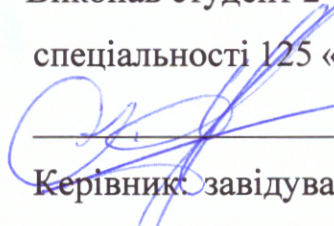


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно–комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

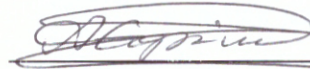
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та інструменти організації служби кібербезпеки
логістичної компанії»

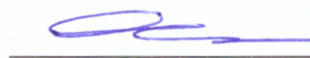
Виконав студент 2-го курсу, групи ЗКБм–24–1
спеціальності 125 «Кібербезпека та захист інформації»

 Анатолій ДОБРИНСЬКИЙ

Керівник, завідувач кафедри комп'ютерної інженерії
та кібербезпеки, к.т.н., доцент

 Андрій ЄФІМЕНКО

Рецензент: доцент кафедри комп'ютерної інженерії та
кібербезпеки, к.т.н., доцент

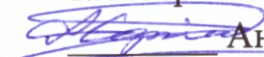
 Юрій РОССІНСЬКИЙ

Житомир 2025

Державний університет «житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Андрій ЄФІМЕНКО

6 жовтня 2025 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу

Студента **Анатолія Васильовича Добринського**

Тема роботи: **Методи та інструменти організації служби кібербезпеки логістичної компанії**

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

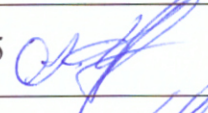
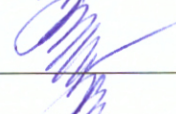
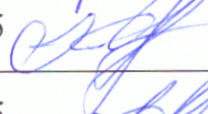
Термін здачі студентом закінченої роботи 26 грудня 2025 р.

Вихідні дані для роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є методи, стратегії, організаційні структури та технологічні рішення (SIEM, SOAR, NIST CSF) для забезпечення кіберстійкості логістичної інфраструктури та мінімізації ризиків порушення безперервності бізнес-процесів.

Об'єктом дослідження є процеси організації та функціонування служби кібербезпеки у великих логістичних компаніях, спрямовані на забезпечення цілісності, конфіденційності та доступності даних у розподілених мережах.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

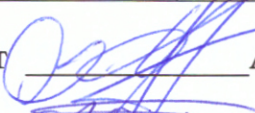
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Володимир ВОРОТНІКОВ	06.10.2025 	06.10.2025 
2	Володимир ВОРОТНІКОВ	06.10.2025 	06.10.2025 
3	Володимир ВОРОТНІКОВ	06.10.2025 	06.10.2025 

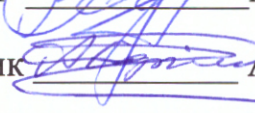
Студент  **Анатолій ДОБРИНСЬКИЙ**

Керівник  **Андрій ЄФІМЕНКО**

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання та затвердження теми	6.10.2025 - 7.10.2025	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо сучасних кіберзагроз у логістичному секторі та методів управління ризиками	8.10.2025 - 9.10.2025	Виконано
3	Аналіз міжнародних стандартів надійності та рамкових програм кібербезпеки (NIST CSF, ISO/IEC 27001), специфічних для ринку Північної Америки	10.10.2025 - 11.10.2025	Виконано
4	Порівняльний аналіз інструментарію кіберзахисту (SIEM, IDS/IPS, DLP) та рішень для автоматизації моніторингу (Wazuh, Splunk, Ansible)	13.10.2025 - 20.10.2025	Виконано
5	Проектування організаційної структури служби кібербезпеки та розробка стратегій зменшення ризиків для розподіленої інфраструктури	21.10.2025 - 1.11.2025	Виконано
6	Архітектурний аналіз IT-інфраструктури компанії FedEx та ідентифікація вразливостей у системах управління транспортом (TMS) і складом (WMS)	2.11.2025 - 7.11.2025	Виконано
7	Розробка та формалізація стандартних операційних процедур (SOP) для реагування на критичні інциденти: Ransomware, DDoS та витік даних	8.11.2025 - 14.11.2025	Виконано
8	Проектування та впровадження системи тренування персоналу (Security Awareness) з використанням методів гейміфікації та симуляції фішингу	18.11.2025 - 1.12.2025	Виконано
9	Оцінка ефективності запропонованих заходів: аналіз реальних кейсів (NotPetya), розрахунок показників рентабельності інвестицій (ROSI) та метрик реагування	2.12.2025 - 27.12.2025	Виконано
10	Оформлення результатів дослідження та написання пояснювальної записки	28.12.2025 - 24.12.2025	Виконано
11	Підготовка презентаційних матеріалів та доповіді	28.12.2025	Виконано
12	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	29.12.2025	Виконано
13	Захист магістерської роботи	30.12.2025	Виконано

Студент  Анатолій ДОБРИНСЬКИЙ

Керівник  Андрій ЄФІМЕНКО

РЕФЕРАТ

Пояснювальна записка до дипломної роботи містить 95 сторінок, 2 ілюстрації, 10 таблиць, список використаних джерел із 30 найменувань та 1 додаток.

Метою роботи є вдосконалення організації роботи служби кібербезпеки логістичного підприємства шляхом комплексного аналізу сучасних загроз, впровадження передових методологій управління ризиками (NIST CSF) та розробки практичних рекомендацій щодо автоматизації процесів реагування на прикладі корпорації FedEx.

В ході дослідження проведено глибокий аналіз ландшафту кіберзагроз для логістичної галузі, де виявлено критичну вразливість ланцюгів постачань до атак типу Ransomware та компрометації партнерських систем. Особлива увага приділена аналізу вразливостей систем управління транспортом (TMS) та складами (WMS), а також специфіці захисту Інтернету речей (IoT). Висвітлено важливість дотримання міжнародних стандартів та нормативних актів Північної Америки, таких як ISO/IEC 27001, CCPA та PIPEDA, для забезпечення комплаєнсу та репутаційної стабільності бізнесу. Результатом цього етапу стало обґрунтування переходу від реактивного захисту до стратегії кіберстійкості (Cyber Resilience).

Проведено структурний аналіз служби кібербезпеки, обґрунтовано ієрархічну модель Центру операцій безпеки (SOC) та роль Керівника з інформаційної безпеки (CISO) у стратегічному управлінні. Розроблено архітектуру захисту на основі інтеграції систем SIEM, IDS/IPS та DLP, а також запропоновано методи автоматизації моніторингу через SOAR-технології. На базі аналізу інциденту NotPetya у FedEx розроблено практичні рекомендації, що включають впровадження моделі Zero Trust, концепції SASE та систем предиктивного захисту на основі штучного інтелекту. Доведено ефективність запропонованих рішень: визначено шляхи мінімізації часу відновлення (RTO) та обґрунтовано економічну доцільність інвестицій через модель ROSI.

Ключові слова: КІБЕРБЕЗПЕКА, ЛОГІСТИКА, FEDEX, NIST CSF, ZERO TRUST, SOC, РЕАГУВАННЯ НА ІНЦИДЕНТИ, СЛУЖБА КІБЕРБЕЗПЕКИ.

ABSTRACT

The explanatory note to the master's thesis consists of 95 pages, 2 illustrations, 10 tables, a list of references including 30 sources, and 1 appendix.

The aim of the work is to improve the organization of the cybersecurity service for a logistics enterprise through a comprehensive analysis of modern threats, the implementation of advanced risk management methodologies (NIST CSF), and the development of practical recommendations for automation based on the FedEx model.

In the course of the research, a profound analysis of the cyber threat landscape for the logistics industry was conducted, revealing the critical vulnerability of supply chains to Ransomware attacks and targeted campaigns aimed at compromising partner systems . Particular attention was paid to analyzing the vulnerabilities of Transport Management Systems (TMS) and Warehouse Management Systems (WMS), as well as the specifics of Internet of Things (IoT) protection . The importance of compliance with international standards and North American regulations, such as ISO/IEC 27001, CCPA, and PIPEDA, to ensure business compliance and reputational stability was highlighted . The result of this stage was the justification for transitioning from reactive defense to a Cyber Resilience strategy.

A structural analysis of the cybersecurity service was performed, justifying the hierarchical model of the Security Operations Center (SOC) and the role of the Chief Information Security Officer (CISO) in strategic management . The protection architecture based on the integration of SIEM, IDS/IPS, and DLP systems was developed, and methods for monitoring automation using SOAR technologies were proposed . Based on the analysis of the NotPetya incident at FedEx, practical recommendations were developed, including the implementation of the Zero Trust model, the SASE concept, and predictive protection systems based on artificial intelligence . The effectiveness of the proposed solutions was proven: ways to minimize Recovery Time Objective (RTO) were identified, and the economic feasibility of investments through the ROSI model was justified .

Keywords: CYBERSECURITY, LOGISTICS, FEDEX, NIST CSF, ZERO TRUST, SOC, INCIDENT RESPONSE, CYBERSECURITY SERVICE.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

- ACL – Access Control List (Список контролю доступу)
- ALE – Annualized Loss Expectancy (Очікувані річні втрати)
- API – Application Programming Interface (Програмний інтерфейс додатка)
- APT – Advanced Persistent Threat (Розвинена стала загроза)
- ARO – Annualized Rate of Occurrence (Очікувана частота виникнення інциденту)
- BIA – Business Impact Analysis (Аналіз впливу на бізнес)
- CCPA – California Consumer Privacy Act (Каліфорнійський закон про приватність споживачів)
- CISO – Chief Information Security Officer (Керівник з інформаційної безпеки)
- CMMC – Cybersecurity Maturity Model Certification (Сертифікація моделі зрілості кібербезпеки)
- CSF – Cybersecurity Framework (Рамкова програма кібербезпеки)
- CVE – Common Vulnerabilities and Exposures (Загальновідомі вразливості та експозиції)
- CVSS – Common Vulnerability Scoring System (Загальна система оцінки вразливостей)
- DAST – Dynamic Application Security Testing (Динамічне тестування безпеки додатків)
- DDoS – Distributed Denial of Service (Розподілена відмова в обслуговуванні)
- DFIR – Digital Forensics and Incident Response (Цифрова криміналістика та реагування на інциденти)
- DLP – Data Loss Prevention (Запобігання витоку даних)
- DRP – Disaster Recovery Plan (План відновлення після катастроф)
- EDR – Endpoint Detection and Response (Система виявлення та реагування на кінцевих точках)
- ERP – Enterprise Resource Planning (Планування ресурсів підприємства)
- IaC – Infrastructure as Code (Інфраструктура як код)
- IAM – Identity and Access Management (Управління ідентифікацією та доступом)
- IDS – Intrusion Detection System (Система виявлення вторгнень)
- IPS – Intrusion Prevention System (Система запобігання вторгненням)
- IoT – Internet of Things (Інтернет речей)

IRP – Incident Response Plan (План реагування на інциденти)

KPI – Key Performance Indicators (Ключові показники ефективності)

KRI – Key Risk Indicators (Ключові індикатори ризику)

MITM – Man-in-the-Middle (Атака «людина посередині»)

MTTD – Mean Time to Detect (Середній час виявлення)

MTTR – Mean Time to Respond (Середній час реагування)

NGFW – Next-Generation Firewall (Міжмережевий екран наступного покоління)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій США)

PQC – Post-Quantum Cryptography (Постквантова криптографія)

RBAC – Role-Based Access Control (Управління доступом на основі ролей)

ROSI – Return on Security Investment (Рентабельність інвестицій у безпеку)

RPO – Recovery Point Objective (Цільова точка відновлення даних)

RTO – Recovery Time Objective (Цільовий час відновлення сервісу)

SASE – Secure Access Service Edge (Безпечний сервіс доступу до периметра)

SAST – Static Application Security Testing (Статичне тестування безпеки додатків)

SBOM – Software Bill of Materials (Програмна специфікація матеріалів)

SIEM – Security Information and Event Management (Управління інформацією та подіями безпеки)

SLA – Service Level Agreement (Угода про рівень обслуговування)

SLE – Single Loss Exposure (Вартість збитків від одного інциденту)

SOAR – Security Orchestration, Automation and Response (Оркестрація, автоматизація та реагування на події безпеки)

SOP – Standard Operating Procedure (Стандартна операційна процедура)

TMS – Transport Management System (Система управління транспортом)

UEM – Unified Endpoint Management (Уніфіковане управління кінцевими точками)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

WMS – Warehouse Management System (Система управління складом)

XSS – Cross-Site Scripting (Міжсайтовий скриптинг)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	6
ВСТУП.....	9
1. АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ КІБЕРБЕЗПЕКИ ДЛЯ ЛОГІСТИЧНИХ КОМПАНІЙ	11
1.1. Аналіз сучасних кіберзагроз для логістичного підприємства.....	11
1.2. Аналіз вразливостей логістичних систем.....	14
1.3. Аналіз Оцінка та ідентифікація потенційних ризиків та їхнього впливу на безперервність бізнесу	18
Висновки до першого розділу:	25
2. АНАЛІЗ СУЧАСНИХ ПРАКТИК ОРГАНІЗАЦІЇ СЛУЖБИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА	27
2.1. Структурний аналіз служби кібербезпеки.....	27
2.2. Оцінка та ідентифікація потенційних ризиків та їхнього впливу на безперервність бізнесу	32
2.3. Аналіз інструментів та технологій кібербезпеки (SIEM, IDS/IPS, DLP) ...	37
2.4. Аналіз рішень для автоматизації моніторингу безпеки.....	41
Висновки до другого розділу:	48
3. ОПЕРАЦІЙНА ДІЯЛЬНІСТЬ СЛУЖБИ КІБЕРБЕЗПЕКИ	50
3.1. Планування політик безпеки (розробка стратегій зменшення ризиків)	50
3.2. Моніторинг та реагування на інциденти (опис SOP-ів).....	57
3.3. Впровадження рішень для тренування персоналу з питань кібербезпеки	64
3.4. Оцінка ефективності заходів.....	69
Висновки до третього розділу:	73
4. ОРГАНІЗАЦІЯ РОБОТИ СЛУЖБИ КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ ЛОГІСТИЧНОЇ КОМПАНІЇ ПІВНІЧНОЇ АМЕРИКИ.....	75
4.1. Аналіз компанії та її IT-інфраструктури.....	75
4.2. Практичні рекомендації для впровадження кіберзахисту	79
4.3. Аналіз інцидентів кібербезпеки	84
4.4. Рекомендації для подальшого розвитку систем кібербезпеки для логістичних компаній	88
Висновки до четвертого розділу:	93
ВИСНОВКИ	95
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	97

ВСТУП

Сучасні логістичні системи, що забезпечують функціонування глобальних ланцюгів постачань, трансформувалися з допоміжних сервісів у критично важливу цифрову інфраструктуру, від якої залежить економічна стабільність цілих регіонів. Для великих операторів Північної Америки, таких як корпорація FedEx, інформаційні активи – від систем управління транспортом (TMS) до хмарних баз даних – є фундаментом безперервності бізнесу. Однак стрімка цифровізація, впровадження технологій Інтернету речей (IoT) та хмарних обчислень призвели до експоненціального розширення поверхні атак. В останні роки логістична галузь стала однією з головних мішеней для транснаціональних кіберзлочинних угруповань, що використовують деструктивне програмне забезпечення типу ransomware, атаки на ланцюги постачань та складні методи соціальної інженерії.

Традиційні підходи до побудови кіберзахисту, що базуються на фрагментарному використанні технічних засобів та ручному управлінні інцидентами, створюють «сліпі зони» та критичні затримки в реагуванні. Як показав досвід масштабних атак, зокрема NotPetya, недостатній рівень сегментації мережі та відсутність злагоджених операційних процедур можуть призвести до багатомільйонних збитків та паралічу критичної інфраструктури. В умовах суворого нормативного регулювання США та Канади (NIST, CCPA, PIPEDA) проблема організації професійної та адаптивної служби кібербезпеки стає пріоритетним завданням для вищого керівництва компаній.

Мета роботи полягає у вдосконаленні організації роботи служби кібербезпеки логістичного підприємства шляхом комплексного аналізу сучасних загроз, дослідження передових практик управління безпекою в Північній Америці та розробки практичних рекомендацій щодо автоматизації процесів моніторингу та реагування на базі моделі FedEx.

Об'єктом дослідження є процеси організації та функціонування служби кібербезпеки у великих логістичних компаніях, спрямовані на забезпечення цілісності, конфіденційності та доступності даних у розподілених мережах.

Предметом дослідження є методи, стратегії, організаційні структури та технологічні рішення (SIEM, SOAR, NIST CSF), що забезпечують кіберстійкість логістичної інфраструктури та мінімізацію ризиків порушення бізнес-процесів.

Методологія роботи полягає у системному аналізі ландшафту кіберзагроз, оцінці ефективності існуючих моделей побудови SOC та розробці формалізованих операційних процедур (SOP) для реагування на критичні інциденти. У роботі визначено архітектурні підходи до побудови систем захисту за принципом «Zero Trust», що враховують специфіку північноамериканського ринку та дозволяють гарантувати стабільність постачань в умовах агресивного кіберсередовища. Практична значущість дослідження підтверджується розробкою стратегій зменшення ризиків та впровадженням програм тренування персоналу, що дозволяють перетворити людський фактор на активний елемент системи захисту підприємства.

1. АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ КІБЕРБЕЗПЕКИ ДЛЯ ЛОГІСТИЧНИХ КОМПАНІЙ

1.1. Аналіз сучасних кіберзагроз для логістичного підприємства

Логістичні компанії є критичними елементами глобальної економічної системи, оскільки забезпечують транспортування, зберігання, митне оформлення та доставку товарів між регіонами і континентами. Вони підтримують стабільність ланцюгів постачань, на яких ґрунтується виробництво, торгівля та міжнародна торгова інфраструктура. Проте цифровізація логістичних процесів, масове впровадження інтернету речей (IoT), використання хмарних платформ, аналітики великих даних (Big Data) та автоматизованих систем управління (TMS, WMS, ERP) значно розширили поверхню потенційних кіберзагроз.

У сучасних умовах логістична галузь належить до однієї з найбільш уразливих щодо кіберінцидентів. Причинами цього є висока залежність від ІТ систем, велика кількість партнерів і підрядників, використання застарілого обладнання в транспортних засобах, а також недостатній рівень зрілості служб кібербезпеки в багатьох компаніях. За даними звіту IBM X–Force Threat Intelligence Index 2024, саме транспортна та логістична галузі увійшли до п'ятірки найчастіше атакованих секторів у світі, поступаючись лише фінансовому та енергетичному [8].

Останні роки характеризуються стрімким зростанням кількості атак, спрямованих не лише на крадіжку фінансових даних, а й на порушення операційної діяльності. Згідно з Verizon DBIR 2024, понад 60 % інцидентів у сфері транспортування мали на меті тимчасове виведення систем із ладу або шантаж через блокування логістичних процесів [9]. Найпоширенішими векторами атак залишаються фішинг та компрометація облікових записів, Ransomware, Supply Chain атаки, DDos, соціальна інженерія, атаки на хмарну інфраструктуру, IoT.

Фішинг залишається найпопулярнішим вектором атаки, оскільки він експлуатує людський фактор, а не лише технічні вразливості. Зловмисники створюють переконливі підробки електронних листів, SMS чи повідомлень у корпоративних месенджерах, які імітують комунікацію від надійного джерела – це може бути внутрішній ІТ-відділ, керівник, важливий партнер чи навіть митниця.

Метою є спонукати співробітника ввести свої облікові дані на шахрайській сторінці або завантажити шкідливий файл. У логістиці такі атаки часто маскуються під повідомлення про невідкладну зміну маршруту, затримку вантажу або потребу оновити фінансові реквізити для оплати перевезень, як це було під час масштабної кампанії PhishLogi у 2023 році, націленої саме на працівників відділів доставки. Успішна компрометація лише одного облікового запису може надати зловмисникам доступ до критичних внутрішніх систем, даних про клієнтів і маршрути.

Найбільш руйнівним з фінансової точки зору є Ransomware – атаки, оскільки вони безпосередньо паралізують операційну діяльність компанії. Шкідливе програмне забезпечення, потрапляючи в корпоративну мережу, швидко шифрує критичні файли та бази даних – зокрема системи керування транспортом (TMS), складського обліку (WMS) та фінансові реєстри. Дані стають недоступними, і зловмисники вимагають великий викуп за ключ дешифрування. У логістичному секторі це миттєво призводить до зупинки відстеження вантажів, неможливості планувати маршрути і зриву термінів постачання, що, як показав інцидент 2023 року з LockBit 3.0 у Північній Америці, спричиняє багатоденні затримки та значні фінансові втрати. Крім шифрування, сучасні угруповання, такі як BlackCat (ALPHV) та Clor, часто практикують подвійне вимагання, викрадаючи дані перед шифруванням і погрожуючи їх оприлюдненням.

Атаки на ланцюг поставок стають особливо небезпечним у логістиці через її високу залежність від стороннього програмного забезпечення та широку мережу партнерів. Атака на ланцюг поставок передбачає проникнення у цільову компанію через її менш захищеного підрядника або постачальника ІТ-рішень. Замість безпосередньої атаки на великого оператора, зловмисники компрометують, наприклад, розробника популярної системи управління транспортом (TMS). Якщо їм вдається впровадити шкідливий код в оновлення чи інсталяційний пакет цього ПЗ, то всі логістичні компанії, які використовують цей продукт, автоматично отримують “ключ” для зловмисників.

DDoS-атаки спрямовані не на викрадення даних, а на знищення доступності сервісів. Зловмисники використовують мережу скомпрометованих пристроїв

(botnet) для генерації величезного обсягу трафіку, який перевантажує веб-сервери логістичної компанії. У результаті легітимні користувачі не можуть отримати доступ до сайту або сервісів. Найчастіше ціллю стають веб-сервери відстеження вантажів онлайн та портали для клієнтів. Навіть нетривалі, але масштабні DDoS-атаки можуть спричинити значні фінансові збитки та підірвати довіру клієнтів, оскільки критично важлива послуга (можливість відстеження) стає недоступною, що може призвести до зриву термінів і контрактів.

Особливу увагу привертають загрози, пов'язані з інтернетом речей, який активно використовується для моніторингу транспорту, контролю температури в холодильних контейнерах, обліку вантажів тощо. Багато IoT-пристроїв працюють із типовими паролями або не отримують оновлень безпеки. Це створює умови для атак типу botnet, коли тисячі пристроїв об'єднуються для здійснення DDoS або внутрішнього сканування мережі. Більшість IoT-пристроїв у логістиці працюють на базі спрощених операційних систем (наприклад, VxWorks, RTOS), не мають повноцінних механізмів оновлення безпеки та часто використовують стандартні облікові записи адміністратора. Це робить їх зручною ціллю для ботнетів, таких як Mirai або Mozi, які у 2023–2024 роках продовжували активно інфікувати промислові пристрої. Окремим різновидом загроз є перехоплення або підробка GPS-сигналу (GPS spoofing/jamming). Зловмисники можуть спотворювати координати транспортних засобів або контейнерів, що унеможливлює точне відстеження.

Хмарні сервіси, що широко використовуються у логістиці (Microsoft Azure, AWS, Oracle Cloud), також стають мішенню для атак. Компанії часто зберігають у хмарі інформацію про контракти, маршрути, персонал і фінансові дані. Вразливості у налаштуваннях доступу до S3-бакетів або Azure Storage призводять до витoku критично важливої інформації. Додатковим ризиком є зловживання обліковими записами адміністраторів. У разі фішингової атаки зловмисник може отримати повний контроль над хмарною інфраструктурою компанії, розгорнути нові інстанси для атаки або ексфільтрувати дані без виявлення системами моніторингу.

