МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ НА ІНФРАСТРУКТУРУ ЕЛЕКТРОННОЇ ПОШТИ ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Богдан СУЛИМА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Богдан СУЛИМА
Ім’я, ПРІЗВИЩЕ

Керівник: Іван ОПІРСЬКИЙ
д.т.н., професор

Рецензент:
к.т.н., доцент

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сулими Богдана Віталійовича

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи виявлення та протидії атакам на інфраструктуру електронної пошти організації”,
керівник кваліфікаційної роботи ОПІРСЬКИЙ Іван, д.т.н., професор.
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

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

2. Строк подання кваліфікаційної роботи “1” червня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *наукові та методичні джерела з безпеки електронної пошти, міжнародні стандарти і рекомендації, технічна документація, матеріали щодо захисту корпоративної поштової інфраструктури.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати архітектуру корпоративної поштової інфраструктури організації.

4.2. Дослідити актуальні загрози та методи виявлення атак на інфраструктуру електронної пошти.

4.3. Визначити технічні й організаційні заходи протидії та розробити практичні рекомендації щодо підвищення кіберстійкості поштової інфраструктури.

5. Перелік ілюстративного матеріалу: презентація PowerPoint

6. Дата видачі завдання “20” лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Опрацювання методичних вимог, затвердження теми та плану	20.02.2026	
2.	Збір та аналіз джерел, нормативної й технічної бази	21.02.2026	
3.	Підготовка вступу та розділу 1	24.02.2026	
4.	Підготовка розділу 2	01.03.2026	
5.	Підготовка розділу 3 та рекомендацій	07.03.2026	
6.	Формування висновків, списку джерел, додатків	10.03.2026	
7.	Остаточне редагування, перевірка та підготовка до захисту	13.03.2026	
8.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ *(підпис)* Богдан СУЛИМА
(Ім’я, ПРІЗВИЩЕ)

Керівник
кваліфікаційної роботи _____ *(підпис)* Іван ОПІРСЬКИЙ
(Ім’я, ПРІЗВИЩЕ)

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

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

Направляється здобувач Сулима Б.В. до захисту кваліфікаційної роботи

(прізвище та ініціали)

за спеціальністю 125 Кібербезпека

(код, найменування спеціальності)

освітньої програми Управління інформаційною та кібернетичною безпекою

(назва)

на тему: “Методи виявлення та протидії атакам на інфраструктуру електронної пошти організації”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач СУЛИМА Богдан у кваліфікаційній роботі дослідив методи виявлення та протидії атакам на інфраструктуру електронної пошти організації, систематизував основні загрози, методи детекції та заходи захисту, а також сформував практичні рекомендації за темою дослідження.

СУЛИМА Богдан показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СУЛИМИ Богдана на позитивну оцінку та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи_____ _Іван ОПІРСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“___”_____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Сулима Б.В. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти СУЛИМИ Богдана
на тему “Методи виявлення та протидії атакам на інфраструктуру електронної пошти організації”

Актуальність. Корпоративна електронна пошта є одним із основних каналів ділових комунікацій і водночас поширеною ціллю кібератак. Зловмисники використовують її для фішингу, спуфінгу, BEC-атак, поширення шкідливого ПЗ та викрадення облікових даних. Тому забезпечення захисту електронної пошти є важливим завданням для збереження конфіденційності, цілісності та доступності корпоративної інформації. Актуальність цієї теми зумовлена постійним зростанням кількості та складності атак на поштові сервіси. Ефективне впровадження сучасних механізмів захисту дозволяє знизити ризики компрометації облікових записів і витоку корпоративних даних.

У зв’язку з цим дослідження методів виявлення та протидії атакам на поштову інфраструктуру є актуальним науково-практичним завданням.

Позитивні сторони.

1. У роботі систематизовано основні загрози для корпоративної електронної пошти.
2. Матеріал викладено послідовно та відповідно до структури кваліфікаційної роботи.
3. За результатами дослідження сформовано практичні рекомендації щодо підвищення захищеності поштової інфраструктури організації.

Недоліки.

Доцільно було б розширити прикладну частину перевіркою ефективності запропонованих заходів на тестовому середовищі або моделі корпоративної інфраструктури.

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

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Обсяг роботи – 88 стор., 6 рис., 13 табл., 42 джерела, 4 додатки.

Об'єкт дослідження – корпоративна інфраструктура електронної пошти організації та процеси її експлуатації.

Предмет дослідження – методи виявлення та протидії атакам на електронну пошту (фішинг, спуфінг, BEC/EAC, шкідливі вкладення, ексфільтрація даних, компрометація акаунтів).

Мета роботи – систематизувати та обґрунтувати комплексний підхід до виявлення і протидії атакам на поштову інфраструктуру організації з урахуванням технічних і організаційних контролів.

Методи дослідження – аналіз стандартів і рекомендацій (RFC/IETF, NIST), порівняльний аналіз механізмів захисту пошти, узагальнення кращих практик SOC/SIEM, ризик-орієнтований підхід до вибору контрзаходів.

Наукова новизна – запропоновано узгоджену модель методів детекції та протидії, що поєднує транспортний захист (TLS, MTA-STS, TLS-RPT), доменну автентифікацію (SPF/DKIM/DMARC), контентний аналіз і sandbox/CDR, поведінкову аналітику BEC/EAC та кореляцію подій у SIEM/SOAR.

Практичне значення – сформовано рекомендації щодо поетапного впровадження контролів, чеклісти SOC для тріажу інцидентів, приклади кореляційних правил і дорожню карту підвищення зрілості поштової безпеки.

Короткий зміст роботи – у розділі 1 проаналізовано архітектуру поштових систем і класи загроз; у розділі 2 систематизовано методи виявлення (автентифікація домену, аналіз заголовків/URL/вкладень, моніторинг логів, hunting); у розділі 3 наведено контрзаходи та процедури реагування; у розділі 4 визначено метрики ефективності, підхід до аудиту та безперервного покращення.

Галузь застосування – результати роботи можуть бути використані під час аудиту, модернізації та експлуатації корпоративної поштової

інфраструктури, а також при розробленні внутрішніх регламентів реагування на інциденти.

Ключові слова: ЕЛЕКТРОННА ПОШТА, ПОШТОВА ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ФІШИНГ, СПУФІНГ, BEC-АТАКИ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ, ВИЯВЛЕННЯ АТАК, ПРОТИДІЯ КІБЕРАТАКАМ, SPF, DKIM, DMARC, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, МОНІТОРИНГ БЕЗПЕКИ.

ABSTRACT

The scope of the work is 88 pages, 6 figures, 13 tables, 42 sources, 4 appendices.

The object of the study is the corporate email infrastructure of the organization and the processes of its operation.

The subject of the study is methods of detecting and countering attacks on email (phishing, spoofing, BEC/EAC, malicious attachments, data exfiltration, account compromise).

The purpose of the study is to systematize and substantiate a comprehensive approach to detecting and countering attacks on the email infrastructure of the organization, taking into account technical and organizational controls.

Research methods are analysis of standards and recommendations (RFC/IETF, NIST), comparative analysis of email protection mechanisms, generalization of SOC/SIEM best practices, risk-based approach to choosing countermeasures.

Scientific novelty – a consistent model of detection and countermeasure methods is proposed, combining transport protection (TLS, MTA-STS, TLS-RPT), domain authentication (SPF/DKIM/DMARC), content analysis and sandbox/CDR, behavioral analytics BEC/EAC and event correlation in SIEM/SOAR.

Practical significance – recommendations for the phased implementation of controls, SOC checklists for incident triage, examples of correlation rules and a roadmap for increasing the maturity of mail security are formed.

Summary of the work – section 1 analyzes the architecture of mail systems and threat classes; section 2 systematizes detection methods (domain authentication, header/URL/attachment analysis, log monitoring, hunting); section 3 provides countermeasures and response procedures; section 4 defines performance metrics, an approach to auditing and continuous improvement.

Field of application - the results of the work can be used during the audit, modernization and operation of corporate postal infrastructure, as well as when developing internal incident response regulations.

Key words: EMAIL, EMAIL INFRASTRUCTURE, CYBERSECURITY, INFORMATION SECURITY, PHISHING, SPOOFING, BEC ATTACKS, MALWARE, EMAIL PROTECTION, ATTACK DETECTION, CYBERATTACK RESPONSE, SPF, DKIM, DMARC, MULTI-FACTOR AUTHENTICATION, SECURITY MONITORING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AiTM	Adversary-in-the-Middle (перехоплення сесій/токенів)
ARC	Authenticated Received Chain (ланцюжок автентифікації для пересланої пошти)
ASN	Autonomous System Number (номер автономної системи)
ATT&CK	MITRE ATT&CK (база знань тактик і технік атак)
BCP	Business Continuity Plan (план безперервності бізнесу)
BEC	Business Email Compromise (компрометація бізнес-листування)
BIMI	Brand Indicators for Message Identification
CA	Conditional Access (умовний доступ)
CDR	Content Disarm & Reconstruction (знешкодження та відновлення контенту)
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CRM	Customer Relationship Management (система взаємодії з клієнтами)
CSF	Cybersecurity Framework (рамка NIST)
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention (запобігання витоку даних)

DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAC	Email Account Compromise (компрометація поштового акаунта)
EDR	Endpoint Detection and Response
FBI	Federal Bureau of Investigation
FN	False Negative (хибнонегативне спрацювання)
FP	False Positive (хибнопозитивне спрацювання)
FPR	False Positive Rate (частка хибнопозитивних)
IAM	Identity and Access Management
IDN	Internationalized Domain Name (міжнародні доменні імена)
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IOC	Indicator of Compromise (індикатор компрометації)
IP	Internet Protocol
IR	Incident Response (реагування на інциденти)
ISO	International Organization for Standardization
JIT	Just-in-Time (тимчасове надання

	привілеїв)
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MFA	Multi-Factor Authentication
MIME	Multipurpose Internet Mail Extensions
MITM	Man-in-the-Middle
ML	Machine Learning (машинне навчання)
MTA	Mail Transfer Agent (поштовий транспорт)
MTA-STS	SMTP MTA Strict Transport Security
MTTD	Mean Time To Detect (середній час до виявлення)
MTTR	Mean Time To Respond/Recover (середній час до реагування/відновлення)
MUA	Mail User Agent (поштовий клієнт)
NIST	National Institute of Standards and Technology
OAuth	Open Authorization (протокол авторизації)
PAM	Privileged Access Management
PDF	Portable Document Format
PKI	Public Key Infrastructure
POP3	Post Office Protocol v3
QR	Quick Response (QR-код)
RFC	Request for Comments (стандарти IETF)
RUA	Reporting URI for Aggregate reports (DMARC агреговані звіти)
S/MIME	Secure/Multipurpose Internet Mail Extensions

SEG	Secure Email Gateway
SIEM	Security Information and Event Management
SLA	Service Level Agreement (угода про рівень сервісу)
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SP	Special Publication (серія публікацій NIST)
SPF	Sender Policy Framework
TLS	Transport Layer Security
TLS-RPT	SMTP TLS Reporting
URL	Uniform Resource Locator
ІБ	Інформаційна безпека
СУІБ	Система управління інформаційною безпекою

ВСТУП

Актуальність теми. Корпоративна електронна пошта використовується як базовий сервіс ділових комунікацій, передачі документів, узгодження фінансових операцій, роботи з підрядниками та внутрішньої координації. Саме тому вона залишається одним із найпривабливіших каналів для кіберзлочинців. На практиці через електронну пошту реалізуються фішингові кампанії, підробка відправника, компрометація бізнес-листування, розсилання шкідливих вкладень, викрадення облікових даних та приховане пересилання повідомлень назовні [10, 11, 14–16]. У сучасних умовах захист поштової інфраструктури має розглядатися як один із ключових елементів загальної кіберстійкості організації.

Важливість проблеми підсилюється тим, що великі постачальники поштових сервісів посилюють вимоги до автентифікації відправників. Зокрема, Google вимагає налаштування SPF або DKIM для всіх відправників, а для масових відправників - одночасного використання SPF, DKIM і DMARC [8]. Yahoo також наполягає на автентифікації та публікації DMARC-політики, а для окремих категорій відправників робить це обов’язковою умовою [9]. Це означає, що питання захисту поштового домену перестало бути суто внутрішньою справою організації й перетворилося на вимогу зовнішнього інформаційного середовища.

Об’єктом дослідження є процеси функціонування та захисту корпоративної інфраструктури електронної пошти організації. Предмет дослідження - методи виявлення та протидії атакам на інфраструктуру електронної пошти організації.

Мета роботи полягає в обґрунтуванні та систематизації комплексу методів, що дозволяють своєчасно виявляти та ефективно стримувати атаки на інфраструктуру електронної пошти організації.

Для досягнення поставленої мети необхідно вирішити такі завдання: проаналізувати архітектуру корпоративної електронної пошти та її місце у

системі захисту організації; систематизувати основні типи поштових атак і характерні індикатори їх реалізації; дослідити методи виявлення атак на основі доменної автентифікації, аналізу заголовків, контенту, URL, вкладень та поведінкової телеметрії; розглянути технічні й організаційні заходи протидії; сформувати основу для практичних рекомендацій щодо поетапного підвищення стійкості поштової інфраструктури.

Наукова новизна одержаних результатів полягає в систематизованому поєднанні технічних механізмів автентифікації пошти, контентного аналізу, поведінкової аналітики та процедурного реагування в єдину логіку контролю поштових загроз. Практичне значення полягає у можливості використання запропонованої структури для розроблення повного набору організаційних та технічних рішень на рівні організації.

Галузь застосування. Матеріали дослідження можуть бути використані для підготовки звітів і методичних матеріалів з кіберзахисту поштової інфраструктури, а також для формування плейбуків (playbooks) реагування SOC на поштові інциденти.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ІНФРАСТРУКТУРИ ЕЛЕКТРОННОЇ ПОШТИ ОРГАНІЗАЦІЇ ТА АНАЛІЗ АКТУАЛЬНИХ ЗАГРОЗ

1.1. Місце корпоративної електронної пошти в системі інформаційної та кібернетичної безпеки організації

Електронна пошта є не лише сервісом передачі повідомлень, а й важливою управлінською та технологічною підсистемою організації. Через неї циркулюють фінансові вказівки, юридично значущі повідомлення, комунікації з підрядниками, логістичні підтвердження, звіти та конфіденційні вкладення. Унаслідок цього компрометація поштового середовища створює ризик одночасного порушення конфіденційності, цілісності та доступності інформації.

З технічного погляду корпоративна поштова інфраструктура спирається на протокол SMTP, який визначає базові механізми передачі електронної пошти в Інтернеті [1]. Водночас класична логіка SMTP історично не забезпечувала достатньої перевірки справжності відправника, що й стало однією з причин широкого поширення спуфінгу та фішингових розсилок [3]. Саме тому сучасний захист електронної пошти розвивається навколо додаткових засобів доменної автентифікації, криптографічної перевірки та поведінкового моніторингу [17].

Поштова інфраструктура інтегрується з іншими підсистемами організації: службою каталогів, системами багатофакторної автентифікації, мережевими шлюзами, SIEM, EDR та процесами реагування на інциденти. Це означає, що безпека електронної пошти не може оцінюватися ізольовано. Якщо поштовий акаунт скомпрометовано, зловмисник часто отримує доступ до ланцюгів листування, контактних графів, файлів і внутрішніх процесів, а також може використовувати цю довіру для подальшого просування атаки [21].

