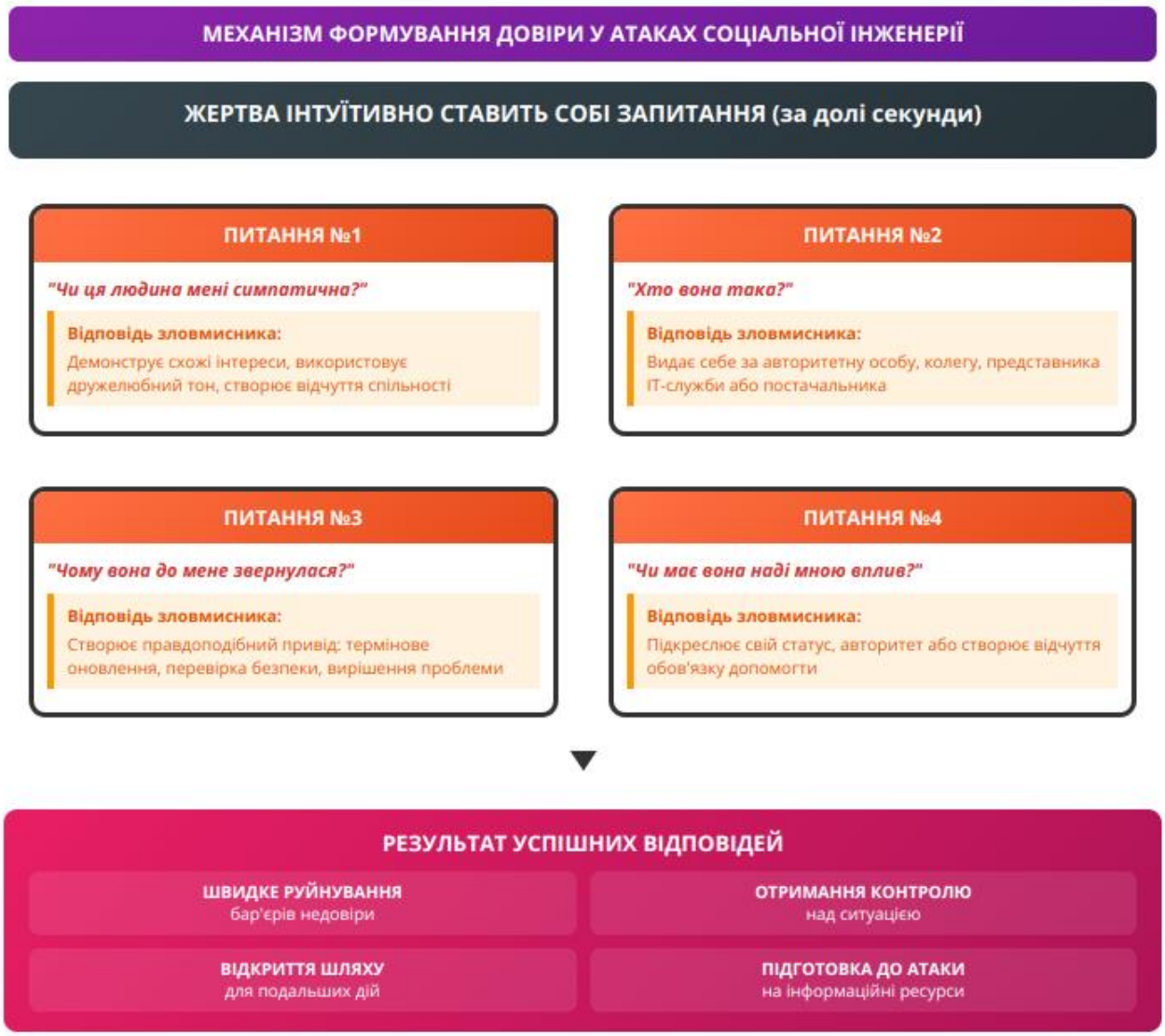

Рисунок А.4. Механізм формування довіри у атаках соціальної інженерії

Продовження додатку А

Таблиця А.1

Техніки створення психологічного тиску в соціальній інженерії

№	Приклад застосування	Зв'язок з принципами Чалдіні	Ключові індикатори	Контрзаходи
1	2	3	4	5
1	Штучна терміновість	Дефіцит + Авторитет	Фрази: "терміново", "негайно", "до кінця дня", жорсткі дедлайни	Правило "паузи" – завжди брати час на обдумування
2	Експлуатація упередження підтвердження	Послідовність + Соціальний доказ	Посилання на реальні події, знання внутрішньої інформації	Незалежна верифікація через альтернативні канали
3	Використання ефекту ореолу	Авторитет + Симпатія	Підкреслення компетентності, статусу, професійності	Розділення оцінки компетентності та довіри до запитів
4	Активація евристики доступності	Дефіцит + Авторитет	Згадування актуальних новин, відомих інцидентів	Перевірка статистичної реальності загроз