Геополітичні чинники та кібершпигунство також впливають на безпеку логістичному бізнесу. Зростання геополітичної напруги у світі призвело до

активізації державного кібершпигунства. Логістичні компанії стають об'єктами інтересу не лише через фінансові вигоди, а й через стратегічне значення транспортних маршрутів. Країни–конкуренти можуть прагнути отримати інформацію про вантажопотоки, контракти з оборонними або енергетичними структурами.

1.2. Аналіз вразливостей логістичних систем

Логістичні системи є складними багаторівневими структурами, що поєднують у собі інформаційні, транспортні, виробничі та управлінські процеси. Вони функціонують на основі інтеграції апаратних і програмних рішень, до яких належать корпоративні мережі, бази даних, веб–портали для клієнтів, системи управління транспортом (TMS – Transportation Management System), управління складами (WMS – Warehouse Management System), системи відстеження перевезень та інші сервіси. Така комплексність створює значну кількість потенційних точок входу для кібератак, а також підвищує ризик виникнення вразливостей, спричинених як технологічними, так і людськими факторами.

Інформаційно–технологічна інфраструктура логістичних підприємств зазвичай побудована на основі взаємодії кількох рівнів: корпоративної мережі офісів, виробничих потужностей, складів, а також розподілених транспортних вузлів. Кожен із цих елементів має власні специфічні вразливості, що можуть бути експлуатовані зловмисниками. Одним із найпоширеніших джерел ризику є використання застарілих або неправильно налаштованих систем. Через інтенсивне використання ІТ–інфраструктури, обмежений бюджет на оновлення програмного забезпечення та високий рівень інтеграції з партнерськими платформами часто спостерігається затримка з установленням оновлень безпеки. Це відкриває можливості для використання відомих експлойтів та компрометації систем.

Окрім технічних чинників, суттєву роль відіграє людський фактор. Неналежна підготовка персоналу, відсутність розуміння основ кібергігієни, нехтування корпоративними політиками безпеки створюють передумови для появи

вразливостей, що можуть бути використані у соціально-інженерних атаках, фішингових кампаніях або випадковому витоку інформації.

Мережевий рівень логістичних систем зазнає впливу широкого спектра потенційних загроз. Основними слабкими місцями є недостатньо сегментовані мережі, відкриті порти, слабе шифрування даних та використання застарілих протоколів (наприклад, FTP або HTTP замість SFTP чи HTTPS). Неналежне налаштування міжмережевих екранів або відсутність систем виявлення вторгнень (IDS/IPS) підвищує ймовірність несанкціонованого доступу до критичних ресурсів.

Логістичні компанії часто мають значну кількість віддалених підрозділів і партнерів, які взаємодіють через VPN або хмарні сервіси. У разі неправильної конфігурації VPN-тунелів або використання слабких методів автентифікації можливе перехоплення трафіку чи несанкціоноване підключення. Додатковим ризиком є використання публічних мереж для підключення мобільних пристроїв працівників або водіїв, що створює можливість атаки типу «людина посередині» (MITM).

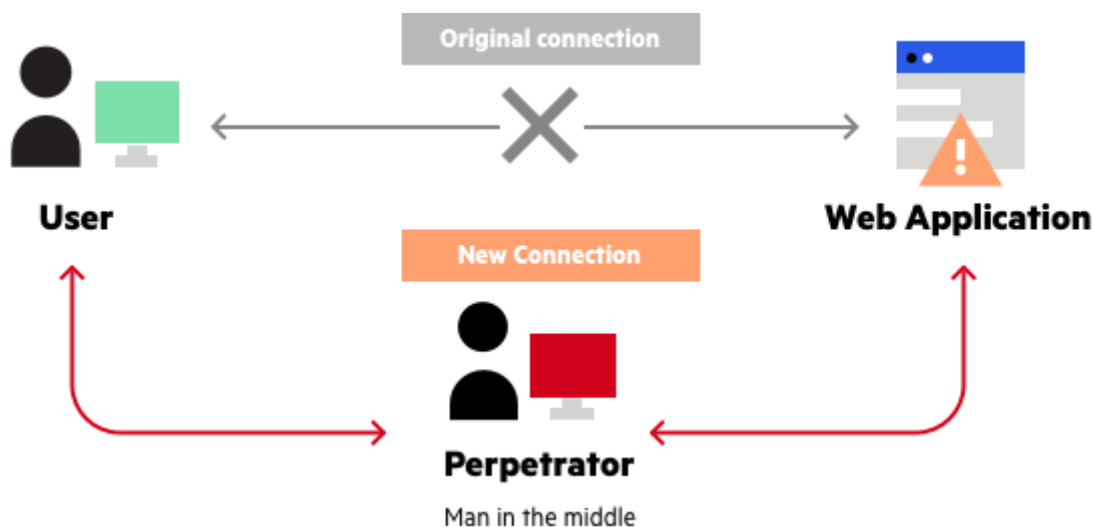


Рисунок 1.1 – Ілюстрація тактики атаки MITM

У сучасних логістичних компаніях ключову роль відіграють бази даних, у яких зберігається конфіденційна інформація про вантажі, маршрути, клієнтів і постачальників. Уразливість баз даних може призвести до витоку комерційної та персональної інформації, що, у свою чергу, порушує вимоги регламентів GDPR, ССРА та інших актів про захист даних. Типові проблеми безпеки включають:

- відсутність шифрування даних у стані спокою або під час передавання;
- використання єдиних облікових записів для кількох користувачів;
- надмірні привілеї для службових акаунтів;
- відсутність регулярного аудиту доступів;
- уразливість до SQL-ін'єкцій через некоректну валідацію вхідних даних.

Сучасні стандарти, зокрема ISO/IEC 27001 та NIST SP 800–53, рекомендують багаторівневу модель контролю доступу (RBAC), ведення журналів усіх змін у базах даних, регулярний моніторинг підозрілої активності та застосування механізмів криптографічного захисту. Логістичні підприємства широко використовують веб–додатки для взаємодії з клієнтами, партнерами та власними співробітниками. Зазвичай це портали для бронювання перевезень, відстеження замовлень, управління складськими залишками, інтегровані API для обміну даними між TMS та ERP–системами. Основними вразливостями цього рівня є:

- відсутність належної автентифікації та авторизації;
- XSS (міжсайтові сценарії) та CSRF (підробка міжсайтових запитів);
- недостатній контроль введених користувачем даних;
- використання бібліотек із відомими уразливостями;
- відсутність механізму журналювання та відстеження помилок без розкриття внутрішньої інформації.

Через інтенсивне використання відкритих API для інтеграції з партнерами підвищується ризик несанкціонованого доступу. У разі відсутності механізмів обмеження швидкості запитів (rate limiting) або використання статичних токенів автентифікації можливе зловживання ресурсами чи отримання конфіденційних даних.

Автоматизація логістичних процесів передбачає використання технологій IoT (сенсорів, сканерів штрих–кодів, GPS–трекерів, RFID–пристроїв). Ці елементи суттєво спрощують керування запасами, моніторинг транспорту й збір аналітичних даних, проте одночасно створюють новий вектор загроз. Багато IoT–пристроїв мають обмежені можливості для оновлення прошивки, не підтримують складні методи шифрування або використовують стандартні паролі. Це створює ризики:

- несанкціонованого підключення до мережі компанії;
- підміни даних про розташування або статус вантажів;
- використання IoT-пристроїв як трампліна для подальших атак.

Безпечна експлуатація таких систем передбачає сегментацію IoT-мереж, ізоляцію від корпоративного трафіку, застосування сертифікованих пристроїв та регулярне оновлення прошивок.

Окрім технічних аспектів, значну частину вразливостей утворюють організаційні недоліки такі як відсутність формалізованої політики безпеки, нечіткий розподіл ролей і відповідальностей, відсутність регулярного навчання персоналу, неналежний контроль доступу до критичної інформації. В умовах розподіленої логістичної діяльності, коли персонал може працювати дистанційно або в польових умовах, особливої ваги набуває політика управління ідентичностями (Identity Management). Недостатня перевірка повноважень користувачів або використання слабких паролів створюють ризик компрометації облікових записів і несанкціонованого доступу до систем управління перевезеннями.

Для систематизації вразливостей доцільно використовувати методики оцінки ризиків, зокрема NIST SP 800–30 та ISO 27005. Вони передбачають ідентифікацію активів, визначення потенційних загроз, оцінку ймовірності реалізації атаки та розрахунок можливих наслідків. У контексті логістичних систем особливу увагу слід приділяти вразливостям, що можуть призвести до зупинки транспортних операцій, втрати даних про маршрути або порушення роботи ланцюгів постачань. Комплексний підхід до оцінки передбачає поєднання технічного аудиту (сканування мережі, тестування на проникнення), організаційного аналізу (перевірка політик, процедур, навчання персоналу) та безперервного моніторингу з використанням SIEM-систем. Результати такого аналізу дозволяють сформувати карту вразливостей підприємства, визначити критичні точки ризику й розробити рекомендації щодо пріоритетних напрямів посилення безпеки.

З метою захисту від цих ризиків необхідно вживати відповідні заходи безпеки, включаючи захист від несанкціонованого доступу до системи, шифрування

важливих даних, регулярний аудит та дотримання вимог до конфіденційності та приватності.

1.3. Аналіз Оцінка та ідентифікація потенційних ризиків та їхнього впливу на безперервність бізнесу

У сучасних умовах цифровізації логістичних процесів управління ризиками кібербезпеки є одним із ключових елементів підтримання стабільної діяльності підприємства. Для логістичних компаній, які забезпечують транспортування, зберігання та доставку товарів у глобальних ланцюгах постачань, навіть короточасне порушення функціонування інформаційних систем може спричинити значні фінансові та репутаційні втрати. Саме тому оцінка та ідентифікація потенційних ризиків набуває стратегічного значення, оскільки дозволяє своєчасно виявляти критичні вразливості, прогнозувати можливі наслідки та забезпечувати безперервність бізнес–процесів.

Під ризиком у сфері кібербезпеки розуміють ймовірність реалізації загрози, яка може завдати шкоди інформаційним активам організації, вплинути на конфіденційність, цілісність або доступність даних. Для логістичних компаній ризик означає не лише можливість втрати даних, але й порушення фізичних процесів постачання, зупинку транспортних операцій, неузгодженість у роботі складів чи систем відстеження вантажів.

Основними характеристиками ризику є:

- ймовірність реалізації;
- потенційний вплив на бізнес;
- рівень вразливості активу;
- вартість відновлення після інциденту.

У практиці оцінки ризиків використовується класичне співвідношення:

$$\text{Ризик} = \text{Загроза} \times \text{Вразливість} \times \text{Вартість активу} \quad (1.1)$$

Ця формула дає можливість розрахувати інтегральний показник ризику та визначити його критичність для конкретного бізнес–процесу.

Світова практика кібербезпеки сформувала низку стандартів і моделей, що визначають порядок ідентифікації та аналізу ризиків. Найпоширенішими є ISO/IEC 27005, NIST SP 800–30, FAIR, OCTAVE, CMMI for Services [2,4,13,14,15].

Стандарт ISO/IEC 27005 є ключовим міжнародним керівництвом, яке надає загальні принципи та детальні вказівки щодо управління ризиками інформаційної безпеки. Цей стандарт функціонує як невід'ємна частина більшої системи ISO/IEC 27001, яка встановлює вимоги до Системи управління інформаційною безпекою (СУІБ). Методологія, визначена в ISO 27005, включає послідовну ітеративну процедуру: спочатку відбувається ідентифікація інформаційних активів, які потребують захисту; далі – визначення загроз і вразливостей, що можуть їх скомпрометувати; потім проводиться аналіз наслідків для бізнесу; і, нарешті, розробляються заходи реагування та управління ризиками, що включають їхне уникнення, передачу, зниження або прийняття [1]. Це забезпечує структурований і послідовний підхід до ризик-менеджменту в організації.

NIST SP 800–30 – це методологія, розроблена Національним інститутом стандартів і технологій США, яка пропонує поетапну процедуру для всебічного аналізу ризиків, спеціально орієнтовану на інформаційні технології та системи. Вона є частиною ширшої Рамкової програми управління ризиками NIST (Risk Management Framework, RMF). Методологія зосереджена на чотирьох ключових фазах: виявлення ризиків (ідентифікація загроз, вразливостей та впливу), оцінка ймовірності та наслідків, контроль (впровадження заходів безпеки для зниження ризиків) та моніторинг ефективності цих заходів на постійній основі. Цей підхід є високоструктурованим і широко використовується в урядових установах, а також приватних компаніях, які прагнуть до високої дисципліни в управлінні ризиками.

FAIR (Factor Analysis of Information Risk) – це інноваційний і кількісний підхід до оцінки ризиків, який відрізняється від традиційних якісних (високий, середній, низький) методів. Основна перевага FAIR полягає в тому, що він дозволяє оцінювати ризики у фінансових одиницях (грошах), перетворюючи технічні загрози на зрозумілу для бізнесу мову. Модель фокусується на аналізі компонентів ризику: частоті ймовірних загроз (threat event frequency) та ймовірних втратах (loss magnitude), а не лише на вразливостях. Такий підхід дає змогу керівництву

приймати обґрунтовані інвестиційні рішення у сфері кібербезпеки, чітко визначаючи, які заходи контролю забезпечать найбільше зниження фінансових збитків, і таким чином пріоритизувати інвестиції.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) є унікальною методикою оцінки ризиків, розробленою Університетом Карнегі–Меллона. Вона орієнтована на внутрішні процеси підприємства і має особливість залучати ключових співробітників з різних відділів (а не лише IT-фахівців) для виявлення ризиків та активів. Методика чітко фокусується на операційно критичних активах організації та включає обов'язкове врахування людського фактора як джерела вразливостей і загроз. Процес OCTAVE допомагає створити профіль захисту, визначити стратегію управління ризиками та розробити заходи безпеки, які безпосередньо відповідають потребам бізнесу та його операційним цілям.

CMMI for Services (Модель інтеграції зрілості можливостей для послуг) – це не класичний стандарт управління ризиками, а скоріше модель зрілості процесів, яка, однак, тісно інтегрує управління ризиками. Вона зосереджена на безперервному вдосконаленні процесів на рівні всієї організації, включаючи й управління ризиками. Модель описує п'ять рівнів зрілості, від початкового (випадкового) до оптимізованого (постійно вдосконалюваного), і надає структурні вимоги до того, як організація повинна планувати, виконувати, вимірювати та вдосконалювати всі свої сервісні функції, серед яких управління ризиками відіграє критичну роль. Застосування CMMI допомагає гарантувати, що управління кіберризиками є стандартизованим, прогнозованим і безперервно вдосконалюваним процесом, а не разовою перевіркою.

Для логістичних компаній доцільно використовувати комбінований підхід, що поєднує якісний та кількісний аналіз. Якісна оцінка дозволяє визначити пріоритети реагування, тоді як кількісно – оцінити фінансові наслідки потенційних інцидентів і обґрунтувати інвестиції у безпеку.

Ідентифікація ризиків є першим і найбільш критично важливим етапом у процесі управління кіберризиками, що вимагає систематичного визначення всіх можливих джерел загроз, цінних активів та потенційних сценаріїв, які можуть

призвести до порушення безпеки. У галузі логістики, де швидкість та надійність ланцюга поставок визначають успіх, збої, спричинені кіберінцидентами, можуть мати руйнівні фінансові та репутаційні наслідки. Тому процес ідентифікації повинен бути всеосяжним та охоплювати всі сфери діяльності компанії.

Активи в логістиці поділяються на кілька критичних категорій, що потребують захисту. До інформаційних ресурсів належать життєво важливі бази даних із деталями вантажів, маршрутів, фінансової звітності та, що особливо важливо, конфіденційні профілі клієнтів та партнерів, чий витік спричиняє значні юридичні та регуляторні ризики. Технічна інфраструктура включає фізичні та хмарні сервери, мережеве обладнання (як-от маршрутизатори та фаєрволи), а також критично важливі системи GPS-відстеження, без яких неможливий моніторинг вантажів у реальному часі. Програмне забезпечення складається з основних операційних інструментів: Системи управління транспортом (TMS), Складом (WMS) та Корпоративні системи (ERP/CRM), вразливість яких є прямим шляхом до паралічу бізнес-процесів. Крім того, не можна забувати про людські ресурси, чії облікові записи та знання є постійною мішенню для фішингових атак і становлять ризик інсайдерських загроз. Нарешті, зовнішні зв'язки, включаючи API-інтеграції з митними, банківськими чи партнерськими системами, є невід'ємною частиною активів, оскільки їхня компрометація відкриває доступ до наскрізного ланцюга поставок.

Для всебічного виявлення потенційних загроз для цих активів використовується низка спеціалізованих методів. Аналіз бізнес-процесів є структурним підходом, що вимагає глибокого вивчення операційних ланцюгів для визначення критичних точок відмови, наприклад, процесу формування маршруту чи митного оформлення, від яких залежить безперервність роботи компанії. Далі застосовується опитування експертів, що залучає фахівців із різних відділів (ІТ, логістики, безпеки), які, завдяки своєму унікальному досвіду, можуть виявити неформальні обхідні шляхи та недокументовані вразливості, що існують у щоденній діяльності. Важливим є аналіз інцидентів, який полягає у вивченні історичних випадків кібератак – як внутрішніх, так і тих, що трапилися у галузі – що дозволяє визначити, які загрози вже реалізувалися, і попередити повторення

відомих сценаріїв. На технічному рівні проводиться сканування вразливостей за допомогою автоматизованих інструментів, які об'єктивно виявляють технічні слабкі місця: не виправлені патчі, неправильні конфігурації або слабкі паролі на серверах та мережевому обладнанні. Завершальним етапом є мозкові штурми та використання матриць ймовірності–впливу, де команди спільно генерують сценарії загроз, а потім оцінюють кожен ризик на двовимірній шкалі за ймовірністю його виникнення та потенційним рівнем збитків, що дозволяє чітко пріоритизувати увагу керівництва на найнебезпечніших ризиках. Ризики логістичних компаній можна поділити на кілька основних категорій, такі як технічні, інформаційні, організаційні, людський фактор, операційні, зовнішні, стратегічні.

Технічні ризики безпосередньо пов'язані з фізичним або віртуальним апаратним забезпеченням та інфраструктурою, що підтримує логістичні процеси. Вони включають усі можливі відмови обладнання, збої мережевої інфраструктури, порушення роботи критично важливих серверів або недоступність хмарних сервісів. Класичними прикладами є вихід із ладу системи управління перевезеннями (TMS), що призводить до неможливості планування рейсів, або збій у GPS–серверах, який унеможлиблює відстеження вантажів. Не менш важливими є інформаційні ризики, які стосуються безпосередньо даних. Ці ризики пов'язані з витоком або знищенням конфіденційної інформації, порушенням її конфіденційності чи цілісності. Наслідком може стати несанкціонований доступ до персональних даних клієнтів, що тягне за собою штрафи, або підміна критичної інформації про вантаж чи пункт призначення, що спричиняє значні операційні збитки.

До організаційних ризиків належать ті загрози, які виникають через неефективність внутрішньої структури управління безпекою. Це може бути відсутність чітко розроблених політик кібербезпеки, застарілі інструкції або неузгодженість дій підрозділів (наприклад, між IT–відділом і відділом логістики) під час реагування на інциденти. Таке порушення внутрішньої дисципліни створює прогалини у захисті, які можуть бути використані зловмисниками. Тісно пов'язаний із цим ризик людського фактора, який охоплює як ненавмисні, так і навмисні дії працівників. Ненавмисні дії – це помилки при роботі з даними, ігнорування правил

безпеки чи потрапляння на фішинг. Навмисні дії включають зловживання наданими доступами або інсайдерську діяльність. В обох випадках співробітник стає точкою входу для реалізації кіберзагрози.

Операційні ризики безпосередньо стосуються перебоїв у роботі логістичних ланцюгів, які виникають внаслідок кібератак на ключові системи, як-от системи моніторингу, маршрутизації чи контролю складів. Реалізація такого ризику, наприклад, через успішну ransomware-атаку на WMS, призводить до зупинки завантаження/розвантаження та зриву графіків доставки. Зовнішні ризики походять від впливу третіх сторін, що особливо актуально для логістики, яка активно співпрацює з партнерами, постачальниками послуг і хмарними провайдерами. Порушення безпеки у партнера (так звана атака на ланцюг поставок) може мати каскадний ефект, відкриваючи зловмисникам шлях до всієї логістичної мережі компанії. Нарешті, стратегічні ризики відображають довгострокові наслідки недостатнього рівня кіберзахисту. Це може бути втрата конкурентоспроможності через застарілі системи безпеки або, що значно гірше, репутаційні втрати та падіння довіри клієнтів після серйозного інциденту, що може коштувати компанії майбутніх контрактів.

Безперервність бізнесу (Business Continuity) – це здатність підприємства підтримувати критично важливі функції навіть у разі кібератак, технічних збоїв або інших непередбачених подій. Для логістичних компаній безперервність означає гарантію виконання замовлень, збереження точності даних, функціонування систем відстеження та можливість комунікації з партнерами й клієнтами.

Ключовими показниками при оцінці впливу є:

- RTO (Recovery Time Objective) – максимальний допустимий час відновлення після інциденту;
- RPO (Recovery Point Objective) – допустимий обсяг втрати даних у результаті події;
- SLA (Service Level Agreement) – рівень доступності системи, визначений у договорах.

Оцінка впливу ризиків на безперервність бізнесу є критичним етапом, який формалізується шляхом побудови BIA (Business Impact Analysis) – аналізу, що

визначає критичні бізнес–процеси, залежності між ними, а також фінансові та операційні наслідки їхньої повної чи часткової зупинки. У логістичній сфері найбільш критичними процесами є планування маршрутів (TMS), управління складом (WMS) та безперервна комунікація з перевізниками й клієнтами. Встановлення часу допустимого простою (RTO) та точки відновлення даних (RPO) для цих систем є життєво необхідним, оскільки навіть короточасний збій у будь–якій із них неминуче призводить до порушення постачань, нарахування штрафних санкцій за невиконання зобов'язань та невідворотної втрати довіри і, як наслідок, клієнтів. Для проведення обґрунтованої оцінки використовуються три основні методології. Кількісний аналіз забезпечує найвищий рівень точності, оскільки він вимірює ризик у конкретних фінансових показниках, перетворюючи абстрактну загрозу на очікувану вартість простою, прямі збитки від втрати даних та необхідні витрати на відновлення. На противагу цьому, якісний аналіз використовує експертну оцінку, швидко класифікуючи ризики за шкалою на кшталт «низький – середній – високий», що є швидким, але суб'єктивним підходом. Найбільш поширеним є напівкількісний аналіз, який поєднує ці методи, використовуючи матриці ризиків. У такій матриці комбінація ймовірності виникнення загрози та потенційного впливу на бізнес формує пріоритетність реагування. Завдяки цьому ризики чітко класифікуються на чотири рівні: від низького (незначний вплив на операції) до критичного (повна зупинка діяльності або невідворотні наслідки), що спрямовує увагу керівництва.

Після оцінки кожен ризик вимагає формування цільової стратегії реагування. Перший варіант – уникнення ризику є найбільш радикальним і передбачає повну відмову від діяльності, пов'язаної з неприйнятним, надмірним ризиком. Найчастіше застосовується зниження ризику, яке полягає у впровадженні комплексу технічних та організаційних заходів: це може бути посилення захисту за допомогою антивірусу, систем запобігання витоку даних (DLP), розгортання SIEM для централізованого моніторингу подій та, безумовно, забезпечення надійного резервного копіювання. Третій підхід – передача ризику, коли фінансові наслідки інциденту перекладаються на третю сторону шляхом страхування кіберризиків або аутсорсингу функцій кібербезпеки спеціалізованим фірмам. В результаті

застосовується прийняття ризику, якщо компанія погоджується з певним його рівнем, оскільки витрати на повну мінімізацію цього ризику перевищують потенційні збитки від його реалізації.

