**Оцінка ризиків та політика інформаційної безпеки компанії «NauStilus»**

**Вступ**

У сучасному цифровому середовищі питання інформаційної безпеки набуває критичного значення для будь-якої організації, особливо в телекомунікаційному секторі. З метою моделювання сценарію оцінки ризиків, у даній роботі розглядається **уявна компанія «NauStilus»,** яка надає телекомунікаційні та хмарні послуги.

Компанія «NauStilus» представлена як умовний оператор зв’язку з розгалуженою ІТ-інфраструктурою, що включає хмарні сервери, мережеві компоненти, системи зберігання даних, клієнтські застосунки, офісні системи та фізичну охорону. Такий підхід дозволяє створити уявну **модель ризиків**, яка охоплює технічні, організаційні, людські та юридичні аспекти.

Для оцінки ризиків використано методологію ***OCTAVE***, яка дозволяє системно ідентифікувати загрози, вразливості, оцінити їхній вплив та розробити стратегії мінімізації. Додаткові пункти, включені до аналізу, мають на меті ***розширити знання в галузі управління ризиками***, забезпечити глибше розуміння стандартів ISO/IEC 27001, NIST SP 800-30, GDPR та українського законодавства.

Робота спрямована як на виконання навчального завдання, так і на спробу *с****формувати практичні навички*** з побудови політики інформаційної безпеки, що б відповідала викликам цифрової трансформації на даному етапі, зі здобутими з курсу знаннями.

**Розширена ідентифікація ресурсів компанії «NauStilus»**

1. *Людські ресурси*

* Адміністративний персонал
* Технічні фахівці (DevOps, SOC, Red Team)
* Користувачі систем (внутрішні та зовнішні)
* Контрагенти, підрядники, консультанти
* Персонал, що обробляє персональні дані (відповідно до GDPR/HIPAA)

1. *Інформаційні системи*

* CRM, ERP, Billing-системи
* Системи управління доступом (IAM, AD)
* Системи резервного копіювання та архівування
* Системи моніторингу (SIEM, Zabbix, Prometheus)
* Системи електронного документообігу
* Системи логування та аудиту

1. *Мережева інфраструктура*

* VPN-шлюзи
* Фаєрволи, маршрутизатори, комутатори
* Системи балансування навантаження
* DNS-сервери, DHCP-сервери
* Системи захисту від DDoS

1. *Дані та інформаційні активи*

* Персональні дані користувачів (GDPR, HIPAA)
* Комерційна та фінансова інформація
* Контрактна документація
* Технічна документація (API, архітектура, конфігурації)
* Логи, метадані, аналітика
* Медичні дані (якщо є - підпадають під HIPAA)

1. *Хмарна інфраструктура*

* Платформи IaaS, PaaS, SaaS
* Контейнери, оркестрація (Docker, Kubernetes)
* Облікові записи хмарних провайдерів
* Сховища об’єктів (S3, Azure Blob)
* Резервні копії в хмарі

1. *Клієнтські застосунки*

* Мобільні додатки
* Веб-портали
* API-шлюзи
* Інтерфейси для партнерів
* Системи автентифікації клієнтів (OAuth, MFA)

1. *Фізична інфраструктура та охорона*

* Серверні приміщення
* Системи відеоспостереження
* Системи контролю доступу (картки, біометрія)
* Системи пожежогасіння
* UPS, генератори, охолодження
* Сейфи, архіви, фізичні носії

1. *Юридичні та нормативні ресурси*

* Політики безпеки
* Угоди про конфіденційність (NDA)
* Угоди про обробку даних (DPA)
* Реєстри відповідності (ISO, GDPR, HIPAA)
* Внутрішні регламенти, інструкції, процедури

**Розширений список вразливостей компанії «NauStilus»**

*Ідентифіковані* початкові вразливості

1. DDoS-вразливість (відсутність захисту на рівні мережі/інфраструктури)
2. Витоки даних через слабку DLP-політику
3. Інфікування систем (відсутність EDR/антивірусу, слабкий контроль доступу)
4. Вразливість хмарних серверів (неправильна конфігурація, відкриті порти, слабка автентифікація)

*Можливі вразливості на основі інцидентів*

Кібервразливості:

1. Відсутність захисту від фішингу (немає навчання, фільтрів, DMARC/SPF)
2. Відсутність MFA для привілейованих облікових записів
3. Вразливості в ПЗ/ОС (непроведений пентест, відсутність патчів)
4. Відсутність контролю змін конфігурацій (немає CI/CD політик, журналів)
5. Використання незахищених протоколів (FTP, Telnet, без TLS)
6. Встановлення сторонніх додатків без перевірки (відсутність політики BYOD)
7. Відсутність outbound-фільтрації (можливість використання інфраструктури для атак)
8. Ненадійне зберігання цифрових сертифікатів/ключів (без HSM, без ротації)
9. Відсутність захисту логів (можливість їх зміни або видалення)

Людський фактор

1. Відсутність навчання з кібергігієни
2. Відсутність політики складності паролів
3. Відсутність контролю доступу до критичних даних
4. Відсутність процесу оновлення ПЗ
5. Відсутність перевірки конфігурацій після змін

Фізичні і технічні

1. Відсутність контролю доступу до серверних
2. Відсутність резервного живлення або охолодження
3. Відсутність моніторингу кабельної інфраструктури
4. Відсутність інвентаризації пристроїв
5. Відсутність захисту систем відеоспостереження

Юридичні та репутація

1. Відсутність політики повідомлення про інциденти (GDPR Art. 33)
2. Відсутність DPA/NDA з підрядниками
3. Відсутність плану кризової комунікації
4. Відсутність контролю над фінансовими документами
5. Відсутність журналу відповідності (compliance register)

**Оцінка ризиків за методологією OCTAVE компанії «NauStilus»**

*DDoS-атаки*

* **Частота та повторюваність:** Висока для телеком-компаній, особливо під час пікових навантажень або політичної активності
* **Вразливість:** Відсутність захисту на рівні мережі, слабка фільтрація трафіку, відсутність CDN/WAF
* **Потенційний вплив:** Втрата доступності сервісів, фінансові втрати, шкода репутації
* **Стратегії мінімізації:** Впровадження DDoS-захисту, використання CDN, резервні канали, трафік-аналіз

*Витоки персональних даних*

* **Частота та повторюваність:** Середня, але критична при наявності слабкої DLP
* **Вразливість:** Відсутність шифрування, слабкий контроль доступу, погано налаштовані DLP
* **Потенційний вплив:** Порушення GDPR/ЗУ, штрафи, втрата довіри клієнтів
* **Стратегії мінімізації:** Впровадження DLP, шифрування даних, навчання персоналу, аудит доступу

*Інфікування шкідливими програмами*

* **Частота та повторюваність:** Висока, особливо через фішинг або незахищені пристрої
* **Вразливість:** Відсутність EDR, слабкий антивірус, відкриті порти, необмежений доступ
* **Потенційний вплив:** Компрометація систем, витік даних, знищення інформації
* **Стратегії мінімізації:** Впровадження EDR, регулярне сканування, обмеження доступу, оновлення ПЗ

*Вразливості хмарних серверів*

* **Частота та повторюваність:** Середня, залежить від конфігурації та провайдера
* **Вразливість:** Відкриті порти, слабка автентифікація, неправильні політики доступу
* **Потенційний вплив:** Витік даних, несанкціонований доступ, втручання в сервіси
* **Стратегії мінімізації:** Аудит конфігурацій, MFA, сегментація доступу, логування активності

*Фішинг/соціальна інженерія*

* **Частота та повторюваність:** Висока, особливо через email та месенджери
* **Вразливість:** Відсутність навчання, слабкі фільтри, відсутність DMARC/SPF
* **Потенційний вплив:** Компрометація облікових записів, витік даних
* **Стратегії мінімізації:** Навчання персоналу, фільтрація пошти, впровадження DMARC/SPF

*Компрометація облікових записів*

* **Частота та повторюваність:** Середня, але критична для привілейованих облікових записів
* **Вразливість:** Відсутність MFA, слабкі паролі, спільні облікові записи
* **Потенційний вплив:** Повний контроль над системами, витік даних
* **Стратегії мінімізації:** MFA, політика паролів, моніторинг входів, ротація облікових даних