Продовження додатку А

Продовження табл. А.1

1	2	3	4	5
5	Створення хибного консенсусу	Соціальний доказ + Послідовність	Заяви про дії інших, посилання на "стандартні процедури"	Самостійна перевірка інформації у колег
6	Емоційне навантаження	Дефіцит + Взаємність	Емоційно забарвлені слова, загрозливий або заохочувальний тон	Техніки емоційної саморегуляції, "холодне" мислення
7	Поступова ескалація запитів	Послідовність + Взаємність	Логічна послідовність дій, кожне наступне прохання здається природним	Оцінка загальної картини, а не окремих запитів
8	Створення штучного дефіциту інформації	Дефіцит + Авторитет	Фрази про "конфіденційність", "обмежену інформацію"	Вимога повної інформації перед прийняттям рішень
9	Використання когнітивного навантаження	Авторитет + Послідовність	Надмірна складність, технічний жаргон, багато кроків	Спрощення та структурування отриманої інформації

Продовження додатку А

Продовження табл. А.1

1	2	3	4	5
10	Мімікрія довіреної особи	Авторитет + Симпатія	Посилання на знайомих осіб, використання внутрішньої термінології	Верифікація особи через незалежні канали зв'язку

Таблиця А.2

Поширеність атак соціальної інженерії у 2024-2025 роках

Показник	**Значення**	**Джерело**
Частка організацій, що зазнали фішингових атак	94%	Egress, 2024 [13]
Частка кібератак, що використовують соціальну інженерію	98%	SentinelOne, 2025 [6]
Середня кількість цільових фішингових атак на генерального директора	57 на рік	Barracuda [7]
Середня кількість атак на IT-персонал	40 на рік	Barracuda [7]
Час натискання на шкідливе посилання після відкриття листа	21 секунда	Verizon [14]
Час введення конфіденційних даних після переходу за посиланням	28 секунд	Verizon [14]

Продовження додатку А

Таблиця А.3

Економічні збитки від атак соціальної інженерії

Тип атаки	**Вартість у 2024 році**	**Джерело**	**Особливості**
Загальна вартість витоку даних	$4,88 млн	IBM Security 2024 [8]	Зростання на 10% від 2023 року
Скомпрометовані облікові дані	$4,81 млн	IBM Security 2024 [8]	Найдовший час виявлення (292 дні)
Атаки на охорону здоров'я	$10,1 млн	IBM Security 2024 [8]	Найвища вартість серед галузей
BEC-атаки (загальні збитки)	$2,77 млрд	FBI IC3 2024 [9]	21,442 випадки у 2024 році
Середня вартість одного BEC	$137,132	FBI IC3 2024 [9]	Зростання від $125,612 у 2023 році

ДОДАТОК Б

Структури існуючих моделей безпеки захисту користувачів інформаційної системи від атак соціальної інженерії