Оцінка ризиків ніколи не є разовою процедурою; це безперервний цикл, оскільки кіберзагрози постійно еволюціонують, а ІТ–інфраструктура компанії змінюється. Тому необхідний постійний моніторинг і періодичний перегляд ризиків. Моніторинг включає аналіз журналів подій у реальному часі для виявлення аномалій та регулярний перегляд політик безпеки для їхньої актуалізації. Оцінки ризиків обов'язково оновлюються після будь-яких значних змін в ІТ–інфраструктурі або впровадження нових систем. Критичною частиною цього процесу є проведення тестувань на проникнення (penetration testing), які імітують реальні атаки для виявлення вразливостей, а також оцінка ефективності вже впроваджених контрзаходів, щоб гарантувати, що загальний профіль ризику компанії перебуває під постійним контролем.

Висновки до першого розділу:

У результаті проведеного аналізу встановлено, що логістичні компанії є одними з найуразливіших секторів до кіберзагроз у сучасному цифровому середовищі. Високий рівень автоматизації процесів, активна взаємодія з зовнішніми партнерами, використання хмарних сервісів, а також залежність від систем управління постачаннями створюють широкий спектр можливостей для кіберзлочинців. Визначено, що основними загрозами для підприємств логістичної галузі є фішинг, атаки на ланцюги постачання, шкідливе програмне забезпечення типу ransomware, компрометація облікових даних, DDoS–атаки, а також порушення конфіденційності клієнтських і партнерських даних. Ці загрози мають потенціал не лише спричинити фінансові втрати, а й серйозно вплинути на репутацію компанії та безперервність бізнес–процесів. У ході аналізу вразливостей логістичних систем встановлено, що найчастіше слабкими місцями виступають неоновлене або неправильно сконфігуроване програмне забезпечення, відсутність сегментації мережі, недостатній рівень контролю доступу, а також людський фактор, що залишається одним із ключових елементів ризику. Також виявлено, що

ефективна оцінка ризиків має базуватися на системному підході, який враховує як технічні, так і організаційні аспекти. Важливо не лише визначати можливі джерела загроз, але й оцінювати їхній потенційний вплив на операційну діяльність підприємства, включно з фінансовими та репутаційними наслідками.

Отже, проведений аналіз дозволяє зробити висновок, що побудова ефективної системи кіберзахисту в логістичних компаніях потребує комплексного підходу, який охоплює виявлення загроз, усунення вразливостей, управління ризиками та формування культури кібербезпеки серед персоналу. Саме ці аспекти становлять основу для подальшого дослідження, спрямованого на розробку оптимальної структури служби кібербезпеки підприємства.

2. АНАЛІЗ СУЧАСНИХ ПРАКТИК ОРГАНІЗАЦІЇ СЛУЖБИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Структурний аналіз служби кібербезпеки

Організація служби кібербезпеки є одним із ключових елементів побудови ефективної системи захисту інформаційних ресурсів підприємства. В умовах цифровізації бізнесу, зростання кількості кіберінцидентів та посилення нормативних вимог до захисту даних, наявність структурованої служби кібербезпеки стає необхідною умовою стабільного функціонування компанії. Сучасна служба кібербезпеки – це не лише технічний підрозділ, який відповідає за налаштування засобів захисту. Це багаторівнева організаційна структура, що поєднує управлінські, аналітичні, технічні та операційні функції. Її діяльність спрямована на забезпечення конфіденційності, цілісності та доступності інформації, а також на підтримку бізнес–процесів у безпечному середовищі.

Розробка функціональної та надійної структури служби кібербезпеки вимагає дотримання низки ключових принципів, які гарантують її ефективність та інтеграцію в загальну бізнес–діяльність компанії. Цілісність є фундаментальним принципом, що визначає необхідність того, що служба безпеки не повинна бути ізольована лише в межах ІТ–відділу, а мусить охоплювати абсолютно всі напрями діяльності підприємства [22,24]. Це означає, що її політики, процедури та контроль мають поширюватися на фінансові операції, критичну логістичну діяльність (включно з TMS і WMS), а також на взаємодію з партнерами та зовнішніми підрядниками. Служба повинна забезпечувати наскрізний захист, оскільки будь–яка неконтрольована «сіра зона» в діяльності компанії, незалежно від того, чи це фізична безпека складу, чи обмін даними з клієнтом, стає потенційним вектором атаки.

Принцип ієрархічності передбачає чіткий та раціональний розподіл повноважень і відповідальності за окремими напрямками безпеки всередині структури. Ця вертикальна та горизонтальна організація дозволяє уникнути дублювання функцій і забезпечує швидке прийняття рішень. Наявність визначених ролей (наприклад, CISO, аналітик SOC, інженер з безпеки) та чітких ланцюжків

підпорядкування є критично важливою для ефективної координації дій при виникненні інцидентів. Завдяки ієрархії, кожен співробітник служби точно знає свою роль у разі кіберкризи, що забезпечує швидке та структуроване реагування, мінімізуючи час простою. Безперервність функціонування служби кібербезпеки є абсолютною вимогою, оскільки кібератаки не мають робочого графіку. Це означає, що всі процеси моніторингу, виявлення та реагування на загрози мають бути цілодобовими (24/7), часто реалізуючись через Центри операційної безпеки (SOC). Забезпечення безперервності вимагає не лише технічних засобів (наприклад, SIEM-систем), але й відповідної ротації персоналу та планування стійкості самих систем безпеки. Якщо моніторинг припиняється навіть на короткий час, компанія стає сліпою перед обличчям активної загрози.

Принцип адаптивності підкреслює, що структура служби безпеки не може бути статичною. Вона повинна бути гнучкою, щоб оперативно реагувати на дві ключові динамічні зміни: зміни у бізнес-моделі компанії (наприклад, перехід на нові хмарні сервіси чи вихід на новий ринок) та розвиток нових кіберзагроз. Служба має мати механізми для швидкого впровадження нових технологій захисту, перегляду політик та перекваліфікації персоналу. Адаптивність гарантує, що заходи безпеки залишаються актуальними, ефективно протидіючи найновішим тактикам і методам зловмисників.

Незважаючи на те, що архітектура служби кібербезпеки може варіюватися залежно від масштабу підприємства, складності його ІТ-інфраструктури та галузевих вимог, існує універсальна модель, що включає низку ключових підрозділів. Кожен із них має чітко визначену відповідальність, забезпечуючи комплексний захист активів.

На чолі служби стоїть Керівник з інформаційної безпеки (CISO – Chief Information Security Officer), який несе відповідальність за стратегічне управління всією сферою інформаційної безпеки компанії. Основні його завдання виходять за рамки технічної реалізації: CISO займається визначенням політики безпеки на рівні всієї організації, управлінням кіберризиками в контексті бізнес-цілей, розробкою планів реагування на інциденти та, що особливо важливо, взаємодією з вищим керівництвом для обґрунтування інвестицій у безпеку та інтеграції захисту в

корпоративну стратегію. Фактично, CISO є мостом між технічним захистом та бізнес-рішеннями.

Відділ управління ризиками та комплаєнсу (Risk & Compliance Unit) – є гарантом того, що діяльність компанії відповідає як внутрішнім, так і зовнішнім вимогам. Його ключова функція полягає у систематичній оцінці кіберризиків, використовуючи кількісні та якісні методи аналізу, а також у розробці внутрішніх нормативних документів, стандартів та процедур безпеки. Важливою частиною роботи є контроль відповідності (комплаєнс) діяльності підприємства міжнародним стандартам (таким як ISO/IEC 27001, NIST) та регуляторним вимогам (наприклад, GDPR або галузеві нормативи), що є критичним для уникнення штрафів і підтримки довіри.

Центр операцій безпеки (SOC) – це серце операційного захисту, що функціонує в режимі 24/7. Його завдання – постійний моніторинг інформаційних систем, виявлення загроз у реальному часі та аналіз подій безпеки, що генеруються різними пристроями. SOC використовує складні інструменти, зокрема SIEM-системи (Security Information and Event Management) для кореляції даних, аналітичні платформи та автоматизовані засоби реагування (SOAR). У разі виявлення загрози саме SOC забезпечує координацію первинних дій для локалізації інциденту.

Відділ технічного захисту відповідає за технічну реалізацію та підтримку всіх захисних заходів на інфраструктурному рівні. Його фахівці займаються налаштуванням та обслуговуванням міжмережевих екранів (фаєрволів), систем виявлення вторгнень, антивірусних рішень, а також впровадженням політик контролю доступу на мережевому та системному рівнях. Крім того, вони забезпечують шифрування даних (як при передачі, так і при зберіганні) та функціонування систем резервного копіювання, що є основою для відновлення після інциденту.

Відділ розслідування інцидентів (Digital Forensics & Incident Response – DFIR) спеціалізується на глибокому аналізі та розслідуванні вже сталих кіберінцидентів. Їхня робота починається після локалізації загрози і полягає у зборі цифрових доказів (судова експертиза), визначенні джерел та методів атак і оцінці нанесеної

шкоди. На основі проведеного розслідування вони готують детальні звіти та рекомендації щодо запобігання повторним інцидентам, допомагаючи відділу технічного захисту посилити слабкі місця.

Відділ управління ідентифікацією та доступом (Identity and Access Management – IAM) відповідає за процеси автентифікації користувачів, розмежування прав доступу на основі ролей та управління життєвим циклом облікових записів. Ключовий принцип, який реалізує IAM, – це принцип «мінімально необхідних прав», гарантуючи, що співробітники мають доступ лише до тих даних і систем, які абсолютно необхідні для виконання їхніх безпосередніх обов’язків, що значно знижує ризик внутрішніх та зовнішніх загроз.

Відділ навчання та підвищення обізнаності персоналу (Security Awareness & Training Unit) – зосереджений на формуванні стійкої культури безпеки серед усіх співробітників. Він організовує регулярні тренінги та семінари, проводить симуляції фішингових атак для перевірки пильності, а також веде інформаційні кампанії та внутрішні сертифікаційні програми. Мета цього відділу – перетворити кожного співробітника з потенційного ризику на першу лінію захисту.

Хоча детально описана ієрархічна структура, яка складається з семи окремих відділів є найкращою практикою для великих корпорацій, які можуть дозволити собі таку спеціалізацію, менші та середні логістичні компанії керуються принципом функціонального об’єднання. Вони не створюють окремі відділи, а натомість інтегрують їхні ключові функції в існуючі структури: стратегічне управління ризиками та комплаєнсом об’єднується на рівні ISM або CISO, технічний захист і базовий моніторинг SOC стає розширеною відповідальністю IT-відділу або єдиного фахівця з безпеки, а високоспеціалізовані функції, як розслідування інцидентів та глибоке навчання персоналу, найчастіше передаються на аутсорсинг зовнішнім експертам. Таким чином, менші компанії досягають необхідного рівня захисту, використовуючи гнучкішу та економічно виправдану модель.

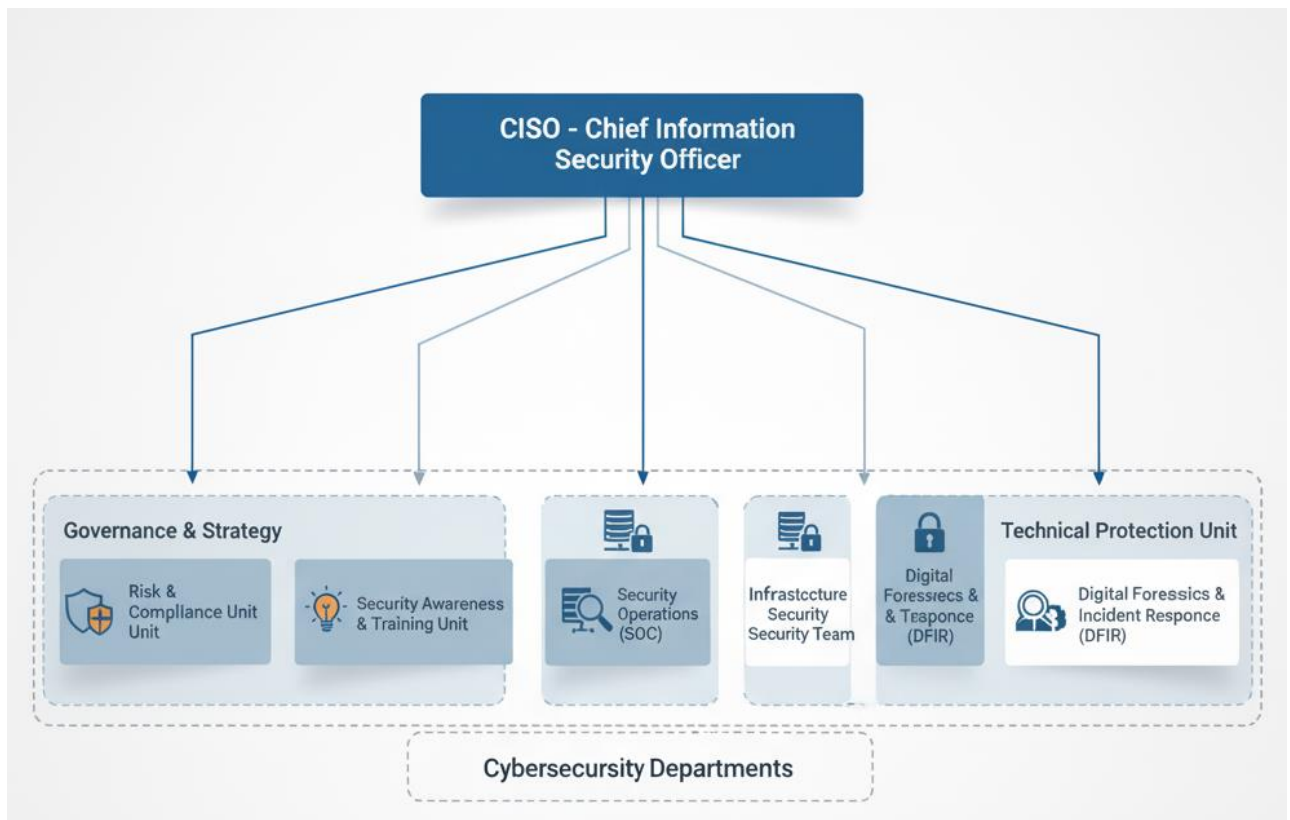


Рисунок 2.1 – Ілюстрація рекомендованої ієрархічної моделі відділу кібербезпеки для великого підприємства

Служба кібербезпеки зазвичай підпорядковується або директору з інформаційних технологій або безпосередньо виконавчому директору, залежно від стратегічної ролі безпеки в організації. У великих міжнародних компаніях служба кібербезпеки функціонує як окремий департамент, який координує свою діяльність із підрозділами ІТ, юридичним відділом, відділом внутрішнього аудиту та управління персоналом. Важливою складовою сучасного підходу є інтеграція кібербезпеки у бізнес-процеси. Це означає, що служба безпеки повинна брати участь не лише у захисті даних, а й у плануванні нових ІТ-рішень, виборі постачальників, аналізі ризиків при укладенні партнерських угод тощо.

Залежно від масштабів і потреб підприємства, існують три основні моделі побудови служби кібербезпеки:

- Централізована модель – усі функції кіберзахисту зосереджені в одному підрозділі. Використовується у компаніях із єдиною інфраструктурою.

- Децентралізована модель – кожен бізнес–напрямок має власну службу безпеки, яка координується головним офісом. Підходить для міжнародних корпорацій.

- Гібридна модель – поєднання централізованого управління з автономністю окремих підрозділів. Вважається оптимальним варіантом для логістичних компаній, що мають розгалужену мережу філій і партнерів.

Попри високий рівень автоматизації, ефективність служби кібербезпеки значною мірою залежить від професіоналізму її співробітників. Ключові компетенції спеціалістів включають знання стандартів безпеки, навички аналізу кіберінцидентів, вміння працювати з аналітичними системами та інструментами моніторингу. Не менш важливою є взаємодія між підрозділами – обмін інформацією, спільна участь у розслідуваннях, координація дій під час кризових ситуацій.

Таким чином, ефективна служба кібербезпеки – це цілісна система, що поєднує управлінські рішення, технічні засоби та людський потенціал. Її функціонування має бути спрямоване не лише на усунення наслідків інцидентів, а й на профілактику загроз та формування проактивної безпекової культури в межах усього підприємства.

2.2. Оцінка та ідентифікація потенційних ризиків та їхнього впливу на безперервність бізнесу

Ефективна модель побудови кіберзахисту є фундаментом для стабільного функціонування будь–якого сучасного підприємства, особливо у галузі логістики, де інформаційні технології інтегровані у всі виробничі, транспортні та управлінські процеси. Модель кіберзахисту визначає логіку, рівні, взаємодію компонентів та принципи управління безпекою в межах організації. У міжнародній практиці сформувалися декілька підходів до організації кіберзахисту, серед яких найпоширенішими з яких є:

- модель управління на основі ризиків;
- модель “Defense in Depth”, Zero Trust Architecture;

- модель безпеки на основі комплаєнсу;
- інтегрована модель управління безпекою.

Модель управління на основі ризиків (Risk-Based Approach) базується на оцінці та пріоритизації ризиків для бізнесу. Ключовою ідеєю є зосередження ресурсів на захисті найважливіших активів, які мають найвищу цінність або найбільшу вразливість. Управління ризиками включає етапи ідентифікації, оцінки, моніторингу та контролю ризиків. Основна перевага цієї моделі полягає у можливості гнучко реагувати на зміни зовнішнього середовища та оптимально розподіляти ресурси.

Принцип моделі “Defense in Depth” полягає у створенні кількох незалежних шарів захисту, кожен із яких виконує власну функцію: мережеву, прикладну, користувацьку тощо [25,29]. Якщо один із рівнів буде скомпрометовано, інші продовжують захищати систему. Така модель забезпечує високу стійкість до складних атак і є стандартом для великих організацій, зокрема логістичних компаній, які мають розгалужену мережеву інфраструктуру.

Zero Trust Architecture опирається на принцип “нікому не довіряй, завжди перевіряй”. Доступ до ресурсів надається лише після багатоетапної автентифікації, незалежно від того, де перебуває користувач – у внутрішній мережі чи за її межами. Zero Trust забезпечує мінімалізацію ризиків внутрішніх загроз і захищає підприємства від атак через скомпрометовані облікові записи або ненадійних партнерів.

Модель безпеки на основі комплаєнсу використовується переважно компаніями, які зобов’язані дотримуватись міжнародних стандартів – ISO/IEC 27001, NIST SP 800–53, PCI DSS тощо. Головна мета полягає у забезпеченні відповідності нормативним вимогам та регулярному аудиту системи кіберзахисту.

Інтегрована модель управління безпекою поєднує технічні, організаційні та кадрові заходи. Передбачає постійну взаємодію між службами ІТ, управління ризиками, внутрішнього аудиту та відділом безпеки. Ця модель розглядає кіберзахист не як окремий процес, а як складову частину корпоративного управління.

Модель кіберзахисту охоплює сукупність організаційних, технічних і процедурних заходів, які формують єдину систему безпеки. Ефективний кіберзахист неможливий без інтеграції цих складових, які умовно поділяються на п'ять ключових рівнів. Детальну структуру рівнів та відповідних заходів, демонструючи цілісний підхід до побудови стійкої кібербезпеки організаці, відображено в таблиці 2.1..

Таблиця 2.1.

Складові моделі кіберзахисту

Рівень моделі кіберзахисту	Основні складові та заходи
Управлінський рівень	Розробка політик безпеки, призначення відповідальних осіб (CISO, керівники підрозділів), формування планів реагування на інциденти, визначення KPI служби безпеки.
Організаційний рівень	Проведення аудитів інформаційної безпеки, навчання персоналу, впровадження процесу контролю доступу, управління підрядниками та постачальниками
Технічний рівень	Мережева сегментація, використання SIEM, IDS/IPS, DLP, антивірусних систем, шифрування даних, авторизація моніторингу та реагування.
Аналітичний рівень	Збір і кореляція подій безпеки, виявлення аномалій, розслідування інцидентів, побудова моделей загроз.
Процесний рівень	Інтеграція кібербезпеки у життєвий цикл IT-проєктів (DevSecOps), документування інцидентів і контроль ефективності дій, перегляд стратегій безпеки відповідно до змін у бізнесі.

Для ефективної оцінки та вдосконалення стану кіберзахисту підприємства застосовуються стандартизовані моделі зрілості (Maturity Models). Ці методики дають можливість не просто зафіксувати поточний рівень безпеки, а й визначити, наскільки формалізовані, керовані та безперервно вдосконалювані відповідні процеси.

CMMI (Capability Maturity Model Integration) – це комплексна модель зрілості, яка визначає п'ять рівнів зрілості процесів безпеки. Ця модель допомагає організації зрозуміти, наскільки її процеси є контрольованими та передбачуваними. Рівні варіюються від початкового, де процеси є непередбачуваними та неконтрольованими, до оптимізованого, де впроваджено механізми безперервного удосконалення на основі кількісних даних та інновацій. Застосування CMMI дозволяє керівництву оцінити, чи має служба кібербезпеки лише реактивний характер, чи працює проактивно, постійно підвищуючи ефективність своїх дій.

NIST CSF – це одна з найбільш популярних і гнучких рамок, розроблена Національним інститутом стандартів і технологій США [3]. Вона описує п'ять ключових функцій, що створюють життєвий цикл управління кіберризиками: Ідентифікація (Identify), Захист (Protect), Виявлення (Detect), Реагування (Respond) та Відновлення (Recover). Фреймворк допомагає організаціям усіх розмірів та секторів, зокрема, він широко використовується урядовими установами та приватним сектором (наприклад, логістичними компаніями у США та Канаді) для пріоритизації інвестицій та ефективного управління ризиками. Це практичний інструмент для комунікації ризиків між технічними спеціалістами та вищим керівництвом.

ISO/IEC 27001 є найбільш визнаним міжнародним стандартом, який встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення Системи управління інформаційною безпекою. Стандарт вимагає від організації системного підходу до управління конфіденційною інформацією, її доступністю та цілісністю. На відміну від моделей зрілості, які фокусуються на оцінці процесів, ISO/IEC 27001 є сертифікаційним стандартом. Його успішне

впровадження та проходження аудиту свідчить про дотримання міжнародних найкращих практик і значно підвищує довіру клієнтів і партнерів.

Порівняння практичної реалізації цих підходів надає керівництву підприємства об'єктивну картину стану кіберзахисту. Використовуючи результати оцінки, можна чітко визначити сильні та слабкі сторони поточної системи, а також сформулювати дорожню карту для її вдосконалення. Це дозволяє ефективно розподілити ресурси, пріоритезувати інвестиції у безпеку та забезпечити неперервну відповідність зовнішнім і внутрішнім вимогам.

При побудові моделі кіберзахисту в логістичній галузі слід звернути увагу на деякі особливості. Логістичні компанії мають унікальні виклики, що зумовлюють необхідність адаптації моделі кіберзахисту до специфіки галузі:

- велика кількість взаємопов'язаних інформаційних систем, зокрема ERP, WMS, TMS, CRM, які потребують узгодженого управління доступом і моніторингу;
- інтенсивний обмін даними з партнерами та клієнтами, що підвищує ризик компрометації через ланцюг поставок;
- використання IoT-пристроїв для відстеження транспорту, вантажів і складів, що створює додаткові вектори атак;
- географічна розгалуженість мережі підрозділів, що ускладнює централізований контроль.

Тому оптимальна модель кіберзахисту для логістичних підприємств має включати такі характеристики:

- централізований моніторинг із використанням SIEM;
- багаторівневий контроль доступу та автентифікації;
- регулярне тестування на проникнення;
- політики сегментації мереж і резервного копіювання;
- наявність кризових процедур і планів відновлення після інцидентів (Disaster Recovery Plans).