*Несанкціонований доступ до систем/мережі*

* **Частота та повторюваність:** Залежить від зовнішньої експозиції
* **Вразливість:** Відсутність сегментації, слабкий контроль доступу
* **Потенційний вплив:** Втручання в критичні системи, зміна конфігурацій
* **Стратегії мінімізації:** VPN, сегментація мережі, контроль доступу, журналювання

*Використання незахищених протоколів*

* **Частота та повторюваність:** Низька, але небезпечна при використанні FTP, Telnet
* **Вразливість:** Відсутність TLS/SSL, передача даних у відкритому вигляді
* **Потенційний вплив:** Перехоплення даних, MITM-атаки
* **Стратегії мінімізації:** Вимкнення незахищених протоколів, впровадження TLS, аудит мережі

*Людський фактор (помилки, слабкі паролі, misconfiguration)*

* **Частота та повторюваність:** Висока, особливо без навчання
* **Вразливість:** Відсутність політик, слабкий контроль змін
* **Потенційний вплив:** Витік, знищення, компрометація даних
* **Стратегії мінімізації:** Навчання, контроль змін, автоматизовані перевірки

*Фізичні загрози (проникнення, шпигунство, підпал)*

* **Частота та повторюваність:** Низька, але з високим впливом
* **Вразливість:** Відсутність охорони, слабкий контроль доступу
* **Потенційний вплив:** Знищення обладнання, витік даних, зупинка сервісів
* **Стратегії мінімізації:** Відеоспостереження, охорона, контроль доступу, сейфи

**Розробка планів з обробки ризиків компанії «NauStilus»**

*DDoS-атаки*

* **Підхід:** Зниження ризику через багаторівневий захист мережі та інфраструктури
* **Обґрунтування:** DDoS-атаки можуть повністю паралізувати сервіси компанії, спричинити фінансові втрати та пошкодити репутацію. Вони є однією з найпоширеніших загроз для телеком-сектору.
* **Необхідні заходи:**

1. Впровадження DDoS-захисту на рівні провайдера (наприклад, Cloudflare, Arbor)
2. Використання CDN для розподілу навантаження
3. Налаштування rate-limiting та фільтрації трафіку
4. Розгортання WAF (Web Application Firewall)
5. Моніторинг аномалій у трафіку через SIEM
6. Резервні канали зв’язку та сценарії переключення

*Витоки персональних даних*

* **Підхід:** Превентивний контроль доступу та захист даних відповідно до GDPR/ЗУ
* **Обґрунтування:** Витік персональних даних може призвести до юридичних санкцій, втрати довіри клієнтів та репутаційних збитків.
* **Необхідні заходи:**

1. Впровадження DLP-систем (Data Loss Prevention)
2. Шифрування даних у транзиті та на зберіганні
3. Аудит доступу до критичних даних
4. Впровадження політик мінімального доступу (Least Privilege)
5. Навчання персоналу щодо обробки персональних даних
6. Регулярне тестування на витоки (Red Team, пентести)

*Інфікування шкідливими програмами*

* **Підхід:** Виявлення та ізоляція загроз через EDR, антивірус та навчання
* **Обґрунтування:** Шкідливе ПЗ може призвести до втрати даних, компрометації систем, шифрування або викрадення інформації.
* **Необхідні заходи:**

1. Впровадження EDR-рішень (CrowdStrike, SentinelOne)
2. Регулярне оновлення антивірусного ПЗ
3. Сканування систем на наявність бекдорів та троянів
4. Обмеження прав користувачів на встановлення ПЗ
5. Навчання персоналу щодо фішингу та соціальної інженерії
6. Впровадження sandbox-оточення для підозрілих файлів

*Вразливості на хмарних серверах*

* **Підхід:** Аудит конфігурацій, контроль доступу та моніторинг активності
* **Обґрунтування:** Неправильна конфігурація хмарних ресурсів - одна з найпоширеніших причин витоку даних та несанкціонованого доступу.
* **Необхідні заходи:**