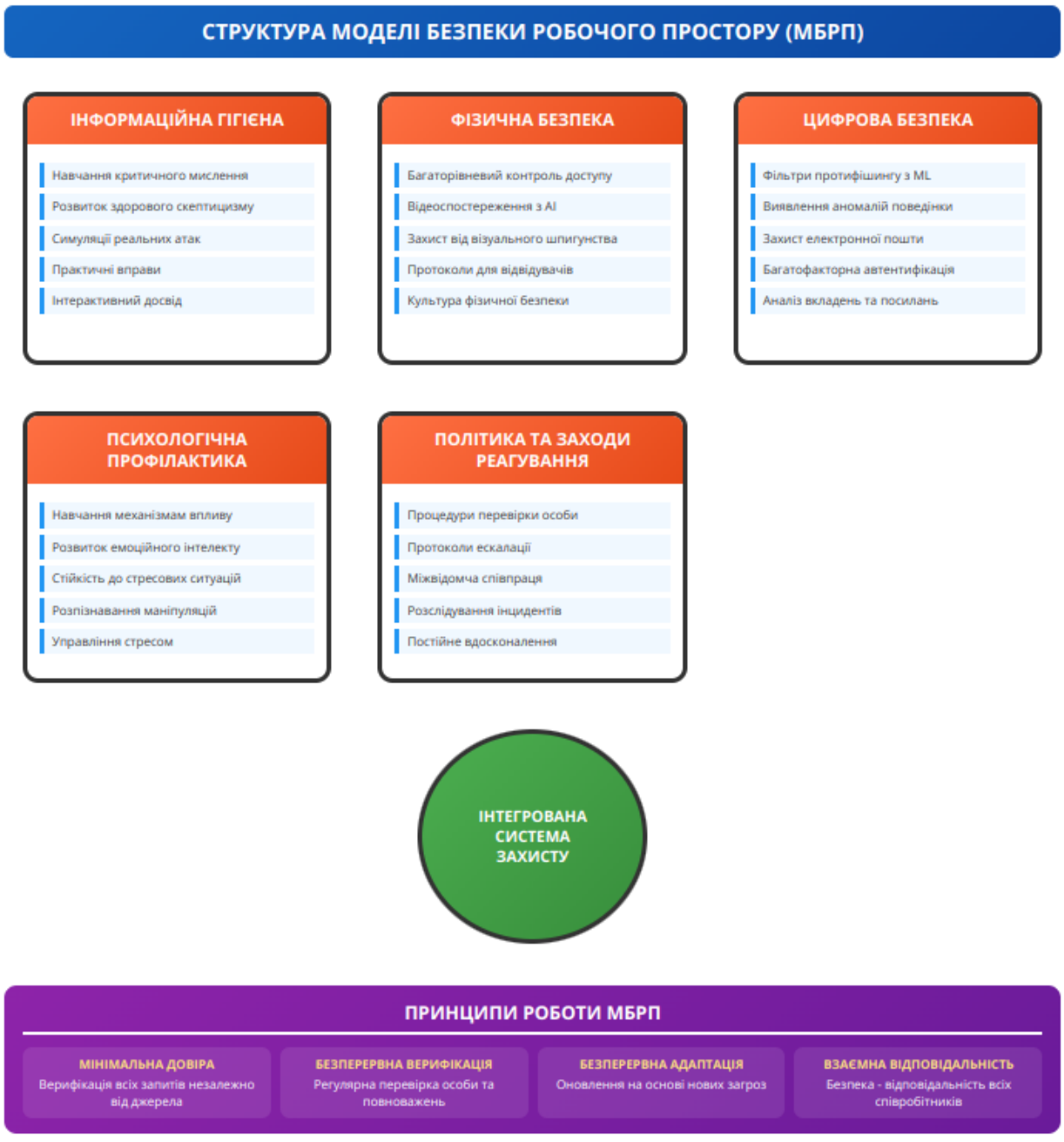

Рисунок Б.1. Структура моделі безпеки робочого простору (МБРП)