Модель кіберзахисту не повинна існувати ізольовано від бізнес-цілей компанії. Вона має інтегруватись у стратегічне планування, управління ризиками та процеси прийняття рішень. Ефективна взаємодія забезпечується за допомогою

участі служби безпеки у всіх етапах і розробці IT-рішень, проведенні оцінки безпеки для нових партнерських угод, створення спільних робочих груп між IT і бізнес-підрозділами, регулярне звітування CISO перед керівництвом компанії. У сучасних умовах дедалі більше компаній переходять до моделі “Безпека як сервіс” (SECaaS), що передбачає часткову або повну передачу функцій кіберзахисту зовнішньому постачальнику. Цей підхід дозволяє знизити витрати, отримати доступ до передових технологій і забезпечити цілодобовий моніторинг безпеки. Проте для логістичних компаній такий підхід потребує ретельного вибору провайдера, перевірки його відповідності стандартам безпеки та контролю за обробкою даних.

Оцінка моделі побудови кіберзахисту показує, що сучасні підприємства повинні дотримуватися принципу багаторівневості, орієнтації на ризики та інтеграції безпеки у всі бізнес-процеси. Найбільш ефективною для логістичної сфери є гібридна модель кіберзахисту, що поєднує централізоване управління з локальною гнучкістю філій. Також важливою тенденцією є перехід від реактивного до проактивного підходу, коли безпека розглядається не лише як засіб реагування, а як стратегічний елемент управління підприємством

2.3. Аналіз інструментів та технологій кібербезпеки (SIEM, IDS/IPS, DLP)

Забезпечення кіберзахисту сучасних логістичних підприємств вимагає впровадження комплексу технологічних рішень, спрямованих на моніторинг, виявлення, попередження та реагування на інциденти безпеки. Зі зростанням обсягів оброблюваних даних, кількості підключених пристроїв та збільшенням кількості атак на критичну інфраструктуру, традиційні засоби захисту стають недостатніми. У цьому контексті провідну роль відіграють такі інструменти, як системи управління інформаційною безпекою (SIEM), системи виявлення та запобігання вторгненням (IDS/IPS), а також системи запобігання витоку даних (DLP). Вони формують основу сучасної архітектури кіберзахисту, забезпечуючи комплексний підхід до контролю інформаційних потоків, моніторингу подій та управління ризиками.

Системи управління інформаційною безпекою (Security Information and Event Management, SIEM) є центральним елементом будь-якої корпоративної системи кіберзахисту. Основна мета SIEM полягає у зборі, нормалізації, кореляції та аналізі подій безпеки, що надходять з різних джерел – серверів, мережевого обладнання, систем автентифікації, прикладних програм, хмарних сервісів тощо. У логістичних компаніях, де використовуються різноманітні технологічні платформи та системи управління транспортом, SIEM виконує функцію інтегратора, який забезпечує централізований огляд стану безпеки в усіх підрозділах підприємства. Основна цінність SIEM полягає в її здатності здійснювати кореляцію подій у режимі реального часу. Це дозволяє виявляти складні багатоступеневі атаки, які неможливо зафіксувати окремими компонентами системи захисту. Наприклад, поєднання подій спроби автентифікації з віддаленої адреси, несанкціонованої зміни конфігураційних файлів і спроби передачі даних у зовнішню мережу може сигналізувати про спробу компрометації облікового запису адміністратора. Саме такі ситуації SIEM-система фіксує як інциденти високого рівня ризику, сповіщаючи фахівців служби безпеки для оперативного реагування.

Особливе значення для логістичних підприємств має можливість інтеграції SIEM з хмарними платформами, сервісами відстеження вантажів і корпоративними ERP-системами. Це дозволяє аналізувати не лише технічні події, а й бізнес-процеси, що створює умови для виявлення аномалій у роботі логістичних ланцюгів. Сучасні SIEM-платформи, такі як Splunk Enterprise Security, IBM QRadar, ArcSight або Wazuh, застосовують елементи машинного навчання для автоматичної класифікації подій і підвищення точності виявлення інцидентів. Важливою тенденцією розвитку SIEM є перехід до концепції Security Operations Center (SOC) як сервісу, що базується на хмарних технологіях. У логістичному секторі це особливо актуально, адже багато компаній мають розподілену структуру філій, складів і транспортних хабів. Централізований SOC, оснащений SIEM-системою, дозволяє здійснювати єдиний моніторинг усіх активів, забезпечуючи при цьому масштабованість і високу швидкість реагування. Таким чином, SIEM виступає не лише технологічним рішенням, а й ключовим компонентом управління ризиками кібербезпеки в логістичному бізнесі.

Другим фундаментальним елементом інфраструктури кіберзахисту є системи виявлення та запобігання вторгненням – IDS (Intrusion Detection System) та IPS (Intrusion Prevention System). Їх основна функція полягає у контролі мережевого трафіку з метою виявлення підозрілої активності, спроб вторгнення або порушення політик безпеки. IDS виконує роль пасивного монітора, який аналізує мережеві пакети та фіксує можливі загрози, тоді як IPS діє проактивно – блокує небажаний трафік у режимі реального часу. У контексті логістичних компаній IDS/IPS є критичними для забезпечення безпечного обміну даними між транспортними засобами, складами, філіями та зовнішніми контрагентами. Сучасні системи цього типу здатні виявляти не лише сигнатурні атаки (з відомими шаблонами), а й аномальні дії, які виходять за межі нормальної поведінки мережі. Це дозволяє виявляти цілеспрямовані атаки, що здійснюються з використанням нульових днів (zero-day exploits).

Важливою особливістю впровадження IDS/IPS у логістичному середовищі є потреба в оптимальному налаштуванні для мінімізації хибних спрацювань. Надмірна кількість сповіщень може призвести до перевантаження аналітиків SOC, тому системи повинні бути адаптовані під специфіку трафіку підприємства. Для цього використовуються технології глибокого аналізу пакетів (Deep Packet Inspection), а також алгоритми поведінкового аналізу, які навчаються на основі історичних даних. З технічної точки зору, сучасні IDS/IPS рішення підтримують інтеграцію з SIEM-системами, що дозволяє здійснювати централізовану кореляцію подій. Наприклад, події виявлення аномальної активності в IDS можуть автоматично передаватися до SIEM для подальшого аналізу в контексті інших джерел даних. Таким чином, формується єдина система захисту, де мережеві сенсори виступають першою лінією оборони, а SIEM забезпечує комплексну аналітику та координацію реагування.

Окремо варто зазначити роль IDS/IPS у захисті промислових і транспортних мереж, які використовують спеціалізовані протоколи (наприклад, MQTT, Modbus або CAN). Для логістичних компаній, які застосовують інтелектуальні системи моніторингу транспорту або автоматизовані склади, це має принципове значення. Наявність IDS/IPS у таких середовищах дозволяє не лише виявляти спроби

втручання, а й забезпечувати безперервність бізнес–процесів, що безпосередньо впливають на ефективність доставки та збереження вантажів.

Системи запобігання витоку даних (Data Loss Prevention, DLP) становлять ще один ключовий елемент комплексної системи захисту інформації логістичних підприємств. Їх призначення полягає у контролі руху конфіденційної інформації, запобіганні несанкціонованій передачі корпоративних даних та моніторингу дій користувачів. У логістичному секторі обробляються величезні обсяги даних, пов'язаних із клієнтами, маршрутами перевезень, договорами, митними деклараціями, страховими документами та фінансовими транзакціями. Витік будь–якої з цих категорій даних може призвести до серйозних фінансових збитків і втрати репутації. DLP–системи дозволяють запобігати подібним інцидентам за рахунок комплексного контролю каналів передачі інформації – електронної пошти, USB–носіїв, хмарних сервісів, веб–додатків та внутрішньої мережі підприємства. Технологічна архітектура DLP включає кілька рівнів контролю: захист даних у русі (Data in Motion), захист даних у стані спокою (Data at Rest) та захист даних у використанні (Data in Use). Такий підхід забезпечує безперервний моніторинг усіх етапів життєвого циклу інформації. Наприклад, система може блокувати спробу копіювання файлу на флеш–накопичувач або надсилання конфіденційного документа через незашифрований канал зв'язку.

DLP є не лише технічним засобом, а й інструментом реалізації політики інформаційної безпеки. Вона дозволяє формалізувати правила доступу, визначати категорії конфіденційних даних та здійснювати аудит дій користувачів. Крім того, сучасні системи DLP застосовують елементи контентного аналізу, що базуються на машинному навчанні, здатні ідентифікувати інформацію за змістом, а не лише за метаданими або шаблонами. Особливе значення DLP має у випадках, коли підприємство взаємодіє з великою кількістю партнерів і підрядників. У таких умовах контроль інформаційних потоків дозволяє запобігти витокам через людський фактор або недбалість зовнішніх постачальників. Таким чином, DLP забезпечує не лише технічний, але й організаційний рівень захисту, сприяючи формуванню культури безпечного поводження з даними.

Для досягнення максимальної ефективності всі розглянуті технології мають бути інтегровані в єдину архітектуру кіберзахисту. SIEM виконує роль аналітичного центру, IDS/IPS – першої лінії оборони, а DLP – бар’єра для захисту конфіденційної інформації. Взаємодія цих систем забезпечує замкнутий цикл кіберзахисту – від виявлення загрози до реагування та запобігання повторним інцидентам. У логістичних компаніях Північної Америки така інтеграція часто реалізується на основі хмарних платформ безпеки, які дозволяють централізовано управляти політиками доступу, оновленнями сигнатур та аналітичними правилами. Завдяки цьому підприємства можуть швидко адаптувати свої системи безпеки до нових типів загроз і забезпечувати відповідність міжнародним стандартам, таким як ISO/IEC 27001, NIST CSF чи SOC 2.

Для ефективного забезпечення кіберзахисту логістичних підприємств необхідно обґрунтовано підбирати інструменти, що відповідають конкретним потребам інфраструктури. Вибір між SIEM, IDS/IPS та DLP–системами залежить від рівня зрілості IT–інфраструктури, обсягів даних, ризик–профілю та ресурсів компанії. В додатку А наведено узагальнене порівняння, яке демонструє ключові характеристики, призначення та відмінності між основними типами рішень у сфері кіберзахисту.

2.4. Аналіз рішень для автоматизації моніторингу безпеки

Сучасний етап розвитку логістичних підприємств характеризується безпрецедентним ускладненням інформаційно–технологічного ландшафту, що зумовлено конвергенцією традиційних корпоративних мереж, хмарних обчислювальних потужностей та розгалужених сегментів Інтернету речей. Як було встановлено в попередніх розділах, логістичні оператори покладаються на динамічну взаємодію систем управління транспортом (TMS) та складами (WMS), які функціонують у режимі реального часу. Проте, саме ця висока швидкість обробки даних створює критичний розрив між виявленням кіберзагрози та технічною здатністю персоналу на неї зреагувати. Традиційні підходи до

управління безпекою, що базуються на ручному втручанні адміністраторів через інтерфейси командного рядка або графічні консолі окремих засобів захисту, вичерпали свій ресурс ефективності. Це призводить до виникнення системної кризи контролю, коли кількість подій безпеки, що генеруються SIEM–системами та мережевими сенсорами, перевищує когнітивні можливості людського персоналу щодо їхнього якісного аналізу та верифікації.

У контексті забезпечення безперервності бізнесу, ручне управління конфігураціями мережевої безпеки створює декілька фундаментальних ризиків.

По–перше, виникає явище «дрейфу конфігурацій» (configuration drift), при якому налаштування безпеки на різних географічно розподілених вузлах логістичної мережі починають відрізнятися через людські помилки, неповне виконання регламентів або забудькуватість персоналу при оновленні правил міжмережєвих екранів.

По–друге, час реакції на інцидент (Mean Time to Respond, MTTR) у ручному режимі вимірюється годинами або навіть днями, що є абсолютно неприйнятним для галузі, де зупинка ланцюга постачань на кілька годин спричиняє багатомільйонні збитки.

По–третє, складність сучасних цілеспрямованих атак (APT) вимагає миттєвої координації між різними засобами захисту – від блокування порту на комутаторі до ізоляції хоста в хмарі – що технічно неможливо здійснити синхронно без використання засобів автоматизації.

Для подолання вказаних дефіцитів безпеки виникає необхідність впровадження концепції оркестрації та автоматизації (Security Orchestration, Automation and Response – SOAR). На відміну від класичних систем моніторингу, які лише констатують факт аномалії, автоматизована екосистема дозволяє трансформувати виявлену загрозу в набір конкретних технічних дій без залучення людини на кожному етапі. У логістичному секторі, де загрози часто мають каскадний характер (наприклад, компрометація одного GPS-трекера може призвести до підміни даних у всій системі моніторингу вантажів), автоматизація дозволяє локалізувати інцидент на етапі його зародження.

Методологічне обґрунтування автоматизації базується на необхідності досягнення детермінованого стану мережі. Кожна політика безпеки, розроблена на управлінському рівні служби кібербезпеки, повинна існувати не лише у вигляді текстового документа, а й у вигляді програмного коду, який автоматично розгортається на інфраструктурі. Це дозволяє реалізувати принцип «Security by Design», де будь-який новий сегмент мережі (наприклад, новий складський термінал або термінал самообслуговування) автоматично отримує еталонні налаштування безпеки в момент підключення до корпоративної мережі. Такий підхід мінімізує вплив людського фактора є причиною понад 60 % інцидентів у сфері транспортування

Впровадження засобів автоматизації налаштувань безпеки стає можливим завдяки розвитку технологій програмно–визначених мереж (SDN) та віртуалізації мережевих функцій (NFV). У минулому мережеве обладнання було закритим та пропрієтарним, що ускладнювало зовнішнє управління. Сучасні маршрутизатори, комутатори та брандмауери підтримують відкриті протоколи управління та API, що відкриває шлях для інструментів інфраструктурної автоматизації. Для логістичного підприємства це означає можливість централізованого управління безпекою тисяч кінцевих пристроїв з єдиної точки контролю. Окрім суто технічних переваг, автоматизація процесів реагування дозволяє оптимізувати навантаження на службу кібербезпеки. Замість виконання рутинних операцій з оновлення патчів або блокування скомпрометованих IP-адрес, фахівці SOC можуть зосередитися на стратегічному аналізі загроз та розслідуванні складних інцидентів (DFIR). Таким чином, автоматизація виступає не як заміна персоналу, а як інструмент масштабування його експертизи на всю цифрову інфраструктуру компанії. Це створює стійкий фундамент для впровадження моделі нульової довіри (Zero Trust), де кожен запит на доступ до логістичних даних автоматично перевіряється за десятками параметрів у реальному часі, що було б неможливо реалізувати при ручному управлінні.

У системі координат сучасного кіберзахисту логістичного підприємства ключовими метриками, що визначають спроможність служби безпеки протидіяти загрозам, є середній час виявлення (Mean Time to Detect – MTDD) та середній час

реагування (Mean Time to Respond – MTTR). В умовах ручного управління ці показники демонструють високу волатильність, оскільки безпосередньо залежать від кваліфікації чергового аналітика, поточної завантаженості персоналу та часу доби. Для логістичного сектору, де інформаційні системи WMS та TMS працюють у режимі 24/7, будь-яка затримка у виявленні аномалії призводить до експоненціального зростання ймовірності успішної ексфільтрації даних або повного шифрування інфраструктури.

Впровадження засобів автоматизації та оркестрації дозволяє стабілізувати ці метрики та перевести їх у площину прогнозованих значень. Автоматизовані сценарії (playbooks) забезпечують миттєву первинну тріаж-обробку сповіщень. Якщо у ручному режимі аналітик витрачає від 15 до 45 хвилин лише на збір контекстної інформації про підозрілу подію (перевірка IP-адреси в базах Threat Intelligence, аналіз прав доступу користувача), то автоматизована система виконує ці дії за секунди. Таким чином, основна роль автоматизації полягає у радикальному скороченні часового вікна, протягом якого зловмисник може здійснювати горизонтальне переміщення (lateral movement) всередині мережі компанії.

Окрім часових показників, автоматизація підвищує якість роботи через усунення феномену «пропущених інцидентів». У великих логістичних мережах щоденна кількість подій безпеки може сягати десятків тисяч. Без автоматизованих фільтрів та засобів кореляції, які пропонує SIEM у поєднанні з оркестрацією, існує високий ризик того, що критичне сповіщення буде проігнороване серед масиву некритичних «шумових» повідомлень.

Безперервність бізнесу (Business Continuity) для логістичної компанії – це не просто теоретична концепція, а здатність підтримувати критичні функції транспортування та зберігання товарів навіть у разі деструктивного кібервпливу. Економічні втрати від кіберінцидентів у цій галузі поділяються на прямі (простій транспорту, штрафні санкції за зрив контрактів) та опосередковані (репутаційні втрати, падіння довіри клієнтів). Як показує досвід атак з використанням Ransomware, прямі фінансові збитки можуть бути критичними для життєздатності підприємства.

З метою обґрунтування інвестицій у засоби автоматизації доцільно використовувати модель оцінки ризику через вартість простою. Формалізовано цей підхід можна представити через розрахунок очікуваних втрат за формулою:

$$ALE = SLE \times ARO, \quad (2.1)$$

де:

- ALE (Annualized Loss Expectancy) – очікувані річні втрати;
- SLE (Single Loss Exposure) – вартість збитків від одного інциденту (включаючи RTO та RPO)
- ARO (Annualized Rate of Occurrence) – ймовірність виникнення інциденту протягом року.

Автоматизація безпосередньо впливає на показник SLE, оскільки мінімізує час допустимого простою (RTO). Для систем управління складом (WMS) кожен час простою може означати сотні невідвантажених одиниць товару. Якщо ручне відновлення системи після збою конфігурації триває 4 години, а автоматизований відкат (rollback) до безпечного стану за допомогою Ansible займає 5 хвилин, економічний ефект від впровадження автоматизації стає очевидним. Таким чином, автоматизація виступає як засіб страхування кіберризиків, де витрати на впровадження технології перекриваються за рахунок зменшення потенційних фінансових втрат від простою інфраструктури.

Також у сучасних умовах логістичні компанії змушені дотримуватися жорстких міжнародних стандартів, таких як ISO/IEC 27001 або NIST CSF. Однією з ключових вимог цих стандартів є забезпечення цілісності та регулярного аудиту конфігурацій мережевого обладнання. Проте, при наявності сотень віддалених складів та тисяч IoT-пристроїв, ручна перевірка відповідності (compliance) кожного вузла встановленим політикам безпеки є практично неможливою.

Автоматизація дозволяє впровадити методологію «безперервного комплаєнсу». Замість проведення аудиту один раз на квартал, автоматизовані скрипти можуть у режимі реального часу перевіряти стан інфраструктури. Якщо будь-який пристрій відхиляється від еталонної конфігурації (наприклад, з'являється неавторизований обліковий запис або відкривається незахищений

порт), система автоматично генерує інцидент у SIEM або самостійно виправляє налаштування. Це забезпечує:

1. Постійну готовність до зовнішніх аудитів без необхідності авральної підготовки документів та перевірки систем.
2. Гарантований захист від вразливостей, спричинених помилками адміністрування.
3. Можливість швидкого масштабування безпекової політики на нові підрозділи компанії

Особливого значення цей аспект набуває при роботі з зовнішніми партнерами та митними органами, де підтвердження високого рівня кіберзахисту є обов'язковою умовою співпраці. Таким чином, автоматизація стає інструментом не лише технічного захисту, а й стратегічного управління репутацією та конкурентоспроможністю логістичного бізнесу на міжнародному ринку.

Попри очевидні переваги, процес автоматизації налаштувань безпеки несе в собі специфічні ризики, які повинні бути ідентифіковані та враховані в межах загальної стратегії управління ризиками. Основним критичним ризиком є так званий «масштабований збій» або каскадна помилка. Оскільки автоматизація дозволяє вносити зміни на сотні пристроїв одночасно, будь-яка логічна помилка в коді сценарію (playbook) або некоректна конфігурація може миттєво паралізувати всю логістичну мережу. У контексті безперервності бізнесу це може призвести до ситуації, коли автоматизована система безпеки сама стає причиною відмови в обслуговуванні (DoS), блокуючи легітимний трафік або критичні бізнес-процеси.

Для мінімізації таких ризиків необхідно впроваджувати багаторівневу систему перевірки сценаріїв автоматизації.

По-перше, використання спеціалізованих інструментів для статичного аналізу коду сценаріїв, які дозволяють виявити синтаксичні помилки та невідповідності безпековим практикам ще до моменту виконання.

По-друге, обов'язкове тестування автоматизованих налаштувань у ізольованих сегментах мережі (Staging environment), що імітують реальну інфраструктуру логістичного підприємства.

По-третє, реалізація механізмів поступового розгортання (Canary deployment), при якому зміни спочатку застосовуються до обмеженої групи пристроїв, і лише після підтвердження їхньої стабільності масштабуються на всю мережу. Такий підхід дозволяє зберегти контроль над процесом та забезпечити можливість миттєвого відкату (rollback) до попереднього стабільного стану в разі виявлення аномалій. Впровадження автоматизації вимагає не лише технологічних змін, а й фундаментальної трансформації організаційної структури служби кібербезпеки. Традиційний поділ на адміністраторів мереж та аналітиків безпеки, який часто створює бюрократичні затримки, стає неефективним. Сучасна модель управління потребує інтеграції цих ролей у межах парадигми DevSecOps, де безпека не є окремим етапом, а інтегрована безпосередньо в цикли розробки та експлуатації IT-систем.

Для персоналу логістичного підприємства це означає необхідність опанування нових компетенцій, зокрема навичок програмування на Python та написання сценаріїв у форматі YAML. Замість рутинного налаштування окремих пристроїв, фахівці з безпеки перетворюються на архітекторів автоматизованих систем захисту. Це вимагає розробки нових програм навчання та підвищення обізнаності, як це передбачено в структурі ієрархічної моделі відділу кібербезпеки. Важливо розуміти, що автоматизація не замінює людину, а навпаки – підвищує вимоги до її кваліфікації, оскільки ціна помилки в автоматизованому сценарії є значно вищою, ніж при ручному налаштуванні. Організаційна гнучкість (адаптивність) стає ключовим принципом функціонування служби безпеки. Служба повинна бути спроможною оперативно переглядати автоматизовані алгоритми реагування відповідно до еволюції ландшафту загроз, про який йшлося в першому розділі. Це дозволяє створити динамічну систему захисту, яка здатна масштабуватися разом із ростом бізнесу компанії, не збільшуючи при цьому навантаження на персонал лінійно.

Завершуючи аналіз сучасних практик організації служби кібербезпеки, можна констатувати, що автоматизація є єдиним життєздатним шляхом забезпечення надійного захисту в умовах гіперпідключеної логістики. Вибір конкретного інструменту для реалізації цієї стратегії повинен базуватися на критеріях

відкритості, масштабованості та простоти інтеграції з існуючими системами (SIEM, IDS/IPS). Враховуючи особливості логістичних систем, а саме велику кількість віддалених об'єктів та різноманітність обладнання, найбільш перспективним виглядає використання агентських (agentless) систем автоматизації, які не потребують встановлення додаткового ПЗ на кінцеві вузли. Це дозволяє охопити захистом навіть застаріле обладнання та IoT-пристрої, які часто мають обмежені ресурси

Висновки до другого розділу:

У результаті проведеного аналізу сучасних практик організації служби кібербезпеки встановлено, що для забезпечення стабільного функціонування логістичного підприємства в умовах інтенсивної цифровізації необхідна багаторівнева організаційна структура, яка інтегрує управлінські, аналітичні та технічні функції. Визначено, що ключову роль у цій структурі відіграє Керівник з інформаційної безпеки (CISO), чия діяльність спрямована на стратегічне управління ризиками та інтеграцію безпекових політик у загальну бізнес-стратегію компанії. У ході дослідження різних моделей побудови служби встановлено, що найбільш оптимальною для логістичної галузі із розгалуженою мережею філій є гібридна модель, яка дозволяє поєднувати переваги централізованого моніторингу через SOC із гнучкістю локальних підрозділів. Дослідження технологічного стеку захисту показало, що сучасна архітектура безпеки базується на синергії систем SIEM, IDS/IPS та DLP, які разом формують замкнутий цикл виявлення, моніторингу та запобігання витокам конфіденційних даних. Виявлено, що ефективність цих інструментів значною мірою залежить від рівня їхньої інтеграції в єдину аналітичну екосистему, що дозволяє виявляти складні багатоступеневі атаки в реальному часі. Встановлено критичну необхідність переходу від традиційних реактивних методів до проактивного захисту через впровадження концепцій автоматизації та оркестрації процесів. Це дозволяє радикально скоротити показники часу реагування на інциденти (MTTR), мінімізувати вплив людського фактора при налаштуванні обладнання та забезпечити безперервну відповідність інфраструктури міжнародним стандартам безпеки.

