УДК 378:[005.92+331.103-057]

Я. Набожний, здобувач гр. ІС 23-М
Центральноукраїнський національний технічний університет

КЛЮЧОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ «НАФТОГАЗ УКРАЇНИ»

Розглядаються інформаційні технології, питання забезпечення інформаційної безпеки стратегічно важливих підприємств, як «Нафтогаз України», що відіграють ключову роль у забезпеченні енергетичної безпеки держави. Закцентовано увагу на тому, що з огляду на зростання кількості кіберзагроз та інформаційних атак, розробка й впровадження ефективних заходів захисту інформації є одним із пріоритетних завдань компанії.

інформаційна безпека, кіберзагрози, інформаційні атаки, інформаційні технології, методи захисту інформації

Постановка проблеми. В умовах сучасного світу, де інформаційні технології проникають у всі сфери діяльності, питання забезпечення інформаційної безпеки стає критично важливим. Це особливо стосується таких стратегічно важливих підприємств, як "Нафтогаз України", що відіграють ключову роль у забезпеченні енергетичної безпеки держави. З огляду на зростання кількості кіберзагроз та інформаційних атак, розробка й впровадження ефективних заходів захисту інформації є одним із пріоритетних завдань компанії.

Головні виклики у сфері інформаційної безпеки для «Нафтогаз України»

1. **Кіберзагрози та атаки**. Зростання кількості та складності кіберзлочинів, включаючи фішинг, DDoS-атаки, програмне забезпечення-вимагач та інші методи злому, ставить під загрозу конфіденційність, цілісність і доступність даних компанії. Наприклад, згідно з дослідженнями, у 2022 році кількість DDoS-атак зросла на 55% у порівнянні з попереднім роком [1].
2. **Захист критичної інфраструктури**. Діяльність "Нафтогазу" пов'язана з управлінням великими обсягами енергетичних ресурсів, і порушення в інформаційних системах можуть мати катастрофічні наслідки для економіки країни. За даними Національного інституту стандартів і технологій (NIST), кіберзагрози для енергетичних підприємств є одним із найвищих пріоритетів у сфері захисту критичної інфраструктури [2].
3. **Інсайдерські загрози**. Співробітники компанії, які мають доступ до конфіденційної інформації, можуть ненавмисно або навмисно створювати ризики для інформаційної безпеки. Дослідження компанії IBM показує, що інсайдерські загрози становлять близько 60% від усіх інцидентів інформаційної безпеки [3].
4. **Недостатній рівень захисту інформації**. У багатьох випадках використовувані технології або політики безпеки не відповідають сучасним стандартам та вимогам. Наприклад, згідно з опитуванням Gartner, близько 40% компаній у світі визнають, що їхні стратегії інформаційної безпеки потребують суттєвого оновлення [4].
5. **Законодавчі та регуляторні виклики**. Забезпечення відповідності вимогам національного законодавства та міжнародних стандартів у сфері інформаційної безпеки вимагає значних ресурсів і постійного моніторингу змін. Наприклад, дотримання стандартів ISO/IEC 27001 стало обов’язковим для багатьох підприємств у галузі енергетики [5].

Чому це важливо?

Будь-яка успішна кібератака на системи "Нафтогаз України" може призвести до серйозних наслідків:

- **Економічних втрат** через порушення бізнес-процесів.
- **Витоку конфіденційної інформації**, включаючи комерційні та стратегічні дані.
- **Зниження довіри** до компанії з боку партнерів, інвесторів та споживачів.
- **Загроз енергетичній безпеці країни**, що може вплинути на стабільність держави загалом.

Отже, постановка проблеми інформаційної безпеки в компанії «Нафтогаз України» є першочерговим завданням для збереження її стійкості, конкурентоспроможності та виконання стратегічних функцій. Необхідність інтеграції сучасних технологій, підвищення обізнаності співробітників і відповідності міжнародним стандартам є ключовими напрямками для зміцнення захисту інформації.