Продовження додатку Б

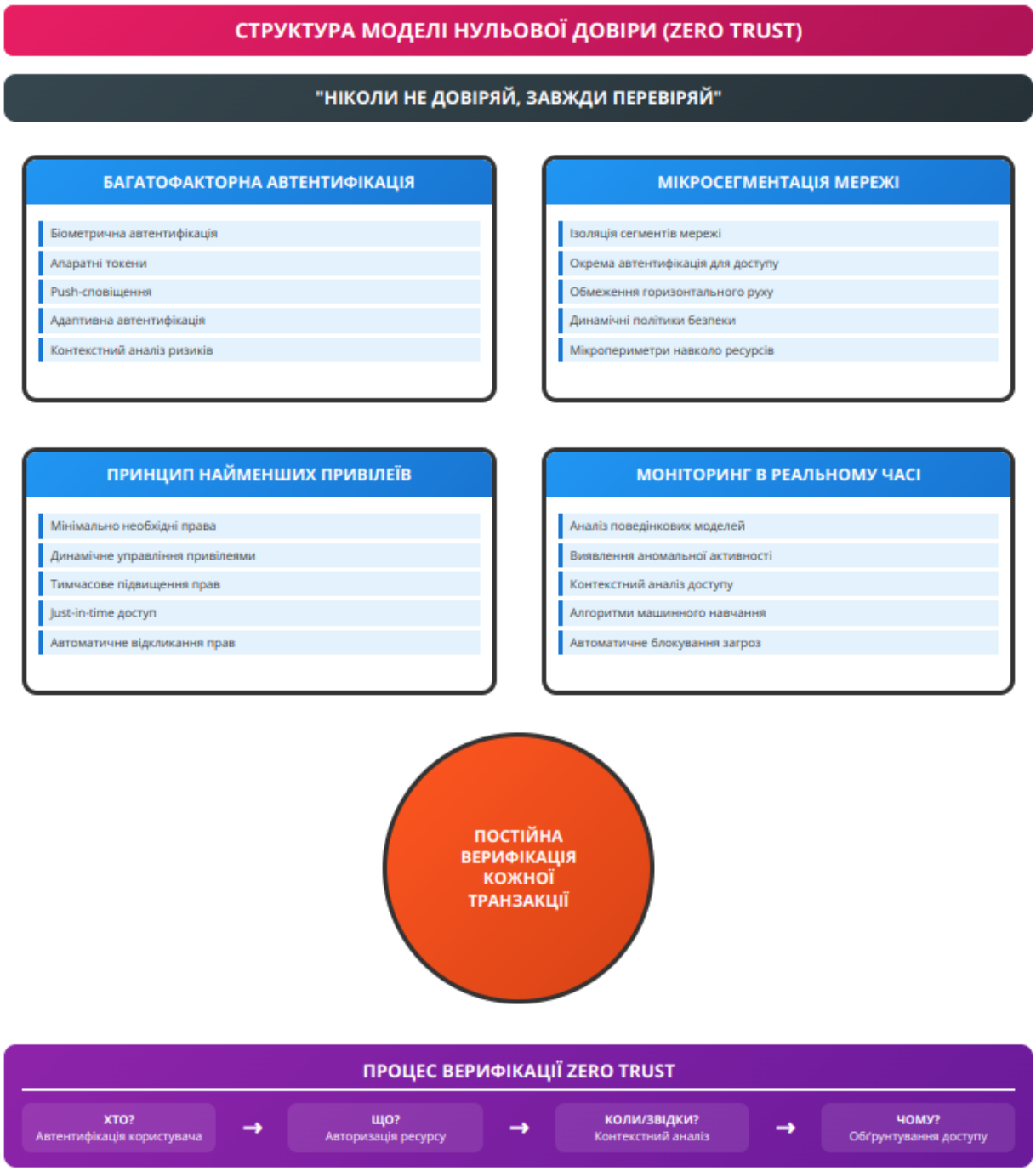

Рисунок Б.2. Структура моделі нульової довіри (Zero Trust)

