Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Кумпана Тімура Ігоровича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи протидії фішингу в корпоративній пошті*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Ткач М.О.			
розділів:				
спеціальний	доц. Ткач М.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Кумпану Т. І.*** **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методи протидії фішингу в корпоративній пошті***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.24 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання.	06.06.2024
Розділ 2	Аналіз методів протидії фішингу.	16.06.2024
Розділ 3	Обчислення витрати на впровадження рекомендацій, визначення економічної ефективності.	18.06.2024

Завдання видано _____ Максим Ткач
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Тімур Кумпан
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 62 с., 2 рис., 3 табл., 4 додатка, 26 джерел.

Об’єкт дослідження: корпоративні сервіси електронної пошти.

Мета роботи: розробити ефективні методи протидії фішингу в корпоративних поштових системах для забезпечення інформаційної безпеки підприємства.

Предмет розробки: аналіз, опис, порівняння.

У першому розділі проаналізовано актуальність теми, подано теоретичні відомості про архітектуру сервісів корпоративної пошти, розглянуто фішингові атаки та їх наслідки. Визначено задачі кваліфікаційної роботи та сформульовано висновки.

У спеціальному розділі наведено загальні відомості про методи протидії фішингу, проаналізовано існуючі комплексні рішення для захисту від фішингових атак. Також розроблено рекомендації щодо впровадження методів протидії фішингу в організації, враховуючи обрану архітектуру корпоративної пошти, та зроблено висновки щодо виконаної роботи.

В економічному розділі оцінено економічну доцільність запропонованих рекомендацій щодо впровадження методів протидії фішингу. Проведено розрахунки капітальних (фіксованих) витрат, поточних (експлуатаційних витрат), загального збитку від успішної фішингової атаки та загального ефекту від впровадження рекомендацій. На основі отриманих результатів сформульовано висновки.

Практична цінність розробки полягає у розробці рекомендацій щодо впровадження методів протидії фішингу у службах корпоративної пошти.

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ФІШИНГ, КОРПОРАТИВНА ПОШТА, ПРОТИДІЯ ФІШИНГУ.

ABSTRACT

Explanatory note: 62 pp., 2 pic., 3 table, 4 app, 26 sources.

Object of research: corporate e-mail services.

Purpose: to develop effective methods of counteracting phishing in corporate email systems to ensure information security of the enterprise.

Subject of development: analysis, description, comparison.

The first chapter analyzes the relevance of the topic, provides theoretical information about the architecture of corporate email services, and discusses phishing attacks and their consequences. The tasks of the qualification work are defined and conclusions are formulated.

The special section provides general information about methods of counteracting phishing, analyzes existing integrated solutions for protection against phishing attacks. Recommendations for the implementation of phishing prevention methods in an organization, taking into account the chosen corporate email architecture, are also developed, and conclusions are drawn on the work done.

The economic section assesses the economic feasibility of the proposed recommendations for the implementation of phishing countermeasures. We calculate the capital (fixed) costs, current (operating) costs, total damage from a successful phishing attack, and the overall effect of implementing the recommendations. Based on the results obtained, conclusions are formulated.

The practical value of the research lies in the development of recommendations for the implementation of phishing countermeasures in corporate email services.

INFORMATION SECURITY, CYBERSECURITY, PHISHING, CORPORATE MAIL, PHISING COUNTERACTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

MFA – Multi-factor Authentication

SPF – Sender Policy Framework

DKIM – DomainKeys Identified Mail

DMARC – Domain-based Message Authentication, Reporting & Conformance

SIEM – Security Information and Event Management

ШІ – штучний інтелект

ЗМІСТ

с.

ВСТУП

У сучасному діловому світі електронна пошта є основним засобом зв'язку, а шахрайські схеми становлять значний ризик для інформаційної безпеки та роботи в цілому. Важливість боротьби з фішингом полягає в кількох причинах. Спочатку частота таких атак щорічно зростає. Зловмисники використовують більш просунуту тактику, щоб обдурити окремих осіб і проникнути в конфіденційні дані, фінансові записи або взяти під контроль цілі системи. Звіти показують, що фішинг є однією з найпоширеніших кіберзагроз у всьому світі. Успішні фішингові атаки можуть серйозно вплинути на організації, наприклад фінансові збитки, витрати на відновлення системи, розкриття конфіденційних даних, шкода іміджу організації та потенційні юридичні наслідки. У середньому один інцидент фішингу може призвести до значних витрат, які досягають десятків тисяч доларів без урахування додаткових понесених збитків

Людський фактор також відіграє важливу роль. Незважаючи на розвиток технологій захисту, співробітники компаній часто стають жертвами фішингу через недостатню обізнаність або недбалість, що підкреслює необхідність постійної освіти і тренінгів для підвищення рівня кіберграмотності. Окрім цього, фішингові атаки стають дедалі витонченішими. Зловмисники використовують нові техніки соціальної інженерії, персоналізовані атаки, підроблені веб-сайти та інші методи для підвищення ефективності своїх атак. Це вимагає від організацій постійного вдосконалення своїх методів захисту та адаптації до нових загроз.

Багато країн впроваджують вимоги та стандарти щодо захисту персональних даних і конфіденційної інформації. Недотримання цих вимог може призвести до значних штрафів та юридичних проблем. Протидія фішингу є важливим аспектом відповідності цим стандартам. Додатково, пандемія COVID-19 значно збільшила кількість віддалених працівників, що створило нові виклики для захисту корпоративної інформації. Віддалені працівники часто використовують менш захищені мережі та пристрої, що робить їх більш вразливими до фішингових атак. Це підкреслює важливість впровадження ефективних методів протидії фішингу в умовах віддаленої роботи.

Враховуючи всі ці фактори, тема протидії фішингу в корпоративній пошті є надзвичайно актуальною і потребує детального дослідження та впровадження ефективних рішень для захисту інформаційних систем і збереження безпеки бізнесу.

Основною метою дослідження є впровадження методів протидії фішинговим атакам в корпоративній пошті, що забезпечить підвищення рівня кібербезпеки та захисту конфіденційної інформації в організаціях.

Об'єктом дослідження є корпоративна електронна пошта, яка використовується в організаціях для внутрішньої та зовнішньої комунікації. Корпоративна пошта є важливим елементом інформаційної інфраструктури компаній, оскільки через неї передається велика кількість конфіденційної інформації, фінансових даних та інших важливих документів.

Предметом дослідження є методи протидії фішинговим атакам на корпоративну електронну пошту. Це включає аналіз існуючих методів захисту, розробку нових стратегій, технологічних рішень та процедур для виявлення, запобігання та реагування на фішингові атаки.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Історія та розвиток фішингу

Перші фішингові атаки почали з'являтися у середині 1990-х років, коли інтернет почав набирати популярності, і зловмисники зрозуміли потенціал використання електронних листів для шахрайства.

Ранні фішингові атаки (1990-ті роки):

У 1996 році перші задокументовані фішингові атаки були спрямовані на користувачів AOL. Зловмисники надсилали повідомлення від імені служби підтримки AOL з проханням надати логін та пароль користувача. Ці атаки використовували прості методи соціальної інженерії та електронну пошту.

Початок використання електронної пошти: Хоча перші спроби були спрямовані на конкретні платформи, з часом електронна пошта стала основним інструментом фішинг-атак.

Еволюція фішингових атак

2000-ті роки:

З поширенням інтернету та електронної пошти фішингові атаки стали масовими. Зловмисники почали використовувати масові розсилки, щоб досягти більшої кількості потенційних жертв.

Фішинг на банківські дані: Атаки почали націлюватися на користувачів банківських сервісів, з метою отримання доступу до їх фінансових даних. Повідомлення містили посилання на підроблені веб-сайти банків.

Поява антивірусних програм: Реакція на фішингові атаки з боку індустрії кібербезпеки призвела до розробки антивірусних програм та фільтрів спаму.

2010-ті роки:

Основною метою фішингових атак стало отримання ідентифікаційних даних для доступу до різних онлайн-сервісів.

З поширенням соціальних мереж фішингові атаки почали націлюватися на користувачів таких платформ, як Facebook, LinkedIn та Twitter.

Зловмисники почали використовувати більш складні методи соціальної інженерії, персоналізовані атаки (спірфішинг) та атаки на конкретних осіб (whaling).

2020-ті роки та далі:

Зловмисники почали використовувати методи інтелектуального аналізу даних для створення дуже цільових атак на конкретних осіб або організації.