У контексті українського законодавства організація захисту електронної пошти має узгоджуватися із загальними вимогами щодо кібербезпеки та захисту інформації в інформаційно-комунікаційних системах [19, 20]. Звідси випливає, що поштову інфраструктуру необхідно розглядати як частину системи управління інформаційною безпекою, а рішення щодо її захисту - як сукупність нормативних, організаційних і технічних заходів.

1.2. Архітектура корпоративної поштової інфраструктури та контрольні точки безпеки

Типова корпоративна поштова інфраструктура включає зовнішніх відправників, вхідний або вихідний захищений поштовий шлюз, транспортний агент електронної пошти, користувацькі клієнти, підсистеми автентифікації домену, системи журналювання та реагування. На рівні практичної експлуатації особливе значення мають сегменти, де можливе виконання первинного контролю: перевірка джерела відправлення, фільтрація контенту, перевірка вкладень, кореляція подій та запуск процедур реагування.

Першою зоною контролю виступає поштовий шлюз або SEG, на якому виконуються антиспам-перевірки, аналіз репутації джерела, сканування URL, перевірка вкладень і сигнатурні або евристичні спрацювання [2]. Другою зоною є DNS-автентифікація домену, яка дозволяє перевірити легітимність джерела надсилання за допомогою SPF, DKIM і DMARC [3–5]. Третьою зоною виступає телеметрія серверів і користувацьких поштових скриньок, де фіксуються спроби створення правил пересилання, аномальні входи, нетипові маршрути листування та інші поведінкові ознаки компрометації [21, 25].

Окрему роль відіграє транспортний захист між поштовими серверами. MTA-STS дозволяє домену декларувати вимогу доставляти пошту лише з використанням валідованого TLS до визначених MX-хостів [6], а TLS-RPT дає змогу отримувати звіти про невдалі або підозрілі TLS-сесії [7]. Ці механізми

особливо важливі для виявлення проблем конфігурації та потенційних спроб примусового зниження рівня захисту під час доставки повідомлень.

Таким чином, безпека поштової інфраструктури повинна будуватися як послідовність контрольних точок, де кожна наступна ланка підсилює попередню. Ілюстрацію такої архітектури наведено на рис. 1.1.

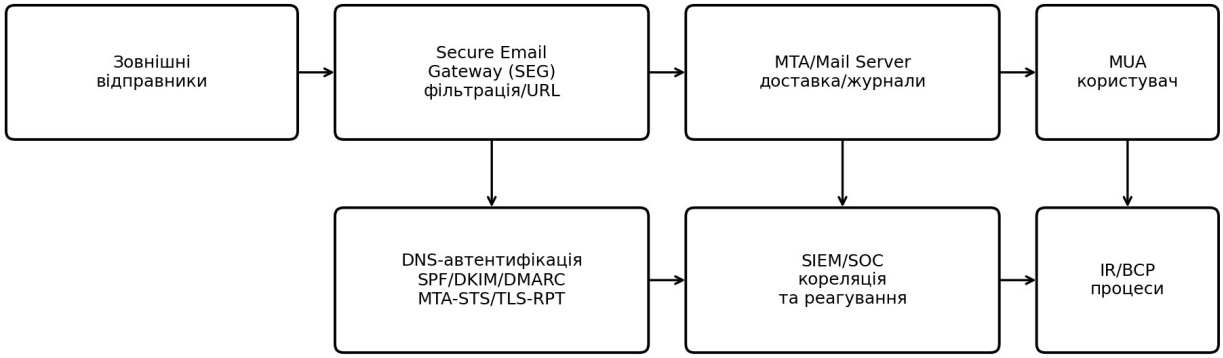

Рис. 1.1. Потік обробки вхідної пошти та контрольні точки захисту

Таблиця 1.1

Ключові компоненти корпоративної поштової інфраструктури та їх значення для безпеки

Компонент	**Функціональне призначення**	**Типові ризики**
Secure Email Gateway (SEG)	Первинна фільтрація листів, URL і вкладень	Пропуск цілеспрямованого фішингу, хибні спрацювання
MTA / Mail Server	Приймання, маршрутизація, збереження журналів	Неправильна конфігурація, компрометація сервера
DNS-автентифікація	Перевірка SPF, DKIM, DMARC, політик домену	Відсутність або помилки записів, обходи через сторонні сервіси
MUA / користувач	Отримання та взаємодія з листами	Клік по URL, запуск вкладень, соціальна інженерія
SIEM / SOC	Кореляція подій і реагування на інциденти	Неповна телеметрія, запізніла ескалація
IR / BCP процеси	Стримування, відновлення та lessons learned	Відсутність playbook-ів, затримка комунікацій

1.3. Основні типи атак на інфраструктуру електронної пошти організації

Найпоширенішими типами атак на корпоративну електронну пошту є фішинг, спуфінг, шкідливі вкладення, Business Email Compromise (BEC), компрометація облікових записів і зловживання правилами пересилання. Попри різноманітність технічних реалізацій, усі ці атаки націлені на використання довіри до електронної пошти як звичного каналу комунікації [10, 14–16].

Фішинг базується на спонуканні користувача до небажаної дії: переходу за шкідливим посиланням, введення облікових даних на підробленій сторінці, запуску вкладення або підтвердження сумнівної операції. MITRE ATT&CK виокремлює spearphishing attachment та spearphishing link як окремі підтехніки, що відповідає сучасному практичному поділу атак на вкладення та посилання [14].

Спуфінг полягає у підробці поля відправника або іншої ідентифікаційної інформації листа. Через відсутність жорсткої початкової автентифікації SMTP зловмисник може намагатися імітувати домен організації, керівника або відомого партнера, якщо домен належним чином не захищений механізмами SPF, DKIM і DMARC [3–5]. У сучасних середовищах додаткове значення має захист від схожих доменів, підміни відображуваного імені та модифікованих маршрутів пересилання.

BEC та EAC є особливо небезпечними, оскільки поєднують технічну компрометацію акаунта або імітацію довіреної особи з контекстом реальних бізнес-процесів. FBI визначає BEC як один із найбільш фінансово руйнівних видів онлайн-злочинності [10]. Зловмисник може використовувати вже скомпрометоване листування, знання платіжних звичок, графіків і контактів для підміни реквізитів або надсилання термінових запитів про оплату.

Після первинного доступу атакувальники нерідко створюють правила пересилання листів, приховують окремі повідомлення або збирають поштові дані для розвідки. MITRE ATT&CK окремо фіксує техніки Email Collection та Email Forwarding Rule, що важливо для побудови детекцій на рівні аудиту поштової скриньки [15, 16]. Це означає, що ефективне виявлення поштових

атак повинно охоплювати не лише етап доставки шкідливого листа, а й подальші дії після первинного успіху.

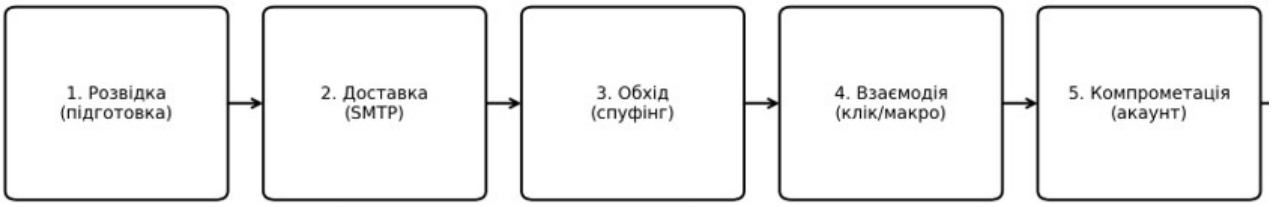

Рис. 1.2. Типовий ланцюг поштової атаки та точки виявлення/протидії

Таблиця 1.2

Класифікація основних поштових атак та їх характерні ознаки

Тип атаки	**Ключові ознаки**	**Наслідки для організації**
Фішинг	Терміновість, шкідливі URL, підроблені сторінки входу	Викрадення облікових даних, первинний доступ
Спуфінг	Невідповідність From, Return-Path, SPF/DKIM/DMARC	Підміна відправника, обман користувачів
Шкідливі вкладення	Архіви, макроси, підозрілі PDF/ISO/IMG	Інфікування, запуск шкідливого ПЗ
BEC/EAC	Контекст реального листування, зміна реквізитів, тиск	Фінансові втрати, компрометація ділових процесів
Email Forwarding Rule	Несанкціоноване правило пересилання	Приховане спостереження, витік листування
Компрометація акаунта	Аномальні входи, нові пристрої, відсутність MFA	Доступ до пошти, внутрішній рух, ескалація

1.4. Нормативні та технічні джерела забезпечення безпеки електронної пошти

Нормативна та технічна база захисту електронної пошти формується з кількох рівнів. Базовий технічний рівень задають RFC-документи IETF, які визначають SMTP, SPF, DKIM, DMARC, MTA-STS та TLS-RPT [1, 3–7]. Саме вони встановлюють логіку функціонування поштових сервісів, правила перевірки джерела надсилання та механізми підвищення довіри до доставки повідомлень.

Методичний рівень представлено документами NIST. Публікація NIST SP 800-45 розглядає рекомендації щодо безпеки електронної пошти загалом [2], а NIST SP 800-177 Rev. 1 описує принципи trustworthy email та підкреслює необхідність використання доменної автентифікації, шифрування транспорту, цілісності та звітності [17]. Окреме значення має NIST SP 800-61 Rev. 3, яка формує підхід до реагування на інциденти та післяінцидентного удосконалення процесів [18].

Операційний рівень формують вимоги та рекомендації великих постачальників сервісів і державних структур. Google та Yahoo публікують вимоги до відправників електронної пошти [8, 9], Microsoft описує механізми anti-spoofing, email authentication і реагування на компрометацію поштових акаунтів [13, 21, 28], FBI та CISA надають рекомендації щодо протидії BEC, фішингу й застосування MFA [10–12].

На національному рівні організація захисту поштової інфраструктури повинна узгоджуватися із законом про основні засади забезпечення кібербезпеки України та законом про захист інформації в інформаційно-комунікаційних системах [19, 20]. Отже, захист електронної пошти слід будувати як частину загальної системи УКБЗІ організації.

Таблиця 1.3

Основні групи джерел, що визначають вимоги до захисту електронної пошти

Група джерел	**Приклади**	**Практична роль**
Технічні стандарти IETF	RFC 5321, RFC 7208, RFC 6376, RFC 7489, RFC 8461, RFC 8460	Визначають протоколи, механізми автентифікації та звітності
Методичні документи NIST	SP 800-45, SP 800-177 Rev.1, SP 800-61 Rev.3	Задають практики побудови довіреної пошти та реагування
Операційні вимоги провайдерів	Google Email sender guidelines, Yahoo Sender Best Practices	Формують зовнішні вимоги до домену та відправника
Офіційні рекомендації з реагування	FBI BEC, CISA MFA/Phishing, Microsoft Defender guidance	Підтримують захист, моніторинг і відновлення після інцидентів
Національне законодавство	Закони України у сфері кібербезпеки та захисту інформації	Визначають правові й організаційні межі захисту

1.5. Модель загроз і ризик-орієнтований підхід до захисту поштової інфраструктури

Побудова захисту корпоративної пошти має спиратися на формалізовану модель загроз, яка пов’язує активи організації, можливі вектори атак та потенційні наслідки для бізнес-процесів. До критичних активів належать домен організації, поштові сервери або хмарна платформа, облікові записи співробітників, журнали подій, правила обробки листів і канали адміністрування. Для практичного моделювання доцільно використовувати логіку ланцюга атаки: первинне проникнення через фішинг або спуфінг, подальша компрометація акаунта, закріплення в середовищі та спроби ексфільтрації даних. У межах MITRE ATT&CK до поштових інцидентів безпосередньо належать техніки Email Collection (T1114) та Email Forwarding Rule (T1114.003), які характеризують збір поштових даних і приховане пересилання повідомлень [15–16].

Ризик-орієнтований підхід передбачає визначення пріоритету контролів через співвідношення імовірності та впливу інциденту. Для більшості організацій найбільший вплив мають BEC-атаки у фінансових процесах, компрометація поштових скриньок керівництва та витік конфіденційної інформації через підконтрольні зловмиснику акаунти. Тому першочерговими заходами мають бути багатофакторна автентифікація, обмеження автоматичного пересилання назовні, контроль делегувань та зміни правил поштових скриньок, а також процедури підтвердження критичних дій поза каналом електронної пошти.

1.6. Типові вразливості конфігурації та організаційні чинники ризику

Суттєву частку інцидентів спричиняють помилки конфігурації та слабкі організаційні процедури. До технічних проблем належать: некоректний SPF

(надмірні include-ланцюги, відсутність жорсткого механізму -all), відсутність ротації DKIM-ключів, DMARC у режимі p=none без підвищення політики, слабкі TLS-налаштування під час доставки та відсутність звітності про проблеми TLS. Організаційні чинники ризику включають: відсутність регламентів реагування на фішинг і BEC, нечіткі канали повідомлення SOC, недостатню сегрегацію обов'язків у фінансових процесах, а також низький рівень обізнаності персоналу. Практично це проявляється у виконанні термінових інструкцій з листів без незалежної верифікації та у відсутності сталої звички перевіряти домени, вкладення й посилання.

1.7. Протокольна основа корпоративної електронної пошти та точки контролю

Розуміння протоколів і форматів електронної пошти є необхідною передумовою для якісної детекції атак. На транспортному рівні доставка повідомлень у мережі Інтернет відбувається за допомогою SMTP, який задає загальну логіку обміну між поштовими серверами, а також визначає поняття «конверта» (envelope) і маршрутних заголовків Received [1]. Для практичного аналізу інцидентів важливо розділяти ідентичність відправника в SMTP-конверті (MAIL FROM/Return-Path) та ідентичність у заголовку From:, оскільки зловмисники часто маніпулюють саме видимими полями листа, залишаючи конверт як технічний інструмент доставки.

Формат повідомлення (заголовки + тіло) визначається стандартами інтернет-повідомлень та доповненнями MIME, які дозволяють передавати багаточастинні повідомлення, вкладення, альтернативні представлення (text/plain, text/html) тощо. З точки зору безпеки MIME-структура є одночасно джерелом ознак для фільтрації (типи вкладень, вкладені архіви, вбудовані об'єкти) і поверхнею атак (маскування типів файлів, подвійні розширення, вкладені контейнери).

На рівні доступу користувачів до поштових скриньок поширені протоколи IMAP/POP та вебінтерфейси. Для SOC важливо враховувати, що окремі інциденти відбуваються не на рівні SMTP-доставки, а на рівні доступу до скриньки: компрометація облікового запису, створення правил пересилання, експорт пошти, підключення сторонніх застосунків через OAuth. Отже, контроль має охоплювати не лише шлюз доставки, але й журнали платформи пошти та автентифікації (IAM).

Ключові точки контролю можна згрупувати в три шари: 1) транспортний шар (SMTP/TLS, політики MTA-STS, звітність TLS-RPT); 2) шар довіри до відправника (SPF/DKIM/DMARC, вирівнювання доменів, аналіз Authentication-Results); 3) шар контенту та поведінки (антиспам/антифішинг, sandbox для вкладень, URL time-of-click, поведінкова аналітика для BEC). Кожен шар знижує ризики по-своєму, а сумарний ефект досягається лише за умов узгодженого налаштування та моніторингу.