Продовження додатку Б

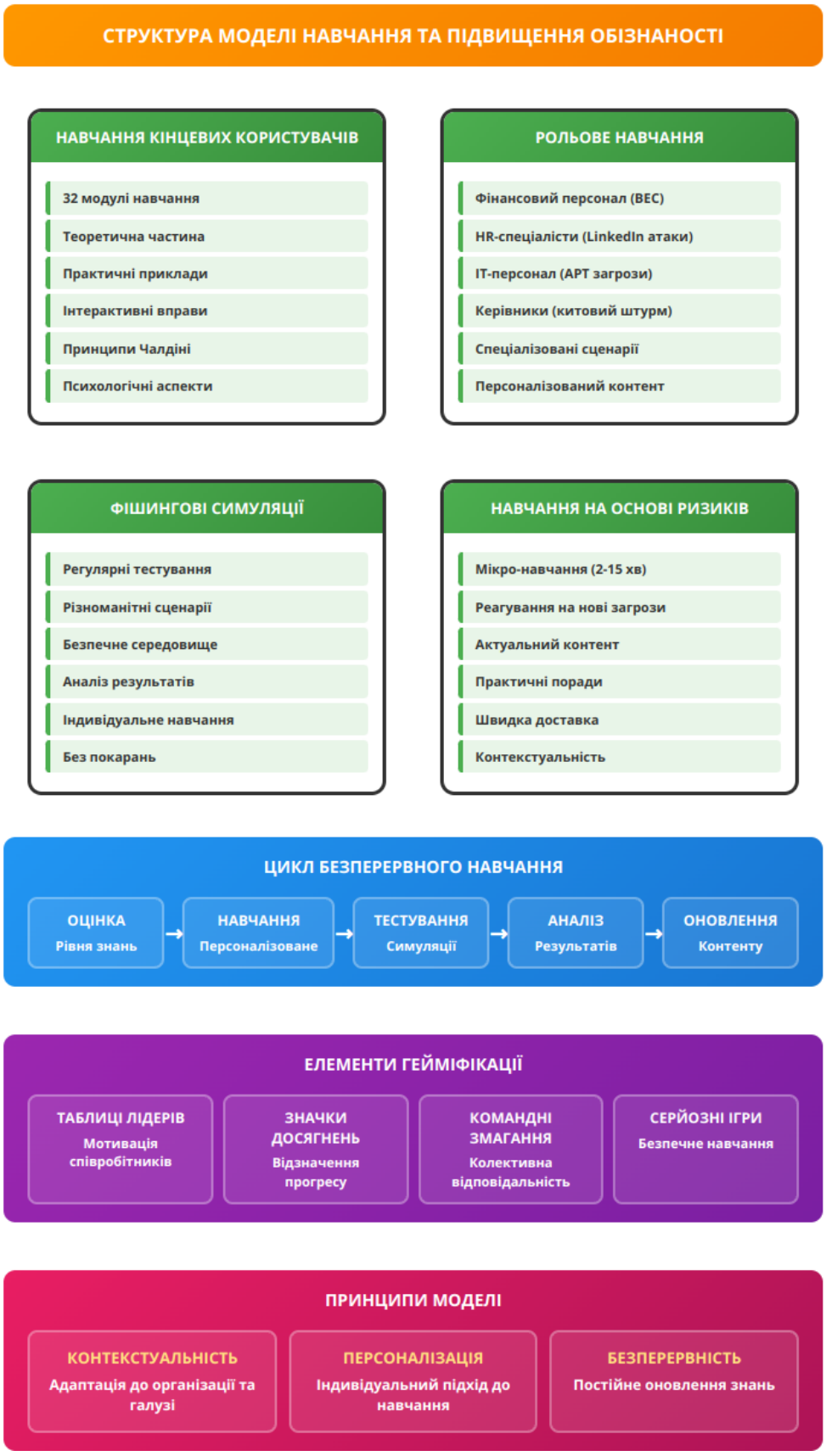

Рисунок Б.3. Структура моделі навчання та підвищення обізнаності

Продовження додатку Б

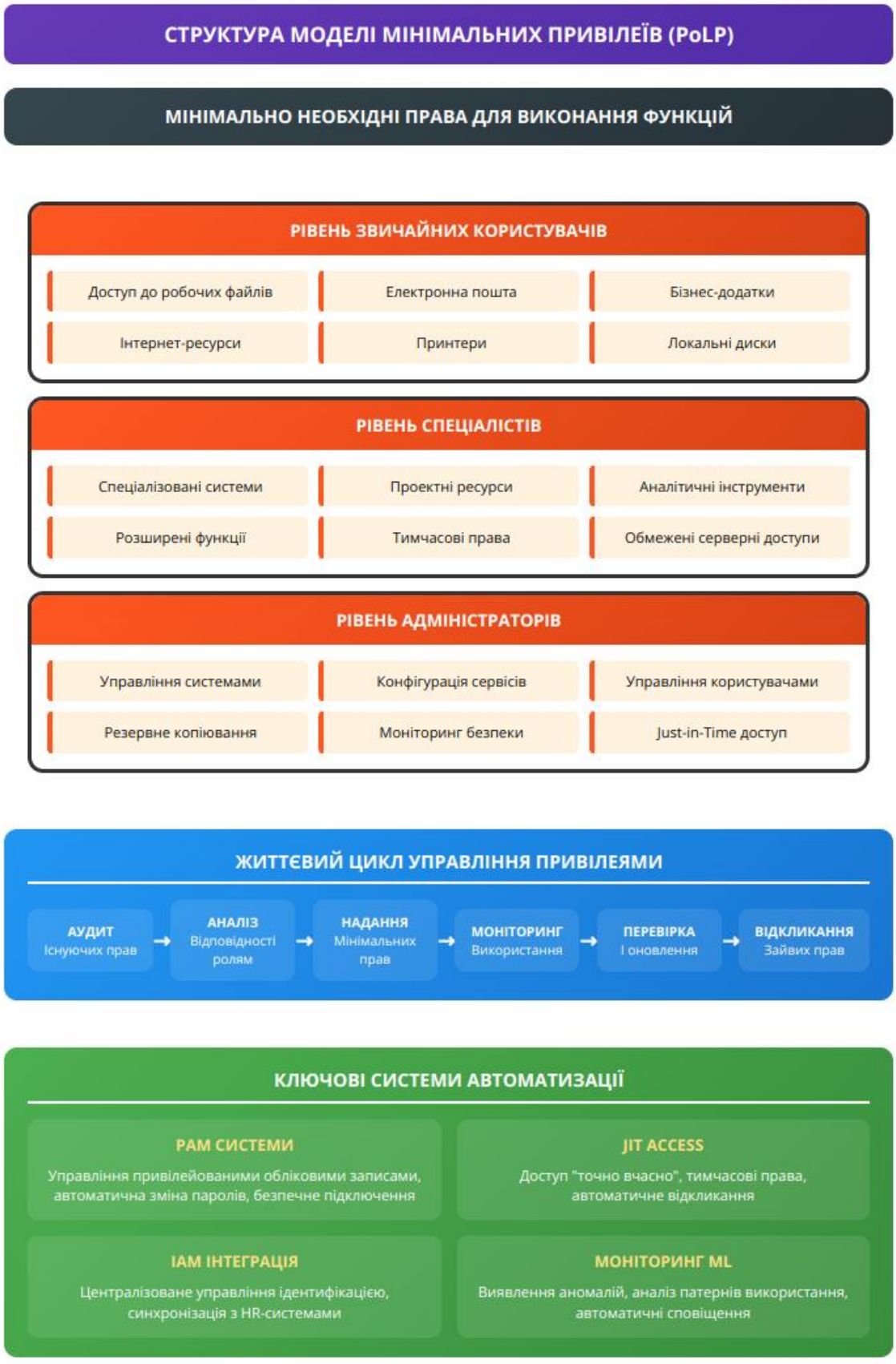