Отже, проведений аналіз сучасних практик організації безпеки дозволяє зробити висновок, що побудова стійкої системи захисту в логістичній компанії потребує не лише впровадження спеціалізованих інструментів, а й повної автоматизації управління мережевими конфігураціями на засадах методології «інфраструктура як код». Це передбачає трансформацію організаційної культури в бік DevSecOps, де безпека стає невід’ємною частиною життєвого циклу ІТ-проектів. Саме ці аспекти становлять основу для подальшого дослідження, спрямованого на практичну розробку та впровадження системи автоматизованого налаштування безпеки мережі за допомогою інструменту Ansible.

3. ОПЕРАЦІЙНА ДІЯЛЬНІСТЬ СЛУЖБИ КІБЕРБЕЗПЕКИ

3.1. Планування політик безпеки (розробка стратегій зменшення ризиків)

Планування політик безпеки є фундаментом операційної діяльності служби кібербезпеки, оскільки саме на цьому етапі концептуальні загрози трансформуються у конкретні організаційні та технічні вимоги. Для логістичних компаній, що функціонують у Північній Америці, цей процес базується на використанні Рамкової програми кібербезпеки NIST (NIST Cybersecurity Framework), яка забезпечує системний підхід до управління ризиками через функції ідентифікації, захисту, виявлення, реагування та відновлення. Планування розпочинається з розробки високорівневої Політики інформаційної безпеки (Enterprise Information Security Policy), яка визначає загальні цілі, відповідальність керівництва та правове поле, у якому діє підприємство. У північноамериканському контексті це обов'язково включає дотримання вимог щодо захисту персональних даних та конфіденційної комерційної інформації, таких як CCPA у США або PIPEDA у Канаді [11,12]. Важливою складовою планування є узгодження стратегій безпеки з бізнес-пріоритетами компанії. Оскільки логістичний бізнес критично залежить від безперервності ланцюгів постачань, політики безпеки повинні бути гнучкими та підтримувати динамічне середовище обміну даними з партнерами. Стратегічне планування передбачає визначення «критичних точок відмови» в інфраструктурі, таких як центральні вузли систем управління транспортом (TMS) або інтегровані бази даних клієнтів. На основі аналізу ризиків, проведеного у першому розділі, служба безпеки розробляє цільовий профіль захисту, який мінімізує ймовірність реалізації найбільш руйнівних загроз, таких як атаки програм-вимагачів (Ransomware) або компрометація ланцюга постачань.

У практиці північноамериканських компаній використовується чотири класичні сценарії реагування на ризик: уникнення, зниження, передача або прийняття. Планування політик зосереджується насамперед на зниженні ризику через впровадження багаторівневої системи контролю. Це передбачає розробку специфічних політик для окремих доменів безпеки, зокрема політики управління

доступом (Access Control Policy), політики шифрування та політики мережевої безпеки . Кожна з цих стратегій має на меті усунення конкретних технічних недоліків, таких як використання слабких методів автентифікації або відсутність сегментації мережі. Стратегія зниження ризику вимагає ретельного підбору технічних інструментів, що були проаналізовані раніше (SIEM, IDS/IPS, DLP), та їхнього регламентного застосування . Наприклад, при плануванні захисту від витоку даних політика повинна чітко визначати класифікацію інформації та правила її обробки в хмарних сховищах та на кінцевих точках . Крім того, важливим елементом є стратегія «передачі ризику», яка в логістиці Північної Америки часто реалізується через механізми кіберстрахування та аутсорсингу критичних функцій безпеки спеціалізованим SOC–провайдером . Таке планування дозволяє компанії залишатися фінансово стійкою навіть у разі успішної реалізації складних кіберзагроз.

Фінальним етапом планування є трансформація стратегій у конкретні операційні процедури, які стають частиною щоденної діяльності персоналу. Планування політик безпеки в логістиці повинно враховувати географічну розгалуженість мережі, де працівники складів, водії та офісний персонал мають різні рівні доступу та ризик–профілі. Організація роботи служби безпеки на цьому рівні передбачає створення стандартних операційних процедур (SOP), які детально описують дії співробітників у типових ситуаціях, наприклад, при виявленні фішингового листа або втраті мобільного пристрою з корпоративним доступом. Системний підхід до планування також включає впровадження моделі «Defense in Depth» (глибокоєшелонований захист), де політики безпеки накладаються одна на одну, створюючи декілька бар'єрів для зловмисника . Це дозволяє гарантувати, що компрометація одного облікового запису не призведе до повного паралічу системи управління перевезеннями. Таким чином, планування політик безпеки не є разовою дією, а являє собою безперервний цикл вдосконалення, що базується на результатах моніторингу та оцінки ефективності впроваджених заходів.

Сучасні логістичні хаби Північної Америки функціонують як високотехнологічні вузли, де автоматизація процесів базується на масовому впровадженні технологій Інтернету речей (IoT), включаючи сенсори, сканери

штрих-кодів, RFID-пристрої та GPS-трекери. Проте інтенсивне використання цих елементів створює специфічний вектор загроз, оскільки більшість таких пристроїв працює на спрощених операційних системах, не підтримує складні методи шифрування та часто використовує стандартні облікові записи адміністратора. Планування політики безпеки для цього сегмента повинно базуватися на принципі повної ізоляції промислового трафіку від корпоративної мережі компанії. Стратегія зменшення ризиків для IoT-інфраструктури передбачає впровадження жорсткої мережевої сегментації, де кожен тип пристроїв (наприклад, системи контролю температури в холодильних контейнерах або автоматизовані складські стелажі) виділяється в окремий VLAN. Це дозволяє запобігти використанню скомпрометованих пристроїв як «трампліна» для подальших атак на критичні корпоративні ресурси або бази даних. Крім того, політика повинна регламентувати регулярне оновлення прошивок та використання сертифікованого обладнання, що значно знижує ризик інфікування ботнетами, такими як Mirai або Mozi, які продовжують активно атакувати промислові пристрої в останні роки.

Окремим аспектом планування є захист від перехоплення або підробки GPS-сигналу (GPS spoofing/jamming), що є критичним для забезпечення точності відстеження вантажів у реальному часі. Стратегія зменшення цього ризику передбачає використання багатоканальних систем моніторингу та верифікації координат через альтернативні джерела даних. Таким чином, політика безпеки логістичного хабу трансформується з суто інформаційної у фізико-кібернетичну стратегію захисту, що забезпечує цілісність як цифрових даних, так і фізичних активів підприємства.

Для логістичних компаній Північної Америки, які глибоко інтегровані в глобальні економічні системи, атаки на ланцюг поставок (Supply Chain attacks) становлять одну з найбільш деструктивних загроз. Планування політик у цьому напрямі вимагає виходу за межі внутрішнього периметра компанії та впровадження суворих стандартів безпеки для всіх партнерів, підрядників та постачальників IT-рішень. Стратегія зменшення ризиків повинна базуватися на проведенні регулярних аудитів безпеки стороннього програмного забезпечення та верифікації прав доступу, що надаються зовнішнім організаціям. Методологія планування

включає впровадження концепції «мінімальної довіри до постачальника». Це означає, що будь-яка інтеграція через API з митними, банківськими або партнерськими системами повинна проходити через суворий контроль автентифікації та обмеження швидкості запитів (rate limiting). Політика безпеки повинна чітко регламентувати порядок оновлення стороннього ПЗ, наприклад, систем управління транспортом (TMS), оскільки впровадження шкідливого коду в інсталяційні пакети оновлень є класичним вектором Supply Chain атак. Крім технічних заходів, стратегія зменшення ризиків у відносинах із третіми сторонами формалізується через юридичні інструменти, зокрема угоди про рівень обслуговування (SLA) та додатки про безпеку даних. Це дозволяє логістичній компанії встановити чіткі вимоги до конфіденційності та приватності, яких повинні дотримуватися партнери. У разі виявлення вразливості у підрядника, заздалегідь сплановані процедури реагування дозволяють оперативно ізолювати відповідні канали зв'язку, мінімізуючи каскадний ефект від інциденту на всю логістичну мережу компанії.

Оскільки логістичні гіганти Північної Америки активно використовують хмарні сервіси (Microsoft Azure, AWS) для зберігання інформації про контракти, маршрути та персонал, планування політик безпеки хмари стає життєво необхідним. Основним ризиком у цьому контексті є неправильна конфігурація доступу до хмарних сховищ, що призводить до витоку критично важливої інформації. Стратегія зменшення ризиків передбачає впровадження політик автоматизованого моніторингу налаштувань S3-бакетів або Azure Storage та обов'язкове шифрування даних як у стані спокою, так і під час транзиту. Організація роботи служби безпеки при управлінні хмарними активами повинна фокусуватися на захисті облікових записів адміністраторів. Враховуючи, що компрометація одного такого акаунта через фішинг може надати зловмиснику повний контроль над усією інфраструктурою, стратегія передбачає обов'язкове використання багатофакторної автентифікації та моніторинг аномальної активності за допомогою SIEM-систем. Таке планування дозволяє логістичній компанії ефективно використовувати масштабованість хмарних технологій,

зберігаючи при цьому високий рівень цілісності та конфіденційності розподілених баз даних.

Ефективне планування операційної діяльності служби безпеки неможливе без розробки детальних сценаріїв дій у разі виникнення критичних збоїв або кібератак. Для логістичних компаній Північної Америки, де зупинка автоматизованого термінала може паралізувати ланцюг постачань на значній території, розробка планів реагування на інциденти (Incident Response Plan – IRP) та планів відновлення після катастроф (Disaster Recovery Plan – DRP) є першочерговим завданням. Процес планування базується на проведенні аналізу впливу на бізнес (Business Impact Analysis – BIA), який дозволяє визначити критичні бізнес-процеси, такі як планування маршрутів у системі TMS або управління завантаженням у WMS. Стратегія реагування повинна бути формалізована через визначення цільових показників часу відновлення (Recovery Time Objective – RTO) та допустимого обсягу втрати даних (Recovery Point Objective – RPO) для кожної критичної системи. У контексті північноамериканського ринку, де вимоги до доступності сервісів регулюються жорсткими угодами про рівень обслуговування (SLA), планування DRP передбачає створення географічно розподілених резервних копій та використання хмарних технологій для швидкого розгортання інфраструктури в разі відмови основного дата-центру. Це дозволяє мінімізувати фінансові втрати та зберегти репутацію компанії перед міжнародними партнерами.

Системне управління вразливостями є однією з найбільш складних ділянок планування через велику кількість віддалених об'єктів та різноманітність програмного забезпечення, що використовується в логістиці. Стратегія зменшення ризиків передбачає впровадження регулярного циклу сканування вразливостей за допомогою автоматизованих інструментів, що дозволяє об'єктивно виявляти технічні слабкі місця, такі як застарілі патчі або неправильні конфігурації на серверах. Для північноамериканських компаній критично важливою є класифікація виявлених вразливостей за шкалою CVSS (Common Vulnerability Scoring System), що дозволяє службі безпеки пріоритизувати ресурси на усунення найнебезпечніших недоліків. Особлива увага при плануванні приділяється політиці «патч-менеджменту» (Patch Management). В умовах розподіленої мережі

підрозділів, де персонал може працювати в польових умовах або дистанційно, політика повинна чітко визначати часові рамки для встановлення критичних оновлень безпеки. Несвоєчасне встановлення оновлень є однією з головних причин успішних атак із використанням Ransomware, тому стратегія передбачає автоматизацію процесу розгортання виправлень та проведення тестувань на проникнення (penetration testing) для перевірки ефективності впроваджених контрзаходів. Такий підхід дозволяє тримати загальний профіль ризику компанії під постійним контролем, незалежно від масштабу її інфраструктури.

Планування політик безпеки в логістичних компаніях невід'ємно пов'язане з дотриманням складного балансу між необхідністю моніторингу дій персоналу та правом співробітників на приватність. Враховуючи, що людський фактор залишається ключовим елементом ризику, стратегія зменшення внутрішніх загроз передбачає впровадження систем Identity and Access Management (IAM), які реалізують принцип «мінімально необхідних прав». Проте регламентація таких систем повинна суворо відповідати трудовому законодавству США та Канади, а також галузевим актам про захист даних, таким як ССРА. Розробка політик моніторингу включає формалізацію правил використання корпоративних ресурсів, електронної пошти та мобільних пристроїв. Для мінімізації ризиків ненавмисних дій співробітників (наприклад, потрапляння на фішинг) планування обов'язково охоплює регулярне навчання та підвищення обізнаності персоналу через спеціалізовані тренінги та симуляції атак. Етичний аспект планування полягає у забезпеченні прозорості: співробітники повинні бути чітко поінформовані про обсяг та мету моніторингу безпеки, що сприяє формуванню здорової культури кібербезпеки всередині підприємства та зменшує ймовірність інсайдерської діяльності.

Завершальним етапом планування політик безпеки є розробка системи критеріїв, яка дозволяє об'єктивно оцінити результативність впроваджених заходів із зменшення ризиків. Для північноамериканських логістичних операторів, які інтегрують кібербезпеку в систему корпоративного управління, використання кількісних метрик (Key Performance Indicators – KPI) є обов'язковою умовою для обґрунтування інвестицій перед керівництвом. Основними показниками

ефективності запланованих політик є рівень відповідності (compliance rate) встановленим стандартам, кількість успішно заблокованих загроз на ранніх стадіях та динаміка зміни середнього часу виявлення (MTTD) і реагування (MTTR) на інциденти. Методологія оцінки базується на поєднанні якісного та кількісного аналізу. Кількісний підхід дозволяє виміряти ризик у фінансових показниках, наприклад, через розрахунок потенційних збитків від простою системи управління складом (WMS) або витрат на відновлення даних після атаки. Важливим елементом планування є врахування показників SLA (Service Level Agreement), визначених у договорах із клієнтами, оскільки будь-яке відхилення від запланованого рівня доступності сервісів безпосередньо впливає на прибутковість бізнесу. Використання таких моделей, як FAIR (Factor Analysis of Information Risk), дозволяє перетворити технічні загрози на зрозумілу для бізнесу мову фінансових ризиків, що значно полегшує процес прийняття стратегічних рішень.

Кіберзагрози постійно еволюціонують, тому планування політик безпеки не може бути разовою процедурою; воно повинно представляти собою безперервний цикл вдосконалення (PDCA – Plan–Do–Check–Act), що відповідає вимогам стандарту ISO/IEC 27001. Стратегія зменшення ризиків передбачає постійний моніторинг журналів подій у реальному часі та періодичний перегляд політик безпеки для їхньої актуалізації відповідно до змін у бізнес-моделі компанії або появи нових типів атак. Особливо це актуально для логістичних компаній Північної Америки, які часто впроваджують нові цифрові рішення для оптимізації маршрутів або управління вантажопотоками. Критичною частиною процесу верифікації ефективності політик є проведення регулярних тестувань на проникнення (penetration testing) та аудиту безпеки після будь-яких значних змін в IT-інфраструктурі. Результати таких перевірок дозволяють службі безпеки ідентифікувати нові вразливості та вносити необхідні корективи в існуючі стратегії захисту. Крім того, адаптивність служби безпеки підтримується через аналіз уроків, отриманих після кожного інциденту (Lessons Learned), що дозволяє запобігати повторенню подібних сценаріїв у майбутньому. Такий проактивний підхід гарантує, що загальний профіль ризику компанії залишається під постійним контролем керівництва.

Підсумовуючи процес планування політик безпеки, можна стверджувати, що розробка стратегій зменшення ризиків у логістичній компанії Північної Америки є комплексною діяльністю, яка поєднує технічні, організаційні та юридичні аспекти. Використання рамок NIST та міжнародних стандартів дозволяє створити стійку структуру захисту, яка здатна масштабуватися разом із ростом бізнесу та ефективно протидіяти широкому спектру загроз – від фішингових атак до складних компрометацій ланцюгів постачань. Сформовані стратегії – від мікросегментації мережі до впровадження політик нульової довіри (Zero Trust) та автоматизації комплаєнсу – формують надійну операційну базу для щоденної роботи служби кібербезпеки. Планування забезпечує не лише технічну стійкість систем TMS та WMS, а й формує культуру кібербезпеки серед персоналу, що є вирішальним фактором у мінімізації впливу людського фактора. Таким чином, успішне планування політик безпеки закладає необхідні умови для переходу до наступного етапу операційної діяльності – безпосереднього моніторингу та реагування на інциденти, де розроблені стратегії будуть втілені у конкретних стандартних операційних процедурах (SOP).

3.2. Моніторинг та реагування на інциденти (опис SOP-ів)

Ефективна операційна діяльність служби кібербезпеки логістичного підприємства в Північній Америці базується на функціонуванні Центру операцій безпеки (SOC), який забезпечує цілодобовий моніторинг інформаційних систем у режимі 24/7. Процес моніторингу не є пасивним спостереженням, а являє собою активний аналіз подій безпеки, що генеруються різнорідними джерелами: від серверів управління транспортом (TMS) до мережевих екранів та хмарних сервісів. Основною метою моніторингу є максимально раннє виявлення аномальної активності, що дозволяє локалізувати загрозу до моменту нанесення суттєвої шкоди бізнес-процесам. Методологічною основою для розробки процедур реагування в таких компаніях є стандарт NIST SP 800–61, який визначає чотири фази життєвого циклу інциденту: підготовку; виявлення та аналіз; стримування, ліквідацію та відновлення; діяльність після інциденту [5]. У логістичній сфері, де

кожна секунда простою автоматизованого складу призводить до накопичення фінансових збитків, чітке дотримання цих фаз є критичним. Планування операційної діяльності передбачає, що для кожного типу загроз (наприклад, атака Ransomware або DDoS) розробляється окремий сценарій реагування, який базується на встановлених показниках часу відновлення (RTO) та допустимій втраті даних (RPO).

Стандартні операційні процедури (Standard Operating Procedures, SOP) є ключовим інструментом, що дозволяє перетворити складні стратегії захисту на зрозумілі покрокові інструкції для технічного персоналу. У великих логістичних корпораціях, де служба безпеки має ієрархічну структуру, SOP забезпечують одноманітність дій аналітиків різних рівнів (Tier 1–3), мінімізуючи вплив людського фактора та ймовірність помилок під час кризових ситуацій. Кожен SOP містить детальний опис тригерів інциденту, перелік необхідних інструментів, алгоритм технічних дій та порядок комунікації з іншими підрозділами компанії. Впровадження SOP у логістиці Північної Америки часто поєднується з використанням систем оркестрації (SOAR), які автоматизують виконання рутинних кроків процедури. Наприклад, при виявленні підозрілої активності в базі даних клієнтів, SOP може передбачати автоматичне блокування облікового запису користувача та ініціювання розслідування відділом Digital Forensics & Incident Response (DFIR). Такий системний підхід дозволяє службі безпеки діяти максимально злагоджено, забезпечуючи дотримання угод про рівень обслуговування (SLA) та підтримуючи репутацію надійної ланки в глобальному ланцюгу постачань.

Процес реагування розпочинається з етапу ідентифікації, на якому подія, зафіксована системами моніторингу (SIEM), аналізується на предмет її критичності та потенційного впливу на бізнес. Для логістичного підприємства надзвичайно важливо відрізнити технічні збої обладнання від цілеспрямованих кібератак. Класифікація інциденту здійснюється на основі матриці ймовірності та впливу, де події поділяються на категорії: низького, середнього, високого та критичного рівнів ризику. Первинна SOP-інструкція для аналітика SOC на цьому етапі включає:

- Перевірку контексту події через кореляцію даних з різних джерел (наприклад, співставлення спроби входу з віддаленої адреси та завантаження нетипового обсягу даних з TMS) .
- Верифікацію інциденту на предмет «хибного спрацювання» (false positive), що дозволяє уникнути зайвого навантаження на команду реагування .
- Негайне сповіщення відповідних груп реагування та керівництва (CISO) у разі підтвердження критичної загрози, що може призвести до зупинки логістичних операцій .

Саме швидкість та точність виконання цієї початкової процедури визначає успіх подальших етапів стримування та відновлення. У північноамериканських логістичних гігантів цей етап максимально автоматизований, що дозволяє ідентифікувати загрози за лічені секунди, забезпечуючи безперервність функціонування складних розподілених мереж.

Атаки типу Ransomware становлять найбільш руйнівну загрозу для логістичного сектору, оскільки вони здатні миттєво паралізувати системи управління складом (WMS) та транспортом (TMS), роблячи дані недоступними та вимагаючи значних викупів. У північноамериканській практиці SOP для реагування на такі інциденти має бути максимально швидким та структурованим, щоб мінімізувати показник часу відновлення RTO. Процедура ініціюється відразу після виявлення підозрілої активності, такої як масове шифрування файлів або несанкціоновані зміни в базах даних.

Першим етапом SOP є негайне стримування (containment), яке передбачає ізоляцію інфікованих вузлів від корпоративної мережі, щоб запобігти горизонтальному поширенню шкідливого ПЗ. Це включає відключення уражених серверів від мережі, блокування скомпрометованих облікових записів та тимчасове припинення роботи VPN-тунелів із партнерами. Паралельно з цим проводиться аналіз джерела атаки – найчастіше це фішинг або використання вразливостей у застарілому ПЗ. Наступний етап – ліквідація та відновлення, де служба безпеки забезпечує розгортання «чистих» систем із резервних копій, дотримуючись цільових показників RPO, щоб уникнути критичної втрати даних про вантажі та маршрути.

Компрометація облікових записів через фішинг або соціальну інженерію є найпоширенішим вектором атак, оскільки експлуатує людський фактор, а не технічні недоліки систем. SOP для таких випадків фокусується на швидкому відновленні ідентичності користувача та аудиті дій, вчинених зловмисником під скомпрометованим акаунтом. Процедура передбачає примусове скидання паролів, впровадження багатофакторної автентифікації та перевірку журналів доступу в SIEM-системі для виявлення ознак несанкціонованої ексфільтрації даних. У разі спрацювання систем запобігання витоку даних (DLP), SOP регламентує дії щодо захисту конфіденційної інформації клієнтів та маршрутів перевезень. Якщо зафіксовано спробу передачі чутливих файлів через незашифровані канали або зовнішні носії, система автоматично блокує транзакцію, а аналітик SOC проводить розслідування для визначення мотивів – випадкова недбалість співробітника чи навмисна інсайдерська діяльність. У північноамериканських компаніях цей процес супроводжується обов’язковим документуванням для звітування перед регуляторними органами (наприклад, згідно з вимогами CCPA) у разі підтвердження витоку персональних даних. Для систематизації дій персоналу нижче наведено табл. 3.1, що порівнює пріоритети та інструменти для різних типів інцидентів.