1.8. Типові архітектури поштових рішень: on-premises, хмара та гібрид

Сучасні організації використовують різні моделі розгортання пошти: локальні (on-premises), хмарні або гібридні. У локальному сценарії (Postfix/Exchange тощо) організація має повний контроль над конфігурацією серверів, TLS-параметрами, журналюванням та інтеграціями, але несе повну відповідальність за патч-менеджмент, доступність і захист периметра. У хмарних сценаріях (Microsoft 365, Google Workspace) частина контролів забезпечується провайдером, однак критичним стає коректне налаштування автентифікації домену, політик доступу, журналювання та управління сторонніми інтеграціями.

Гібридна модель поширена для організацій, які поступово мігрують до хмари або зберігають окремі потоки на локальній інфраструктурі. У цьому випадку складність безпеки зростає через збільшення кількості поштових релєїв, різні політики на сегментах і необхідність узгодження DKIM-підпису та

DMARC-alignment для всіх каналів надсилання. Практично це означає, що інвентаризація легітимних джерел є обов'язковим кроком перед посиленням DMARC-політики до quarantine/reject.

Окрему роль відіграє Secure Email Gateway (SEG). У багатьох архітектурах SEG виконує функції «переднього фільтра»: перевірка репутації IP/доменів, антиспам/антифішинг, sandbox, CDR, аналіз URL, DLP і керування політиками. У хмарних платформах SEG може бути вбудованим сервісом або стороннім шлюзом між Інтернетом та хмарною поштою. Правильне розміщення SEG визначає, чи бачить він вихідну пошту (важливо для стримування компрометованих розсилок) і чи має доступ до телеметрії для кореляції в SIEM.

1.9. Технічні вразливості та помилки конфігурації як чинники поштових інцидентів

Інциденти часто виникають через накопичення типових помилок конфігурації. До поширених проблем належать: (1) SPF, що перевищує ліміти DNS-запитів або містить надмірні include-ланцюги; (2) відсутність ротації DKIM-ключів або використання слабких ключів; (3) DMARC у режимі p=none без плану посилення; (4) невірне вирівнювання доменів (alignment); (5) неконтрольовані сторонні відправники (CRM, маркетинг); (6) відкриті пересилання назовні або відсутність контролю винятків; (7) слабкі TLS-параметри або відсутність MTA-STS.

Важливим є і рівень DNS-захисту. Оскільки SPF/DKIM/DMARC, MTA-STS і TLS-RPT залежать від DNS, зловмисник може намагатися вплинути на DNS-інфраструктуру (компрометація реєстратора, викрадення облікового запису DNS-провайдера) для зміни політик домену. Тому на практиці доцільно підсилювати доступ до DNS через MFA, розмежування ролей, журналювання змін та періодичний аудит критичних записів.

Ще один клас проблем — «тіньові» піддомени й домени-супутники. Часто DMARC налаштовано лише для основного домену, а піддомени або домени

бренду залишаються без політик. Зловмисники використовують це для імітації адрес із піддоменів, або для реєстрації схожих доменів (typosquatting). Тому аудит доменного простору має включати перелік доменів організації, їхні SPF/DKIM/DMARC політики та контроль оновлень.

1.10. Соціальна інженерія та BEC як центральний ризик для бізнес-процесів

BEC орієнтований на конкретні бізнес-процеси (платежі, закупівлі, зміна реквізитів, юридичні погодження). Типовий сценарій включає: первинне проникнення (фішинг або компрометація пароля), збір інформації з листування, побудову контексту (ланцюжки листів, шаблони підписів), а потім — надсилання інструкції про переказ чи зміну реквізитів від імені керівника або партнера. Ключовим контрзаходом є процедурна верифікація: підтвердження критичних дій через незалежний канал комунікації, розділення обов’язків та ліміти на платежі.

З технічного боку BEC складно детектувати, якщо використано легітимно скомпрометований акаунт. Тоді SPF/DKIM/DMARC проходять перевірки, а листи виглядають «правильними». У таких випадках основним інструментом виявлення стають поведінкові ознаки: нетипова географія входу, незвичні часові інтервали активності, створення правил пересилання, спроби експортів/пошуку в архіві, нетипові адресати та зміни у стилі комунікації. Це підтверджує необхідність інтегрувати поштову телеметрію в SIEM та мати кореляційні правила для BEC-сценаріїв.

Висновки до розділу 1

У першому розділі встановлено, що корпоративна електронна пошта є критичною частиною інформаційної інфраструктури організації та одночасно одним із головних каналів реалізації сучасних кібератак.

Проаналізовано типову архітектуру поштової інфраструктури і визначено контрольні точки, на яких доцільно реалізовувати перевірку джерела, контенту, вкладень, телеметрії та процедур реагування.

Систематизовано основні типи поштових атак - фішинг, спуфінг, BEC/EAC, шкідливі вкладення, компрометацію акаунтів і правила пересилання - та показано, що їх ефективне виявлення потребує багаторівневого підходу.

Визначено, що сучасні вимоги до безпеки електронної пошти формуються поєднанням технічних стандартів IETF, рекомендацій NIST, вимог великих постачальників сервісів, офіційних порад CISA/FBI/Microsoft і національного законодавства України.

Розділ 2 МЕТОДИ ВИЯВЛЕННЯ АТАК НА ІНФРАСТРУКТУРУ ЕЛЕКТРОННОЇ ПОШТИ ОРГАНІЗАЦІЇ

2.1. Доменна автентифікація як базовий метод виявлення підробки відправника

Найбільш фундаментальною групою методів виявлення атак на електронну пошту є перевірка походження повідомлення за допомогою DNS-автентифікації домену. SPF дозволяє домену опублікувати перелік дозволених джерел надсилання пошти і дає можливість приймаючій стороні перевіряти, чи відповідає IP-адреса відправника опублікованій політиці [3]. На практиці SPF є важливим бар’єром проти масового спуфінгу, але не захищає видиме поле From без додаткового механізму вирівнювання.

DKIM додає до листа криптографічний підпис, який перевіряється через DNS-опублікований відкритий ключ [4]. Це дозволяє переконатися, що повідомлення не було змінено після підписання та пов’язане з доменом-підписувачем. Утім DKIM сам по собі не задає політику поводження з невдалими перевірками, тому його ефективність зростає у поєднанні з DMARC.

DMARC поєднує результати SPF і DKIM із вимогою alignment, тобто узгодження домену в полі From із доменом SPF або DKIM [5]. Окрім цього, DMARC надає домену можливість декларувати політику обробки невдалих повідомлень та отримувати агреговані звіти від приймаючих систем. Саме наявність звітів робить DMARC не лише засобом політики, а й важливим джерелом телеметрії для виявлення спроб підробки домену, тіньових сервісів відправлення або помилок конфігурації.

Важливість цієї групи методів посилюється тим, що сучасні великі постачальники сервісів вимагають коректного впровадження SPF, DKIM і DMARC для забезпечення доставлюваності та довіри до домену [8, 9]. Отже, доменна автентифікація є одночасно інструментом безпеки, механізмом видимості атак і критерієм операційної зрілості організації.

Рис. 2.1. Комплекс методів виявлення атак на корпоративну електронну пошту

Таблиця 2.1

Порівняльна характеристика SPF, DKIM та DMARC як інструментів виявлення підробки відправника

Механізм	**Що перевіряє**	**Сильні сторони**	**Обмеження**
SPF	Дозволені IP/хости для MAIL FROM	Простий контроль джерела надсилання	Не захищає поле From, проблеми при пересиланні
DKIM	Цілісність листа та домен-підписувач	Криптографічна перевірка, незалежність від IP	Потрібне коректне налаштування селекторів і ключів
DMARC	Alignment From + політика + звітність	Видимість спуфінгу, можливість quarantine/reject	Потребує якісного SPF/DKIM та поетапного впровадження

2.2. Аналіз заголовків, контенту, URL та вкладень

Наступний рівень виявлення атак пов’язаний з аналізом заголовків, контенту повідомлення, URL та вкладених файлів. Заголовки листа містять цінну телеметрію: маршрут Received, результати Authentication-Results, відомості про Return-Path, ARC, невідповідності між полями From і Reply-To.

Саме аналіз цих елементів дозволяє розпізнавати спуфінг, нетипові шляхи доставки та спроби маскування джерела повідомлення [13].

Контентний аналіз спрямований на виявлення характерних ознак соціальної інженерії: терміновості, фінансового тиску, вимог змінити реквізити, фраз на кшталт «лише сьогодні», «негайно», «конфіденційно», а також нетипових мовних конструкцій і стилістичних відхилень. CISA прямо вказує, що фішинг часто є першою фазою ширшого ланцюга атаки, а тому виявлення підозрілих листів повинно відбуватися до моменту взаємодії користувача з ними [11].

Аналіз URL включає перевірку репутації доменів, пошук typosquatting, використання одноразових або нетипових доменів, порівняння домену посилання з легітимним брендом, а також механізми time-of-click у захищених поштових шлюзах. На практиці це дозволяє виявляти фішингові посилання, навіть якщо під час первинної доставки сторінка ще не містила шкідливого контенту.

Вкладення перевіряються за допомогою сигнатурних, евристичних і поведінкових методів. Особливу увагу необхідно приділяти архівам, документам з активним вмістом, контейнерним форматам, PDF-файлам із вкладеними об’єктами та вкладенням, що потребують запуску макросів або скриптів. З погляду MITRE ATT&CK spearphishing attachment залишається окремою підтехнікою, а отже контроль вкладень має бути обов’язковою складовою системи виявлення [14].

Таблиця 2.2

Типові індикатори підозрілих листів для первинного тріажу

Індикатор	Приклад прояву	Імовірна загроза
Невідповідність From і Reply-To	Лист від керівника, але Reply-To на сторонньому домені	Спуфінг / BEC
Authentication fail	SPF fail, DKIM fail, DMARC fail	Підробка домену або помилка конфігурації
Термінові фінансові вимоги	Прохання терміново змінити реквізити чи оплатити рахунок	BEC / шахрайство
Підозрілий URL	Схожий домен, коротке посилання, сторонній TLD	Фішинг / credential harvesting
Нетипове вкладення	ISO, IMG, JS, архів з паролем	Шкідливе вкладення
Раптова зміна стилю листування	Нетипова мова, граматика, нетиповий час	Компрометація акаунта імперсонація

2.3. Поведінкова аналітика, телеметрія та SIEM-кореляція

Більш складні атаки, зокрема BEC та EAC, не завжди можуть бути впевнено виявлені лише за сигнатурними або контентними ознаками. У таких випадках особливого значення набуває поведінкова аналітика, яка дозволяє порівнювати поточні дії користувача з його типовим профілем активності. Аналізуються час входу, географія, IP-адреси, пристрої, поява нових правил пересилання, спроби доступу до архівних листів та нетипові маршрути комунікації [21, 25, 27, 28].

Microsoft у своїх матеріалах щодо anti-spoofing і реагування на компрометовані поштові акаунти звертає увагу на важливість аналізу заголовків, результатів композитної автентифікації, пересилання та ознак захоплення поштової скриньки [21, 28]. На практиці це означає, що організація повинна збирати телеметрію не лише з поштового шлюзу, а й із самої платформи електронної пошти, систем автентифікації та SIEM.

У SIEM доцільно будувати кореляційні правила для таких послідовностей: невдала DMARC-перевірка + масова зовнішня доставка; аномальний вхід + створення правила пересилання; фішинговий лист + клік по URL + подальший вхід у поштовий акаунт з нового пристрою. Такий підхід дозволяє переходити

від детекції окремого листа до виявлення завершеного ланцюга атаки та зменшує ймовірність пропуску BEC-сценаріїв.

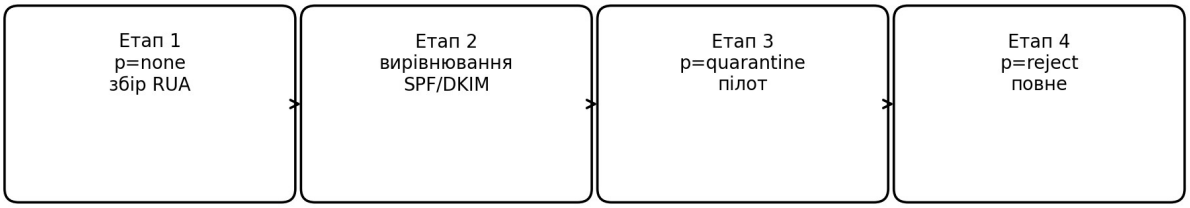

Рис. 2.2. Поетапне впровадження DMARC-політики як джерела телеметрії та інструмента посилення детекції

2.4. Моніторинг DMARC-звітування та виявлення спроб підміни домену

Практична цінність DMARC полягає не лише в застосуванні політики quarantine або reject, а й у постійному отриманні телеметрії через агреговані звіти rua. Аналіз таких звітів дає змогу визначати реальні джерела надсилання, результати SPF і DKIM, а також ступінь вирівнювання домену у полі From. Це дозволяє виявляти як цілеспрямовані спроби підміни бренду, так і помилки конфігурації легітимних сервісів, що надсилають пошту від імені організації [5, 17].

Для практичної детекції доцільно застосовувати порогові правила: поява нових ASN або географій у звітах, різке зростання частки fail, повторювані підміни піддоменів і нестандартні джерела надсилання. У поєднанні з журналами шлюзу та SOC-моніторингом це дає змогу своєчасно відокремити атаку на бренд від внутрішньої помилки конфігурації.

Таблиця 2.3

Джерела телеметрії для виявлення підміни домену та компрометації акаунта

Джерело	Що контролюється	Типові сигнали

DMARC-звіти (rua)	Джерела відправлення, SPF/DKIM/alignment	Нові ASN, сплеск fail, підміна піддоменів
Логи поштового шлюзу	URL, вкладення, рішення фільтрів	Повторні кампанії, масова доставка
Аудит поштової скриньки	Правила, пересилання, делегування	Зовнішнє пересилання, приховане видалення
Логи автентифікації	Географія, IP, MFA, сесії	Аномальний вхід, зміна MFA, новий пристрій

2.5. Детекція компрометації поштових акаунтів: правила пересилання та збір пошти

Ознаками компрометації поштової скриньки є створення правил автоматичного пересилання на зовнішні адреси, приховане видалення або переміщення листів, додавання делегатів, а також зміни параметрів MFA чи recovery-налаштувань. Такі дії часто супроводжують BEC та EAC-інциденти, коли зловмисник намагається зберегти непомітний доступ до листування [10, 21].

У межах MITRE ATT&CK ці сценарії пов’язані з техніками Email Collection (T1114) та Email Forwarding Rule (T1114.003), тому їх доцільно окремо контролювати і корелювати з аномальними входами, змінами правил поштової скриньки та несподіваною масовою зовнішньою комунікацією [15–16].

2.6. Практика тріажу SOC: класифікація інцидентів та пріоритезація

Ефективність виявлення поштових атак залежить від швидкого та стандартизованого тріажу. Доцільно уніфікувати класи інцидентів щонайменше на п’ять груп: фішинг, спуфінг, BEC, шкідливе вкладення та компрометація акаунта. Для кожної групи слід визначити мінімальний набір артефактів: повні заголовки листа, URL, хеш вкладення, результати DMARC/SPF/DKIM, журнали шлюзу та події автентифікації.