З розвитком мобільних технологій фішингові атаки почали націлюватися на користувачів смартфонів та планшетів через SMS (smishing) та мобільні додатки.

Фішингові атаки стали більш витонченими завдяки використанню штучного інтелекту та машинного навчання для автоматизації та підвищення ефективності атак.

Пандемія COVID-19 сприяла збільшенню фішингових атак, пов'язаних із темами, віддаленою роботою та державними програмами допомоги.

Рис.1 - Хронологія розвитку фішингу

1.2 Класифікація фішингових атак

Фішингові атаки можна класифікувати за різними критеріями, включаючи методи, цілі, канали розповсюдження та ступінь персоналізації. Ось основні типи фішингових атак та їх особливості:

1. Масовий фішинг - це форма кібератаки, що націлена на велику аудиторію без специфічного вибору цілей. Зловмисники надсилають величезну кількість електронних листів з підробленими повідомленнями, сподіваючись, що частка одержувачів впаде в пастку. Ці атаки використовують загальні теми, такі як обіцянки виграшів у лотерею, фальшиві банківські проблеми або пропозиції на безкоштовні подарунки, щоб залучити увагу і викликати реакцію у потенційних жертв.
2. Спірфішинг цілеспрямована форма фішингової атаки, яка націлена на конкретних осіб або організації. У цьому типі атаки зловмисники збирають інформацію про своїх цільових жертв, щоб персоналізувати і зробити свої підроблені повідомлення більш переконливими. Вони можуть використовувати реальні імена, посади та інші особисті дані, щоб створити враження легітимності та змусити жертву відкрити шкідливий вміст або надати конфіденційну інформацію.
3. Вейлінг є специфічним видом спірфішингу, спрямованим на високопосадовців, таких як генеральні директори, фінансові директори та інші керівники компаній. Цей тип атаки використовує деталізовану інформацію про діяльність організації та особисту інформацію про її керівників, щоб створювати вельми переконливі повідомлення. Зловмисники можуть використовувати підроблені інвойси, запити на переказ коштів або інші фінансові маніпуляції, сподіваючись викликати реакцію керівництва компанії та отримати доступ до цінної інформації чи фінансових ресурсів.
4. Смішинг - це форма фішингових атак, які здійснюються через SMS або інші текстові повідомлення. Зловмисники відправляють користувачам

текстові повідомлення з посиланнями на підроблені веб-сайти або шкідливі додатки, сподіваючись, що отримувачі перейдуть за посиланням або завантажать додаток, який може використовуватися для крадіжки особистої інформації або фінансових даних. Часто такі атаки стосуються тем, пов'язаних з банківськими послугами, кур'єрськими доставками або обіцянками виграшів в конкурсах, що дозволяє зловмисникам залучати увагу та зловживати довірою користувачів.

5. Вішинг - це форма фішингових атак, які здійснюються через телефонні дзвінки. Зловмисники телефонують жертвам, вигадуючи себе представниками банків, урядових установ або інших довірених організацій, з метою отримання конфіденційної інформації. Вони використовують соціальну інженерію, щоб переконати свою жертву надати особисті або фінансові дані, в той час як вони насправді намагаються здійснити шахрайські дії. Такі атаки важко виявити, оскільки зловмисники часто використовують переконливі та маніпулятивні методи, щоб отримати доступ до цінної інформації своїх жертв.
6. Клон-фішинг - це форма атаки, яка використовує підроблені копії легітимних електронних листів для маніпуляції жертвами. Зловмисники копіюють реальні листи, внесують зміни, наприклад, вставляють шкідливі посилання або вкладення, та відправляють їх від імені правильних відправників. Ця стратегія спрямована на те, щоб збудити довіру у жертв та викликати їхню реакцію, враховуючи, що листи виглядають як звичайна легітимна кореспонденція.
7. Фармінг - це форма фішингових атак, що спрямована на перенаправлення користувачів на підроблені веб-сайти, навіть якщо вони вводять правильні URL-адреси у веб-браузері. Зловмисники використовують різні методи, такі як зміна налаштувань DNS або зараження комп'ютерів шкідливими програмами, щоб перенаправити трафік на свої шахрайські веб-ресурси. Жертви можуть навіть не підозрювати про атаку, оскільки вони вважають,

що вони потрапляють на правильний сайт за введеним URL, в той час як фактично їхні дані можуть бути зловживані зловмисниками.

8. Людина посередині (Man-in-the-Middle, MITM) - це атака, при якій зловмисник перехоплює і змінює комунікацію між двома сторонами, не дозволяючи їм знати про це. Зловмисники використовують вразливості у мережевих з'єднаннях, щоб отримувати доступ до передачі даних і змінювати їх в своїй користь. Ця техніка може бути використана для перехоплення логінів, паролів та іншої конфіденційної інформації, що пересилається між користувачами і серверами.
9. Спуфінг - це метод обману, коли зловмисники підробляють ідентифікаційні дані або параметри комунікації, маскуючи справжню ідентичність або джерело даних. Ця техніка дозволяє їм обхідно заходів безпеки, таких як багатофакторна автентифікація, SPF, DKIM і DMARC, що призначені для захисту від фальсифікації.

Таблиця 1.1 – Класифікація фішингових атак

Типи фішингових атак	Опис	Методи	Особливості
Масовий фішинг	Спрямовані на велику кількість користувачів без конкретного націлення	Надсилання тисячі електронних листів із підробленими повідомленнями	Використовують повідомлення з відомими темами, такими як виграш в лотереї, банківські проблеми
Спірфішинг	Спрямований на конкретних осіб або організації	Використання інформацію про ціль, щоб зробити повідомлення більш переконливими	Використовують реальних імен, посад та іншої інформації, щоб створити враження легітимності

Вейлінг	Є підтипом спірфішингу, але націлений на високопосадовців	Використання детальної інформації про компанії та її керівників	Атаки включають запити на переказ коштів або інші фінансові операції
Смішинг	Фішингові атаки, які здійснюються через SMS	Надсилання текстових повідомлень із посиланнями на підроблені веб-сайти	Використовуються теми, пов'язані з банківськими послугами, виграшами
Вішинг	Фішингові атаки, що здійснюються через телефонні дзвінки	Дзвонять жертвам, видаючи себе за представників легітимних організацій	Використання соціальної інженерії для переконання жертви надати особисті дані
Клон-фішинг	Атаки, які використовують підроблені копії легітимних електронних листів	Зловмисники копіюють справжні електронні листи	Жертви можуть легко довірити таким листам
Фармінг	Фішингові атаки, спрямовані на перенаправлення користувачів на підроблені веб-сайти навіть при введенні правильних URL-адрес	Зловмисники змінюють налаштування DNS або заражають комп'ютери шкідливими програмами	Жертви не підозрюють про атаку, оскільки вони вводять правильні адреси у веб-браузерах
MITM	Атаки, при яких зловмисник перехоплює та змінює комунікацію між двома сторонами	Використання вразливостей у мережевих з'єднаннях для перехоплення даних	Може використовуватись для збору логінів, паролів та іншої конфіденційної інформації
Спуфінг	Техніка обману, коли зловмисники підроблюють ідентифікаційні дані чи параметри комунікації	Маскування справжньої ідентичності або джерела даних	Обман захисту систем безпеки, таких як багатофакторна автентифікація, SPF, DKIM і DMARC

1.3 Огляд методів протидії фішингу

Протидія фішинговим атакам вимагає комплексного підходу, що включає технологічні рішення, освітні заходи та організаційні політики. Одним із основних технологічних рішень є антифішингові фільтри, які аналізують вхідні електронні листи для виявлення ознак фішингу. Ці фільтри використовують методи аналізу ключових слів, заголовків та перевірки автентичності відправників, що дозволяє автоматизувати процес і забезпечити високу швидкість обробки. Проте можливі помилкові спрацьовування або пропуски нових видів атак.

Системи виявлення загроз на основі машинного навчання використовують алгоритми для аналізу та виявлення фішингових атак шляхом аналізу поведінкових моделей, виявлення аномалій та класифікації листів. Вони мають високу точність і здатність адаптуватися до нових загроз, але потребують значних ресурсів та регулярного навчання моделей. Багатофакторна автентифікація (MFA) значно підвищує безпеку навіть при компрометації пароля, використовуючи комбінацію паролів, токенів, біометрії та SMS-кодів, хоча може створювати незручності для користувачів.