Таблиця 3.1

Порівняння процедур реагування за типом кіберінциденту

Етап реагування	Сценарій: Ransomware	Сценарій: Фішинг / Витік даних	Сценарій: DDoS-атака
Основний тригер	Шифрування файлів, аномальна дискова активність	Спрацювання DLP-правил, вхід з аномальної локації	Недоступність веб-порталів, перевантаження каналів
Ключова дія	Ізоляція сегмента мережі, відкат до бекапів	Блокування акаунта, скидання паролів, аналіз логів	Перенаправлення трафіку обмеження швидкості
Пріоритетний KPI	RTO	Конфіденційність та цілісність даних	Доступність (Uptime) за SLA
Інструмент захисту	SIEM, EDR, Системи бекапу	DLP, IAM, SIEM	IDS/IPS, WAF, хмарні фільтри

Для логістичного бізнесу доступність веб-серверів відстеження вантажів та порталів для клієнтів є критичною для підтримання довіри та виконання контрактних зобов'язань. DDoS-атаки спрямовані на створення штучного дефіциту ресурсів, що паралізує можливість клієнтів моніторити статус своїх замовлень у реальному часі. SOP для протидії таким загрозам базується на активному використанні систем виявлення та запобігання вторгненням (IDS/IPS), а також хмарних сервісів очищення трафіку.

Алгоритм дій персоналу при виявленні DDoS-атаки включає:

1. Ідентифікацію аномального сплеску трафіку за допомогою SIEM-системи та мережевих моніторів.
2. Активацію політик обмеження швидкості запитів (rate limiting) на рівні API та веб-серверів для мінімізації впливу ботнетів.
3. Перенаправлення вхідного трафіку через спеціалізовані центри очищення (scrubbing centers) партнерських хмарних провайдерів (наприклад, Cloudflare або Azure DDoS Protection), що дозволяє відсіяти шкідливі пакети та пропустити легітимні запити користувачів.
4. Постійний моніторинг стану системи до повного припинення атаки та подальший аналіз логів для вдосконалення сигнатур виявлення.

Чітке виконання цієї процедури дозволяє зберегти доступність критично важливих послуг навіть під час масштабних атак, що забезпечує стабільність логістичного ланцюга та відповідність вимогам SLA.

Після успішного завершення фази стримування загрози, операційна діяльність служби кібербезпеки переходить до етапу глибокого аналізу та розслідування, що виконується підрозділом Digital Forensics & Incident Response (DFIR). Основним завданням на цьому етапі є не лише відновлення систем, а й ретельний збір цифрових доказів (судова експертиза), визначення джерел і методів атаки, а також оцінка реальної нанесеної шкоди. Для північноамериканських компаній цей етап має вирішальне значення, оскільки зібрані докази можуть бути використані в судових процесах проти зловмисників або для підтвердження виконання вимог регуляторів щодо захисту даних. Стандартна операційна процедура з цифрового розслідування включає створення образів пам'яті (memory dumps), копіювання

журналів подій SIEM та аналіз мережевого трафіку до моменту інциденту. Фахівці DFIR використовують спеціалізовані інструменти для виявлення прихованих артефактів шкідливого ПЗ та відновлення хронології дій зловмисника всередині системи управління перевезеннями (TMS) або складського обліку (WMS). Результатом цього процесу є детальний технічний звіт, який слугує базою для посилення слабких місць у системі технічного захисту та запобігання повторним інцидентам у майбутньому.

Управління кіберінцидентом у великій логістичній компанії вимагає чіткої координації не лише всередині IT-відділу, а й між юридичним відділом, департаментом зв'язків із громадськістю (PR), відділом аудиту та управління персоналом. SOP-комунікації визначає ієрархію сповіщень: від внутрішніх технічних груп до вищого керівництва (CISO та CEO). Несвоєчасна або некоректна комунікація може призвести до паніки серед клієнтів, падіння вартості акцій та порушення законодавчих вимог щодо розкриття інформації про витік даних (наприклад, згідно з нормами CCPA). Для логістичного бізнесу, який глибоко інтегрований у міжнародну торгівлю, критично важливо підтримувати прозорість щодо статусу виконання замовлень під час відновлення систем. Координація дій дозволяє уникнути каскадного ефекту, коли порушення безпеки в одній компанії паралізує операції партнерів. Для систематизації цих процесів у табл. 3.2 наведено матрицю відповідальності під час реагування на критичний інцидент.

Таблиця 3.2

Матриця комунікацій та відповідальності при реагуванні на інцидент

Підрозділ	Роль у процесі реагування	Об'єкт комунікації	Основний KPI
SOC / DFIR	Технічне виявлення, ізоляція та аналіз	CISO, IT-директор	MTTR
Юридичний відділ	Аналіз правових наслідків, звітування регуляторам	Урядові органи (NIST/TSA context), Регулятори	Compliance

1	2	3	4
Відділ PR / Comms	Інформування клієнтів та медіа, управління репутацією	Клієнти, Громадськість	Довіра клієнтів
CISO / Менеджмент	Прийняття стратегічних рішень щодо зупинки сервісів	Рада директорів, Акціонери	RTO

Завершальною та найбільш важливою фазою операційного циклу реагування є аналіз отриманого досвіду (Lessons Learned). Згідно з принципом адаптивності, структура та політики служби безпеки не можуть залишатися статичними; вони повинні постійно вдосконалюватися на основі реальних кейсів. SOP–звітування передбачає проведення наради після кожного серйозного інциденту для обговорення того, які заходи захисту спрацювали ефективно, а які виявилися недостатніми.

Процес «Lessons Learned» включає:

- Аналіз ефективності виявлення загрози системами SIEM та IDS/IPS для корекції правил і сигнатур.
- Перегляд та оновлення існуючих SOP–ів на основі виявлених під час реагування затримок або помилок.
- Оцінку роботи персоналу та визначення потреби в додатковому навчанні або зміні прав доступу в системі IAM.
- Підготовку фінального звіту для вищого керівництва, який включає оцінку фінансових збитків, вартості відновлення та рекомендацій щодо інвестицій у нові технології захисту.

Такий проактивний підхід дозволяє логістичній компанії не лише усувати наслідки атак, а й формувати зрілу культуру безпеки, де кожна помилка стає кроком до підвищення стійкості всієї системи. Це гарантує, що служба

кібербезпеки залишається ефективним бар'єром на шляху еволюціонуючих загроз у динамічному цифровому середовищі Північної Америки

3.3. Впровадження рішень для тренування персоналу з питань кібербезпеки

У сучасних умовах функціонування логістичних гігантів Північної Америки, де цифровізація охоплює всі ланки ланцюга постачань, людський фактор залишається одним із найбільш критичних джерел ризику. Як було встановлено в аналізі загроз, зловмисники дедалі частіше експлуатують не технічні вразливості систем, а психологічні аспекти поведінки працівників через фішинг та соціальну інженерію. Саме тому впровадження рішень для тренування персоналу (Security Awareness Training) стає не просто допоміжним заходом, а фундаментальною складовою операційної діяльності служби кібербезпеки, за яку відповідає спеціалізований підрозділ – Security Awareness & Training Unit. Методологія навчання в північноамериканському контексті базується на принципі безперервності та адаптивності. Замість застарілих щорічних лекцій, компанії впроваджують інтерактивні платформи, які дозволяють кожному співробітнику проходити короткі, але регулярні навчальні модулі. Основна мета такої стратегії – не лише надати технічні знання, а й сформувати стійку культуру кібербезпеки, де кожен працівник розуміє свою відповідальність за захист корпоративних даних та систем управління перевезеннями (TMS). Це дозволяє перетворити персонал із потенційного джерела вразливостей на першу активну лінію захисту підприємства.

Одним із найбільш ефективних інструментів тренування персоналу є проведення контрольованих симуляцій фішингових атак. Оскільки фішинг залишається найпопулярнішим вектором вторгнення в логістичні мережі, працівники повинні вміти ідентифікувати підозрілі повідомлення в реальних робочих умовах. Служба кібербезпеки розробляє сценарії, які імітують актуальні загрози: повідомлення про зміну маршруту, затримку вантажу або запити на оновлення фінансових реквізитів від «партнерів».

Процес симуляції організовується наступним чином.

1. Здійснюється розробка фішингових шаблонів, що максимально точно відтворюють стилістику та методику реальних злоумисників.
2. Проводиться масова або таргетована розсилка цих повідомлень серед співробітників різних підрозділів.
3. Система автоматично фіксує дії користувачів: хто відкрив лист, хто перейшов за посиланням, а хто ввів облікові дані на підробленій сторінці.

Важливо, що метою таких симуляцій є не покарання працівників, а ідентифікація груп ризику, які потребують додаткового навчання. Працівники, які «попалися» на симуляцію, миттєво отримують коротке роз'яснювальне повідомлення, що вказує на ознаки, які вони пропустили. Такий підхід дозволяє суттєво знизити ймовірність успішної реальної атаки, оскільки пильність персоналу підтримується на постійно високому рівні.

Для об'єктивної оцінки зрілості культури кібербезпеки в північноамериканських логістичних компаніях використовується система кількісних показників. Вимірювання результатів навчання дозволяє CISO обґрунтовувати витрати на тренувальні платформи та коригувати стратегію зменшення ризиків. Основними метриками в цьому контексті є коефіцієнт кліків (Click Rate) – відсоток працівників, які піддалися на симуляцію, та коефіцієнт звітування (Reporting Rate) – відсоток тих, хто використав спеціальну кнопку «Повідомити про фішинг» в поштовому клієнті.

Для логістичного сектору, де динаміка робочих процесів є надзвичайно високою, встановлення цільових KPI є критичним. Наприклад, успішною вважається програма, яка дозволяє знизити Click Rate з початкових 20–30% до стабільних 2–5% протягом року. Нижче наведено табл. 3.3, яка демонструє типові метрики та їхній вплив на загальну безпеку підприємства.

Таблиця 3.3

Ключові показники KPI програми навчання персоналу

Метрика	Опис показника	Цільове значення (Best Practice)	Вплив на безпеку
Phish-prone %	Відсоток працівників, вразливих до соціальної інженерії	< 5%	Зменшення поверхні атаки через людський фактор

1	2	3	4
Reporting Rate	Відсоток вчасно ідентифікованих та повідомлених загроз	> 70%	Прискорення виявлення інцидентів (MTTD)
Completion Rate	Відсоток персоналу, що завершив обов'язкові модулі	> 95%	Забезпечення базового рівня кібергігієни
Dwell Time reduction	Скорочення часу перебування зловмисника в мережі	Зменшення на 30–50%	Мінімізація збитків від інцидентів

Високий показник Reporting Rate є особливо цінним, оскільки він перетворює кожного співробітника на «живий сенсор» системи моніторингу, дозволяючи SOC отримувати інформацію про нові кампанії зловмисників ще до того, як вони будуть зафіксовані технічними засобами захисту.

Ефективність програми навчання в північноамериканських логістичних корпораціях прямо залежить від релевантності навчального контенту конкретним робочим обов'язкам персоналу. Універсальний підхід до навчання часто ігнорується працівниками через відсутність прямого зв'язку з їхньою щоденною діяльністю. Тому служба кібербезпеки розробляє диференційовані навчальні траєкторії, адаптовані до ризик-профілів різних груп співробітників. Для персоналу, задіяного безпосередньо в логістичних операціях (водії та кур'єри), основний акцент робиться на безпеці мобільних пристроїв та захисті GPS-даних. Навчання включає правила використання публічних Wi-Fi мереж, розпізнавання спроб підробки координат та фізичну безпеку терміналів збору даних. Складські працівники проходять тренінги з безпечної експлуатації IoT-пристроїв, сканерів та систем управління складом (WMS), фокусуючись на недопустимості використання стандартних паролів та важливості повідомлення про аномальну поведінку автоматизованого обладнання.

Окрему категорію становить вищий менеджмент та фінансовий відділ, які є головними мішенями для атак типу BEC (Business Email Compromise) та

цілеспрямованого фішингу. Для них розробляються складні сценарії, що імітують запити на термінову зміну банківських реквізитів або підроблені повідомлення від «керівництва» чи «митних органів». Такий рольовий розподіл дозволяє забезпечити адресність знань та мінімізувати ризики в найбільш вразливих точках бізнес–процесів.

Таблиця 3.4

Розподіл навчальних тем за категоріями персоналу

Категорія персоналу	Ключові теми навчання	Пріоритетні загрози	Джерела ризику
Водії / Кур'єри	Безпека мобільних ОС, GPS–гігієна, захист пристроїв	MITM, GPS–спуфінг	Публічні мережі, втрата девайсів
Складський персонал	Робота з IoT, безпека WMS–терміналів, фізичний доступ	Ботнети, саботаж IoT	Стандартні паролі, доступ сторонніх
Офіс / Логісти	Фішинг, захист облікових даних у TMS/ERP	Ransomware, витік даних	Соціальна інженерія, слабкі паролі
Менеджмент	БЕС–атаки, управління ризиками, комплаєнс	Фрод, шпигунство	Соціальна інженерія, витік стратегії

Одним із головних викликів для північноамериканських логістичних компаній є підтримка інтересу співробітників до питань безпеки на тривалій дистанції. Традиційні методи навчання часто сприймаються як рутинне навантаження, що призводить до формального проходження тестів. Для вирішення цієї проблеми служба безпеки впроваджує елементи гейміфікації, перетворюючи процес навчання на змагання 16.Гейміфікація включає систему балів, рейтингів та значків (badges) за успішне проходження модулів або швидке звітування про підозрілі

листи. У логістичному секторі ефективним є проведення командних змагань між різними терміналами або регіональними офісами. Команда з найменшим показником Phish-prone% за квартал отримує корпоративні бонуси або публічне визнання. Це стимулює горизонтальну підтримку всередині колективу, де досвідчені працівники допомагають новачкам ідентифікувати загрози. Математично рівень залученості та успішності можна оцінити через інтегральний показник «Оцінки обізнаності» Awareness Score:

$$AS = \frac{(M_{comp} \times w_1) + (S_{pass} \times w_2) + (R_{ratio} \times w_3)}{100}, \quad (3.1)$$

де:

M_{comp} – відсоток завершених модулів;

S_{pass} – успішність проходження тестів;

R_{ratio} – коефіцієнт вчасного звітування про загрози;

w_1, w_2, w_3 – вагові коефіцієнти значущості кожного показника.

Для масштабування культури безпеки у великих розподілених логістичних мережах недостатньо зусиль лише центрального офісу безпеки. Світова практика, особливо в США та Канаді, передбачає створення мережі «Security Champions» – співробітників бізнес-підрозділів (логістів, менеджерів складів), які проявляють підвищений інтерес до ІТ-безпеки. Ці працівники не є фахівцями з кібербезпеки, але вони стають «голосом» служби безпеки на місцях.

Роль «Security Champions» включає:

1. Надання первинних консультацій колегам з питань безпечного поводження з даними.
2. Зворотний зв'язок зі службою безпеки щодо зручності та реалістичності впроваджених політику в «польових умовах».
3. Допомогу в розслідуванні інцидентів людського фактора на локальному рівні.

Впровадження такої мережі дозволяє значно скоротити дистанцію між технічним підрозділом кібербезпеки та операційним персоналом. Це створює атмосферу взаємної відповідальності, де безпека сприймається не як зовнішнє обмеження, а як невід'ємна частина професійної культури логіста. Таким чином,

завдяки поєднанню диференційованого навчання, гейміфікації та інституту активістів, логістична компанія створює надійний «людський бар'єр» проти сучасних кіберзагроз.

3.4. Оцінка ефективності заходів

Оцінка ефективності заходів із забезпечення кібербезпеки в логістичних компаніях Північної Америки є складним багатofакторним процесом, який виходить за межі простої перевірки відсутності інцидентів. Оскільки абсолютна безпека є недосяжною, ефективність служби оцінюється через її здатність мінімізувати ризики до прийняттого рівня та забезпечувати швидке відновлення бізнес-процесів у разі атаки. Методологічною базою для такої оцінки слугують стандарти NIST SP 800–55 «Performance Measurement Guide for Information Security», які пропонують систему вимірюваних показників для аналізу впровадження, результативності та впливу засобів контролю на операційну діяльність підприємства [6]. Системний підхід до оцінки передбачає поділ показників на три рівні: операційні, тактичні та стратегічні. Операційні показники відображають щоденну роботу технічних засобів (наприклад, відсоток заблокованих спам-повідомлень або кількість виявлених вразливостей). Тактичні показники характеризують ефективність процесів, таких як реагування на інциденти або навчання персоналу. Стратегічні показники орієнтовані на вище керівництво та відображають загальний рівень захищеності активів і відповідність витрат на безпеку потенційним збиткам. Для логістичного сектору особливе значення має інтеграція цих показників у систему управління якістю та безперервністю бізнесу, що дозволяє розглядати кібербезпеку як один із критичних факторів надійності всього ланцюга постачань.

Основним інструментом вимірювання успішності операційної діяльності служби безпеки є система ключових показників ефективності (Key Performance Indicators – KPI). У північноамериканських логістичних гігантах ці показники зазвичай виводяться на інтерактивні дашборди в режимі реального часу, що

дозволяє CISO оперативно коригувати роботу підрозділів. До найбільш значущих показників належать:

1. Mean Time to Detect – середній час від моменту виникнення інциденту до його ідентифікації. Чим нижчий цей показник, тим ефективніше працюють системи моніторингу та «людські сенсори» (навчений персонал).

2. Mean Time to Respond – середній час, необхідний для повної локалізації та усунення загрози. Для логістики цей показник прямо корелює з мінімізацією фінансових втрат від простою складів або транспорту.

3. Patch Latency – середній час між випуском критичного оновлення безпеки та його фактичним встановленням на пристрої в розподіленій мережі.

4. Vulnerability Remediation Rate – відсоток вчасно усунених вразливостей відповідно до встановлених пріоритетів (наприклад, за шкалою CVSS).

Окрім KPI, служба безпеки використовує ключові індикатори ризику (Key Risk Indicators – KRI), які сигналізують про потенційне зростання загрози до того, як вона перетвориться на інцидент. Наприклад, різке зростання кількості невдалих спроб входу в систему управління транспортом (TMS) або збільшення обсягу вихідного трафіку з бази даних клієнтів є критичними KRI, що потребують негайної уваги. Нижче наведено табл.3.5, яка демонструє взаємозв'язок між операційними діями та їхніми показниками.

Таблиця 3.5

Матриця показників ефективності операційної діяльності

Операційний процес	Ключовий показник (KPI)	Цільовий орієнтир (North America Benchmark)	Інструмент вимірювання
Моніторинг	MTTD	< 2 годин для критичних атак	SIEM / SOAR
Реагування	MTTR	< 4 годин для локальних інцидентів	Incident Tracking System

1	2	3	4
Навчання	Click Rate	< 3% протягом року	Phishing (KnowBe4 platfrom)
Управління активами	Inventory Accuracy	> 98% охоплення пристроїв	CMDB / Asset Discovery

Окрім кількісних метрик, для оцінки довгострокової ефективності заходів використовується аналіз рівнів зрілості. У США для компаній, що працюють з державними замовленнями або в критичних секторах, дедалі частіше застосовується модель CMMC (Cybersecurity Maturity Model Certification) або рівні впровадження NIST CSF (Implementation Tiers) [17,3]. Ці моделі дозволяють оцінити, наскільки процеси безпеки є формалізованими, повторюваними та адаптивними.

Для логістичної компанії перехід з «Часткового» (Tier 1) до «Адаптивного» (Tier 4) рівня зрілості означає еволюцію від реактивного гасіння пожеж до проактивного управління ризиками, де безпека інтегрована в кожен цифровий проєкт. Оцінка зрілості дозволяє виявити прогалини в організації служби: наприклад, якщо технічні засоби захисту є сучасними, але SOP–процедури не документуються або не оновлюються, загальний рівень зрілості буде низьким, що підвищує ризики в разі складних АРТ–атак. Такий якісний аналіз доповнює кількісні метрики, створюючи цілісну картину ефективності служби безпеки.

У бізнес–культурі Північної Америки кібербезпека розглядається не лише як технічна функція, а як повноцінна інвестиція в стабільність підприємства. Для логістичних гігантів, де бюджети на ІТ–безпеку можуть сягати мільйонів доларів, служба безпеки повинна демонструвати фінансову ефективність впроваджених заходів. Основним інструментом для цього є показник рентабельності інвестицій у безпеку (Return on Security Investment – ROSI). На відміну від класичного ROI, цей показник розраховується на основі «заощаджених» коштів, які компанія не втратила завдяки запобіганню інцидентам.

Формула розрахунку ROSI для логістичного оператора базується на оцінці грошових втрат від потенційного простою. Розрахунок виглядає наступним чином:

$$ROSI = \frac{(ALE \times P) - Cost}{Cost}, \quad (3.2)$$

де:

- *ALE* (Annual Loss Expectancy) – очікувані річні втрати від імовірних атак;
- *P* (Mitigation Ratio) – коефіцієнт ефективності впровадженого засобу захисту;
- *Cost* – сукупна вартість рішення (ліцензії, підтримка, персонал).

Наприклад, якщо впровадження системи автоматизованого реагування дозволяє знизити ймовірність успішної атаки Ransomware на 80%, а потенційні збитки від зупинки логістичного хабу становлять 500 000 доларів, то розрахунок ROSI дозволяє чітко продемонструвати Раді директорів доцільність витрат на кіберзахист. Такий підхід робить службу безпеки зрозумілим і прозорим партнером для бізнесу, що є критично важливим для отримання фінансування на нові проєкти.

Оцінка ефективності не може вважатися повною без проведення зовнішніх перевірок, які дозволяють поглянути на систему захисту очима зловмисника. У північноамериканських логістичних компаніях широкого розповсюдження набули практики Red Teaming та регулярні тестування на проникнення (Penetration Testing). На відміну від щоденного моніторингу, ці заходи спрямовані на виявлення складних ланцюжків вразливостей, які можуть бути непомітні для стандартних засобів захисту.

Процес незалежної оцінки включає:

1. Зовнішні тести на проникнення, що імітують спроби зламу периметра компанії через публічні веб–портали або VPN–шлюзи.
2. Внутрішні аудити, спрямовані на перевірку стійкості мережі до горизонтального переміщення зловмисника (lateral movement) після компрометації одного робочого місця.

3. Red Teaming операції, що є повномасштабною симуляцією цілеспрямованої атаки (APT), де команда етичних хакерів намагається досягти конкретної бізнес-цілі (наприклад, отримати доступ до бази даних клієнтів), використовуючи методи соціальної інженерії та технічні вразливості.

Результати таких перевірок слугують «холодним душем» для служби безпеки, оскільки вони демонструють реальний стан захищеності в умовах, максимально наближених до бойових. Кожна виявлена прогалина стає підставою для коригування SOP-процедур та оновлення стратегій зменшення ризиків.

Кінцевим продуктом етапу оцінки ефективності є квартальні та річні звіти, що подаються Керівником з інформаційної безпеки (CISO) вищому менеджменту компанії. У логістичному секторі Північної Америки такі звіти не повинні бути перевантажені суто технічними даними (кількістю заблокованих вірусів чи портів). Натомість вони фокусуються на управлінських аспектах: динаміці залишкового ризику, стані комплаєнсу (відповідності законам) та рівні готовності до відновлення після катастроф. Важливим складником звітування є аналіз репутаційних ризиків. Логістична компанія, яка може довести високу ефективність своєї служби безпеки через проходження міжнародних сертифікацій та успішні результати аудитів, отримує значну конкурентну перевагу на ринку США та Канади. Це підвищує довіру великих партнерів, таких як урядові структури або транснаціональні ритейлери, для яких безпека ланцюга постачань є критичною вимогою. Таким чином, оцінка ефективності заходів закриває цикл операційної діяльності, забезпечуючи зворотний зв'язок для постійного вдосконалення всієї системи кіберзахисту підприємства.