Рисунок Б.4. Структура моделі мінімальних привілеїв (PoLP)

Продовження додатку Б

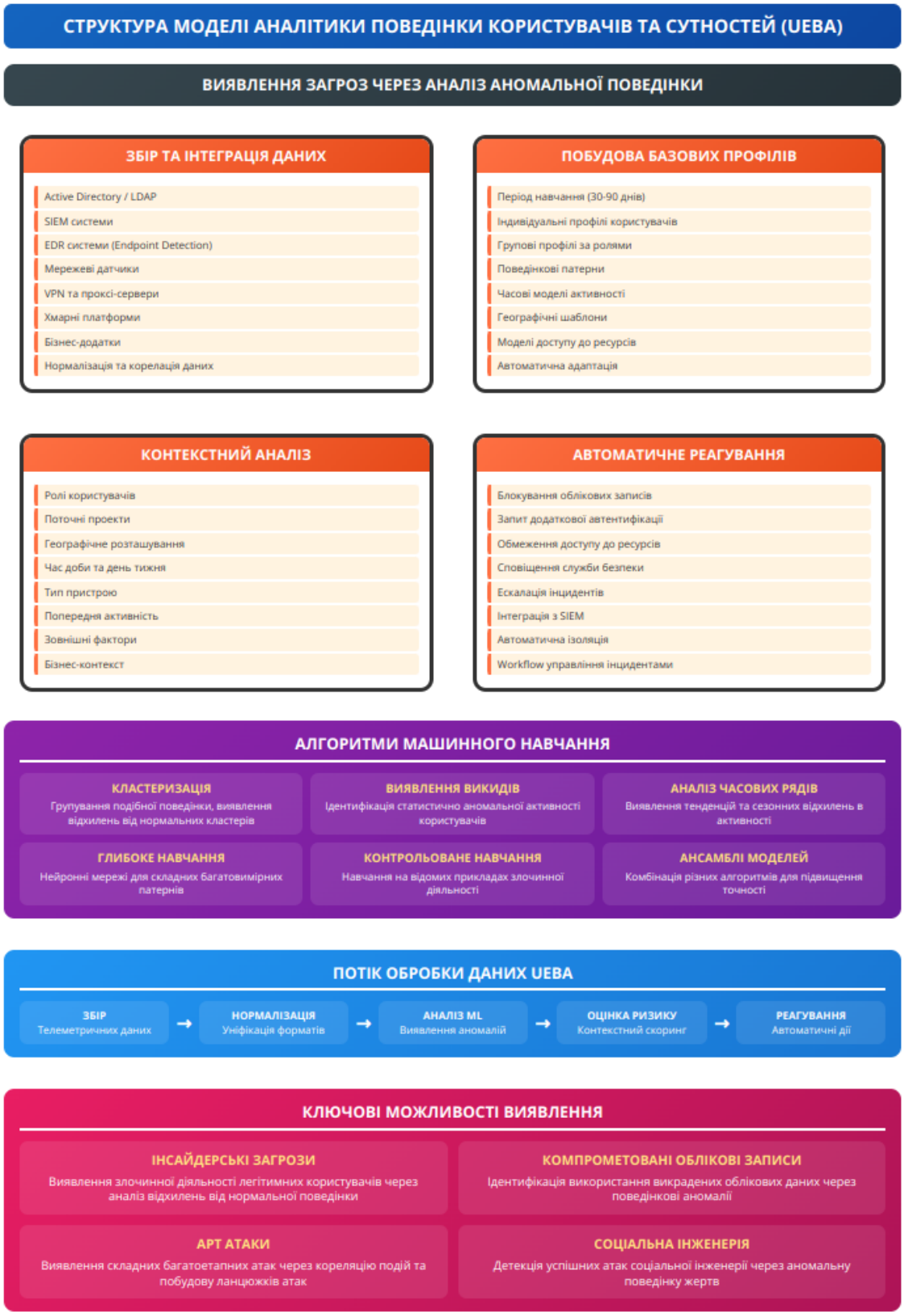

Рисунок Б.5. Структура моделі аналітики поведінки користувачів та сутностей (UEBA)