Протокол DMARC підвищує надійність автентифікації відправників електронних листів, зменшуючи ймовірність успішного фішингу за рахунок перевірки SPF котрий являється частиною DMARC, яка дозволяє визначити, з яких серверів може надходити електронна пошта від певного домену, та DKIM котрий являє собою механізм дозволяє підписувати електронні листи цифровим підписом, що підтверджує їхнє походження від певного домену. Однак, налаштування та підтримка DMARC можуть бути складними. Безпечні шлюзи електронної пошти (Secure Email Gateways, SEG) фільтрують вхідні та вихідні електронні листи для виявлення загроз шляхом сканування вкладень, перевірки посилань та аналізу вмісту, забезпечуючи комплексний захист, але вимагають високих витрат на впровадження та підтримку.

Освітні заходи включають регулярне навчання та тренінги для співробітників, що підвищують їхню обізнаність про фішинг через онлайн-курси, семінари, інтерактивні тренінги та симуляції фішингових атак. Це допомагає співробітникам краще розпізнавати фішингові атаки, але вимагає постійного оновлення знань та повторних тренінгів. Формування культури кібербезпеки в організації сприяє підвищенню уваги до безпеки на всіх рівнях через політики безпеки, підтримку керівництва та регулярні інформаційні кампанії. Цей процес є тривалим і потребує постійної підтримки.

Організаційні політики включають впровадження чітких політик безпеки та процедур реагування на інциденти, створення інструкцій та процедур реагування, регулярні перевірки та аудит. Це забезпечує підготовленість до інцидентів і зменшення часу реагування, але потребує постійного оновлення та підтримки політик. Сегментація мережі, що передбачає розділення мережі на сегменти для зменшення ризиків розповсюдження атак, використовує віртуальні локальні мережі (VLAN) та ізоляцію критичних систем, зменшуючи можливості для зловмисників переміщатися мережею, але налаштування та управління цим процесом є складними.

Таким чином, протидія фішинговим атакам вимагає багатогранного підходу, що включає технологічні рішення, освітні заходи та організаційні політики, які доповнюють одне одного для забезпечення високого рівня захисту від фішингових загроз.

Нижче наведено огляд основних методів і стратегій, які використовуються сьогодні:

1. Технологічні рішення

- Антифішингові фільтри аналізують вхідні електронні листи для виявлення ознак фішингу, використовуючи ключові слова, аналіз заголовків та перевірку автентичності відправників. Цей автоматизований процес

забезпечує високу швидкість обробки, але може допускати помилкові спрацьовування або пропуски нових видів атак.

- Системи виявлення загроз на основі машинного навчання використовують алгоритми для аналізу та виявлення фішингових атак, а також аналізують поведінкові моделі, виявляють аномалії та класифікують листи. Ці системи відзначаються високою точністю та здатністю адаптуватися до нових загроз, але вимагають значних ресурсів та регулярного навчання моделей.
- Багатофакторна автентифікація (MFA) забезпечує додаткові методи перевірки користувача, такі як комбінація паролів, токенів, біометрії та SMS-кодів. Цей підхід значно підвищує безпеку навіть при компрометації пароля, але може створювати незручності для користувачів.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) є протоколом автентифікації електронної пошти, що дозволяє визначати політику обробки повідомлень, які не проходять перевірку SPF та DKIM. Він підвищує надійність автентифікації відправників та зменшує ймовірність успішного фішингу, але потребує складності налаштування та підтримки.
- Безпечні шлюзи електронної пошти (Secure Email Gateways, SEG) фільтрують вхідні та вихідні листи для виявлення загроз шляхом сканування вкладень, перевірки посилань та аналізу вмісту. Вони забезпечують комплексний захист від різних типів загроз.

2. Освітні заходи

- Навчання та тренінги для співробітників з фішингу включають регулярні навчальні сесії, такі як онлайн-курси, семінари, інтерактивні тренінги та симуляції фішингових атак. Ці заходи сприяють підвищенню обізнаності та здатності розпізнавати фішингові атаки, але потребують постійного оновлення знань і проведення повторних тренінгів.

- Культура кібербезпеки включає формування у організації уваги до безпеки на всіх рівнях за допомогою політик безпеки, підтримки керівництва, регулярних нагадувань та інформаційних кампаній. Це сприяє створенню свідомого ставлення до кібербезпеки серед співробітників, але є тривалим процесом впровадження та підтримки культури безпеки.

3. Організаційні політики

- Політики безпеки та процедури реагування включають впровадження чітких інструкцій і процедур для реагування на інциденти, а також регулярні перевірки та аудит. Це сприяє підготовленості до інцидентів і зменшенню часу реагування, але потребує постійного оновлення та підтримки політик.
- Сегментація мережі передбачає розділення мережі на сегменти за допомогою віртуальних локальних мереж (VLAN) та ізоляції критичних систем. Це дозволяє зменшити ризики розповсюдження атак і зменшити можливості для зловмисників переміщатися мережею, але вимагає складності налаштування та управління.

1.4 Статистика фішингових атак

Аналіз статистичних даних щодо фішингових атак у корпоративному середовищі дозволяє зрозуміти масштаби проблеми, виявити тенденції та визначити найбільш уразливі сфери. Ось огляд останніх статистичних даних про фішингові атаки:

1. Загальна кількість фішингових атак

Згідно з дослідженнями, кількість фішингових атак постійно зростає. За даними компанії Proofpoint, у 2023 році кількість фішингових атак зросла на 22% у порівнянні з попереднім роком.

Звіт Phishing Activity Trends Report, опублікований Anti-Phishing Working Group (APWG), показує, що у середньому реєструється понад 200 000 фішингових атак щомісяця.

2. Уразливість корпоративних середовищ

Згідно з даними Verizon Data Breach Investigations Report (DBIR) за 2023 рік, понад 80% організацій зазнали хоча б однієї фішингової атаки за рік.

Звіт показує, що близько 30% фішингових листів відкриваються користувачами, з яких 12% переходять за посиланнями або відкривають вкладення.

3. Спірфішинг та Вейлінг

Спірфішинг та вейлінг складають значну частину фішингових атак у корпоративному середовищі. Згідно з дослідженням SANS Institute, близько 65% організацій повідомляють про атаки, спрямовані на конкретних співробітників.

Згідно з FBI's Internet Crime Complaint Center (IC3), збитки від вейлінг-атак у 2022 році склали понад $1,8 млрд.

4. Бізнес електронна пошта компрометація (BEC)

BEC-атаки є одними з найбільш дорогих. За даними IC3, загальні втрати від BEC-атак у 2022 році перевищили $2,4 млрд.

Згідно з дослідженням, близько 75% компаній зі списку Fortune 500 повідомили про принаймні одну спробу BEC-атаки протягом останнього року.

5. Роль людського фактору

Згідно з дослідженням IBM, 95% всіх кіберінцидентів, включаючи фішингові атаки, стали можливими через людські помилки.

Звіт KnowBe4 за 2023 рік показав, що після проведення тренінгів з кібербезпеки кількість співробітників, що піддаються фішинговим атакам, зменшилась на 70%.

6. Використання мобільних пристроїв

За даними у 2023 році кількість смішинг-атак зросла на 35%. Близько 30% співробітників повідомили про отримання підозрілих SMS.

Дослідження показують, що більше 60% фішингових атак націлені на мобільні пристрої, оскільки користувачі менш обережні при взаємодії з мобільними додатками та повідомленнями.

1.5 Висновки

Фішинг є однією з найбільших сучасних кіберзагроз, що постійно розвивається та удосконалюється. Зародившись наприкінці 1990-х років, фішинг пройшов шлях від примітивних атак до складних схем із використанням соціальної інженерії.

Фішингові атаки класифікуються за способом доставки (електронна пошта, смс, соціальні мережі), метою (крадіжка даних, фінансові шахрайства) та цільовою аудиторією (індивідуальні користувачі, корпорації). Це допомагає краще зрозуміти та визначити загрозу.

Сучасні методи протидії включають багатофакторну аутентифікацію, антивірусні програми, фільтрацію фішингових листів та навчання користувачів розпізнавати атаки. Технології машинного навчання також активно використовуються для виявлення фішингових спроб.

Корпоративна пошта є однією з основних мішеней через високу цінність корпоративної інформації. Загрози можуть включати викрадення облікових даних, розсилання шкідливих вкладень та доступ до конфіденційної інформації компанії.

Статистика показує зростання кількості фішингових атак останніми роками, що підкреслює важливість оновлення методів захисту та підвищення обізнаності працівників.