Висновки до третього розділу:

У результаті дослідження операційної діяльності служби кібербезпеки встановлено, що успішне функціонування системи захисту в логістичній галузі Північної Америки потребує переходу від статичного контролю до динамічного управління ризиками. Визначено, що планування політик безпеки на засадах стандартів NIST дозволяє створити стійку структуру, яка враховує специфіку розгалуженої інфраструктури, хмарних сервісів та IoT-пристроїв. Встановлено, що

ключовим фактором операційної стійкості є наявність деталізованих стандартних операційних процедур (SOP), які регламентують дії персоналу в критичних ситуаціях, таких як атаки Ransomware або витік конфіденційних даних клієнтів.

Доведено, що мінімізація впливу людського фактора через впровадження безперервних програм навчання (Security Awareness) та симуляцій фішингових атак дозволяє значно знизити загальну поверхню атаки підприємства. Розроблена система метрик та показників ефективності (KPI, ROSI) забезпечує прозорість роботи служби безпеки для бізнес-керівництва та дозволяє обґрунтувати необхідність інвестицій у сучасні технології захисту. Отже, інтегрований підхід до операційної діяльності, що поєднує технічну досконалість, організаційну злагодженість та економічну доцільність, є основою для побудови ефективної служби кібербезпеки в сучасному цифровому середовищі.

4. ОРГАНІЗАЦІЯ РОБОТИ СЛУЖБИ КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ ЛОГІСТИЧНОЇ КОМПАНІЇ ПІВНІЧНОЇ АМЕРИКИ

4.1. Аналіз компанії та її IT-інфраструктури

Корпорація FedEx (Federal Express) є одним із найпотужніших світових операторів логістичних послуг, чия діяльність відіграє критичну роль у забезпеченні економічної стабільності Північної Америки. Заснована у США, компанія еволюціонувала від авіакур'єрської служби до глобального технологічного гіганта, який щодня обробляє мільйони відправлень через розгалужену мережу наземних та авіаційних маршрутів [10]. Для цілей нашого дослідження важливо розуміти, що FedEx – це не просто транспортна компанія, а цифрова екосистема, де фізичне переміщення вантажів повністю дублюється інформаційними потоками в режимі реального часу. Станом на сьогодні, компанія оперує через декілька основних підрозділів: FedEx Express, FedEx Ground та FedEx Freight, кожен з яких має свою специфічну IT-інфраструктуру, але інтегрований у загальну систему кіберзахисту корпорації.

Стратегічне значення FedEx для північноамериканського регіону зумовлює надзвичайно високі вимоги до її кіберстійкості. Будь-яка зупинка в роботі центральних хабів, таких як «SuperHub» у Мемфісі, може призвести до каскадного ефекту в ланцюгах постачань медикаментів, промислового обладнання та товарів першої необхідності по всьому континенту. Саме тому організація служби кібербезпеки в компанії розглядається як критична функція бізнесу, що безпосередньо впливає на національну безпеку та економічну стабільність США та Канади.

IT-інфраструктура FedEx являє собою складний гібридний ландшафт, який поєднує традиційні дата-центри (on-premise) з потужними хмарними платформами, такими як Microsoft Azure та Oracle Cloud. Основу цієї системи складають системи управління транспортом (TMS) та складськими операціями (WMS), які забезпечують координацію між тисячами літаків, вантажівок та складських приміщень. Ключовим елементом інфраструктури є платформа FedEx Dataworks, яка використовує технології машинного навчання та великих даних для

оптимізації маршрутів і прогнозування термінів доставки. З погляду кібербезпеки, така архітектура створює величезну поверхню атаки, що потребує впровадження моделі нульової довіри (Zero Trust) на всіх рівнях. Окремим викликом для служби безпеки є рівень периферійних обчислень (Edge Computing) та Інтернету речей (IoT). Десятки тисяч кур'єрських сканерів, GPS–трекерів на фурах та автоматизованих сортувальних ліній на складах постійно генерують дані, які повинні передаватися через захищені канали. Велика кількість цих пристроїв функціонує за межами традиційного офісного периметра, часто використовуючи мобільні мережі 5G, що вимагає специфічних заходів захисту, таких як шифрування трафіку та строга багатофакторна автентифікація для кожного підключення. Такий розподілений характер інфраструктури FedEx робить її ідеальним майданчиком для аналізу сучасних методів організації SOC та SIEM–моніторингу, що були описані в попередніх розділах.

В межах IT–ландшафту FedEx критичні активи поділяються на декілька категорій, кожна з яких має свій профіль ризику та вимоги до захисту. До першої категорії належать операційні дані реального часу: інформація про місцезнаходження вантажів, плани польотів та графіки доставки. Втрата цілісності цих даних може призвести до фізичних аварій або колапсу логістичної мережі. Друга категорія – це конфіденційна інформація клієнтів (РІІ) та фінансові дані, витік яких загрожує компанії величезними штрафами згідно з регламентами CCPA та іншими законодавчими актами Північної Америки. Для захисту цих активів у FedEx реалізована глибока мережева сегментація. Використовуючи принципи програмно–визначених мереж (SDN), служба безпеки розділяє корпоративні ресурси, системи управління складами та публічні веб–сервіси на ізольовані зони. Це дозволяє локалізувати потенційне проникнення зловмисника в межах одного сегмента, запобігаючи доступу до центральних баз даних. Така організація мережі є критично важливою для забезпечення безперервності бізнесу, оскільки дозволяє проводити технічні роботи або ізолювати підозрілий трафік без зупинки всієї глобальної логістичної машини.

Сучасна бізнес–модель FedEx базується на глибокій цифровій інтеграції з тисячами партнерів: від малого бізнесу до транснаціональних ритейлерів та митних

органів. Ключовим технічним інструментом цієї взаємодії є розвинена екосистема прикладних програмних інтерфейсів (API), що дозволяють клієнтам інтегрувати функціонал FedEx (розрахунок вартості, створення накладних, відстеження) безпосередньо у свої ERP та e-commerce системи. З погляду кібербезпеки, кожне таке з'єднання є потенційним вектором атаки, оскільки компрометація партнерського API-ключа може відкрити зловмиснику доступ до внутрішніх логістичних операцій або конфіденційної інформації про вантажі.

Для захисту цих точок доступу FedEx використовує спеціалізовані шлюзи безпеки API (API Security Gateways), які здійснюють безперервну перевірку автентичності запитів, обмеження швидкості (rate limiting) та глибокий аналіз вмісту пакетів для виявлення ознак ін'єкцій коду. Окрему увагу приділено публічним веб-порталам, таким як FedEx Ship Manager. Оскільки ці ресурси доступні з будь-якої точки світу, вони постійно перебувають під прицілом автоматизованих ботнетів, що намагаються здійснити перебір паролів (brute force) або викрасти дані через вразливості веб-додатків. Служба безпеки FedEx впроваджує тут передові системи верифікації особи та адаптивний захист від DDoS-атак, що дозволяє зберігати доступність сервісів навіть за умов інтенсивного ворожого впливу.

Незважаючи на активну хмарну трансформацію, FedEx, як корпорація з багаторічною історією, стикається з проблемою «технічного боргу» – наявністю застарілих (legacy) систем, що були розроблені десятиліття тому. Багато з цих систем досі виконують критичні функції в обробці залізничних маніфестів або управлінні старими складськими терміналами. Головна небезпека полягає в тому, що такі системи часто не підтримують сучасні протоколи шифрування, не мають регулярних оновлень безпеки та можуть містити вразливості, які вже давно відомі зловмисникам. У логістичній компанії, де злиття та поглинання різних підрозділів (наприклад, інтеграція FedEx Express та TNT) відбувалися в різні часи, неоднорідність IT-ландшафту створює додаткові ризики. Служба кібербезпеки FedEx змушена застосовувати стратегію «віртуального патчингу» та додаткової ізоляції для таких систем. Це означає, що застаріле ПЗ поміщається у максимально обмежені сегменти мережі з жорстким контролем вхідного та вихідного трафіку

через спеціалізовані проксі-сервери та міжмережеві екрани наступного покоління (NGFW). Це дозволяє використовувати функціонал старих систем, мінімізуючи ймовірність їх використання як точки входу для шифрувальників типу Ransomware.

Окремим і надзвичайно важливим сегментом інфраструктури FedEx є парк мобільних пристроїв, який налічує сотні тисяч одиниць: від спеціалізованих захищених терміналів кур'єрів (Handheld Devices) до корпоративних смартфонів менеджерів. Кожен такий пристрій є кінцевою точкою мережі, що має доступ до внутрішніх баз даних та систем відстеження вантажів. У польових умовах ці девайси працюють через різномірні мережі зв'язку (4G/5G, публічний Wi-Fi), що робить їх вразливими до перехоплення даних або атак типу «людина посередині» (Man-in-the-Middle). Для управління цим масивом пристроїв FedEx використовує системи Unified Endpoint Management (UEM), які дозволяють централізовано впроваджувати політики безпеки: обов'язкове шифрування пам'яті, заборону на встановлення стороннього ПЗ та можливість дистанційного знищення даних у разі втрати пристрою. Крім того, на мобільних терміналах встановлюються спеціалізовані агенти виявлення загроз (Mobile Threat Defense), які в реальному часі аналізують стан операційної системи на предмет ознак зламу (jailbreak/root) або наявності шкідливого коду. Це забезпечує цілісність логістичного ланцюга постачань на «останній милі», де безпосередньо відбувається взаємодія з клієнтом та вантажем.

Таблиця 4.1

Технічні параметри та вразливості основних елементів

ІТ-інфраструктури FedEx

Елемент інфраструктури	Тип платформ / Технологій	Ключові вразливості	Заходи захисту
Центральні TMS/WMS	Oracle, Mainframes, Cloud (Azure)	SQL-ін'єкції, помилки конфігурації	Сегментація, DB-encryption
Edge-пристрої (IoT)	Сканери, RFID-рідери, GPS	Слабкі паролі, відсутність патчів	Ізольовані VLAN, 802.1X

1	2	3	4
Партнерські API	REST API, JSON, SOAP	Компрометація токенів, BOLA	API Gateway, OAuth 2.0
Мобільні термінали	Android-based, iOS	Крадіжка девайса, MITM-атаки	UEM/MDM, VPN, Biometrics

Отже, проведений аналіз IT-інфраструктури компанії FedEx демонструє надзвичайно складну та гетерогенну систему, де критичні бізнес-процеси залежать від злагодженої роботи хмарних платформ, застарілих мейнфреймів та сотень тисяч периферійних IoT-пристроїв. Така архітектура створює широку поверхню атаки, що вимагає не лише технічного захисту кожної окремої точки, а й побудови цілісної екосистеми безпеки, здатної адаптуватися до динамічних змін логістичного ланцюга. Розуміння цих технічних особливостей та вразливостей дозволяє перейти до розробки прикладних рекомендацій, спрямованих на посилення кіберстійкості компанії в умовах сучасного ринку Північної Америки.

4.2. Практичні рекомендації для впровадження кіберзахисту

Для підвищення ефективності роботи служби кібербезпеки в умовах масштабу FedEx, першочерговою рекомендацією є перехід від традиційної ізольованої моделі безпеки до інтегрованої парадигми DevSecOps. Враховуючи високу швидкість розробки нових цифрових сервісів у FedEx Dataworks, безпека повинна бути впроваджена безпосередньо в життєвий цикл розробки програмного забезпечення (SDLC). Це передбачає автоматизацію перевірок коду на вразливості та інтеграцію сканерів безпеки в CI/CD конвеєри, що дозволить виявляти помилки конфігурації ще до того, як вони потраплять у продуктивне середовище. На організаційному рівні рекомендується посилити роль CISO (Керівника з інформаційної безпеки), забезпечивши його пряму участь у засіданнях Ради директорів та прийнятті стратегічних рішень щодо цифровізації. Окремим кроком має стати створення крос-функціональних команд «Security Champions» у кожному з операційних

підрозділів (Express, Ground, Freight). Ці фахівці, будучи зануреними в специфіку логістичних операцій, зможуть оперативніше ідентифікувати специфічні ризики та виступати містком між центральним SOC та технічним персоналом «на місцях». Такий підхід забезпечує не лише технічну, а й культурну трансформацію компанії, де безпека сприймається як спільна відповідальність.

Враховуючи розгалуженість мережі FedEx та велику кількість зовнішніх точок підключення (API, партнерські мережі), критично важливою рекомендацією є повний перехід до архітектури Zero Trust («Нікому не довіряй, завжди перевіряй»). В межах цієї моделі кожен запит на доступ до внутрішніх систем TMS або баз даних клієнтів повинен проходити сувору верифікацію, незалежно від того, звідки він походить – зсередини корпоративної мережі чи з віддаленого термінала кур'єра. Основним інструментом реалізації Zero Trust має стати глибока мікросегментація мережі на рівні додатків та робочих навантажень. Рекомендується використовувати програмно–визначені мережеві екрани для ізоляції кожного критичного сервісу в окремий мікропериметр. Наприклад, система управління сортувальною лінією на складі повинна мати доступ лише до необхідних API–ендпоінтів, не маючи прямого зв'язку з сегментом фінансової звітності. Це дозволяє радикально обмежити можливість горизонтального переміщення зловмисника всередині мережі lateral movemen у разі успішної компрометації однієї кінцевої точки, що є критично важливим для протидії атакам шифрувальників.

Третім блоком рекомендацій є впровадження систем SOAR (Security Orchestration, Automation, and Response) для автоматизації рутинних операцій SOC. У логістичному гіганті, де щодня фіксуються мільярди подій безпеки, ручне реагування на кожне сповіщення є фізично неможливим. Використання SOAR дозволяє розробляти та виконувати автоматизовані сценарії (playbooks) для типових інцидентів, таких як блокування скомпрометованих акаунтів або ізоляція хостів з підозрілою активністю. Це дозволяє скоротити час реакції (MTTR) з годин до лічених секунд, що безпосередньо впливає на збереження показників RTO компанії. Паралельно з цим рекомендується автоматизувати процес контролю відповідності (Compliance as Code). Для компанії, що працює в Північній Америці,

дотримання стандартів NIST та CCPA є юридичною вимогою. Автоматизовані системи повинні безперервно сканувати хмарну та наземну інфраструктуру на предмет відхилень від «еталонних» налаштувань безпеки. У разі виявлення незашифрованого S3-бакета з даними клієнтів або відкритого критичного порту на сервері, система має автоматично вносити виправлення та генерувати звіт про інцидент. Це забезпечує постійну готовність до зовнішніх аудитів та мінімізує ризик отримання величезних штрафів від регуляторів.

Враховуючи стратегічну роль FedEx у глобальній економіці, компрометація одного з її технологічних партнерів або постачальників програмного забезпечення може мати руйнівні наслідки для всієї корпорації. Рекомендується впровадити посилену програму Third-Party Risk Management (TPRM), яка базується на стандартах NIST SP 800-161 [7]. Практична реалізація цієї рекомендації передбачає перехід від разових перевірок партнерів до безперервного моніторингу їхньої кіберстійкості.

Службі безпеки FedEx доцільно впровадити наступні кроки:

1. Впровадження вимоги щодо надання постачальниками «Програмної специфікації матеріалів» (SBOM – Software Bill of Materials) для всього критичного ПЗ, що використовується в системах управління вантажами. Це дозволить компанії миттєво ідентифікувати, чи містять партнерські додатки вразливі компоненти (наприклад, бібліотеки типу Log4j).

2. Автоматизація оцінки безпеки партнерів через спеціалізовані платформи (наприклад, SecurityScorecard або BitSight), що дозволяють у режимі реального часу отримувати дані про стан захищеності зовнішніх мереж, з якими інтегрована FedEx.

3. Встановлення жорстких технічних лімітів на рівні API-шлюзів для партнерських підключень, що передбачають автоматичне розірвання сесії у разі виявлення аномальної поведінки або спроб доступу до несанкціонованих сегментів бази даних.

Для FedEx «остання миля» – це не лише етап доставки, а й величезна мережа вразливих кінцевих точок (сканери, планшети водіїв, бортові системи). Рекомендується впровадження концепції SASE (Secure Access Service Edge), яка

об'єднує мережеві функції та функції безпеки в єдину хмарну платформу. Це дозволить забезпечити захищений доступ кур'єрів до систем TMS незалежно від їхнього місцезнаходження, переносючи перевірку безпеки ближче до самого користувача, а не до центрального дата-центру.

На практичному рівні захист «останньої милі» має включати:

- Використання технології Micro-VPN для кожного окремого логістичного додатка на мобільному терміналі. Це гарантує, що навіть якщо пристрій буде скомпрометований через особистий трафік водія, зломисник не зможе отримати доступ до корпоративного каналу передачі даних про вантажі.
- Впровадження апаратно-довірчих модулів (TPM) у всі нові моделі сканерів та терміналів, що дозволить забезпечити цілісність завантаження операційної системи та унеможливить запуск неавторизованого шкідливого коду на рівні «заліза».
- Динамічна гео-адаптивна автентифікація: якщо термінал кур'єра фіксує спробу доступу з локації, яка не відповідає його денному маршруту, система повинна автоматично вимагати додатковий фактор верифікації або тимчасово блокувати доступ до бази даних клієнтів.

Традиційний моніторинг, що базується на спрацюванні сигнатур, є недостатнім для протидії цілеспрямованим атакам (APT). Рекомендується створення всередині SOC FedEx окремої групи Threat Hunting, завданням якої є активний пошук ознак присутності зломисників, що вже могли обійти периметральні засоби захисту. Цей процес повинен базуватися на матриці MITRE ATT&CK, яка класифікує тактики та техніки сучасних хакерських угруповань [16]. Проактивний підхід має базуватися на використанні даних кіберрозвідки (Cyber Threat Intelligence). FedEx повинна не лише отримувати дані про нові загрози від урядових структур США (наприклад, CISA), а й самостійно аналізувати специфічні для логістики індикатори компрометації (IoC). Математично ефективність цього підходу можна оцінити через зниження часу перебування зломисника в мережі:

$$E_{hunt} = \frac{DT_{arg} - DT_{hunt}}{DT_{arg}} \times 100\%, \quad (4.1)$$

де:

- DT_{arg} – середній час перебування зловмисника до виявлення стандартними засобами;
- DT_{hunt} – час виявлення групою Threat Hunting.

Зменшення цього показника безпосередньо впливає на обсяг потенційних фінансових збитків, оскільки зловмисник має менше часу для збору та ексфільтрації критичних даних про ланцюги постачань. Порівняння традиційної та рекомендованої моделі організації безпеки для FedEx представлено в табл.4.2.

Таблиця 4.2

Порівняння традиційної та рекомендованої моделі організації безпеки для FedEx

Параметр порівняння	Традиційна модель (Реактивна)	Рекомендована модель (Проактивна / Zero Trust)
Довіра до мережі	Довіра внутрішнім сегментам (VPN/Intranet)	Повна відсутність довіри, верифікація кожного запиту
Управління API	Базова автентифікація (статичні ключі)	Динамічні токени, поведінковий аналіз API-трафіку
Реагування на інциденти	Ручне виконання SOP аналітиками	Автоматизовані playbooks через SOAR-системи
Робота з персоналом	Щорічні інструктажі	Гейміфіковане навчання та мережа Security Champions
Моніторинг	Виявлення за сигнатурами (відомі атаки)	Threat Hunting та аналіз аномалій (AI/ML)

Впровадження запропонованих рекомендацій дозволить компанії FedEx перейти від традиційної реактивної моделі захисту до проактивної екосистеми, що

базується на принципах Zero Trust та автоматизації процесів реагування через SOAR. Поєднання технічних інновацій, таких як SASE та SBOM, із організаційними змінами у межах парадигми DevSecOps, створює надійний фундамент для захисту складних ланцюгів постачань. Така стратегія забезпечує не лише технічну стійкість інфраструктури, а й економічну ефективність інвестицій у безпеку, що є вирішальним фактором для підтримання лідерства на логістичному ринку Північної Америки.

4.3. Аналіз інцидентів кібербезпеки

Для логістичних гігантів Північної Америки аналіз минулих інцидентів є не просто фіксацією збитків, а критично важливим інструментом для навчання та адаптації служби кібербезпеки. Вивчення реальних кейсів дозволяє ідентифікувати розриви між запланованими політиками безпеки та їхньою фактичною ефективністю під час реальної атаки. У цьому контексті досвід корпорації FedEx є унікальним, оскільки компанія пройшла через один із найбільш масштабних та руйнівних кіберінцидентів у світовій історії – атаку шифрувальника NotPetya у 2017 році [18]. Розбір цього кейсу дозволяє проаналізувати механізми каскадного поширення загроз у глобальних мережах та оцінити стійкість логістичної інфраструктури до деструктивних впливів. Аналіз інцидентів у межах даного дослідження базується на вивченні технічних векторів вторгнення, швидкості реагування SOC та довгострокового впливу на бізнес–показники компанії. Такий підхід дозволяє верифікувати теоретичні моделі, описані в другому та третьому розділах, та продемонструвати, як відсутність мікросегментації або затримки в патч–менеджменті можуть призвести до багатомільйонних втрат. Для FedEx цей досвід став каталізатором повної реорганізації служби безпеки та переходу до сучасних стандартів захисту, які ми розглядаємо як еталонні для галузі.

Інцидент, що стався у червні 2017 року, розпочався з компрометації ланцюга постачань програмного забезпечення для бухгалтерського обліку, що використовувалося в українському офісі нещодавно придбаного FedEx підрозділу TNT Express. Шкідливе програмне забезпечення NotPetya, маскуючись під вірус–

вимагач, насправді мало деструктивний характер і було спрямоване на безповоротне знищення даних через перезапис головного завантажувального запису (MBR). Технічна складність атаки полягала у використанні експлойтів EternalBlue та EternalRomance у поєднанні з інструментом Mimikatz для викрадення облікових даних, що дозволило вірусу миттєво поширитися по всій корпоративній мережі FedEx через встановлені VPN-тунелі між офісами. Наслідки для FedEx були катастрофічними. Оскільки на той момент інтеграція IT-систем TNT та FedEx ще тривала, застаріла інфраструктура TNT виявилася найбільш вразливою. Протягом кількох годин було зашифровано тисячі серверів та робочих станцій по всьому світу. Це призвело до повної зупинки автоматизованих сортувальних ліній, систем відстеження вантажів та порталів взаємодії з клієнтами. Співробітники компанії були змушені перейти на ручну обробку накладних, що критично сповільнило логістичні операції та спричинило величезні черги в терміналах. Цей кейс наочно продемонстрував, як вразливість в одному регіональному офісі може паралізувати глобальну корпорацію за лічені хвилини.

Згідно з офіційними звітами FedEx для Комісії з цінних паперів і бірж США (SEC), сукупні збитки від атаки NotPetya склали приблизно 300 мільйонів доларів [10]. Ця сума включала витрати на відновлення IT-інфраструктури, заміну пошкодженого обладнання, послуги зовнішніх консультантів з кібербезпеки та прямі втрати доходів через неможливість надання послуг клієнтам протягом тривалого часу. Проте фінансові цифри не повною мірою відображають масштаб катастрофи: компанія втратила значну частину ринкової частки в Європі, оскільки клієнти, стурбовані безпекою своїх даних та вантажів, почали переходити до конкурентів. Операційний вплив інциденту тривав місяцями. Служба безпеки FedEx зіткнулася з необхідністю повної перебудови мережевої архітектури «на ходу». Було встановлено, що відсутність належної сегментації між підрозділами дозволила вірусу безперешкодно переміщатися між країнами. Цей інцидент став жорстоким уроком, який підтвердив правильність впровадження моделі Zero Trust: якби мережевий доступ був обмежений на рівні окремих додатків, руйнівний ефект міг би бути локалізований лише в межах одного сегмента. Таким чином, атака

NotPetya стала не лише трагедією, а й точкою відліку для створення однієї з найпотужніших систем кіберзахисту в сучасній логістиці Північної Америки.