ДОДАТОК В

Структура та алгоритм впровадження механізму захисту користувачів інформаційної системи від атак соціальної інженерії

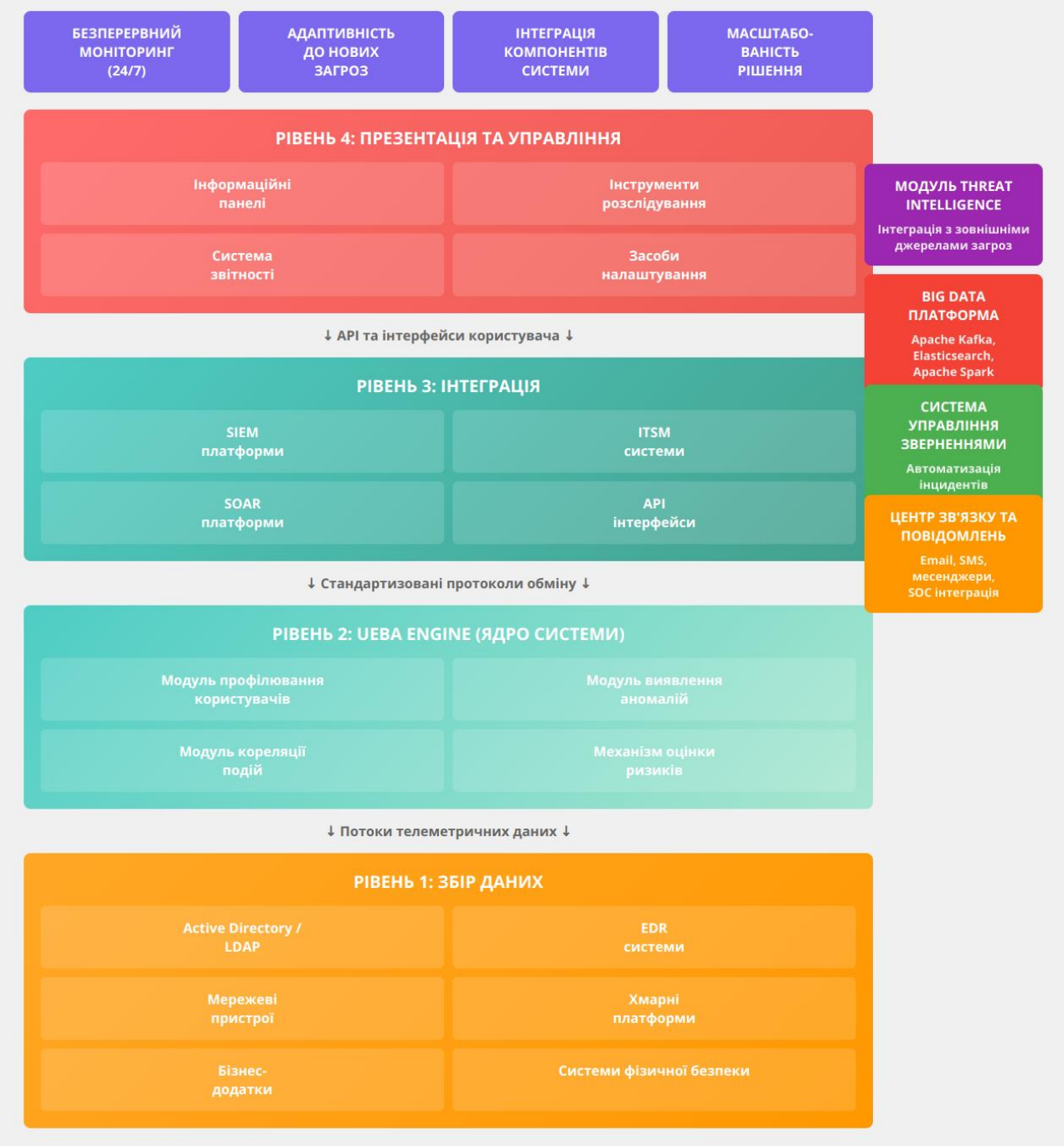

Рисунок В.1. Структура механізму захисту користувачів інформаційної системи від атак соціальної інженерії - Стрілки на рисунку показують напрямок потоків даних та взаємодії між компонентами системи. UEBA Engine це центральний елемент моделі UEBA, що забезпечує аналіз поведінки користувачів та виявлення загроз соціальної інженерії через машинне навчання та кореляцію подій.