Пріоритезація має враховувати критичність адресата, наявність фінансових інструкцій, ознаки постексплуатації (пересилання, делегування, приховане видалення листів), а також масштаби розсилання. Такий підхід скорочує час MTTD і MTTR та підвищує відтворюваність рішень аналітиків SOC [18].

2.7. Ознаки та індикатори для виявлення фішингу: заголовки, лексика, URL та контекст

У детекції фішингу доцільно застосовувати багаторівневий набір ознак. На рівні заголовків аналізуються: ланцюжок Received, результати автентифікації (Authentication-Results), можливі ознаки підміни Reply-To, а також нетипові параметри клієнта відправника. На рівні вмісту оцінюються тригери соціальної інженерії (терміновість, погрози, авторитет), структура повідомлення (кнопки, заклики до входу), нестандартні вкладені форми та лексичні патерни.

URL-аналіз є критично важливим, оскільки більшість фішингових атак використовують посилання на підробні сторінки входу. URL розглядається як об’єкт із власними ознаками: довжина та ентропія домену, кількість піддоменів, використання скорочувачів, punycode/IDN, редиректи, свіжість домену, репутація IP та ASN. Особливо корисний підхід time-of-click, коли перевірка виконується під час кліку користувача, оскільки зловмисники можуть змінювати вміст сторінки після доставки листа.

Контекстні ознаки дозволяють зменшити хибнопозитивні спрацювання. Наприклад, лист із проханням «терміново оплатити» трактується інакше, якщо

він надійшов адресату з фінансового підрозділу від нового домену та містить зміну реквізитів. Комбінування сигналів (новий домен + терміновість + фінанси + зовнішній URL) підвищує точність тріажу, тому у SIEM/SEG бажано використовувати правила на основі композиції ознак.

2.8. Машинне навчання в антифішингу: ознаки, моделі та ризики обходу

Антифішингові рішення застосовують машинне навчання для класифікації листів. Типова побудова включає підготовку набору ознак і навчання моделей, що відрізняють фішингові повідомлення від легітимних. До груп ознак належать: лексичні (n-грамні, частотні, ключові слова), структурні (наявність HTML, кнопок, форм), технічні (домени, результати SPF/DKIM/DMARC, маршрути) та поведінкові (історія взаємодії користувачів, частота кліків).

Водночас ML-моделі мають ризики обходу: модифікації тексту, заміна символів, вставка «шуму», використання зображень замість тексту або легітимних хостингів для розміщення фішингового контенту. Тому в корпоративному середовищі важливо поєднувати ML-підхід із правилами, репутаційними джерелами та sandbox-перевірками, а також постійно вимірювати precision/recall, FPR та операційні показники MTTD/MTTR.

2.9. Кореляція подій у SIEM і автоматизація реагування (SOAR) для поштових інцидентів

Ефективність виявлення поштових атак зростає, коли сигнали з різних джерел об’єднуються в SIEM. Джерела включають: події SEG, журнали SMTP/MTA, DMARC-агреговані звіти, логи автентифікації (MFA/Conditional Access), аудит поштової скриньки (правила, пересилання, делегування) та

телеметрію кінцевих точок (EDR). Кореляція дозволяє будувати сценарії: фішинговий лист → клік → ризиковий вхід → створення правила пересилання → спроба BEC.

SOAR-автоматизація використовується для швидких дій: видалення листів зі скриньок, блокування доменів/URL, відкликання сесій, тимчасове блокування акаунта, створення інциденту та сповіщення відповідальних осіб. Для дій із високим впливом застосовується підхід людина в контурі ухвалення рішення (human-in-the-loop), коли ключові кроки підтверджує SOC-аналітик.

2.10. Захист транспортного рівня та детекція downgrade-атак: TLS, MTA-STS, TLS-RPT

Захист транспортного рівня в електронній пошті базується на коректному використанні TLS, а також на політиках MTA-STS і телеметрії TLS-RPT. Ці механізми дозволяють не лише підвищити конфіденційність доставки, а й виявляти проблеми узгодження шифрування та спроби downgrade-атак.

2.11. Контроль автентифікації та вирівнювання доменів: інтерпретація Authentication-Results

Практичний аналіз поштових атак потребує коректної інтерпретації заголовка Authentication-Results, а також перевірки alignment між доменом From і доменами, що пройшли SPF або DKIM. Саме ця логіка лежить в основі адекватного використання DMARC під час виявлення спуфінгу.

2.12. Поглиблена перевірка вкладень: макроси, контейнери, sandbox та CDR

Поглиблена перевірка вкладень має охоплювати як статичний аналіз типу файлу, так і динамічне виконання у sandbox. Для корпоративного середовища особливо критичні документи з макросами, архіви з паролем, PDF із вбудованими об’єктами та контейнерні формати.

2.13. Хмарні сценарії атак: OAuth-зловживання, сторонні застосунки та ексфільтрація пошти

У хмарних середовищах з’являються специфічні сценарії атак, пов’язані не лише з паролями, а й з токенами та сторонніми застосунками. Зловмисники можуть домагатися надання дозволів (consent phishing), коли користувач погоджується на доступ застосунку до пошти/контактів. У результаті навіть без пароля атакувальник може читати повідомлення, відправляти листи або налаштовувати правила. Для детекції таких сценаріїв важливо контролювати журнали consent, перелік застосунків, обсяги доступу та нетипові операції з даними. [40].

Ексфільтрація пошти у хмарі може проявлятися через масовий експорт листів, читання великих обсягів повідомлень, часті запити до поштового API або створення правил пересилання на зовнішні адреси. Тому необхідно мати контроль за правилами inbox, пересиланням, делегуванням та змінами конфігурації. Це також підкреслює важливість інтеграції журналів поштової платформи з SIEM, щоб корелювати доступи, зміну налаштувань і подальші дії зловмисника.

2.14. Форензіка поштових заголовків: Received-ланцюжок, Return-Path, Reply-To та аномалії маршруту

Форензічний аналіз поштових заголовків є базовою навичкою для SOC, оскільки саме заголовки містять технічні артефакти про шлях доставки та параметри автентифікації. У практиці розслідувань аналізують: (1) Received-ланцюжок, який описує послідовність серверів, що обробляли лист; (2) Return-Path (конвертний відправник), який використовується для bounce-повідомлень і часто відрізняється від From:; (3) Reply-To, який може бути підмінений для переведення відповіді на сторонню адресу; (4) Message-ID та інші службові поля, що інколи дозволяють ідентифікувати інструменти розсилки або фішингові комплекти.

Типові аномалії маршруту включають: нетипові домени/хости в Received, «дірки» у ланцюжку, невідповідність часових міток, згадки про рідкісні поштові клієнти, або доставка через неочікувані географічні сегменти. У поєднанні з Authentication-Results такі ознаки допомагають відокремлювати легітимні пересилання від зловмисної інфраструктури. Для автоматизації частину аналізу можна реалізувати у вигляді регулярних правил у SIEM (наприклад, виявлення нових доменів у Reply-To або різкої зміни типового маршруту для домену партнера). [34]

2.15. ARC, пересилання та збереження довіри: детекція атак у складних ланцюжках доставки

Окремою практичною проблемою є пересилання (forwarding) та повторна обробка листів через проміжні системи (розсилки, helpdesk, шлюзи), що може порушувати SPF і інколи DKIM. У таких сценаріях механізм ARC (Authenticated Received Chain) дозволяє зберегти інформацію про результати автентифікації на попередніх вузлах і забезпечити кращу інтерпретацію довіри

під час кінцевого отримання листа. Для SOC це означає, що переслані листи не слід автоматично вважати підозрілими лише через SPF fail; необхідно враховувати DKIM/DMARC, ARC-ланцюжок і контекст відправника.

З позиції детекції важливо розділяти легітимні сценарії пересилання від спроб обходу. Зловмисники можуть використовувати легітимні поштові сервіси або скомпрометовані скриньки як «ретранслятори» для підвищення довіри. Тому корисними є детекції на основі: нових проміжних доменів у ланцюжку, невідповідності доменів у From/Reply-To, підозрілих URL, а також нетипових шаблонів листування. У практичній політиці рекомендується мати окремі правила для пересланих листів: знижувати вагу SPF, але підвищувати вагу контентних і контекстних ознак.

2.16. DLP-ознаки та захист від витоку даних через пошту: детекція ексфільтрації

Електронна пошта часто використовується як канал витоку даних: як випадково (помилка адресата), так і навмисно (внутрішній інсайдер або компрометований акаунт). Деякі організації впроваджують DLP-контроль на рівні поштових шлюзів або хмарних платформ: пошук конфіденційних патернів (персональні дані, фінансові реквізити), контроль вкладень, політики шифрування та блокування пересилання назовні. З точки зору детекції корисними є сигнали: різке збільшення обсягу вихідних вкладень, надсилання на нові зовнішні домени, масові листи з вкладеннями, або надсилання архівів/контейнерів у нестандартні години.

Для SOC доцільно мати окремі правила на ексфільтрацію: (1) outbound-листи з вкладеннями > певного розміру до зовнішніх доменів; (2) створення правила автоматичного пересилання + паралельне збільшення обсягу вихідного трафіку; (3) спроби надсилати зашифровані архіви або «невідомі» типи файлів.

Такі правила мають враховувати бізнес-контекст (наприклад, легітимні великі листи від бухгалтерії) і працювати як тригер для тріажу.

2.17. Threat hunting у поштовій телеметрії: гіпотези, запити та типові патерни

Окрім реактивної детекції, організація може застосовувати threat hunting — проактивний пошук ознак компрометації у поштових даних. Основою hunting є гіпотези, наприклад: «чи є в організації приховані правила пересилання назовні?», «чи були входи з нетипових локацій без MFA?», «чи з’явилися нові домени у Reply-To для фінансових листів?». Під такі гіпотези формуються запити до журналів платформи пошти, SEG та SIEM.

Приклади практичних hunting-патернів: (1) знайти всі нові правила inbox, створені за останні N днів, що пересилають листи назовні; (2) знайти акаунти з великою кількістю невдалих входів, після яких з’явилися успішні входи; (3) знайти листи, де From належить домену партнера, але DMARC fail або Reply-To веде на інший домен; (4) знайти вибірки за ключовими словами BEC («invoice», «urgent», «wire», «change bank details») у поєднанні з новими доменами. Такі пошуки дозволяють знаходити «тихі» інциденти до того, як вони завдадуть збитків.

2.18. Оцінювання якості детекцій: тестові сценарії, контроль хибних спрацювань і зворотний зв’язок

Щоб детекції залишались ефективними, необхідно регулярно їх перевіряти. Практичні підходи включають: (1) симуляції фішингу з вимірюванням кліків і реакцій користувачів; (2) тестові кампанії з контрольними листами для перевірки SEG-правил; (3) періодичні перевірки DMARC/TLS-RPT телеметрії; (4) аналіз хибнопозитивних/хибнонегативних

кейсів із подальшим коригуванням правил. Зворотний зв’язок від користувачів (кнопка Report Phishing) є важливим каналом, який підвищує покриття детекції.

Окрема увага має приділятися балансуванню безпеки та доставлюваності. Надмірно жорсткі правила можуть блокувати легітимні листи і створювати операційні ризики. Тому в зрілій моделі часто застосовується поєднання карантину, м’яких політик для сумнівних кейсів і жорстких політик для підтверджених загроз. Це дозволяє зменшити ризик пропуску атак без критичних втрат для бізнес-процесів.

2.19. Приклади кореляційних правил SIEM для поштових атак (без реалізації коду)

Нижче наведено приклади логіки кореляційних правил, які можуть застосовуватися у SIEM для підвищення якості детекції. Опис подано концептуально (без конкретної мови запитів), щоб його можна було адаптувати під будь-яку платформу (Microsoft Sentinel, Splunk тощо).

Правило 1 (фішинг-ланцюжок): подія «лист позначено як підозрілий» або «URL має погану репутацію» на SEG → протягом N хвилин фіксується клік користувача по URL → протягом M хвилин фіксується ризиковий вхід у пошту (новий пристрій/гео/IP) → після цього з’являється нове правило пересилання або делегування. Така послідовність є сильною ознакою успішного фішингу з постексплуатацією.

Правило 2 (BEC-ознаки): лист із фінансовими ключовими словами (invoice, payment, urgent, bank details) → зовнішній відправник або новий домен у Reply-To → відсутність історії комунікації з доменом/адресою → адресат належить до фінансових ролей. У разі спрацювання запускається playbook підтвердження через незалежний канал.

Правило 3 (експлуатація скриньки): успішний вхід у пошту після великої кількості невдалих входів → створення/зміна правил inbox → пересилання

назовні або приховане переміщення листів → паралельне зростання обсягу вихідних листів. Комбінація сигналів вказує на компрометацію акаунта та спроби приховати активність.

Правило 4 (атака на бренд): різке зростання DMARC fail за даними RUA-звітів → поява нових IP/ASN у джерелах → лист із From домену організації доставляється масово на зовнішні домени. Це може свідчити як про спуфінг бренду, так і про витік каналу розсилки.

Правило 5 (TLS downgrade): зростання частки доставок без TLS або з помилками TLS-RPT для критичних партнерських доменів → одночасно зростає кількість фішингових листів «від партнера». Це не доводить атаку, але є сигналом для технічної перевірки маршруту та сертифікатів.

2.20. Кейсовий сценарій атаки на пошту: kill-chain від фішингу до BEC (приклад)

Нижче наведено узагальнений сценарій атаки, який часто зустрічається у практиці. Він демонструє, чому потрібні багаторівневі методи виявлення та протидії.

Етап 1 — Розвідка: зловмисник збирає дані про організацію (публічні контакти, постачальники, шаблони листування). Етап 2 — Доставка: надсилає фішинговий лист із посиланням на підробну сторінку входу або вкладенням. Етап 3 — Компрометація: користувач вводить дані або відкриває вкладення, що призводить до викрадення токена/пароля або виконання шкідливого коду. Етап 4 — Закріплення: атакувальник заходить у пошту, створює правило пересилання назовні, додає делегата або змінює налаштування MFA. Етап 5 — Розвиток: аналізує ланцюжки листування, знаходить фінансові процеси, підготовлює BEC-лист. Етап 6 — Вплив: надсилає інструкцію про переказ або зміну реквізитів, маскує активність через правила inbox. Етап 7 —

Приховування: видаляє або переміщує листи, щоб жертва не бачила ознак компрометації.

Детекція у цьому сценарії можлива на кожному етапі: (1) на етапі доставки — SPF/DKIM/DMARC і контентний аналіз; (2) на етапі компрометації — сигнали клік/ризиковий вхід; (3) на етапі закріплення — аудит правил пересилання та делегувань; (4) на етапі впливу — BEC-патерни в листах і процедурні контрзаходи. Отже, ефективність забезпечується не одним механізмом, а узгодженою системою контролів. [41]

2.21. Практичний чекліст для SOC: артефакти й питання для тріажу поштових інцидентів

Для уніфікованого тріажу SOC доцільно використовувати стандартизований чекліст. Мінімальний набір артефактів має включати повні заголовки листа, результати SPF/DKIM/DMARC, оригінальні та розгорнуті URL, хеші вкладень, журнали кліків, журнали автентифікації користувача, дані про правила пересилання та делегування, а також журнал дій у поштовій скриньці.