Окрім масштабних атак типу NotPetya, FedEx, як і інші логістичні гіганти Північної Америки, постійно стикається з інцидентами, пов'язаними з безпекою партнерських екосистем та хмарних сховищ. Логістика «останньої милі» та транскордонна торгівля вимагають тисяч інтеграцій через API з митними брокерами, інтернет-магазинами та фінансовими установами. Кожна така точка інтеграції є потенційним «слабким місцем». Характерним прикладом став інцидент 2018 року, коли дослідники безпеки виявили незахищене хмарне сховище (Amazon S3 bucket), що належало одному з підрозділів компанії. У відкритому доступі опинилися тисячі сканованих документів клієнтів (паспорти, водійські посвідчення), що було наслідком помилки в налаштуваннях доступу (misconfiguration). Хоча цей інцидент не призвів до операційної зупинки, він завдав серйозного репутаційного удару та підкреслив ризики, пов'язані з використанням хмарної інфраструктури без належного автоматизованого контролю комплаєнсу. Аналіз цього кейсу показав, що традиційні методи моніторингу периметра не працюють у хмарному середовищі, де одна некоректна зміна в правах доступу (IAM) може призвести до миттєвого оприлюднення гігабайтів конфіденційних даних. Саме цей випадок став поштовхом для впровадження політики «Cloud-First Security», яка передбачає обов'язкове шифрування всіх даних у хмарі та автоматичну перевірку конфігурацій сховищ за допомогою інструментів Cloud Security Posture Management (CSPM).

Аналіз дій служби кібербезпеки FedEx під час ліквідації наслідків атаки NotPetya дозволив виявити критичні недоліки в тодішніх стандартних операційних процедурах (SOP). Основним бар'єром для швидкого відновлення виявилася відсутність «тривожної кнопки» (Kill Switch) – механізму миттєвої ізоляції цілих географічних сегментів мережі. У 2017 році команда SOC намагалася блокувати трафік вірусу на рівні окремих портів та IP-адрес, що було неефективним проти шкідливого ПЗ, яке використовувало легітимні інструменти адміністрування (WMI та PSEXEC) для поширення. Ще одним «вузьким місцем» стала комунікація. У перші години атаки внутрішні канали зв'язку (електронна пошта та корпоративні

месенджери) були паралізовані разом із основною інфраструктурою, що позбавило команду реагування можливості злагоджено координувати дії. Це призвело до того, що відновлення систем розпочалося хаотично, без чіткої пріоритезації бізнес-процесів. Після аналізу цього досвіду FedEx повністю переглянула свої SOP-и реагування, запровадивши незалежні від основної мережі канали екстреного зв'язку (Out-of-band communication) та автоматизовані сценарії SOAR, які ми розглядали в підрозділі 3.2. Сьогодні при виявленні подібної активності система автоматично розриває VPN-з'єднання між регіональними офісами, не чекаючи ручного підтвердження аналітика.

Усвідомлення того, що атака NotPetya потрапила в мережу через скомпрометований софт українського підрядника, змусило FedEx радикально змінити підхід до вибору та контролю постачальників ПЗ. Раніше оцінка безпеки партнерів була формальною процедурою (заповнення опитувальників один раз на рік). Тепер компанія впровадила модель динамічного управління ризиками ланцюга постачань.

Нова стратегія включає:

1. Технічний аудит коду. Будь-яке ПЗ, що інтегрується з критичними системами FedEx (TMS/WMS), проходить обов'язкове сканування в пісочниці (Sandbox) та аналіз наявності відомих вразливостей у відкритих бібліотеках (SCA – Software Composition Analysis).

2. Мережева ізоляція партнерів. Зовнішні підрядники тепер не отримують доступу до загального корпоративного сегмента. Для кожної партнерської інтеграції створюється окремий мікросегмент із нульовою довірою (Zero Trust Network Access), де доступ дозволено лише до конкретного API-ендпоінту.

3. Кіберстрахування та юридичні гарантії. У контракти з постачальниками введено жорсткі пункти про фінансову відповідальність за інциденти кібербезпеки та обов'язковість проходження регулярних незалежних аудитів SOC 2 Type II.

Для наочності порівнюємо стан служби безпеки до та після аналізу критичних інцидентів у таблиці 4.3.

Еволюція системи кібербезпеки FedEx після аналізу масштабних інцидентів

Критерій	Стан до 2017 року (Реактивний)	Стан після 2017 року (Адаптивний)
Мережева архітектура	Слабка сегментація, відкриті VPN-тунелі	Мікросегментація, модель Zero Trust (SASE)
Реагування на інциденти	Ручні дії аналітиків, затримки в ізоляції	Автоматизація через SOAR, сценарії «Kill Switch»
Контроль підрядників	Формальні опитувальники, довіра до ПЗ	SBOM, безперервний моніторинг ризиків партнерів
Патч-менеджмент	Пріоритет на доступність систем	Пріоритет на усунення критичних вразливостей
Відновлення (DRP)	Часткове резервування даних	Повномасштабне хмарне резервування з низьким RTO

Розбір реальних кейсів FedEx, зокрема атаки NotPetya та витоків даних з хмарних сховищ, підтверджує, що в сучасному логістичному бізнесі технічна досконалість не гарантує безпеки без належної організації процесів реагування та управління ризиками третіх сторін. Ці інциденти стали для компанії «дорогою школою», яка призвела до повної реорганізації служби кібербезпеки та переходу на засади проактивного захисту. Досвід FedEx наочно демонструє, що ефективна служба безпеки – це не та, що ніколи не помиляється, а та, що здатна миттєво локалізувати удар та перетворити отриманий досвід на нові рівні захисту.

4.4. Рекомендації для подальшого розвитку систем кібербезпеки для логістичних компаній

У найближчій перспективі розвиток систем кібербезпеки логістичних гігантів, таких як FedEx, буде нерозривно пов'язаний із переходом від реактивних методів

виявлення до предиктивної аналітики на основі штучного інтелекту. Обсяги даних, що генеруються глобальними логістичними мережами, вже сьогодні перевищують можливості людського аналізу. Рекомендується впровадження систем AI-driven Threat Hunting, які здатні самостійно ідентифікувати ледь помітні аномалії в поведінці користувачів та пристроїв (UEBA – User and Entity Behavior Analytics), що можуть свідчити про підготовку до атаки ще до моменту спрацювання стандартних сигнатур. Машинне навчання дозволить логістичним компаніям автоматизувати процес класифікації трафіку та динамічного створення правил для міжмережевих екранів. Наприклад, AI може автоматично виявляти нові ботнети, що намагаються атакувати IoT-пристрої на складах, та створювати відповідні фільтри в режимі реального часу. Крім того, ШІ стане ключовим інструментом у боротьбі з «дипфейками» та складними фішинговими кампаніями, аналізуючи лінгвістичні патерни повідомлень та виявляючи спроби соціальної інженерії на ранніх стадіях. Це дозволить перетворити службу безпеки на інтелектуальний центр, що діє на випередження зловмисників.

Логістична галузь Північної Америки активно рухається в бік автоматизації перевезень: від безпілотних фур на магістралях до дронів-доставщиків на «останній милі». Ці технології відкривають нові вектори атак, такі як дистанційне перехоплення управління (hijacking) або маніпуляція сенсорами автономних систем. Рекомендується розробка специфічних протоколів безпеки для V2X (Vehicle-to-Everything) комунікацій, які забезпечуватимуть цілісність та автентичність даних, що передаються між транспортним засобом, дорожньою інфраструктурою та хмарним центром управління.

Стратегія захисту автономних систем повинна базуватися на:

1. Апаратному шифруванні всіх команд управління на рівні контролерів транспортного засобу.
2. Резервуванні каналів навігації: поєднання GPS із інерціальними системами та візуальною орієнтацією для протидії атакам типу GPS-spoofing.
3. Впровадженні систем виявлення вторгнень для внутрішніх шин даних (CAN-bus) транспортних засобів, що дозволить блокувати спроби несанкціонованого втручання в роботу двигуна або гальмівної системи. Це

вимагатиме від служби кібербезпеки логістичного підприємства нових компетенцій у сфері вбудованих систем та робототехніки.

Хоча комерційні квантові комп'ютери ще перебувають на етапі розробки, потенційна загроза, яку вони несуть для сучасної криптографії, вимагає планування вже сьогодні. Здатність квантових систем миттєво зламувати традиційні алгоритми шифрування (RSA, ECC) ставить під удар конфіденційність довгострокових контрактів та персональних даних клієнтів логістичних компаній. Рекомендується розпочати поступову адаптацію IT-інфраструктури до стандартів постквантової криптографії (Post-Quantum Cryptography – PQC), що розробляються NIST. Для логістичного бізнесу це означає аудит усіх існуючих систем шифрування та розробку плану переходу на квантово-стійкі алгоритми для захисту найбільш критичних даних. Крім того, великі корпорації можуть розглядати впровадження технологій квантового розподілу ключів (QKD) для забезпечення абсолютної безпеки зв'язку між центральними дата-центрами. Такий проактивний підхід дозволить уникнути ризику «зламай зараз, розшифруй потім» (harvest now, decrypt later), який є актуальним для державних та промислових шпигунів.

Фінальною рекомендацією є перехід від концепції «кіберзахисту» до стратегії кіберстійкості (Cyber Resilience). Це передбачає визнання того, що будь-яка система може бути скомпрометована, тому головна мета – забезпечити виживання бізнесу та мінімально необхідне функціонування під час та після атаки. Служба кібербезпеки майбутнього повинна бути максимально інтегрована в плани управління кризами та безперервності бізнесу, розглядаючи цифрову безпеку як частину загальної корпоративної стійкості.

Пріоритетні напрями розвитку систем кібербезпеки до 2030 року

Технологічний тренд	Вплив на логістику	Ключовий інструмент / Технологія	Термін впровадження
AI/ML Security	Предиктивне виявлення складних атак та ботнетів	AI-driven SIEM, UEBA, SOAR	1–3 роки
Autonomous Fleet Security	Захист безпілотних фур та дронів–доставщиків	V2X Security, CAN-IDS, Hardware-Trust	3–7 років
Zero Trust 2.0	Повна мікросегментація на рівні ідентичності	SASE, Cloud-Native Security Enforcement	1–5 років
Post-Quantum Crypto	Захист від злому шифрування квантовими ПК	NIST PQC Standards, Hybrid-encryption	5–10 років
Cyber Insurance Integration	Оптимізація витрат на основі автоматизованого аудиту	Continuous Risk Monitoring platforms	1–2 роки

Подальший розвиток служби кібербезпеки логістичного гіганта FedEx неможливий без глибокої інтеграції функцій захисту в загальну систему корпоративного управління (Enterprise Risk Management – ERM). У північноамериканському бізнес-середовищі кібербезпека дедалі частіше розглядається не як технічна проблема, а як фундаментальний бізнес-ризик, що впливає на капіталізацію компанії та її інвестиційну привабливість. Рекомендується впровадження динамічної моделі звітності, де показники кіберстійкості безпосередньо корелюють із фінансовими прогнозами та планами

розширення присутності на ринку. Це передбачає створення постійно діючого комітету з кіберризиків при Раді директорів, який забезпечуватиме нагляд за виконанням стратегії захисту та адекватністю фінансування нових технологічних ініціатив.

Важливим вектором розвитку є еволюція підходів до кіберстрахування. Враховуючи досвід NotPetya, FedEx та подібні компанії повинні переходити від базових страхових полісів до складних партнерств із страховими інститутами, де вартість премії безпосередньо залежить від результатів автоматизованого аудиту безпеки. Рекомендується впровадження систем безперервного моніторингу комплаєнсу, які в реальному часі надають страховикам підтвердження високого рівня захищеності інфраструктури. Це не лише дозволяє оптимізувати витрати на передачу ризиків, а й стимулює компанію до постійної підтримки технічних засобів захисту в актуальному стані, створюючи замкнений цикл економічно обґрунтованої безпеки.

Протягом наступного десятиліття очікується значне посилення державного регулювання кібербезпеки в транспортному секторі США та Канади. Рекомендується проактивна підготовка служби безпеки до впровадження нових директив TSA та CISA, які, ймовірно, вимагатимуть вищого рівня прозорості та обов'язкового звітування про інциденти в надкороткі терміни (до 24 годин). Для FedEx це означає необхідність подальшої автоматизації процесів збору цифрових доказів (forensics) та формування юридично значущих звітів без залучення значного людського ресурсу. Розвиток системи безпеки повинен враховувати потреби транскордонної співпраці, де дані про загрози автоматично обмінюються між державними органами та приватним сектором через захищені платформи Threat Intelligence. Особлива увага має бути приділена гармонізації політик безпеки між північноамериканськими та міжнародними підрозділами компанії. Рекомендується розробка єдиного глобального стандарту безпеки «FedEx Cyber Standard», який би базувався на найсуворіших вимогах NIST, але враховував локальні особливості конфіденційності даних у Європі та Азії. Це дозволить уникнути правових конфліктів при передачі інформації про вантажі та клієнтів через міжнародні кордони та забезпечить одноманітність захисту всього

глобального ланцюга постачань. Таким чином, розвиток служби безпеки FedEx спрямований на створення глобальної, інтелектуальної та юридично стійкої системи, здатної захистити інтереси компанії в епоху тотальної цифрової прозорості.

Нарешті, майбутнє кібербезпеки в логістиці полягає у трансформації захисту з витратної частини бюджету на конкурентну перевагу. Для клієнтів FedEx у Північній Америці надійність та конфіденційність даних про доставку стають такими ж важливими, як і швидкість самого перевезення. Рекомендується впровадження публічних інтерфейсів (dashboards) безпеки для великих корпоративних клієнтів, де вони зможуть у реальному часі бачити статус захищеності своїх логістичних каналів та підтвердження цілісності ланцюга постачань. Це створює нову екосистему довіри, де безпека стає невидимою, але відчутною гарантією якості послуг.

Впровадження технологій блокчейн для верифікації маніфестів та відстеження життєвого циклу критичних вантажів дозволить виключити можливість підміни даних або несанкціонованого втручання в логістичні процеси. Розвиток таких технологій у поєднанні з квантово-стійким шифруванням та штучним інтелектом зробить FedEx не просто транспортним оператором, а еталоном цифрової безпеки в індустрії. Таким чином, запропоновані рекомендації формують цілісну програму розвитку, яка дозволить компанії не лише вижити в умовах зростаючої агресивності кіберпростору, а й диктувати нові стандарти безпеки для всього світового ринку логістики.

Висновки до четвертого розділу:

У результаті практичного аналізу організації роботи служби кібербезпеки на прикладі корпорації FedEx встановлено, що сучасна логістична інфраструктура Північної Америки є надзвичайно складною цифровою екосистемою, де критичні бізнес-процеси залежать від стабільності тисяч взаємопов'язаних вузлів. Проведений аудит ІТ-ландшафту компанії показав, що поєднання хмарних технологій, розгалуженої мережі периферійних пристроїв та застарілих систем створює специфічні ризики, які неможливо нівелювати за допомогою лише

традиційних засобів захисту. Виявлено, що найбільш критичними точками вразливості є партнерські інтеграції через API та мобільна інфраструктура «останньої милі».

Аналіз реальних інцидентів, зокрема руйнівної атаки NotPetya у 2017 році, довів, що відсутність належної сегментації та затримки в реагуванні можуть призвести до катастрофічних фінансових та репутаційних втрат. Цей досвід став каталізатором для розробки та впровадження практичних рекомендацій щодо реорганізації служби безпеки на засадах моделі Zero Trust та впровадження принципів DevSecOps. Обґрунтовано, що автоматизація процесів моніторингу за допомогою SOAR-технологій та перехід до проактивного пошуку загроз (Threat Hunting) є обов'язковими умовами для підтримання стійкості ланцюга постачань у сучасному динамічному середовищі.

Перспективний аналіз розвитку систем безпеки дозволив визначити ключові технологічні тренди, такі як використання штучного інтелекту для предиктивного захисту, забезпечення безпеки автономного транспорту та підготовка до викликів квантової епохи. Встановлено, що перехід від парадигми захисту до стратегії кіберстійкості (Cyber Resilience) та інтеграція безпекових метрик у систему корпоративного управління є вирішальними факторами довгострокового успіху. Таким чином, проведена робота дозволяє стверджувати, що ефективна організація служби кібербезпеки в логістичній компанії Північної Америки потребує комплексного поєднання технологічних інновацій, організаційної гнучкості та глибокого розуміння економічних ризиків цифрового світу.

ВИСНОВКИ

У процесі виконання дипломної роботи вирішено актуальне науково–прикладне завдання вдосконалення організації роботи служби кібербезпеки великої логістичної компанії Північної Америки шляхом розробки комплексної стратегії захисту, формалізації операційних процедур та впровадження проактивних методів управління ризиками. У ході дослідження проведено глибокий аналіз ландшафту сучасних кіберзагроз, який виявив критичну вразливість логістичних ланцюгів постачань до атак програм–вимагачів та цілеспрямованих кампаній з компрометації партнерських систем. Аргументовано, що традиційна периметральна модель захисту є неефективною для розподілених інфраструктур, що потребує переходу до архітектури нульової довіри та посилення контролю периферійних обчислень.

На основі методології стандартів NIST CSF та ISO/IEC 27001 розроблено операційну модель служби кібербезпеки, яка інтегрує процеси безперервного моніторингу, автоматизованого реагування та проактивного пошуку загроз. Теоретично обґрунтовано та практично деталізовано стандартні операційні процедури, які дозволяють типізувати дії персоналу Центру операцій безпеки у критичних ситуаціях. Особливу увагу приділено розробці програм підвищення обізнаності персоналу, що забезпечують трансформацію людського фактора з вектора вразливості на активний бар'єр захисту, що підтверджується суттєвим зниженням показників вразливості співробітників до методів соціальної інженерії.

Практична ціність роботи підтверджена результатами аналізу діяльності корпорації FedEx та розробкою прикладних рекомендацій щодо модернізації її системи захисту. Детальний розбір інциденту NotPetya дозволив виявити недоліки в сегментації мережі та управлінні оновленнями, що лягло в основу запропонованих рішень з впровадження архітектури безпечного доступу та автоматизації контролю програмного забезпечення від постачальників. Запропонована методика оцінки рентабельності інвестицій у безпеку та використання часових метрик виявлення і реагування доводять доцільність впровадження розроблених заходів. Результати дослідження свідчать, що перехід до парадигми кіберстійкості дозволяє суттєво скоротити час відновлення

критичних сервісів навіть у разі масштабних деструктивних впливів. Отримані результати можуть бути використані логістичними підприємствами для підвищення надійності функціонування в умовах агресивного кіберсередовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: <https://www.iso.org/standard/27001>
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: <https://www.iso.org/standard/75281>
3. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: <https://www.nist.gov/cyberframework>
4. NIST Special Publication 800–30 Rev. 1. Guide for Conducting Risk Assessments. URL: <https://csrc.nist.gov/pubs/sp/800/30/r1/final>
5. NIST Special Publication 800–61 Rev. 2. Computer Security Incident Handling Guide. URL: <https://csrc.nist.gov/pubs/sp/800/61/r2/final>
6. NIST Special Publication 800–55 Rev. 1. Performance Measurement Guide for Information Security. URL: <https://csrc.nist.gov/pubs/sp/800/55/r1/final>
7. NIST Special Publication 800–161 Rev. 1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. URL: <https://csrc.nist.gov/pubs/sp/800/161/r1/final>
8. IBM X–Force Threat Intelligence Index 2024. IBM Security. URL: <https://www.ibm.com/reports/threat-intelligence>
9. 2024 Data Breach Investigations Report (DBIR). Verizon. URL: <https://www.verizon.com/business/resources/reports/dbir/>
10. FedEx Corporation. Annual Report (Form 10–K) 2023. SEC Filings. URL: <https://investors.fedex.com>
11. California Consumer Privacy Act (CCPA). Official Website. URL: <https://oag.ca.gov/privacy/ccpa>
12. Personal Information Protection and Electronic Documents Act (PIPEDA). Office of the Privacy Commissioner of Canada. URL: <https://www.priv.gc.ca>
13. FAIR Institute. Factors in Analysis of Information Risk (FAIR) Methodology. URL: <https://www.fairinstitute.org/>

- 14.OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Carnegie Mellon University. URL: <https://resources.sei.cmu.edu/>
- 15.CMMI for Services, Version 2.0. CMMI Institute. URL: <https://cmmiinstitute.com/>
- 16.MITRE ATT&CK Matrix for Enterprise. URL: <https://attack.mitre.org/>
- 17.Cybersecurity Maturity Model Certification (CMMC) 2.0. US Department of Defense. URL: <https://it-us.com/cmmc/cmmc-2-0/>
- 18.Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (Focus on NotPetya/TNT Express). Doubleday, 2019. 352 p.
- 19.Chaddad A. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Syngress, 2021. 412 p.
- 20.Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. 320 p.
- 21.Graham J., Howard R., Olson R. Cyber Security Essentials. Auerbach Publications, 2010. 336 p.
- 22.Бурячок В. Л., Толубко В. Б. Інформаційна та кібербезпека: соціотехнічний аспект. Київ: ДУТ, 2015. 288 с.
- 23.Додонов О. Г., Ланде Д. В. Комп'ютерна мережева моніторологія. Київ: Наукова думка, 2014. 256 с.
- 24.Корченко О. О. Побудова систем захисту інформації. Київ: МК–Прес, 2006. 320 с.
- 25.Гнатюк С. О. Сучасні концепції кібербезпеки: від Defense in Depth до Zero Trust. Захист інформації. 2023. Т. 25, № 2. С. 45–56.
- 26.Козаченко Г. В. Управління ризиками підприємства: логістичний аспект. Економіка та управління. 2022. № 4. С. 12–20.
- 27.Cybersecurity in the Logistics Sector: Challenges and Opportunities. Journal of Supply Chain Management. 2023. Vol. 14, Issue 3. pp. 102–115.
- 28.The Impact of Ransomware on Global Supply Chains: Post–Pandemic Analysis. International Journal of Cyber Warfare and Terrorism. 2024. Vol. 12, No. 1.

- 29.Zero Trust Architecture (NIST SP 800–207). URL:
<https://csrc.nist.gov/pubs/sp/800/207/final>
- 30.CISA. Federal Information Security Modernization Act (FISMA). URL:
<https://www.cisa.gov/fisma>

ДОДАТКИ

Порівняльна таблиця характеристик, призначення та відмінності між основними типами рішень у сфері кіберзахисту

Критерій	SIEM	IDS/IPS	DLP
Основне призначення	Централізований збір, кореляція та аналіз подій безпеки з усієї IT-інфраструктури	Виявлення та запобігання вторгненням у мережу	Захист від несанкціонованого витоку конфіденційних даних
Рівень роботи	Інфраструктурний (мережа, сервери, додатки, журнали подій)	Мережевий або хостовий	На рівні кінцевих пристроїв, електронної пошти, хмарних сховищ
Тип даних, що обробляються	Логи, події безпеки, системні повідомлення	Мережевий трафік, пакети даних	Вміст файлів, документи, повідомлення
Спосіб реагування	Аналітика та сповіщення, автоматизовані дії через playbooks	Автоматичне блокування атак або повідомлення адміністратора	Блокування, шифрування або моніторинг передачі даних
Приклади реалізацій	Splunk, IBM QRadar, Wazuh, Azure Sentinel	Snort, Suricata, Zeek, Cisco Firepower	Symantec DLP, Forcepoint DLP, Microsoft Purview DLP
Переваги	Глибока аналітика, централізований моніторинг, підтримка машинного навчання	Оперативне виявлення атак, реальний час, ефективність проти відомих загроз	Контроль чутливої інформації, запобігання витоку, відповідність політикам
Обмеження	Висока вартість, потреба у кваліфікованих аналітиках	Висока кількість помилкових спрацювань, потреба в налаштуванні сигнатур	Складність налаштування політик, вплив на продуктивність
Типові сфери застосування	Великі корпоративні мережі, SOC, хмарні середовища	Мережі з високими вимогами до безпеки (банки, логістика, оборона)	Компанії, що обробляють персональні або фінансові дані