Для боротьби з фішингом потрібен багаторівневий підхід, що включає технічні заходи та постійне навчання користувачів. Важливо використовувати передові технології безпеки, моніторити підозрілу активність та впроваджувати політики безпеки на рівні організації.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Вразливості корпоративної пошти

Корпоративні системи електронної пошти є однією з основних цілей фішингових атак через їхню важливість для бізнесу та великий обсяг інформації, що передається через них. Виявлення та аналіз слабких місць у цих системах є критично важливим для запобігання фішинговим атакам. Ось основні вразливості корпоративної пошти:

1. Недостатній захист облікових записів

Використання слабких або повторно використаних паролів збільшує ризик компрометації облікових записів. Зловмисники можуть легко зламати такі паролі за допомогою атаки "brute force" або використання вкрадених паролів з інших джерел.

Відсутність багатофакторної автентифікації (MFA): Відсутність MFA значно полегшує доступ до облікових записів навіть при компрометації пароля. MFA додає додатковий рівень захисту, що значно ускладнює зловмисникам доступ до облікових записів.

2. Недоліки у налаштуваннях електронної пошти

Відсутність або неправильна конфігурація SPF, DKIM і DMARC, ці протоколи використовуються для перевірки автентичності відправників електронної пошти та запобігання спуфінгу. Відсутність або неправильна конфігурація цих протоколів дозволяє зловмисникам підробляти адреси відправників і надсилати фішингові листи від імені легітимних доменів.

Неефективні або недостатньо налаштовані фільтри спаму можуть пропускати фішингові листи у вхідні скриньки користувачів, що підвищує ризик успішних атак.

3. Людський фактор

Співробітники, які не пройшли навчання з кібербезпеки, частіше стають жертвами фішингових атак. Вони можуть не розпізнати ознаки фішингових листів або ненавмисно розкрити конфіденційну інформацію.

Зловмисники використовують методи соціальної інженерії для маніпуляції співробітниками, щоб змусити їх розкрити конфіденційну інформацію або виконати шкідливі дії.

4. Технічні вразливості

Вразливості у програмному забезпеченні поштових серверів: Використання застарілого або незахищеного програмного забезпечення поштових серверів може дозволити зловмисникам здійснювати атаки на сервери, отримувати доступ до електронної пошти або навіть повністю компрометувати систему.

Неправильне налаштування безпеки серверів і клієнтів електронної пошти може створювати можливості для зловмисників здійснювати атаки, такі як "man-in-the-middle" або перехоплення трафіку.

5. Відсутність моніторингу та реагування

Відсутність постійного моніторингу активності поштових серверів та облікових записів може призвести до того, що фішингові атаки залишаться непоміченими до моменту, коли завдано значних збитків.

Відсутність чітких процедур реагування на фішингові атаки може призвести до затримок у виявленні та зупиненні атак, що збільшує ризик компрометації даних.

Таблиця 2.1 – Основні вразливості та їх причини

Основна вразливість	Причина
Недостатній захист облікових записів	Слабкі паролі; Відсутність багатофакторної автентифікації
Недоліки у налаштуваннях електронної пошти	Відсутність або неправильна конфігурація SPF, DKIM і DMARC; Недостатній фільтр спаму
Людський фактор	Недостатня обізнаність співробітників; Соціальна інженерія
Технічні вразливості	Вразливості у програмному забезпеченні поштових серверів; Недоліки у налаштуваннях безпеки
Відсутність моніторингу та реагування	Недостатній моніторинг; Відсутність плану реагування

2.2 Методи протидії фішингу в корпоративній пошті

Методи протидії фішингу в корпоративній пошті включають впровадження технологій фільтрації спаму та антивірусного захисту, навчання співробітників розпізнавати підозрілі листи та виконання регулярних симуляцій фішингових атак для підвищення обізнаності і готовності до потенційних загроз.

2.2.1 Програми навчання та підвищення обізнаності співробітників

Освітні заходи є критичним елементом у боротьбі з фішинговими атаками. Вони допомагають підвищити обізнаність співробітників про загрози та розвивають навички розпізнавання фішингових спроб. Ось основні компоненти програм навчання та підвищення обізнаності співробітників:

1. Початкове навчання нових співробітників: Проведення навчання з кібербезпеки під час введення нових співробітників у роботу включає основи кібербезпеки, розпізнавання фішингових листів та правила безпечного використання електронної пошти та інтернету через вебінари, інтерактивні тренінги та відеоуроки.
2. Регулярні тренінги та оновлення знань: Постійне оновлення знань співробітників щодо нових загроз та методів протидії, включаючи новітні методи фішингу, техніки соціальної інженерії та практичні поради щодо безпеки через щомісячні або щоквартальні тренінги, оновлення політик безпеки та розсилку інформаційних бюлетенів.
3. Симуляції фішингових атак: Проведення фішингових тестів для оцінки готовності співробітників до реальних атак, включаючи відправку фальшивих фішингових листів з подальшим аналізом результатів і зворотнім зв'язком.
4. Інтерактивні навчальні програми: Використання інтерактивних методів навчання, таких як вікторини, навчальні ігри та симуляції реальних ситуацій через інтерактивні платформи для онлайн-навчання та додатки для мобільних пристроїв.
5. Політики безпеки та інструкції: Розробка та впровадження чітких політик та інструкцій щодо використання електронної пошти та поводження з конфіденційною інформацією, включаючи правила створення та зберігання паролів, процедури повідомлення про підозрілі листи та правила використання особистих пристроїв через документування політик, розсилку інструкцій та регулярні перевірки дотримання політик.
6. Культура кібербезпеки: Формування культури кібербезпеки на всіх рівнях організації через підтримку з боку керівництва, регулярне інформування про важливість кібербезпеки, заохочення співробітників до відповідального ставлення до безпеки через інформаційні кампанії, плакати, інформаційні стенди та внутрішні комунікації.

7. Зворотний зв'язок та оцінка ефективності: Постійна оцінка ефективності навчальних програм і заходів з підвищення обізнаності через збір відгуків від співробітників, аналіз результатів симуляцій фішингових атак та моніторинг втілення тактик інформаційної безпеки.

2.2.2 Впровадження фільтрів, систем виявлення та реагування на фішингові атаки

Використання технологічних рішень є ключовим елементом у захисті корпоративної електронної пошти від фішингових атак. Ці рішення включають впровадження фільтрів, систем виявлення та реагування на фішингові атаки. Нижче наведено основні технологічні рішення, що можуть бути використані для захисту корпоративної пошти:

1. Спам-фільтри та антифішингові фільтри

Спам-фільтри та антифішингові фільтри використовуються для автоматичного перевірки вхідних листів на підозрілість. Вони використовують технології машинного навчання та штучного інтелекту для аналізу вмісту листів і виявлення характерних ознак фішингових спроб. Наприклад, Microsoft Office 365 Advanced Threat Protection (ATP) аналізує листи на наявність шкідливих вкладень та посилань, що спрямовують на фішингові сайти. Google Workspace Security і Barracuda Email Security Gateway також відомі своєю ефективністю у фільтрації шкідливих листів.

2. Протоколи автентифікації електронної пошти

SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) і DMARC (Domain-based Message Authentication, Reporting & Conformance) є основними протоколами, що дозволяють перевіряти автентичність відправників листів і запобігати спуфінгу. SPF вказує на те, які IP-адреси мають право відправляти листи від імені домену. DKIM підписує листи цифровим підписом,

що підтверджує їхню автентичність. DMARC встановлює правила для обробки листів, які не вдалося автентифікувати за допомогою SPF або DKIM, що допомагає уникнути спаму і фішингу. Налаштування цих протоколів для домену компанії є важливим етапом у забезпеченні безпеки електронної пошти.

3. Системи виявлення загроз та реагування (TDR)

Системи виявлення загроз (Threat Detection and Response, TDR) інтегруються з SIEM-системами (Security Information and Event Management) для автоматичного виявлення та реагування на фішингові атаки в реальному часі. Вони використовують технології машинного навчання для аналізу поведінки користувачів і виявлення аномалій, що можуть вказувати на фішингові спроби. Приклади таких систем включають FireEye Email Security, Cisco Advanced Malware Protection (AMP) і Microsoft Defender for Office 365. Вони дозволяють ефективно виявляти шкідливі листи, а також реагувати на них шляхом блокування або ізоляції загрози.