Окрім збору артефактів, аналітик повинен поставити контрольні питання: чи є фінансові або кадрові інструкції, чи відомий відправник адресату, чи змінювалися реквізити, чи є ознаки компрометації акаунта, чи потрібно активувати BEC-процедуру підтвердження через незалежний канал. Такий підхід зменшує суб’єктивність тріажу та пришвидшує прийняття рішень.

2.22. Криптографічний захист листування: S/MIME як сигнал довіри та інструмент протидії підміні

Криптографічні механізми захисту електронної пошти можуть виступати одночасно контрзаходом і джерелом сигналів для детекції. Найпоширеніший

корпоративний підхід — застосування S/MIME для цифрового підпису та, за потреби, шифрування повідомлень. Цифровий підпис S/MIME забезпечує цілісність листа та підтверджує, що лист був сформований власником сертифіката, а шифрування — конфіденційність даних у тілі повідомлення. На практиці S/MIME доцільно впроваджувати насамперед для критичних процесів (фінанси, юридичні погодження, робота з платіжними інструкціями), де необхідні гарантії цілісності та неможливість непомітної підміни.

З позиції виявлення атак криптографічні підписи корисні як «якір довіри»: якщо для певного типу листів підпис є обов'язковим, то відсутність підпису стає аномалією та підставою для додаткової перевірки. Аналогічно, якщо організація підписує вихідну пошту S/MIME, але раптом з'являються листи з «того ж» імені без підпису, це може бути індикатором спуфінгу або підміни каналу комунікації. Отже, вимога підпису для критичних листів знижує ризики BEC, але потребує керованої PKI-інфраструктури, підтримки клієнтів і дисципліни процесів.

Водночас важливо враховувати обмеження: S/MIME не замінює SPF/DKIM/DMARC і не захищає від компрометації акаунта, якщо зловмисник отримав доступ до ключів або підписує листи з легітимного клієнта. Тому S/MIME розглядається як додатковий шар defense-in-depth, який підсилює довіру до критичних повідомлень і допомагає формалізувати правила тріажу. [35] [36]

2.23. Візуальна довіра до бренду: BIMI, логотипи та ризики хибної впевненості користувачів

Окрім технічної автентифікації, у практиці з'явилися механізми підсилення візуальної довіри до домену, зокрема BIMI (Brand Indicators for Message Identification). BIMI дозволяє відображати підтверджений логотип бренду у поштових клієнтах за умови коректно налаштованого DMARC (як

правило, на рівні quarantine/reject). З одного боку, це може зменшувати успішність підробок, оскільки користувачі бачать «офіційний» логотип. З іншого боку, BIMI може створювати ризик хибної впевненості: користувачі можуть вважати лист без логотипу підозрілим, але водночас ігнорувати інші ознаки загрози в листах із логотипом, якщо атакувальник використав легітимно скомпрометований акаунт.

Тому BIMI варто розглядати як допоміжний інструмент, який працює лише у зв'язці з DMARC і навчанням персоналу. Для SOC важливо враховувати, що «наявність/відсутність логотипу» не є надійною ознакою безпеки, а скоріше фактором користувацького інтерфейсу. Практична рекомендація: у навчальних матеріалах чітко пояснювати, що навіть «правильний» вигляд листа не гарантує його безпечність, і завжди потрібна перевірка доменів, URL та контексту. [37] [38] [39]

2.24. DNSSEC та цілісність DNS-записів як фактор надійності SPF/DKIM/DMARC

Оскільки ключові механізми автентифікації електронної пошти залежать від DNS (SPF, DKIM, DMARC, MTA-STS, TLS-RPT), цілісність і доступність DNS-записів безпосередньо впливають на безпеку поштового домену. DNSSEC забезпечує криптографічне підписання відповідей DNS, що зменшує ризик підміни записів під час резолвінгу. У контексті електронної пошти це означає, що зловмиснику складніше підмінити DKIM-ключі або DMARC-політики через атаки на канали DNS-резолвінгу.

Водночас DNSSEC не вирішує проблему компрометації облікового запису DNS-провайдера або реєстратора домену, тому ключовими залишаються організаційні заходи: MFA для доступу до DNS, журналювання змін, контроль ролей, процедури підтвердження критичних змін (change management). Практично доцільно мати «еталон» критичних DNS-записів і автоматизовані

перевірки відхилень, оскільки навіть випадкова помилка у DMARC або MTA-STS може вплинути на доставку і безпеку. [41] [42]

2.25. Нові тактики фішингу: QR-фішинг, зображення замість тексту та обхід контентних фільтрів

Зловмисники адаптують фішингові кампанії до розвитку фільтрів. Однією з сучасних тактик є використання QR-кодів у листах (QR-phishing), коли посилання «заховане» в зображенні, а користувач відкриває його зі смартфона. Такий підхід може обходити частину URL-фільтрів, якщо перевірка орієнтована на текстові посилання. Інша тактика — використання зображень замість тексту (image-based phishing), що знижує ефективність лексичного аналізу.

Для протидії таким обхідним технікам доцільно: (1) застосовувати аналіз зображень у SEG (за можливості) або принаймні правила, що підвищують ризик, якщо лист містить лише зображення; (2) блокувати або маркувати листи з вкладеними QR-кодами для додаткової перевірки; (3) навчати персонал розпізнавати QR-фішинг і не сканувати коди з неочікуваних листів; (4) використовувати time-of-click перевірки та ізоляцію браузера (remote browser isolation) для підозрілих посилань. Таким чином, контентні обходи компенсуються комбінуванням технічних і поведінкових контролів.

2.26. Техніки обходу автентифікації: підміна display-name, lookalike домени та підробка ланцюжків листування

Навіть за наявності SPF/DKIM/DMARC зловмисники можуть застосовувати прийоми, спрямовані на людське сприйняття. Поширений обхід — підміна відображуваного імені (display-name spoofing), коли поле From:

містить легітимне ім’я (наприклад, «Директор»), але фактична адреса належить іншому домену. Інший варіант — використання lookalike доменів (typosquatting та IDN-homoglyph), де різниця в 1–2 символи майже непомітна. Також атакувальники підробляють ланцюжки листування (thread hijacking): додають префікси Re:/Fwd:, копіюють стиль попередніх листів, інколи вставляють фрагменти реальної переписки, отримані з витоків або з компрометованих акаунтів.

Для детекції таких обходів доцільно застосовувати комбінацію: (1) політики маркування зовнішніх відправників; (2) правила, що підвищують ризик при розбіжності display-name і домену; (3) виявлення схожих доменів (string distance, punycode) і попередження користувачів; (4) контекстні ознаки: чи є в домені історія комунікацій, чи збігаються адресати, чи є зміна реквізитів. У випадках BEC критичними залишаються процедурні контрзаходи (підтвердження поза поштою), оскільки «візуально правдоподібні» листи часто обходять суто технічні фільтри.

2.27. Приклади типових артефактів фішингу та BEC для навчання користувачів і SOC

Для навчання користувачів і SOC доцільно мати каталог типових артефактів фішингу та BEC: нетипові домени у From або Reply-To, розбіжність між Return-Path і From, посилання на нові або схожі домени, прохання терміново виконати платіж, змінити реквізити або зберігати конфіденційність, вкладення з макросами чи архіви з паролем.

Практична користь такого каталогу полягає в тому, що він допомагає одночасно навчати персонал і стандартизувати первинний аналіз інцидентів. Для користувача це короткий набір сигналів небезпеки, а для SOC — орієнтир, які ознаки потрібно перевірити насамперед під час фішингового або BEC-кейсу.

Висновки до розділу 2

У другому розділі розглянуто ключові методи виявлення атак на електронну пошту: доменну автентифікацію, аналіз заголовків і контенту, перевірку URL та вкладень, а також поведінкову аналітику на основі телеметрії.

Показано, що SPF, DKIM і DMARC формують базовий рівень виявлення підробки відправника, але для виявлення складних сценаріїв BEC/EAC необхідно поєднувати ці засоби з аналізом контексту, телеметрії та кореляцією подій у SIEM.

Отримані результати формують теоретичну та практичну основу для побудови комплексної моделі захисту, розроблення етапів реагування та підготовки прикладних рекомендацій щодо підвищення кіберстійкості поштової інфраструктури організації.

Розділ 3 МЕТОДИ ПРОТИДІЇ АТАКАМ НА ІНФРАСТРУКТУРУ ЕЛЕКТРОННОЇ ПОШТИ ОРГАНІЗАЦІЇ

3.1. Багаторівнева модель захисту поштової інфраструктури

Методи протидії атакам на інфраструктуру електронної пошти повинні будуватися за принципом багаторівневого захисту. Якщо розділ 2 був зосереджений на виявленні шкідливої активності, то на цьому етапі увага переноситься на організацію таких контрзаходів, які або не допускають реалізації атаки, або істотно зменшують її наслідки. На практиці йдеться про поєднання доменної автентифікації, транспортного захисту, антифішингових політик, захисту кінцевих точок, обмеження привілеїв, резервування, а також узгоджених процедур реагування [17], [18].

Базовим рубежем протидії є правильна побудова маршруту проходження листа: від DNS-політик домену до поштового шлюзу, сервера обробки й користувацького клієнта. На кожному з цих етапів застосовуються власні засоби стримування. Для домену це SPF, DKIM і DMARC; для транспортного каналу - MTA-STS і TLS-RPT; для шлюзу - антиспам, антифішинг, перевірка URL, sandbox, репутаційні механізми; для кінцевих вузлів - EDR, контроль макросів і обмеження небезпечних типів вкладень [6], [7], [13], [25].

Важливо розуміти, що окремий контроль не може повністю усунути ризик. Наприклад, DMARC добре протидіє класичному спуфінгу бренду, але не захищає від компрометації легітимного акаунта або від BEC-атаки, що походить із реально зламаної поштової скриньки. З цієї причини ефективна протидія передбачає не тільки блокування листа на вході, а й додаткові політики поведінкового аналізу, сегментацію доступу, контроль дій користувача та дії SOC після виявлення аномалії [10], [21].

Окрему увагу слід приділити ситуаціям, коли легітимне повідомлення модифікується проміжними сервісами, наприклад під час пересилання або

проходження через системи додавання підписів чи списків розсилки. У таких випадках стандартна логіка SPF або DKIM може порушуватися, хоча лист походить із законного джерела. Для збереження контексту автентифікації застосовується ARC - Authenticated Received Chain, який дозволяє фіксувати ланцюг перевірок і робити більш обґрунтоване рішення щодо довіри до повідомлення [22], [26].

Ще один важливий напрям протидії пов'язаний із криптографічним захистом змісту листів. У сценаріях, де електронна пошта використовується для юридично значущих або фінансово критичних дій, доцільним є застосування S/MIME. Цей механізм забезпечує цифровий підпис, перевірку цілісності та за потреби конфіденційність повідомлення. Хоча S/MIME не вирішує проблему фішингу як таку, він підвищує довіру до офіційних повідомлень організації та знижує ризик їх непомітної модифікації [23].

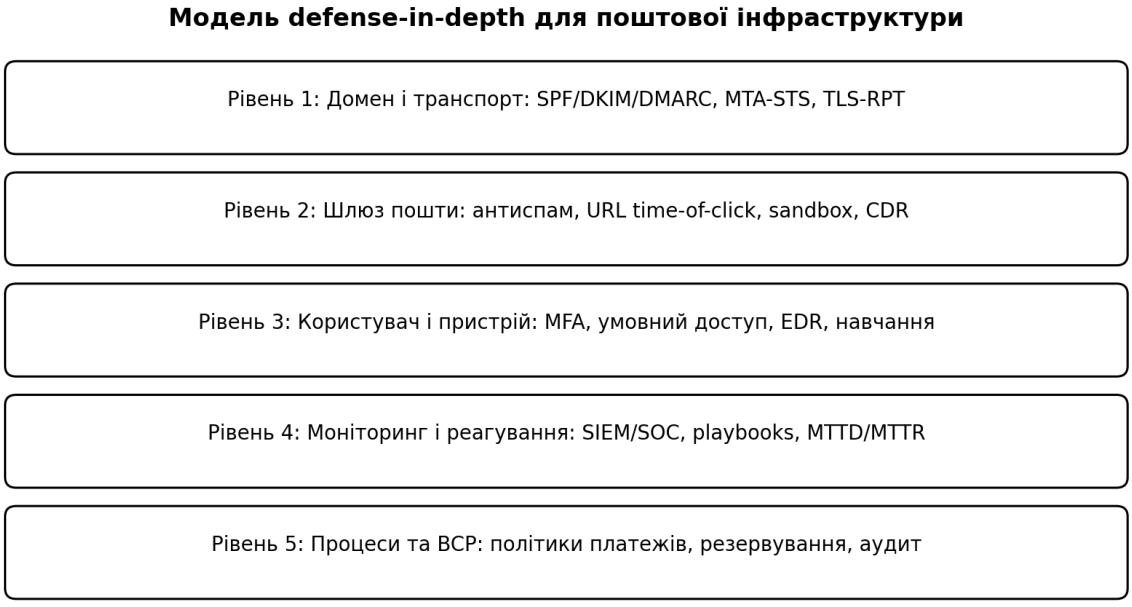

Рис. 3.1. Багаторівнева модель захисту поштової інфраструктури організації

Таблиця 3.1

Матриця відповідності загроз і основних контрзаходів

Загроза	**Базові контрзаходи**	**Додаткові заходи**

Спуфінг домену	SPF, DKIM, DMARC	ARC, моніторинг RUA/RUF-звітів
Фішинг із URL	SEG, URL reputation, time-of-click	навчання користувачів, browser isolation
Шкідливі вкладення	sandbox, AV, CDR	EDR, блокування типів файлів, контроль макросів
BEC/EAC	MFA, умовний доступ, аудит правил	двоканальне підтвердження платежів, SIEM-кореляція
Компрометація MTA/маршруту	MTA-STS, TLS-RPT, hardening	сегментація, резервування, SOC-моніторинг

3.2. Технічні та організаційні контрзаходи проти фішингу, спуфінгу та BEC

Успішна протидія фішингу починається не з одиничного фільтра, а з правильно побудованої політики безпечної доставки пошти. Microsoft у документації щодо anti-phishing protection та anti-spoofing protection звертає увагу на необхідність комбінувати інтелектуальний аналіз спуфінгу, захист від impersonation, перевірку доменів, а також настройки для індикаторів недостовірного відправника у клієнтах [27], [28], [29]. Для корпоративного середовища це означає, що технічна протидія має супроводжуватися чітко визначеними винятками, пріоритетами й регулярним переглядом політик.

Одним з найважливіших запобіжників проти захоплення акаунтів є багатофакторна автентифікація. CISA підкреслює, що MFA є простим і водночас високоефективним заходом для блокування типових сценаріїв компрометації доступу [12], [30]. Проте у випадку сучасних AiTM-фішингових атак однієї MFA може бути недостатньо. Тому організація повинна поєднувати MFA з умовним доступом, перевіркою стану пристрою, ризикових входів,

географічних аномалій, а також із можливістю швидко відкликати токени та активні сесії після інциденту [21], [25].