1. Аудит хмарних конфігурацій (наприклад, за допомогою ScoutSuite, Prowler)
2. Впровадження MFA для доступу до хмарних платформ
3. Сегментація доступу до ресурсів (IAM, RBAC)
4. Логування та моніторинг активності через CloudTrail, Azure Monitor
5. Шифрування даних у хмарі
6. Впровадження політик безпеки на рівні хмарного провайдера (CSPM)

*Фішинг або соціальна інженерія*

* **Підхід:** Зниження ризику через навчання персоналу та технічні фільтри
* **Обґрунтування:** Фішинг - один із найпоширеніших методів проникнення, який експлуатує людський фактор. Навіть технічно захищені системи можуть бути скомпрометовані через необізнаність співробітників.
* **Необхідні заходи:**

1. Проведення регулярного навчання з кібергігієни
2. Впровадження фільтрації пошти (антифішинг, антиспам)
3. Налаштування DMARC, SPF, DKIM для доменів
4. Симуляція фішингових атак (Red Team)
5. Впровадження механізмів повідомлення про підозрілі листи
6. Обмеження доступу до критичних систем через email-посилання

*Компрометація облікових записів*

* **Підхід:** Превентивний контроль автентифікації та моніторинг доступу
* **Обґрунтування:** Компрометація привілейованих облікових записів може призвести до повного контролю над системами, витоку даних та порушення безпеки.
* **Необхідні заходи:**

1. Впровадження багатофакторної автентифікації (MFA)
2. Політика складності паролів та їх ротація
3. Впровадження PAM (Privileged Access Management)
4. Моніторинг входів та спроб автентифікації
5. Аудит прав доступу та їх регулярний перегляд
6. Відокремлення облікових записів за ролями

*Несанкціонований доступ до систем або мережі*

* **Підхід:** Сегментація мережі та контроль доступу
* **Обґрунтування:** Відсутність ізоляції між сервісами дозволяє зловмиснику переміщатися по інфраструктурі після первинного проникнення.
* **Необхідні заходи:**

1. Впровадження VLAN та мережевої сегментації
2. Використання VPN для доступу до внутрішніх ресурсів
3. Контроль доступу через ACL та IAM
4. Моніторинг мережевої активності через IDS/IPS
5. Аудит мережевих маршрутів та відкритих портів
6. Впровадження Zero Trust моделі

*Використання незахищених протоколів*

* **Підхід:** Вимкнення небезпечних протоколів та впровадження шифрування
* **Обґрунтування:** Протоколи без шифрування (FTP, Telnet) дозволяють перехоплювати дані, що передаються, і здійснювати MITM-атаки.
* **Необхідні заходи:**

1. Вимкнення FTP, Telnet, HTTP без TLS
2. Впровадження HTTPS, SFTP, SSH
3. Аудит конфігурацій мережевих пристроїв
4. Впровадження TLS 1.2+ для всіх сервісів
5. Навчання персоналу щодо безпечних протоколів
6. Моніторинг використання протоколів через SIEM

*Людський фактор (помилки, слабкі паролі, misconfiguration)*

* **Підхід:** Навчання, автоматизація перевірок та контроль змін
* **Обґрунтування:** Людські помилки - одна з найчастіших причин інцидентів, особливо в умовах недостатньої підготовки або перевантаження персоналу.
* **Необхідні заходи:**

1. Впровадження системи контролю змін (Change Management)
2. Автоматизовані перевірки конфігурацій (наприклад, CIS Benchmarks)
3. Навчання щодо безпечної роботи з системами
4. Впровадження політик складності паролів
5. Аудит прав доступу та конфігурацій
6. Впровадження системи внутрішніх перевірок (peer review)

*Фізичні загрози (проникнення, шпигунство, підпал)*

* **Підхід:** Фізичний контроль доступу та приховане спостереження
* **Обґрунтування:** Фізичне проникнення або знищення обладнання може спричинити повну втрату даних, порушення безперервності бізнесу та юридичні наслідки.
* **Необхідні заходи:**

1. Впровадження систем контролю доступу (картки, біометрія)
2. Відеоспостереження з архівацією записів
3. Приховане спостереження у випадках шпигунства
4. Системи пожежогасіння та резервного живлення
5. Фізична охорона критичних зон
6. Внутрішнє розслідування з фіксацією дій зловмисника