4. Антивірусні програми

Антивірусні програми використовуються для сканування вкладень і вмісту електронних листів на наявність шкідливих програм і вірусів. Вони використовують сигнатурний аналіз (пошук відомих підписів вірусів) і евристичний аналіз (виявлення нових атак на основі відомих сценаріїв) для виявлення загроз. Приклади таких рішень включають Symantec Email Security.cloud, Trend Micro Email Security і McAfee Email Protection, які є популярними серед підприємств для захисту електронної пошти.

5. Засоби шифрування електронної пошти

Засоби шифрування електронної пошти використовуються для захисту конфіденційної інформації, що передається через електронну пошту. Вони можуть використовувати різні технології, такі як TLS (Transport Layer Security), PGP (Pretty Good Privacy) і S/MIME (Secure/Multipurpose Internet Mail Extensions).

Ці технології забезпечують шифрування листів на рівні транспортного шару або засобами електронної пошти, що дозволяє лише відправникам і отримувачам розшифровувати інформацію. Приклади рішень включають Microsoft Office Message Encryption, ZixEncrypt і Virtru Email Encryption.

6. Багатофакторна автентифікація (MFA):

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) використовуються для захисту облікових записів від несанкціонованого доступу, навіть у випадку, коли паролі були компрометовані. Вони вимагають додаткової перевірки ідентичності користувача, такої як одноразові паролі (OTP), біометричні дані або апаратні токени. Приклади рішень включають Google Authenticator, Microsoft Authenticator, Duo Security і Yubikey, які дозволяють компаніям інтегрувати додаткові заходи безпеки для захисту доступу до електронної пошти та інших систем.

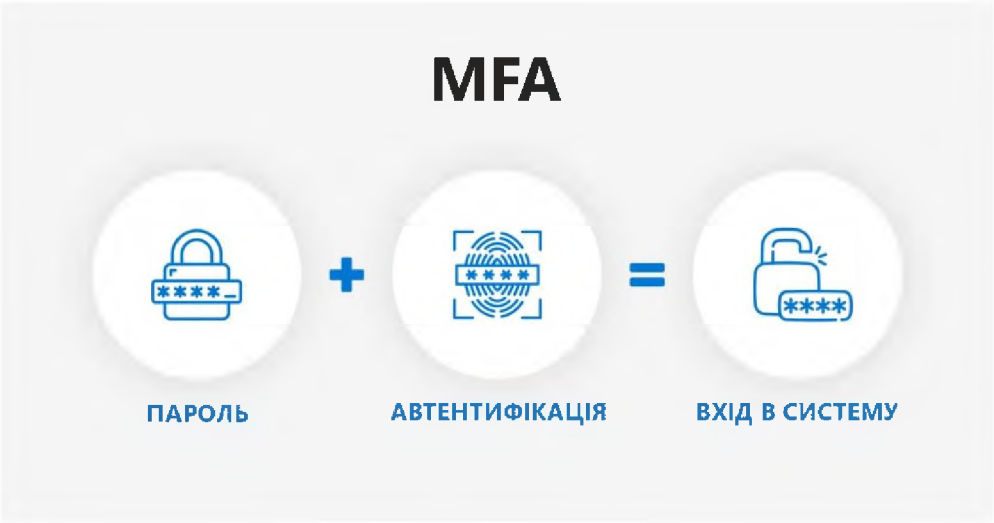

Рис. 2 Принцип MFA

7. Моніторинг та аналітика

Моніторинг та аналітика забезпечують постійний нагляд і аналіз трафіку електронної пошти для виявлення підозрілої активності. Вони використовують SIEM-системи для збору, кореляції та аналізу даних безпеки, що дозволяє оперативно реагувати на потенційні загрози. Приклади таких систем включають Splunk, IBM QRadar, ArcS Sight і LogRhythm, які надають інтегроване середовище для моніторингу і реагування на події безпеки електронної пошти.

2.2.3 Розробка та впровадження для запобігання фішинговим атакам

Розробка і впровадження ефективних політик безпеки є критичним елементом для зменшення ризику фішингових атак в корпоративному середовищі. Ось ключові аспекти політик і процедур, що можуть бути включені:

1. Освітні програми та навчання

Встановлення вимог до регулярного навчання співробітників щодо фішингових атак, їх розпізнавання та відповіді на них.

Організація тренінгів, вебінарів та інтерактивних сеансів для всіх рівнів персоналу. Використання симуляцій фішингових атак для практичного навчання.

2. Встановлення правил безпеки електронної пошти

Розробка конкретних правил щодо використання корпоративної електронної пошти, включаючи вимоги до створення паролів, обмеження використання особистих пристроїв та управління конфіденційністю.

3. Використання протоколів автентифікації електронної пошти

Запровадження SPF, DKIM та DMARC для підтвердження автентичності відправників та захисту від спуфінгу.

4. Політика використання вкладень та посилань

Встановлення правил щодо перевірки вкладень та посилань у листах перед їх відкриттям. Використання антивірусних програм для сканування вкладень.

5. Процедури виявлення та відповіді на інциденти

Розробка процедур для швидкого виявлення підозрілих листів та реагування на фішингові атаки. Визначення ролей та відповідальностей у випадку інциденту.

6. Моніторинг та аудит

Встановлення систем моніторингу активності електронної пошти для виявлення аномальних дій та потенційних загроз.

7. Оновлення та оцінка ефективності

Регулярне оновлення політик і процедур з урахуванням нових загроз і технологічних рішень. Проведення оцінки ефективності політик та аналіз інцидентів.

2.2.4 Використання багатофакторної аутентифікації та шифрування листів

1. Багатофакторна аутентифікація (MFA)

Багатофакторна аутентифікація (MFA) є ефективним засобом для забезпечення безпеки корпоративних облікових записів, включаючи доступ до електронної пошти. Вона вимагає використання двох або більше методів перевірки особи перед наданням доступу. Наприклад, використання SMS-кодів, мобільних додатків аутентифікації або апаратних пристроїв разом з основним паролем дозволяє значно знизити ризик несанкціонованого доступу через компрометацію паролів. Навіть якщо зловмисник дізнається пароль, без додаткового фактора входу в систему не отримати.

2. Шифрування листів

Захист конфіденційності електронних листів вимагає застосування криптографічних методів, що забезпечують безпеку передачі інформації. Використання шифрування TLS для захисту транспортного каналу та технологій S/MIME або PGP для енд-ту-енд шифрування гарантує, що дані залишаються конфіденційними від винятків під час їх передачі. Шифрування може бути реалізоване на рівні поштових серверів або за допомогою спеціалізованих програм, які забезпечують надійність процесу шифрування та розшифрування листів.

2.3 Наслідки фішингу для організації

Фішинг є однією з найпоширеніших та небезпечних кіберзагроз для організацій. Він може мати серйозні наслідки для фінансового стану, репутації та операційної діяльності компаній. Оцінка наслідків фішингових атак включає в себе різноманітні аспекти, від фінансових втрат до зниження продуктивності та репутаційних ризиків.

1. Фінансові втрати:

Фішингові атаки можуть призводити до прямого викрадення коштів через шахрайські транзакції. Наприклад, атаки типу Business Email Compromise (BEC) можуть призвести до значних фінансових збитків, коли зловмисники успішно змушують компанії здійснювати великі платежі на підроблені рахунки.

Окрім прямих фінансових втрат, фішингові атаки можуть спричиняти значні витрати на відновлення систем, розслідування інцидентів, юридичні витрати та покриття штрафів за недотримання вимог регуляторів.

2. Втрати даних:

Атаки можуть призводити до викрадення конфіденційних даних, таких як особисті дані співробітників, фінансова інформація або інтелектуальна власність. Це може мати серйозні наслідки для конкурентоспроможності та довіри клієнтів до компанії.

Витрати часу на розслідування та відновлення після фішингових атак можуть значно знизити продуктивність співробітників. Крім того, потреба в навчанні та тренінгах для підвищення обізнаності про кіберзагрози також вимагає ресурсів і часу.

3. Репутаційні втрати:

Фішингові атаки можуть негативно вплинути на репутацію компанії, особливо якщо компрометація даних призводить до втрати довіри клієнтів або партнерів. Негативне висвітлення в ЗМІ може додатково погіршити ситуацію.

Компанії, що зазнали фішингових атак, можуть втратити клієнтів, які перестануть довіряти їхній здатності захищати особисті дані та фінансову інформацію.

4. Юридичні та регуляторні наслідки:

Недотримання вимог регуляторів щодо захисту даних може призвести до значних штрафів і санкцій. Наприклад, порушення Загального регламенту щодо захисту даних (GDPR) в ЄС може призвести до великих фінансових штрафів.