Продовження додатку В

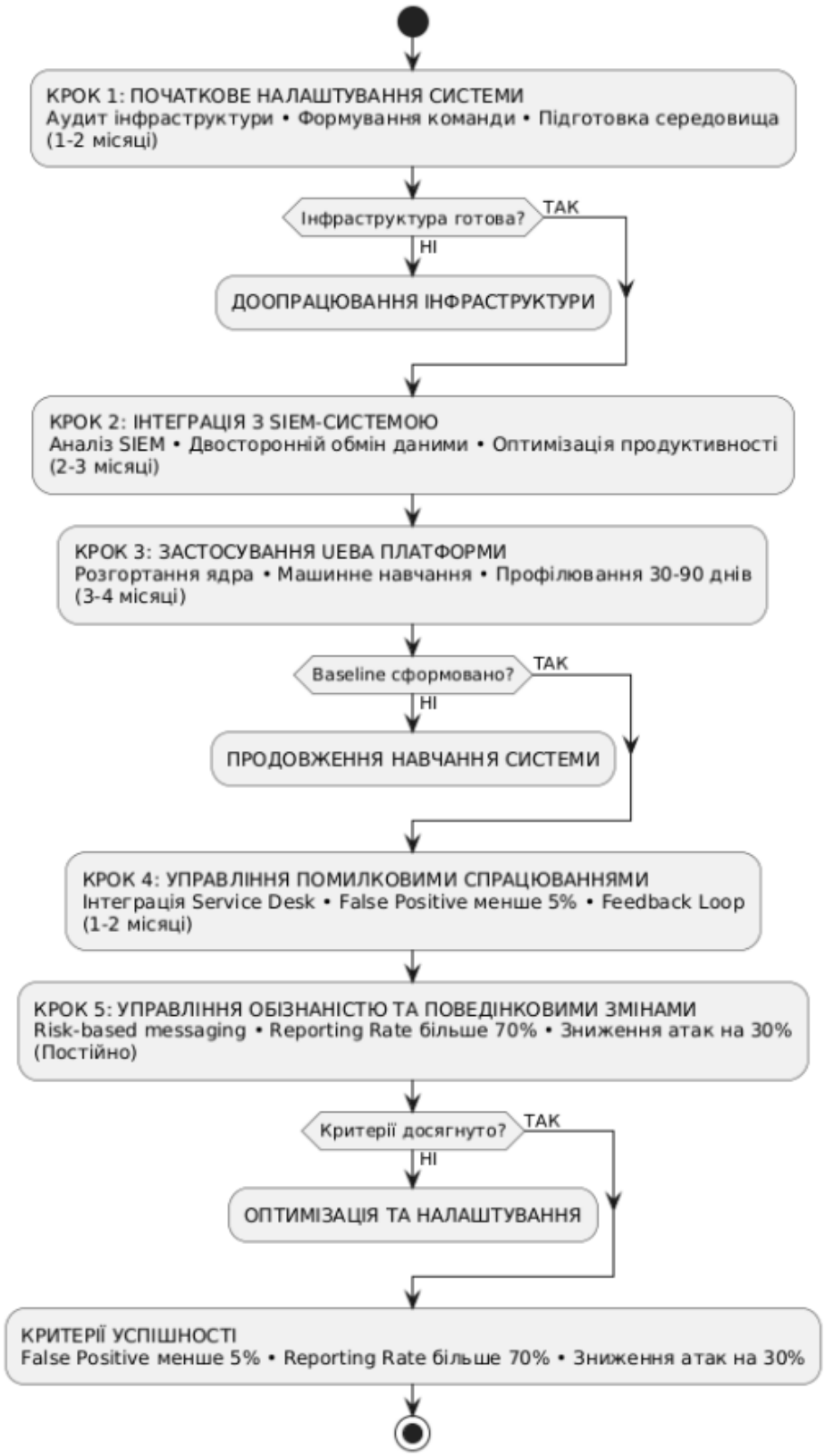

Рисунок В.2. Алгоритм впровадження механізму захисту користувачів інформаційної системи від атак соціальної інженерії