Контрзаходи проти BEC не можуть бути суто технічними. Через те що зловмисники намагаються імітувати звичні бізнес-процеси та довірених контрагентів, слід вводити організаційні правила: підтвердження зміни платіжних реквізитів через незалежний канал, двоетапне погодження термінових платежів, обмеження прав одного користувача на весь фінансовий цикл, а також обов'язкову перевірку листів із нетиповими вимогами [10], [18]. Саме поєднання організаційних процедур і технічного моніторингу знижує успішність BEC-сценаріїв.

Для поштових акаунтів керівників, фінансових працівників, HR та закупівель доцільно застосовувати посилені профілі захисту. Вони можуть передбачати жорсткіші пороги фішингових політик, окремі правила моніторингу impersonation, заборону зовнішнього автоматичного пересилання, а також пріоритетне опрацювання інцидентів. Такий підхід відповідає ризик-орієнтованій логіці NIST CSF 2.0, де захист будується від критичності бізнес-функції та наслідків компрометації [18], [30].

Окрему практичну роль відіграє керованість легітимних масових розсилок. Коректна підтримка механізмів List-Unsubscribe і one-click unsubscribe не є прямим антиатакувальним контролем, проте зменшує кількість скарг, підвищує репутацію домену та допомагає відрізняти санкціоновані кампанії організації від зловмисної імітації. Це особливо важливо для великих доменів, де поштовий канал використовується і для операційної, і для маркетингової комунікації [8], [24].

Таблиця 3.2

Організаційні та технічні заходи протидії поштовим атакам

Група заходів	**Приклади реалізації**	**Очікуваний ефект**
Доменна автентифікація	SPF/DKIM/DMARC, ARC	зменшення спуфінгу та

		підробки бренду
Захист акаунтів	MFA, умовний доступ, контроль сесій	зниження ризику EAC та крадіжки доступу
Політики пошти	антифішинг, антиспуф, quarantine, allow/block lists	менше доставлених шкідливих листів
Організаційні процедури	перевірка реквізитів, двоканальне підтвердження	зменшення BEC-втрат
Навчання	тренування фішингу, інструктажі, playbooks	зростання стійкості персоналу

3.3. Реагування на інциденти та відновлення працездатності

Навіть за наявності розвиненої системи фільтрації організація повинна виходити з того, що частина поштових атак може пройти початковий рубіж захисту. Саме тому ключове значення має не лише профілактика, а й якість реагування на інцидент. NIST SP 800-61 Rev. 3 визначає реагування як безперервний управлінський і технічний процес, який включає підготовку, виявлення, аналіз, стримування, ліквідацію, відновлення та подальше вдосконалення [18].

Для інцидентів електронної пошти це означає необхідність швидко зібрати технічні артефакти: повні заголовки листа, вкладення, URL, результати перевірок SPF/DKIM/DMARC, журнали автентифікації, дії в поштовій скриньці, створені правила пересилання і події кінцевої точки. На основі цього виконується тріаж: визначається, чи йдеться про спробу фішингу, масову кампанію, компрометацію акаунта або BEC-сценарій [11], [21].

Стримування інциденту в контексті електронної пошти включає видалення або quarantine вже доставлених листів, блокування пов'язаних доменів і URL, ізоляцію вкладень, примусову зміну пароля, відкликання токенів, видалення правил пересилання та перевірку інших поштових скриньок на аналогічні індикатори. Якщо інцидент має фінансовий або юридичний вимір, слід

паралельно активувати бізнес-процедури та альтернативні канали комунікації [10], [21].

Етап відновлення полягає не тільки у поверненні сервісу до нормального стану, а й у перевірці, що загроза не збереглася в латентній формі. Необхідно повторно оцінити конфігурації безпеки, перевірити оновлені політики, провести аналіз охоплення інциденту та зафіксувати lessons learned. Для організації з розвиненою системою управління безпекою це стає підставою для оновлення playbooks, навчальних програм і контрольних переліків [17], [18], [33].

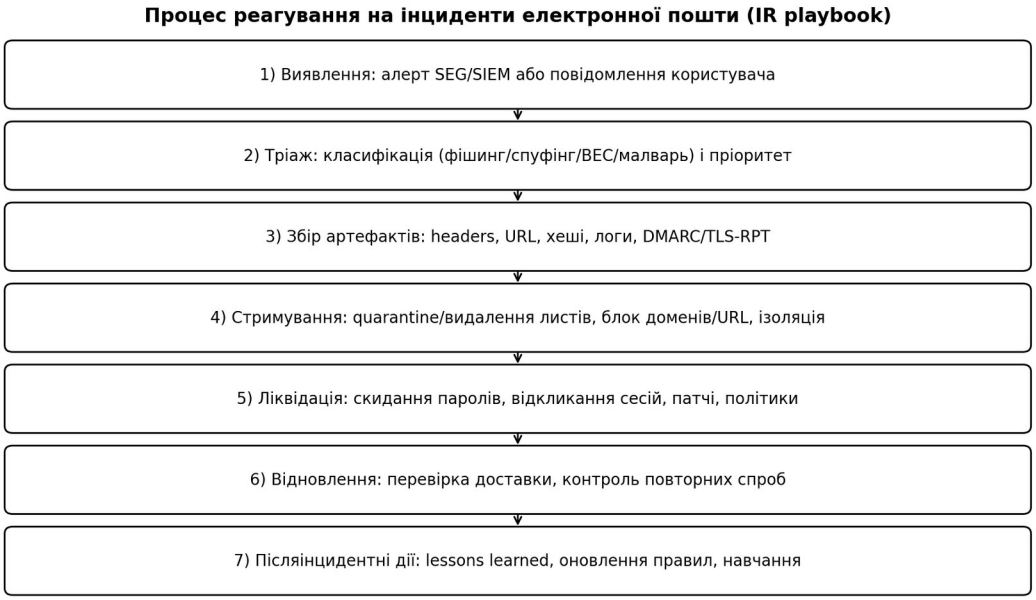

Рис. 3.2. Узагальнений процес реагування на інциденти електронної пошти

3.4. Побудова багаторівневого захисту: Defense-in-Depth для електронної пошти

Побудова ефективного захисту поштової інфраструктури базується на принципі defense-in-depth, коли декілька шарів контролів покривають різні етапи атаки: від доставки листа до постексплуатації у поштовій скриньці. На практиці організації впроваджують поєднання доменної автентифікації, транспортних політик, шлюзових контролів, контролів доступу та моніторингу з реагуванням.

Критично важливо забезпечити узгодженість політик на всіх каналах надсилання. Якщо автентифікація домену, політики шлюзу, контроль акаунтів і процеси SOC працюють розрізнено, виникають як операційні ризики, так і вікна для обходу захисту. Саме тому багаторівнева модель повинна розглядатися як цілісна система, а не як набір окремих технічних налаштувань.

3.5. Політики вихідної пошти: запобігання компрометованим розсилкам і захист репутації домену

Захист електронної пошти охоплює не лише вхідний, а й вихідний трафік. Компрометація поштового акаунта може призвести до масових розсилок спаму або фішингу від імені організації, що швидко псує репутацію домену та призводить до блокувань з боку провайдерів. Для протидії цьому доцільно встановлювати ліміти на вихідну розсилку, контролювати підозрілі шаблони вихідних листів, налаштовувати алерти на нетипову активність і забезпечувати швидке відкликання сесій.

Окремо важливо впроваджувати політики протидії ексфільтрації через пошту: контроль автоматичного пересилання назовні, обмеження на надсилання конфіденційних даних, DLP-правила (за наявності), а також аудит делегувань та спільних скриньок. У сукупності ці заходи зменшують ризик

того, що пошта буде використана як канал витоку або як платформа для подальших атак.

3.6. Захист облікових записів: MFA, умовний доступ та політики сесій

Оскільки значна частина поштових інцидентів пов’язана з компрометацією акаунтів, одним із базових контрзаходів є MFA. Однак сучасні атаки можуть бути спрямовані на викрадення або перехоплення сесій, тому багатофакторна автентифікація має доповнюватися політиками умовного доступу: перевіркою пристрою, географії, ризиковості входу та можливістю оперативного відкликання токенів.

Для зниження ризику внутрішніх зловживань або помилок важливо застосовувати принцип найменших привілеїв. Адміністративні ролі в поштовій системі мають бути розмежовані, використання привілейованих акаунтів — журналюватися, а доступ до критичних функцій — захищатися додатковими контролями.

3.7. Навчання персоналу та організаційні процедури як складова протидії фішингу/BEC

Людський фактор залишається ключовим у поштових атаках, тому технічні засоби мають доповнюватися навчанням персоналу. Ефективні програми включають регулярні короткі тренінги, симуляції фішингу, інструкції щодо перевірки доменів, вкладень, URL, а також чіткий механізм повідомлення SOC про підозрілий лист. Важливо не карати співробітників за помилки, а формувати культуру безпеки та швидкого інформування.

Для BEC-критичних процесів (фінанси, закупівлі) необхідні формалізовані процедури: підтвердження зміни реквізитів через незалежний канал, двоетапне

погодження платежів, використання «контактів із довідника», а не контактів із листа. Такі процедури суттєво знижують ймовірність успішної атаки навіть у разі компрометації поштового листування.

3.8. Плейбуки реагування та відновлення поштових сервісів

Плейбуки реагування потрібні для того, щоб зменшити час від виявлення до локалізації інциденту. Для фішингу типовими кроками є: видалення листів зі скриньок, блокування доменів/URL, оновлення правил SEG, комунікація з користувачами. Для компрометації акаунта необхідні: скидання пароля, відкликання токенів, перевірка правил пересилання, аудит делегувань, пошук слідів ексфільтрації. Для BEC додатково активується фінансовий протокол взаємодії та фіксації доказів.

Відновлення поштових сервісів має враховувати безперервність бізнесу: наявність резервних каналів комунікації, можливість тимчасового обмеження окремих функцій (наприклад, зовнішнього пересилання), а також контроль повторних спроб атаки. Після завершення інциденту важливо провести lessons learned, оновити правила детекції та навчальні матеріали, а також перевірити, чи не залишилися приховані механізми доступу.

3.9. Політики зберігання та захисту даних у пошті: retention, архівування та юридичні вимоги

Захист поштової інфраструктури включає не лише протидію атакам, але й керування даними: строки зберігання, архівування, можливість відновлення та контроль доступу до історичних листів. У багатьох організаціях пошта містить юридично значущі відомості, комерційні таємниці, персональні дані. Тому

політика retention визначає, які категорії листів зберігаються, як довго, хто має доступ до архівів і як фіксуються операції доступу.

З позиції кіберзахисту архівування зменшує ризики втрати даних у разі інциденту, а також полегшує розслідування. Однак архіви є привабливою ціллю для зловмисників, тому доступ до них має бути посилений: MFA, розмежування ролей, журналювання доступів, контроль експортів. Окремо доцільно застосовувати політики, які унеможливлюють масовий експорт пошти без підвищених привілеїв або без погодження.

3.10. Захист домену та керування брендом: моніторинг схожих доменів і протидія typosquatting

Кіберзахист пошти напряму пов’язаний із захистом бренду: спуфінг та typosquatting часто націлені на те, щоб користувачі не помітили підміни домену. Тому доцільно організувати моніторинг реєстрації схожих доменів, появи піддоменів, а також періодичний аудит DMARC-політик для всіх доменів, які можуть використовуватись у комунікаціях організації. Практично це включає: контроль доменів, які належать організації; реєстрацію критичних варіацій домену; використання DMARC-звітування як джерела ознак атак на бренд.

Для протидії атакам на бренд корисна взаємодія між ІБ та комунікаційними/юридичними підрозділами: оперативні повідомлення користувачам і партнерам про шахрайські кампанії, налаштування політик «довіри» до каналів, а також реагування на фішингові домени через процедури takedown (скарги хостерам/реєстраторам). Зріла організація має плейбук, який визначає, хто ініціює takedown, які дані збираються, і як фіксуються результати.

3.11. Безпечна конфігурація поштової платформи: контрольні базові налаштування (базовий профіль налаштувань (baseline)

Окрім окремих контролів, необхідно сформувати базовий профіль налаштувань (baseline) безпечної конфігурації поштової платформи. Такий базовий профіль налаштувань (baseline) включає: вимогу MFA для всіх користувачів, окремі політики для привілейованих ролей, заборону або контроль автоматичного пересилання назовні, контроль делегувань, блокування небезпечних типів вкладень, налаштування quarantine, інтеграцію журналів із SIEM, правила алертів на ризикові входи та зміни конфігурації. Baseline має бути документований і регулярно перевірятися (аудит/скан).

3.12. Управління постачальниками та сторонніми сервісами надсилання (CRM, маркетинг, helpdesk)

Окремим джерелом ризику є сторонні сервіси, які надсилають пошту від імені домену організації: CRM, маркетингові платформи, helpdesk, білінг. Якщо такі сервіси не налаштовані з DKIM-підписом і коректним DMARC-alignment, вони або створять проблеми доставлюваності при посиленні політик, або стануть «слабкою ланкою», яку зловмисник може використати для компрометованих розсилок. Тому необхідні: інвентаризація сервісів, визначення відповідальних, контроль SPF include, окремі DKIM-ключі, ротація, а також періодичний аудит за DMARC-звітуванням.

У рамках управління постачальниками доцільно оцінювати: політики безпеки сервісу, підтримку MFA/SSO, можливість журналювання, процедури повідомлення про інциденти, механізми ізоляції та обмеження доступів. З практичного погляду важливо мінімізувати кількість сервісів, що мають право надсилати пошту від домену, і забезпечити централізоване керування політиками.

3.13. Процедури takedown фішингових доменів та взаємодія з зовнішніми сторонами

Оперативне реагування на фішингові домени й сторінки є важливою складовою протидії атакам. Процедури takedown включають: збір доказів (URL, скріншоти, WHOIS, хостинг), визначення контактів хостера/реєстратора, подачу скарг, а також комунікацію з партнерами і користувачами. Зріла організація має заздалегідь підготовлений плейбук: хто відповідає за ініціацію, які SLA, як фіксуються результати. Це дозволяє швидко зменшувати тривалість кампаній і кількість постраждалих.

Взаємодія з банками та правоохоронними органами особливо актуальна для BEC. У разі підозри на шахрайський переказ критично важливий фактор часу: чим швидше активовано процедури відкату/блокування транзакції, тим вища ймовірність мінімізувати фінансові втрати. Тому BEC-плейбук має містити контактні дані і алгоритм дій для фінансового підрозділу.

3.14. Документування політик та інтеграція у СУІБ: регламенти, ролі, відповідальність

Технічні контролі мають бути підкріплені документованими політиками та регламентами, що інтегруються у систему управління інформаційною безпекою (СУІБ). Доцільно мати окремі документи: політика використання електронної пошти, порядок обробки підозрілих листів, регламент реагування SOC, процедури BEC-підтвердження, вимоги до доменної автентифікації і до підключення сторонніх відправників. Ролі та відповідальність повинні бути визначені (RACI): хто адмініструє SPF/DKIM/DMARC, хто аналізує звіти, хто приймає рішення про quarantine/reject, хто проводить навчання і хто відповідає за взаємодію з зовнішніми сторонами.