Компанії можуть зіштовхнутися з судовими позовами від постраждалих клієнтів або партнерів, які можуть вимагати компенсації за втрати, спричинені фішинговими атаками.

5. Операційні наслідки:

Фішингові атаки можуть призводити до переривання важливих бізнес-процесів, що може вплинути на здатність компанії надавати послуги або виконувати свої зобов'язання перед клієнтами.

Після фішингових атак компанії часто змушені інвестувати значні ресурси у вдосконалення своїх систем захисту, що включає оновлення програмного забезпечення, впровадження нових технологій та навчання персоналу.

Приклади впливу фішингових атак:

В 2013-2015 роках дві компанії, Google та Facebook, стали жертвами фішингової схеми, внаслідок чого було втрачено понад 100 мільйонів доларів. Зловмисник видавав себе за представника тайванського виробника апаратного забезпечення і успішно отримав платежі.

Бельгійський банк Crelan Bank втратив 75 мільйонів євро внаслідок фішингової атаки, яка була спрямована на високопосадовців компанії, що призвело до переказу значних сум на підроблені рахунки.

2.4 Рекомендації щодо покращення захисту від фішингу

Рекомендації щодо покращення захисту від фішингу включають впровадження двофакторної аутентифікації для доступу до електронної пошти, посилення освіти співробітників щодо впізнавання фішингових атак і реакції на них, а також постійне оновлення політик безпеки з урахуванням нових загроз і технологічних рішень.

2.4.1 Стратегія і планування для запобігання фішинговим атакам

Запобігання фішинговим атакам потребує систематичного підходу та постійного удосконалення стратегій. Ось ключові пропозиції щодо довгострокових заходів:

1. Систематичне навчання та підвищення обізнаності

Впроваджувати систематичних освітні заходи для всіх працівників щодо фішингових атак, включаючи обов'язкові курси та інтерактивні симуляції для підвищення усвідомленості про типи атак і способи захисту. Для цього необхідно розробити навчальні матеріали, організувати регулярні тренінги та оцінити ефективність програми через звітність та тестування навичок співробітників у виявленні підозрілих повідомлень

2. Регулярне оновлення політик безпеки

Регулярно оновлювати і адаптувати політики безпеки електронної пошти, враховуючи нові загрози і технології. Для досягнення цієї мети необхідно проводити систематичну перевірку і аналіз інцидентів, що стосуються безпеки пошти, а також впроваджувати нові заходи безпеки. Наприклад, розширювати застосування DMARC для покращення відсіювання спаму та фішингових атак,

а також впроваджувати системи аналізу поведінки користувачів для виявлення аномальних дій і попередження можливих загроз.

3. Вдосконалення технічних рішень

Впровадити технології захисту електронної пошти та систем виявлення загроз шляхом інтеграції штучного інтелекту та машинного навчання. Це дозволить автоматизувати процес виявлення фішингових атак і підвищити точність їх розпізнавання. Крім того, рекомендується регулярно оновлювати антивірусні та антиспамові фільтри для забезпечення ефективного відсіювання вірусів та небажаної пошти. Інтеграція цих технологій допоможе підвищити загальний рівень безпеки електронної пошти і зменшити ризики кібератак.

4. Посилення інтернаціонального співробітництва

Укладення міжнародних угод щодо обміну інформацією про нові фішингові загрози для підвищення глобального рівня кібербезпеки. Для досягнення цієї мети необхідно активно брати участь у міжнародних конференціях і форумах з кібербезпеки, де спільно аналізуватимуться та вирішуватимуться глобальні проблеми безпеки в інтернеті. Такий підхід сприятиме обміну найкращими практиками, ресурсами та інформацією про виявлені загрози, що зробить реакцію на кібератаки більш координованою та ефективною на міжнародному рівні.

5. Аудит та оцінка ефективності

Регулярно проводити аудити безпеки електронної пошти для оцінки ефективності заходів забезпечення безпеки. Для досягнення цієї мети необхідно встановлювати чіткі метрики безпеки та систематично вимірювати їх, аналізувати інциденти, що стосуються безпеки поштових систем, і вдосконалювати заходи на основі виявлених слабких місць. Такий підхід дозволить ефективно визначати рівень захищеності електронної пошти і вчасно впроваджувати вдосконалення для запобігання можливим кіберзагрозам.

2.4.2 Інноваційні технології для підвищення рівня захисту у майбутньому

З плином часу технології швидко розвиваються, що відкриває нові можливості для захисту від кіберзагроз. Ось деякі інноваційні технології та методи, які можуть допомогти підвищити рівень захисту корпоративної електронної пошти:

1. ШІ та машинне навчання для виявлення загроз:

Використання штучного інтелекту для аналізу великих обсягів даних і виявлення відхилень в поведінці користувачів або характеристиках електронних листів, що можуть вказувати на фішингові атаки.

Розробка систем, які автоматично вчаться розпізнавати та блокувати фішингові повідомлення перед їх доставкою до поштових скриньок користувачів.

2. Застосування розширених систем аналізу поведінки:

Впровадження систем, які аналізують звичайну поведінку користувачів в мережі і виявляють аномалії, такі як незвичайні запити на доступ до ресурсів, несподівані зміни у структурі електронної пошти тощо.

3. Використання квантових технологій для шифрування:

Дослідження можливостей застосування квантових обчислювальних технологій для створення надійних систем шифрування, які будуть майже непроникними для сучасних методів криптоаналізу.

4. Розвиток блокчейн-технологій для захисту інформації:

Використання блокчейн-технологій для створення безпечних та недозволених систем обміну інформацією, що гарантує конфіденційність і недоступність даних для зловмисників.

5. Інтеграція кіберфізичних систем:

Застосування інтернету речей (IoT) і кіберфізичних систем для моніторингу та захисту інфраструктури в реальному часі, що дозволяє швидше виявляти та реагувати на потенційні загрози.

Дані інноваційні технології відкривають нові перспективи для забезпечення безпеки електронної пошти в корпоративному середовищі. Їх впровадження будуть вимагати комплексного підходу, включаючи належне тестування, налаштування і інтеграцію з існуючими системами безпеки.

2.4.3 Рекомендації для компаній щодо захисту від фішингових атак в корпоративному середовищі

Запобігання фішинговим атакам є критично важливим завданням для будь-якої організації, що працює з електронною поштою. Ось деякі узагальнені рекомендації на основі кращих практик:

1. Освіта та навчання персоналу:

Навчання співробітників розпізнавати фішингові атаки та поводитися у випадку їх отримання. Проведення регулярних симуляцій фішингових атак для оцінки рівня готовності персоналу і виявлення слабких місць для підвищення їхньої обізнаності та здатності розпізнавати шахрайські повідомлення.

2. Захист технічних інфраструктур:

Використання мультифакторної аутентифікації (MFA). Впровадження багатофакторної аутентифікації для усіх корпоративних облікових записів. Використання шифрування для захисту конфіденційної інформації в електронній пошті для зменшення ризику несанкціонованого доступу до облікових записів, вимагаючи від користувачів додаткового підтвердження своєї ідентичності

3. Управління політиками безпеки:

Регулярне оновлення і адаптація політик безпеки електронної пошти відповідно до змінюючихся загроз і технологій. Впровадження Domain-based Message Authentication, Reporting and Conformance (DMARC) для підвищення автентифікації електронної пошти.

4. Використання інноваційних технологій:

Застосування штучного інтелекту і машинного навчання. Використання ШІ для виявлення аномалій та автоматичного розпізнавання фішингових повідомлень. Впровадження розширених систем аналізу поведінки користувачів. Використання систем, які аналізують звичайну поведінку користувачів для виявлення аномалій.

5. Співпраця із зовнішніми експертами і організаціями:

Участь в кібербезпечних спільнотах і обмін інформацією. Активна участь в міжнародних ініціативах та обмін даними про нові загрози. Регулярне проведення аудитів та оцінка ефективності заходів безпеки для виявлення потенційних проблем і удосконалення стратегій дозволить ідентифікувати потенційні слабкі місця в системах безпеки організації. Це необхідно для постійного вдосконалення стратегій і заходів безпеки, що дозволяє підтримувати високий рівень захищеності в умовах постійно змінюючихся кіберзагроз.

2.5 Висновки

Вразливість корпоративної пошти робить її привабливою ціллю для фішингових атак, що можуть призвести до значних збитків для організацій. Основні загрози включають крадіжку облікових даних, розповсюдження шкідливого програмного забезпечення та фінансові шахрайства.

Для протидії фішингу в корпоративній пошті застосовуються різні методи:

Освітні заходи – важливо проводити програми навчання та підвищення обізнаності співробітників.

Технологічні рішення – впровадження фільтрів, систем виявлення та реагування на фішингові атаки є критично важливим.

Політики безпеки – розробка та впровадження політик безпеки, які визначають правила та процедури для запобігання фішинговим атакам, є важливим кроком.

Аутентифікація та шифрування – використання багатофакторної аутентифікації (MFA) та шифрування листів забезпечує додатковий рівень захисту, ускладнюючи доступ для зловмисників.

Оцінка наслідків фішингу для організації показує, що такі атаки можуть призвести до фінансових втрат, втрати конфіденційної інформації та пошкодження репутації компанії. Тому захист від фішингу повинен бути пріоритетом для будь-якої організації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У розділі економічного аспекту визначається ефективність впровадження методів протидії фішингу в інформаційні системи цільових організацій. Для досягнення цієї мети необхідно розрахувати фіксовані (капітальні) витрати, річні експлуатаційні витрати та річний економічний ефект від впровадження запропонованих рекомендацій. Особливу увагу слід приділити розробці політики безпеки інформації, яка визначається тривалістю роботи спеціаліста з інформаційної безпеки від складання технічного завдання до оформлення документації.

3.1 Розрахунок фіксованих витрат на впровадження методів протидії фішингу

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Створення політики інформаційної безпеки потребує ретельного підходу та значного часу на виконання кожного етапу, від розробки технічного завдання до оформлення документації, особливо якщо над цим працює лише один спеціаліст з інформаційної безпеки:

$$t = t_{\text{ТЗ}} + t_{\text{В}} + t_{\text{а}} + t_{\text{ВЗ}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}} \tag{3.1}$$

$t_{\text{ТЗ}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{\text{В}}$ – тривалість розробки концепції безпеки у організації;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків;

$t_{\text{ВЗ}}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$– тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки.

Відповідно до формули 3.1, трудомісткість розробки політики безпеки буде дорівнювати:

$$t = 4 + 16 + 4 + 6 + 4 + 16 + 8 = 58 \text{ год.}$$

3.1.2 Розрахунок витрат на створення політик безпеки

Витрати на розробку політики безпеки $К_{рп}$ охоплюють заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ та вартість машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч} \quad (3.2)$$

Середня заробітна плата спеціаліста з інформаційної безпеки враховуючи основну і додаткову оплату, а також відрахування на соціальні потреби, на 2024 рік становить 180 грн на годину. Витрати на заробітну плату розраховуються за наступною формулою:

$$З_{зп} = t * 190 \quad (3.3)$$

Отже в результаті заробітна плата за розробку політик безпеки інформації буде дорівнювати:

$$З_{зп} = 58 * 180 = 10440 \text{ грн.}$$

Вартість машинного часу для розробки політики безпеки інформації вираховується за формулою:

$$З_{мч} = t * C_{мч} \tag{3.4}$$

Де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P * t_{нал} * C_e + \frac{Ф_{зал} * Н_а}{F_p} + \frac{К_{лпз} * Н_{апз}}{F_p} \tag{3.5}$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$– кількість задіяних робочих станцій при написанні політики;

C_e – тариф на електричну енергію, грн./кВт*година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920)

Вартість 1 години машинного часу ПК буде дорівнювати:

$$C_{мч} = 0{,}5 * 1 * 6 + \frac{4780 * 0{,}3}{1920} + \frac{1312 * 0{,}1}{1920} = 3{,}82 \text{ грн.}$$

Тоді вартість витрат машинного часу буде:

$$З_{мч} = 104 * 3{,}82 = 397{,}28 \text{ грн.}$$

Отже, згідно формулі 3.2, витрати на розробку політики безпеки будуть складати:

$$К_{рп} = 10440 + 397{,}28 = 10837{,}28 \text{ грн.}$$

Для розрахунку вартості впровадження методів протидії фішингу в організації, кількість працівників прийнята за 100. У таблиці вказані рекомендовані методи протидії фішингу та вартість їх впровадження.

Таблиця 3.1 – Вартість методів протидії фішингу

Методи протидії фішингу	Фіксована вартість, грн	Щорічні витрати, грн
ESET Cybersecurity Awareness Training	0	60000
Fido2	110000	0
Egres Defend	0	34800

Капітальні витрати на впровадження запропонованих методів розраховуються за формулою:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення для цього консультантів, тис. грн.;

$К_{зпз}$ – вартість закупівель ліцензійного програмного забезпечення, тис. грн.;

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.;

Візьмемо до уваги ситуацію де виключно використовується ліцензійне програмне забезпечення, програми навчання за річною підпискою, а витрати на обладнання занесемо в його вартість. У такому випадку капітальні витрати організації будуть дорівнювати:

$$К = 10{,}84 + 110 + 60 = 180{,}84 \text{ тис. грн.}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання системи протидії фішингу

Витрати на рекомендовані методи протидії фішингу на щорічній основі включають ті, що реалізуються за допомогою регулярної підписки. Щоб визначити річні експлуатаційні витрати, потрібно скористатися формулою:

$$С = С_{навч} + С_{пз} + С_{з} \tag{3.7}$$

$С_{навч}$ – регулярні витрати на навчання працівників, тис. грн.;

$С_{пз}$ – регулярні витрати на продовження дії ліцензійного ПЗ, тис. грн.;

$С_{з}$ – річний фонд заробітної плати технічного персоналу, що обслуговує систему протидії фішинговим атакам, тис. грн.

Станом на 2024 рік, середня заробітна плата спеціаліста з інформаційної безпеки становить 180 грн на годину з урахуванням основної і додаткової заробітної плати, а також відрахування на соціальні потреби. Для обслуговування систем протидії фішингу тому:

$$С_з = 180 * 160 * 12 = \ 345600 \text{ грн.}$$

Відповідно до формули 3.7, річні експлуатаційні витрати для організації будуть становити:

$$С = 60 + 348 + 345{,}6 = 753{,}6 \text{ грн.}$$

3.3 Визначення річного економічного ефекту від впровадження запропонованих рекомендацій з впровадження методів протидії фішингу

Для розрахунку економічного ефекту від впровадження запропонованих рекомендацій потрібно оцінити величину можливого збитку. Через неможливість стовідсотково передбачити наслідки атаки, для розрахунку вартості такого збитку можна використати наступну спрощену модель оцінки:

Необхідні вхідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла чи сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_С$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу персоналу, осіб;

$Ч_С$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі;

О - обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

І - число атакованих вузлів або корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_{п} + П_{в} + V \tag{3.8}$$

$П_{п}$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_{в}$ – вартість відновлення працездатності вузла або сегмента корпоративної пошти, грн;

V - втрати від зниження обсягу продажів, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_{п} = \frac{\sum З_{с}}{F} * t_{п} \tag{3.9}$$

де F – місячний фонд робочого часу (при 40-ка годинному робочому тижні становить 176 годин).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_{в} = П_{ви} + П_{пв} \tag{3.10}$$

де $П_{ви}$ – витрати на повторне введення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегменту корпоративної мережі.

Витрати на повторне введення інформації розраховується за формулою:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} \quad (3.11)$$

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються за формулою:

$$П_{пв} = \frac{\sum З_о}{F} * t_в \quad (3.12)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента визначаючи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} * (t_в + t_п + t_{ви}) \quad (3.13)$$

$F_г$ – річний фонд часу роботи організації (52 тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить приблизно 2080 годин.