3.15. Практичні базові налаштування для корпоративних платформ (узагальнені рекомендації)

Незалежно від конкретної платформи (локальна або хмарна) існує набір практик, які можна вважати «мінімальним базисом». До нього належать: обов’язкове MFA, контроль ризикових входів, заборона або жорсткий контроль автоматичного пересилання назовні, окремі політики для привілейованих ролей, журналювання адміністративних дій, а також інтеграція логів з SIEM. На рівні пошти важливо увімкнути антиспам/антифішинг, sandbox або еквівалентні механізми, URL-перевірки, а також базові обмеження для небезпечних типів вкладень.

Окремою практикою є використання «маркування зовнішньої пошти» (external sender tagging), коли листи від зовнішніх доменів позначаються в інтерфейсі користувача. Це не є повноцінним захистом, але знижує ризик соціальної інженерії, коли зловмисник намагається видати себе за внутрішнього співробітника. Важливо, щоб таке маркування не викликало «звикання» і супроводжувалося навчанням та зрозумілими інструкціями: що робити, якщо лист виглядає підозрілим.

3.16. Контроль спільних скриньок, делегувань і ланцюжків погоджень у бізнес-процесах

У багатьох організаціях використовуються спільні скриньки (finance@, hr@, procurement@) і делегування доступу. Такі об’єкти є підвищеним ризиком: компрометація спільної скриньки дає доступ до великих обсягів листування і може бути використана для BEC. Тому необхідно: обмежувати коло осіб з доступом, застосовувати MFA, журналювати делегування, контролювати експорт, а також встановлювати алерти на зміну учасників і правил inbox.

Для фінансових ланцюжків погодження доцільно формалізувати процеси так, щоб електронна пошта не була єдиним джерелом «істини». Наприклад, зміна реквізитів має підтверджуватися через довідник контактів або через систему документообігу з електронним підписом, а не через лист. Таким чином, навіть при компрометації поштового листування, атакувальнику складніше змінити критичні параметри.

3.17. Резервування, відновлення та план дій при недоступності пошти

Кіберстійкість поштової інфраструктури включає здатність відновлювати роботу після інцидентів і забезпечувати альтернативні канали комунікації. План безперервності повинен визначати: (1) які бізнес-процеси критично залежать від пошти; (2) які альтернативні канали використовуються при відмові (месенджери/телефон/корпоративний портал); (3) як відновлюється доступ до пошти після інциденту; (4) як перевіряється, що загроза усунена (відкликані сесії, перевірені правила, очищені скриньки).

Для локальних платформ важливими є резервні копії конфігурацій, журналів, поштових сховищ і механізми швидкого відновлення. Для хмарних платформ акцент зміщується на можливість оперативного блокування акаунтів, відновлення доступу, а також на політики збереження/архівування, які дозволяють відновити дані після видалення. Регулярні вправи (tabletop) допомагають перевіряти, що план відновлення працює, а відповідальні особи розуміють свої дії.

3.18. Привілейований доступ і адміністрування пошти: PAM, журнали та контроль змін

Адміністрування поштової інфраструктури є критичним ризиком, оскільки привілейовані ролі дозволяють змінювати маршрути пошти, правила фільтрації,

політики доступу, налаштування домену, а також здійснювати експорт даних. Тому доцільно застосовувати принципи Privileged Access Management (PAM): окремі адміністративні облікові записи, тимчасове надання привілеїв (JIT), MFA, контроль робочих станцій адміністраторів, журналювання та регулярний перегляд дій.

Контроль змін важливий і з операційного погляду. Зміни в DMARC, MTA-STS або правилах SEG можуть впливати на доставку. Тому зміни мають проходити погодження, мати тестовий етап і план відкату. Журнали адміністративних дій повинні надходити до SIEM, а SOC має мати правила оповіщення про ризикові зміни (наприклад, вимкнення захистів, створення широких винятків або підключення нового каналу відправлення).

3.19. Міжнародні практики та стандарти: узгодження поштових контролів з ISO/IEC 27001 та CIS Controls

Для системного впровадження поштових контролів корисно узгоджувати їх із вимогами та кращими практиками систем управління безпекою. Зокрема, ISO/IEC 27001 передбачає управління ризиками, контроль доступу, управління інцидентами, безперервність і відповідність вимогам. Поштові контрзаходи (MFA, журналювання, політики використання пошти, реагування на інциденти) природно вписуються в ці домени контролів. CIS Controls також містить практики, релевантні пошті: управління ідентичностями, безпечна конфігурація, захист від шкідливого ПЗ, журналювання та моніторинг.

Узгодження з такими рамками має практичний плюс: простіше планувати аудит і підтверджувати, що поштовий захист не є набором «разових налаштувань», а частиною керованої системи. У рамках кваліфікаційної роботи це підсилює аргументацію системності підходу та задає основу для переліку контрольних точок перевірки.

Висновки до розділу 3

У третьому розділі встановлено, що ефективна протидія атакам на поштову інфраструктуру має будуватися за принципом defense-in-depth, де кожен контроль компенсує обмеження іншого.

Показано, що технічні контрзаходи - SPF, DKIM, DMARC, ARC, MTA-STS, антифішингові політики, sandbox, MFA та умовний доступ - повинні підсилюватися організаційними процедурами, особливо в сценаріях BEC.

Обґрунтовано, що якісне реагування на поштові інциденти є невід'ємною складовою захисту, а його результативність визначається швидкістю збору артефактів, стримування, відновлення та подальшого вдосконалення правил безпеки.

Розділ 4 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ

4.1. Показники ефективності системи виявлення та протидії атакам

Оцінювання результативності захисту поштової інфраструктури повинно спиратися не лише на факт відсутності інцидентів, а й на вимірювані технічні та організаційні показники. Такий підхід відповідає логіці NIST CSF 2.0, ISO/IEC 27001 та CIS Controls, де управління безпекою розглядається як безперервний цикл зворотного зв'язку, моніторингу й удосконалення [30], [31], [32].

Для систем детекції найбільш інформативними є метрики precision, recall, false positive rate, частка успішно класифікованих шкідливих листів, а також кількість повторних інцидентів одного типу. Якщо фільтри дають надмірно багато хибнопозитивних спрацьовувань, користувачі та адміністратори поступово втрачають до них довіру. Якщо ж система має низький recall, значна частина реальних атак залишатиметься непоміченою. Тому оцінювання повинно шукати баланс між точністю та повнотою виявлення.

Для процесів реагування ключовими показниками є MTTD - середній час до виявлення інциденту, MTTC - середній час до локалізації та MTTR - середній час до відновлення. Для BEC та компрометації акаунтів важливим є також час до відкликання активних сесій, час до видалення шкідливих листів із скриньок та частка інцидентів, де було своєчасно активовано альтернативні бізнес-процедури [18], [21].

Окрема група метрик стосується стану конфігурації: частка легітимних потоків із DMARC pass, відсоток поштових акаунтів із MFA, кількість активних зовнішніх пересилань, покриття журналюванням поштових подій, кількість критичних винятків у політиках фільтрації. Саме ці показники дозволяють

переходити від реактивного управління до проактивного, коли ризики видно ще до появи інциденту.

Таблиця 4.1

Приклад системи показників для оцінювання поштової безпеки

Показник	Зміст	Практичне призначення
Precision	частка істинно шкідливих листів серед усіх спрацювань	контроль якості фільтрів
Recall	частка виявлених загроз серед усіх реальних загроз	контроль повноти детекції
MTTD	середній час до виявлення	оцінка швидкості помічання інциденту
MTTR	середній час до відновлення	оцінка ефективності реагування
DMARC pass-rate	частка легітимної пошти з коректною автентифікацією	контроль якості конфігурації
MFA coverage	частка акаунтів із MFA	контроль захисту облікових записів

4.2. Дорожня карта впровадження комплексу засобів захисту

Практичне впровадження захисту поштової інфраструктури доцільно здійснювати поетапно. На першому етапі організація має провести інвентаризацію доменів, серверів, хмарних поштових сервісів, зовнішніх відправників, сервісів масових розсилок і критичних груп користувачів. Без цього неможливо коректно налаштувати SPF, DKIM і DMARC або визначити, які потоки є легітимними, а які становлять ризик [5], [17].

Другий етап передбачає впровадження базових технічних контролів: MFA для критичних груп, сегментацію ролей, обмеження автоматичного пересилання назовні, централізований збір логів і запуск політик SPF/DKIM/DMARC у режимі спостереження. На цьому ж етапі формуються

початкові правила для антифішингових політик, quarantine, перевірки вкладень і блокування потенційно небезпечних типів файлів [12], [27], [29].

Третій етап стосується підвищення зрілості системи. Організація переходить від режиму спостереження до жорсткіших політик DMARC, розширює поведінкову аналітику, впроваджує SIEM-кореляцію, інтегрує телеметрію з поштової платформи, кінцевих точок і проксі. На цьому етапі також корисно впроваджувати ARC, MTA-STS і TLS-RPT для підвищення цілісності маршруту доставки [6], [7], [22], [26].

Четвертий етап пов'язаний з управлінською зрілістю: створенням playbooks, регулярними навчаннями, tabletop-вправами для BEC, аудитом винятків, побудовою Current і Target Profile відповідно до CSF 2.0, а також формуванням системи звітності для керівництва [30], [31], [33]. У результаті організація переходить від набору розрізнених інструментів до повноцінної керованої підсистеми захисту електронної пошти.

Таблиця 4.2

Орієнтовна дорожня карта впровадження засобів захисту електронної пошти

Етап	**Основні дії**	**Результат**
1. Інвентаризація	облік доменів, сервісів і потоків пошти	видимість легітимних джерел
2. Базові контрзаходи	MFA, журнали, SPF/DKIM/DMARC p=none	базове зниження ризику
3. Посилення	quarantine/reject, SIEM, ARC, MTA-STS, TLS-RPT	підвищення якості детекції і стримування
4. Зрілість	playbooks, вправи, KPI/KRI, профілі CSF	керований і вимірюваний процес безпеки

4.3. Практичні рекомендації для організації

Для більшості організацій доцільно починати не зі складних ML-моделей, а з наведення ладу в базовій конфігурації. Якщо не інвентаризовані домени й

сервіси розсилок, не впроваджено MFA або відсутній контроль пересилання пошти, то навіть найдосконаліші антифішингові алгоритми не дадуть стійкого результату. Практика показує, що зрілість захисту насамперед визначається дисципліною процесів і якістю гігієнічних налаштувань.

До критичних рекомендацій належать: поетапне доведення DMARC до політики reject там, де це можливо; використання окремих профілів захисту для керівників і фінансових ролей; регулярний перегляд allow-листів; формалізація каналу повідомлення про підозрілу пошту; резервне копіювання та перевірка можливості швидкого відновлення критичних скриньок; а також обов'язкова взаємодія ІТ, ІБ і бізнес-підрозділів у разі поштових інцидентів [10], [18], [29], [33].

З управлінської точки зору корисно встановлювати не лише технічні метрики, але й показники дисципліни: відсоток пройдених навчань, час підтвердження інциденту власником бізнес-процесу, кількість прострочених винятків, частку погоджених ризиків. Саме така інтеграція СУІБ із практикою експлуатації поштового каналу дозволяє перетворити захист електронної пошти з вузькотехнічної задачі на керований елемент загальної кіберстійкості організації [19], [20], [32].

4.4. Модель зрілості поштової безпеки та аудит налаштувань

Оцінювання зрілості поштової безпеки доцільно проводити за рівнями: базова гігієна → автентифікація домену → поглиблена детекція → зрілі процеси реагування. На базовому рівні контролюються MFA, обмеження пересилання, актуальність клієнтів і серверів, базові антиспам-політики. На рівні автентифікації — коректні SPF/DKIM/DMARC політики та аналіз звітності. На рівні поглибленої детекції — sandbox, URL time-of-click, SIEM-кореляція. На рівні процесної зрілості — плейбуки SOC, вправи, KPI/KRI та регулярні аудити.

Регулярний аудит дозволяє виявляти деградацію конфігурацій: появу нових відправників без DKIM, помилки SPF, відсутність звітів TLS-RPT, неконтрольовані винятки. Практично аудит має включати інвентаризацію доменів, перевірку політик, аналіз журналів пересилання, огляд інтеграцій із сторонніми застосунками та оцінку виконання процедур підтвердження для BEC.

4.5. Орієнтовне економічне обґрунтування: витрати, ризики та ефект від контролів

Економічне обґрунтування заходів безпеки може спиратися на ризик-орієнтовану модель: очікувані втрати від інциденту порівнюються з витратами на контроль. Для поштових інцидентів ключовими складовими втрат є: прямі фінансові збитки (BEC), витрати на відновлення, простої бізнес-процесів, штрафи/наслідки витоку даних, репутаційні втрати. З іншого боку, витрати включають ліцензії на SEG/SIEM/EDR, час персоналу SOC/адміністраторів, навчання співробітників та підтримку політик.

Ефект від впровадження контролів проявляється як зменшення імовірності інцидентів (наприклад, DMARC p=reject знижує спуфінг домену), так і зменшення наслідків (швидке видалення листів і відкликання сесій знижують масштаб компрометації). Для демонстрації ефекту доцільно використовувати метрики MTTD/MTTR, частку успішних фішингових кліків у симуляціях, кількість повторних інцидентів, а також показники доставлюваності та репутації домену.

4.6. Дорожня карта впровадження та контрольні точки якості

Рекомендована дорожня карта повинна містити контрольні точки якості, щоб зміни були керованими. Наприклад: (1) підготовка — інвентаризація

відправників і аудит доменів; (2) SPF/DKIM — досягнення стабільного pass; (3) DMARC p=none — збір телеметрії; (4) DMARC quarantine — контроль FP і винятків; (5) DMARC reject — стабілізація; (6) впровадження MTA-STS/TLS-RPT; (7) підключення sandbox/URL time-of-click; (8) SIEM-кореляція і SOAR; (9) вправи SOC та навчання.

Контрольні точки повинні включати як технічні критерії (прохідність автентифікації, падіння FP), так і процесні (SLA реагування, здатність видалити шкідливі листи за визначений час). Таким чином організація отримує не просто набір розрізнених налаштувань, а послідовну програму підвищення кіберстійкості поштової інфраструктури.

4.7. Проєктування системи показників і дашбордів для керування поштовою безпекою

Щоб керувати поштовою безпекою на практиці, необхідно мати набір вимірюваних показників і спосіб їх регулярного відстеження. Доцільно розділяти показники на технічні (якість детекції, DMARC pass-rate, TLS compliance), операційні (MTTD/MTTR, кількість інцидентів, SLA тріажу) та поведінкові (частка повідомлень про фішинг, результати симуляцій). На основі цих показників будуються дашборди для керівництва ІБ та операційних команд.

Приклад структури дашборду: (1) «Стан автентифікації» — частка SPF/DKIM/DMARC pass, топ-джерела fail; (2) «Фішинг/спам» — кількість заблокованих листів, основні категорії, FPR; (3) «BEC-ризики» — інциденти з фінансовими ознаками, правила пересилання, ризикові входи; (4) «Транспорт» — TLS успішність, MTA-STS/TLS-RPT проблеми; (5) «Реагування» — MTTD/MTTR, виконання плейбуків. Такий дашборд робить процес керованим і дозволяє обґрунтовувати пріоритети розвитку.

4.8. План практичної верифікації: сценарії тестування контролів і перевірка готовності

Після впровадження контролів необхідно перевіряти їхню працездатність у контрольованих умовах. План верифікації може включати: (1) тестові надсилання з різними SPF/DKIM/DMARC комбінаціями; (2) перевірку обробки шкідливих вкладень у sandbox та реакції EDR; (3) тестові фішингові листи з безпечними URL для перевірки time-of-click; (4) сценарії компрометації акаунта в лабораторному середовищі (створення правил пересилання) і перевірку детекцій у SIEM; (5) tabletop-вправи для BEC (процедури підтвердження та взаємодії).

Результати тестів мають фіксуватися у вигляді чеклістів і звітів, а виявлені прогалини — перетворюватися на задачі покращення. Це дозволяє підтримувати ефективність системи в умовах змін інфраструктури, нових загроз та оновлення політик провайдерів.

4.9. Управління змінами та безперервне покращення: цикл PDCA для поштової безпеки

Поштова безпека є динамічною: змінюються загрози, бізнес-процеси, постачальники та вимоги провайдерів. Тому доцільно застосовувати цикл безперервного покращення (PDCA): Plan — планування контролів і метрик; Do — впровадження політик і технічних налаштувань; Check — вимірювання результативності; Act — коригування правил, навчання та оновлення процесів.

У рамках управління змінами важливо вести журнал змін конфігурацій, мати процедури тестування, узгодження та можливості відкату. Це особливо актуально для DMARC і транспортних політик, які можуть впливати на доставлюваність. Таким чином організація знижує операційні ризики та підвищує керованість поштової інфраструктури.

4.10. Формалізація ризиків і контроль відповідності: KRI, аудит та підготовка до перевірок

Окрім KPI, які відображають результативність, організація має відстежувати KRI — індикатори ризику. Для поштової безпеки KRI можуть включати: частку акаунтів без MFA, кількість дозволених пересилань назовні, кількість сторонніх відправників без DKIM-alignment, частоту ризикових входів, зростання DMARC fail та кількість інцидентів з фінансовими ознаками. Регулярний аудит цих показників дозволяє своєчасно виявляти деградацію контролів.

Підготовка до перевірок (внутрішніх або зовнішніх) включає збирання доказів: скріншоти/експорти налаштувань SPF/DKIM/DMARC, звіти DMARC і TLS-RPT, журнали SIEM про інциденти, записи навчань і симуляцій фішингу, а також затверджені регламенти реагування. Такий підхід зменшує ризик «паперової безпеки» і робить захист електронної пошти вимірюваним і підтверджуваним.

Висновки до розділу 4

У четвертому розділі визначено систему кількісних та якісних показників, за допомогою яких організація може оцінювати ефективність виявлення, стримування й відновлення після поштових атак.

Запропоновано поетапну дорожню карту впровадження засобів захисту, що охоплює інвентаризацію, базові контрзаходи, посилення технічної зрілості та формування керованої системи звітності й удосконалення.

Сформульовано практичні рекомендації, спрямовані на досягнення реальної операційної стійкості, а не лише формального дотримання вимог безпеки.

ВИСНОВКИ

1. Оцінено сучасний стан проблеми захисту корпоративної електронної пошти та встановлено, що поштова інфраструктура залишається одним із найуразливіших каналів реалізації фішингу, спуфінгу, BEC/EAC, шкідливих вкладень, компрометації облікових записів і прихованого пересилання повідомлень.

2. Проаналізовано архітектуру корпоративної поштової інфраструктури, визначено її ключові контрольні точки та систематизовано актуальні загрози й типові помилки конфігурації, що впливають на безпеку електронної пошти організації.

3. Визначено та узагальнено методи виявлення атак на інфраструктуру електронної пошти на основі SPF, DKIM, DMARC, аналізу заголовків, контенту, URL і вкладень, а також поведінкової аналітики, моніторингу телеметрії та кореляції подій у SIEM/SOAR.

4. Обґрунтовано технічні й організаційні заходи протидії атакам на поштову інфраструктуру, зокрема багаторівневий захист, MFA, умовний доступ, ARC, MTA-STS, TLS-RPT, захист кінцевих точок, навчання персоналу, процедури підтвердження фінансових операцій і стандартизовані playbooks реагування.

5. Запропоновано практичні рекомендації щодо поетапного підвищення кіберстійкості поштової інфраструктури організації, включаючи безпечну базову конфігурацію поштових платформ, контроль сторонніх сервісів надсилання, резервування, моніторинг схожих доменів і дорожню карту впровадження засобів захисту.

6. Практичне значення одержаних результатів полягає в можливості їх використання під час аудиту й модернізації поштової інфраструктури, налаштування захисних контролів, побудови процесів SOC, оцінювання ефективності захисту за допомогою KPI/KRI та підготовки організації до реагування на сучасні поштові інциденти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Klensin J. Simple Mail Transfer Protocol : RFC 5321. RFC Editor, 2008. URL: https://datatracker.ietf.org/doc/html/rfc5321 (дата звернення: 04.03.2026).

2. Tracy M., Scarfone K. Guidelines on Electronic Mail Security : NIST SP 800-45 Version 2. NIST, 2007. URL: https://csrc.nist.gov/pubs/sp/800/45/ver2/final (дата звернення: 04.03.2026).

3. Kitterman S. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 : RFC 7208. RFC Editor, 2014. URL: https://datatracker.ietf.org/doc/html/rfc7208 (дата звернення: 04.03.2026).

4. Crocker D., Hansen T., Kucherawy M. DomainKeys Identified Mail (DKIM) Signatures : RFC 6376. RFC Editor, 2011. URL: https://datatracker.ietf.org/doc/html/rfc6376 (дата звернення: 04.03.2026).

5. Kucherawy M., Zwicky E. Domain-based Message Authentication, Reporting, and Conformance (DMARC) : RFC 7489. RFC Editor, 2015. URL: https://datatracker.ietf.org/doc/html/rfc7489 (дата звернення: 04.03.2026).

6. Margolis D., Risher M., Ramakrishnan B. et al. SMTP MTA Strict Transport Security (MTA-STS) : RFC 8461. RFC Editor, 2018. URL: https://datatracker.ietf.org/doc/html/rfc8461 (дата звернення: 04.03.2026).

7. Margolis D., Brotman A., Ramakrishnan B. et al. SMTP TLS Reporting : RFC 8460. RFC Editor, 2018. URL: https://datatracker.ietf.org/doc/html/rfc8460 (дата звернення: 04.03.2026).

8. Google Workspace Admin Help. Email sender guidelines. URL: https://support.google.com/a/answer/81126?hl=en (дата звернення: 04.03.2026).

9. Yahoo Sender Hub. Sender Best Practices. URL: https://senders.yahooinc.com/best-practices/ (дата звернення: 04.03.2026).

10. Federal Bureau of Investigation. Business Email Compromise. URL: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise (дата звернення: 04.03.2026).

11. Cybersecurity and Infrastructure Security Agency. Phishing Guidance: Stopping the Attack Cycle at Phase One. URL: https://www.cisa.gov/resources-

tools/resources/phishing-guidance-stopping-attack-cycle-phase-one (дата звернення: 04.03.2026).

12. Cybersecurity and Infrastructure Security Agency. Require Multifactor Authentication. URL: https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication (дата звернення: 04.03.2026).

13. Microsoft Learn. Email authentication - Microsoft Defender for Office 365. URL: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about (дата звернення: 04.03.2026).

14. MITRE ATT&CK. Phishing (T1566). URL: https://attack.mitre.org/techniques/T1566/ (дата звернення: 04.03.2026).

15. MITRE ATT&CK. Email Collection (T1114). URL: https://attack.mitre.org/techniques/T1114/ (дата звернення: 04.03.2026).

16. MITRE ATT&CK. Email Forwarding Rule (T1114.003). URL: https://attack.mitre.org/techniques/T1114/003/ (дата звернення: 04.03.2026).

17. Rose S., Borchert O., Mitchell S., Connelly S. Trustworthy Email : NIST SP 800-177 Revision 1. NIST, 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf (дата звернення: 04.03.2026).

18. Nelson A. et al. Incident Response Recommendations and Considerations for Cyber Risk Management : NIST SP 800-61 Rev. 3. NIST, 2025. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (дата звернення: 04.03.2026).

19. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 04.03.2026).

20. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80 (дата звернення: 04.03.2026).

21. Microsoft Learn. Responding to a Compromised Email Account. URL: https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account (дата звернення: 04.03.2026).

22. Andersen K., Long B., Blank S., Kucherawy M. The Authenticated Received Chain (ARC) Protocol : RFC 8617. RFC Editor, 2019. URL: https://datatracker.ietf.org/doc/html/rfc8617 (дата звернення: 04.03.2026).

23. Schaad J., Ramsdell B., Turner S. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification : RFC 8551. RFC Editor, 2019. URL: https://datatracker.ietf.org/doc/html/rfc8551 (дата звернення: 04.03.2026).

24. Levine J., Herkula T. Signaling One-Click Functionality for List Email Headers : RFC 8058. RFC Editor, 2017. URL: https://datatracker.ietf.org/doc/html/rfc8058 (дата звернення: 04.03.2026).

25. Microsoft Learn. SecOps guide for email authentication in Microsoft 365. URL: https://learn.microsoft.com/en-us/defender-office-365/email-auth-sec-ops-guide (дата звернення: 04.03.2026).

26. Microsoft Learn. Configure trusted ARC sealers. URL: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-arc-configure (дата звернення: 04.03.2026).

27. Microsoft Learn. Anti-phishing policies in cloud organizations. URL: https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about (дата звернення: 04.03.2026).

28. Microsoft Learn. Anti-spoofing protection - Microsoft Defender for Office 365. URL: https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-protection-spoofing-about (дата звернення: 04.03.2026).

29. Microsoft Learn. Recommendations for Microsoft 365 security settings for Office 365. URL: https://learn.microsoft.com/en-us/defender-office-365/recommended-settings-for-eop-and-office365 (дата звернення: 04.03.2026).

30. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 04.03.2026).

31. CIS Critical Security Controls Version 8.1. URL: https://www.cisecurity.org/controls/v8-1 (дата звернення: 04.03.2026).

32. ISO/IEC 27001:2022 Information security management systems - Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 04.03.2026).

33. Cybersecurity and Infrastructure Security Agency. Secure Your Business. URL: https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business (дата звернення: 04.03.2026).

34. Kucherawy M. Interoperability Issues between DMARC and Indirect Email Flows : RFC 7960. RFC Editor, 2016. URL: https://datatracker.ietf.org/doc/html/rfc7960 (дата звернення: 05.03.2026).

35. BIMI Group. BIMI (Brand Indicators for Message Identification) — Specification. URL: https://bimigroup.org/ (дата звернення: 05.03.2026).

36. Google Workspace Admin Help. Set up BIMI to display your brand logo in Gmail. URL: https://support.google.com/a/answer/10911320 (дата звернення: 05.03.2026).

37. Arends R. та ін. DNS Security Introduction and Requirements : RFC 4033. IETF, 2005. URL: https://datatracker.ietf.org/doc/html/rfc4033 (дата звернення: 05.03.2026).

38. Arends R. та ін. Resource Records for the DNS Security Extensions : RFC 4034. IETF, 2005. URL: https://datatracker.ietf.org/doc/html/rfc4034 (дата звернення: 05.03.2026).

39. Arends R. та ін. Protocol Modifications for the DNS Security Extensions : RFC 4035. IETF, 2005. URL: https://datatracker.ietf.org/doc/html/rfc4035 (дата звернення: 05.03.2026).

40. Microsoft Security. Consent phishing: how attackers trick users into granting permissions. URL: https://learn.microsoft.com/security/ (дата звернення: 05.03.2026).

41. CISA. Phishing Guidance and resources (incl. QR-code phishing). URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/phishing (дата звернення: 05.03.2026).

42. Microsoft Security Blog. QR code phishing (quishing) – recommended protections. URL: https://www.microsoft.com/security/blog/ (дата звернення: 05.03.2026).

ДОДАТКИ

Додаток А

Контрольний перелік базових налаштувань поштової безпеки

– Інвентаризовано всі легітимні джерела надсилання пошти організації (корпоративний сервер, хмарна платформа, CRM, маркетингові сервіси, helpdesk).

– Для домену налаштовано SPF із мінімізацією зайвих include-ланцюгів та перевірено коректність обробки пересилання.

– Увімкнено DKIM-підписування для всіх каналів надсилання й визначено процедуру регулярної ротації ключів.

– Опубліковано DMARC-політику з адресами для звітів; проаналізовано DMARC RUA-статистику та підготовлено перехід до quarantine/reject.

– Увімкнено MFA для всіх користувачів пошти та адміністраторів; реалізовано контроль ризикових входів і перевірку умов доступу.

– Обмежено автоматичне пересилання назовні, налаштовано аудит правил поштових скриньок, делегувань та прихованих фільтрів.

– На рівні шлюзу застосовано антифішингові політики, аналіз вкладень, sandbox/CDR та перевірку URL у режимі time-of-click.

– Логи поштової платформи, шлюзу та автентифікації інтегровано до SIEM; створено правила кореляції для фішингу, BEC/EAC і спуфінгу.

– Розроблено playbook реагування на поштові інциденти, включаючи вилучення листів зі скриньок, блокування доменів/URL і відкликання сесій.

– Проведено навчання співробітників і визначено офіційний канал повідомлення про підозрілі листи.

Додаток Б

Приклади DNS-записів для автентифікації домену та захисту транспорту

SPF: v=spf1 ip4:203.0.113.10 include:_spf.google.com -all

DMARC: v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@domain.tld; adkim=s; aspf=s; pct=100

TLS-RPT: v=TLSRPTv1; rua=mailto:tlsrpt@domain.tld

_mta-sts.domain.tld TXT "v=STSv1; id=20260304"

Політика MTA-STS публікується за адресою: https://mta-sts.domain.tld/.well-known/mta-sts.txt

Додаток В

Фрагмент журналу ризиків для поштової інфраструктури

Таблиця В.1

Приклад фрагмента журналу ризиків

Ризик	**Імовірність**	**Вплив**	**Базові контрзаходи**	**Власник**
Спуфінг домену та зловживання брендом	Середня	Високий	SPF/DKIM/ DMARC, моніторинг звітів	SecOps
BEC/EAC у фінансових процесах	Середня	Високий	MFA, перевірка реквізитів поза поштою	Фінансовий відділ
Шкідливі вкладення та ransomware	Висока	Високий	Sandbox, CDR, EDR, резервні копії	IT/SOC
Компрометація облікового запису	Висока	Середній	MFA, Conditional Access, аудит правил	IAM/Адміністратор

Додаток Г

Короткий playbook SOC для інцидентів типу фішинг/BEC

– Зафіксувати артефакти: повні заголовки листа, URL, вкладення, хеші файлів, часові мітки, скріншоти та ідентифікатори повідомлень.

– Класифікувати подію як фішинг URL, шкідливе вкладення, спуфінг домену, BEC/EAC або компрометацію поштового акаунта.

– Виконати стримування: заблокувати домен/URL на SEG і проксі, помістити листи у quarantine, видалити їх із скриньок користувачів.

– За наявності ознак захоплення акаунта скинути пароль, відкликати токени та активні сесії, перевірити правила пересилання і делегування.

– Повідомити відповідальних стейкхолдерів; для BEC активувати фінансовий протокол підтвердження операцій та зв’язку з банком.

– Після інциденту оновити правила виявлення, провести розбір lessons learned і, за потреби, повторне навчання користувачів.