Таким чином збитки від атаки на вузол або сегмент корпоративної мережі складе:

$$В = \sum_i \sum_n U \quad (3.14)$$

Для організацій зі штабом 100 працівників, 3 з яких є обслуговуючим персоналом, витрати будуть складати:

$$П_{ви} = \frac{1455000}{176} * 3 = 24801 \text{ грн.}$$

$$П_{пв} = \frac{86400}{176} * 3 = 1473 \text{ грн.}$$

$$П_{в} = 24801 + 1473 = 26274 \text{ грн.}$$

Втрати від зниження очікуваного обсягу за час простою вираховується за формулою 3.13 і дорівнює:

$$V = \frac{43200000}{2080} * (3 + 3 + 3) = 186923 \text{ грн.}$$

А упущена вигода за формулою 3.8 буде складати:

$$U = 26274 + 186923 = 213197 \text{ грн.}$$

Таким чином, при 15 атаках на рік, збитки для організації лише внаслідок простою складатимуть:

$$B = 15 * 213197 = 3197955 \text{ грн.}$$

Основний ефект від дотримання рекомендацій про впровадження методів протидії фішингу визначається з урахуванням ризиків порушення інформаційної безпеки становить:

$$E = B * R - C \tag{3.15}$$

Відповідно до формули 3.15, загальний ефект від слідування рекомендаціям для організації складе:

$$E = 3197955 * 0{,}66 - 753600 = 1357050{,}3 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованих рекомендацій з впровадження методів протидії фішингу

Для проведення оцінки економічної ефективності запропонованих рекомендацій з впровадження методів протидії фішингу, визначемо та проаналізуємо наступні показники:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає ROSI;

б) термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій у впровадження системи інформаційної безпеки. Для обчислення ROSI необхідно використати формулу:

$$ROSI = \frac{\text{Е}}{\text{К}} \tag{3.16}$$

де Е – загальний ефект від слідування рекомендаціям (формула 3.15), тис. грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = \frac{1357{,}05}{180{,}84} = 7{,}5$$

Термін окупності капітальних інвестицій вказує на те, через якмй період чачу капітальні інвестиції повертаються за рахунок отриманого ефекту від впровадження рекомендованих методів протидії фішинговим атакам. Його обчислення здійснюється за наступною формулою:

$$T_o = \frac{K}{E} \tag{3.17}$$

Отже відповідно до формули 3.17, термін окупності для організації буде становити:

$$T_o = \frac{180,84}{1357,05} = 0,13 \text{ років} = 1,56 \text{ місяців} = 47,5 \text{ днів}$$

3.5 Висновки

Розглядаючи економічну доцільність рекомендацій щодо протидії фішинговим атакам у корпоративному середовищі, слід враховувати кілька ключових аспектів.

Освітні заходи та підвищення обізнаності співробітників потребують витрат на розробку навчальних програм, організацію тренінгів та залучення спеціалістів. Однак такі заходи значно знижують ризик успішних фішингових атак, що веде до меншої кількості інцидентів безпеки та скорочення витрат на їх усунення, а також уникнення потенційних фінансових втрат.

Впровадження технологічних рішень, таких як фільтри та системи виявлення й реагування на фішингові атаки, також потребує значних інвестицій, але забезпечує додатковий рівень захисту, знижуючи ймовірність успішних атак.

Розробка та впровадження політик безпеки, включаючи використання багатофакторної аутентифікації та шифрування листів, сприяють підвищенню рівня захисту корпоративної пошти. Витрати на ці заходи є виправданими, оскільки вони запобігають потенційним збиткам від фішингових атак, які можуть

включати витік конфіденційної інформації, фінансові втрати та порушення репутації компанії.

Оцінка наслідків фішингу для організації показує, що ефективні заходи безпеки є економічно ефективним рішенням.

ВИСНОВКИ

На основі проведеного дослідження з теми "Методи протидії фішингу в корпоративній пошті" можна зробити наступні основні висновки:

В кваліфікаційній роботі було проаналізовано та обговорено актуальність теми фішингу, фішингові атаки залишаються однією з найбільш поширених загроз для корпоративних систем електронної пошти, оскільки вони можуть призвести до витоку конфіденційної інформації та фінансових втрат.

Досліджено різноманітні типи фішингу, із зосередженням на їхніх особливостях і методах виявлення.

В спеціальному розділі було розглянуто різні стратегії та технології захисту, такі як багатофакторна аутентифікація, системи виявлення аномалій, шифрування електронних листів та впровадження політик безпеки, які спрямовані на запобігання і виявлення фішингових атак.

Значення освіти та підвищення обізнаності серед співробітників щодо фішингу підкреслене як критичний аспект в ефективній боротьбі з цією загрозою.

Обговорено перспективні напрямки використання штучного інтелекту, машинного навчання, розширених систем аналізу поведінки та інших передових технологій для покращення систем захисту від фішингових атак.

В економічному розділі було визначено економічну ефективність впровадження методів протидії фішингу в інформаційну систему організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Anderson, R., & Moore, T. (2009). Information Security Economics – and Beyond. Journal of Information Security.

2. APWG. (2023). Phishing Activity Trends Report. Anti-Phishing Working Group.

3. Barton, K., & Barton, K. (2022). Phishing in the Enterprise: Strategies for Prevention and Detection. Cybersecurity Journal.

4. Chiew, K. L., Chang, V., & Tiong, W. K. (2018). Utilisation of Machine Learning in Phishing Email Detection: A Review. Journal of Network and Computer Applications.

5. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

6. Jakobsson, M., & Myers, S. (2007). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. John Wiley & Sons.

7. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. Journal of Information Security and Applications.

8. Olmstead, K., & Smith, A. (2017). Americans and Cybersecurity. Pew Research Center.

9. Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. Southwest Decision Sciences Institute Conference Proceedings.

10. Siciliano, R. (2018). Identify Theft and Cybersecurity: How to Protect Your Business and Your Clients. Cyber Defense Magazine.

11. Symantec. (2022). Internet Security Threat Report. Symantec Corporation.

12. Verizon. (2023). Data Breach Investigations Report. Verizon Enterprise.

13. Xu, Y., & Chau, M. (2018). Analyzing the Risk of Phishing Webpages Using Machine Learning. Journal of Internet Services and Applications.

14. Young, A., & Yung, M. (2016). Cryptovirology: Malware, Misuse, and Deception. Springer.

15. Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding Phish: Evaluating Anti-Phishing Tools. Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS).

16. Zhuhadar, L., Yang, R., & Lytras, M. (2020). Real-Time Phishing Email Detection Using Machine Learning Techniques. Journal of Ambient Intelligence and Humanized Computing.

17. Braz, C., & Robert, J. M. (2006). Security and Usability: The Case of the User Authentication Methods. Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services.

18. Cranor, L. F. (2008). A Framework for Reasoning About the Human in the Loop. Proceedings of the 1st Conference on Usability, Psychology, and Security.

19. Herzberg, A., & Gbara, A. (2004). TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks.

20. Деркач, Ю., & Міщенко, О. (2020). Використання машинного навчання для виявлення фішингових електронних листів. Вісник Київського національного університету імені Тараса Шевченка. Серія: Прикладна математика та інформатика, 34, 48-55.

21. Завірюха, О. П., & Довбня, В. В. (2018). Методи захисту від фішингових атак у системах електронної пошти. Збірник наукових праць Національного університету «Полтавська політехніка імені Юрія Кондратюка», 2(87), 134-141.

22. Ковальчук, Л., & Лавренюк, І. (2019). Політики безпеки інформаційних систем як засіб протидії фішинговим атакам. Наукові праці Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології, 3(99), 96-102.

23. Котляр, В., & Головач, Т. (2020). Технології захисту корпоративних мереж від фішингових атак. Збірник наукових праць Одеського національного політехнічного університету, 4, 105-110.

24. Мельник, І., & Соколов, О. (2022). Використання блокчейн-технологій для підвищення безпеки електронної пошти. Вісник Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», 5, 123-129.

25. Петренко, О., & Васильєв, Ю. (2021). Аналіз ефективності використання багатофакторної аутентифікації для захисту корпоративної пошти. Журнал Національного університету оборони України, 8(43), 76-83.

26. Руденко, В., & Коваленко, С. (2019). Освітні заходи для підвищення обізнаності співробітників щодо фішингових атак. Науковий вісник Національного університету біоресурсів і природокористування України, 287, 144-150.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	12	
6	А4	2 Розділ	18	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Кумпан кваліфікаційна робота.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ім’я, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу студента групи 125-20-2

Кумпана Тімура Ігоровича

на тему: Методи протидиї фішингу в корпоративній пошті

Метою кваліфікаційної роботи є розробка, впровадження та покращення системи протидії фішингу в корпоративній пошті, що спрямована на забезпечення надійного захисту інформації від несанкціонованого доступу, витоку даних та інших загроз інформаційній безпеці підприємства.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

Практичне значення результатів кваліфікаційної роботи є методи протидії фішингу в корпоративній пошті за допомогою яких організація зможе мінімізувати ризики та зменшити потенційні економічні збитки від атак на підприємство.

За час дипломування Кумпан Т.І проявив себе фахівцем, здатним вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи доц. Ткач М.О.

Керівник спец. розділу доц. Ткач М.О.