Аналіз останніх досліджень та публікацій. У сфері інформаційної безпеки стратегічних підприємств, таких як "Нафтогаз України", активно проводяться дослідження, спрямовані на оцінку ризиків та вдосконалення методів захисту інформації. Зокрема, останні публікації свідчать про кілька ключових тенденцій та результатів:

1. Адаптація міжнародних стандартів. У роботах багатьох українських та зарубіжних авторів акцентується увага на важливості впровадження стандартів ISO/IEC 27001 для підвищення рівня інформаційної безпеки. Дослідження демонструють, що відповідність цим стандартам дозволяє зменшити ризики витоку даних та покращити управління інформаційними процесами.
2. Інноваційні технології захисту. Аналітичні звіти від провідних компаній, таких як Gartner та Forrester, наголошують на використанні штучного інтелекту (AI) та машинного навчання (ML) для виявлення й реагування на кіберзагрози в режимі реального часу. Це особливо актуально для великих енергетичних компаній.
3. Вивчення інцидентів кібербезпеки. Останні дослідження відображають значний інтерес до аналізу реальних випадків атак на енергетичний сектор. Наприклад, публікації від ENISA (Агентства Європейського Союзу з кібербезпеки) описують кібератаки на критичну інфраструктуру та пропонують рекомендації щодо їхнього попередження.
4. Управління інсайдерськими загрозами. За даними досліджень, близько 60% порушень інформаційної безпеки відбуваються через дії співробітників. Наукові статті пропонують рішення, такі як автоматизація моніторингу дій персоналу та підвищення обізнаності працівників щодо загроз.
5. Регуляторні аспекти. У наукових публікаціях наголошується на важливості гармонізації національного законодавства з міжнародними вимогами. Наприклад, Директива NIS2 ЄС часто згадується як основа для вдосконалення українських норм у сфері кібербезпеки.

Загалом, аналіз останніх досліджень демонструє, що ефективна інформаційна безпека потребує комплексного підходу, який включає технічні, організаційні та нормативно-правові заходи. "Нафтогаз України" може скористатися цими напрацюваннями для створення більш стійкої системи захисту інформації.

Мета й завдання дослідження.

Мета дослідження: дослідити та проаналізувати стан інформаційної безпеки сучасного підприємства, можливості розробки моделі зрілості інформаційної безпеки підприємства, визначити напрями оптимізації підвищення рівня безпеки газопостачальної компанії «Нафтогаз України» в умовах цифровізації.

Завданнями роботи є:

1) здійснити аналіз сучасного стану дослідження проблеми інформаційної безпеки підприємства в умовах цифровізації;

2) визначити джерельну базу та методи дослідження;

3) проаналізувати систему інформаційної безпеки газопостачальної компанії «Нафтогаз України»;

4) дослідити існуючі системи захисту, проаналізувати інциденти інформаційної безпеки;

5) визначити труднощі і проблеми в організації системи інформаційної безпеки підприємства;

6) розробити модель зрілості інформаційної безпеки підприємства;

7) окреслити напрями оптимізації підвищення рівня інформаційної безпеки газопостачальної компанії «Нафтогаз України»;

8) розробити рекомендації щодо використання інноваційних технологій для створення ефективних моделей інформаційної безпеки сучасного підприємства.

Виклад основного матеріалу. Інформаційна безпека є одним із ключових елементів стратегічного управління компанією "Нафтогаз України", що забезпечує її стійкість до зовнішніх і внутрішніх загроз, а також ефективну роботу національної енергетичної системи. У даній статті висвітлено основні аспекти інформаційної безпеки компанії, які враховують як технічні, так і організаційні заходи.

Перш за все, захист конфіденційної інформації є пріоритетом для "Нафтогазу". У компанії впроваджено сучасні технології шифрування даних, що дозволяють запобігти несанкціонованому доступу до чутливих даних. Зокрема, використання сертифікованих систем захисту відповідає міжнародним стандартам ISO/IEC 27001. Цей стандарт регулює вимоги до створення, впровадження та підтримки систем управління інформаційною безпекою (СУІБ), що є основою кіберзахисту в компанії [6].

Другою важливою складовою є моніторинг кіберзагроз і реагування на інциденти. "Нафтогаз" використовує системи раннього виявлення атак та інструменти аналізу мережевого трафіку. Завдяки цьому компанія має змогу оперативно виявляти спроби втручання, як-от фішингові атаки або зломи облікових записів. Усі підозрілі дії фіксуються, а відповідальні фахівці проводять детальний аналіз інцидентів.

Значна увага приділяється навчанню персоналу. Працівники компанії проходять регулярні тренінги з інформаційної безпеки, що включають вивчення базових принципів захисту даних, розпізнавання кіберзагроз та правильні дії у разі підозрілих ситуацій. Підвищення обізнаності персоналу є критичним фактором зменшення ризику успішних атак через людський фактор.

Не менш важливим аспектом є співпраця з державними органами та міжнародними організаціями. «Нафтогаз України» активно співпрацює з Державною службою спеціального зв'язку та захисту інформації України, а також бере участь у глобальних ініціативах із протидії кіберзагрозам. Таке партнерство дозволяє обмінюватися досвідом, отримувати актуальну інформацію про загрози та підвищувати ефективність заходів безпеки.

Для захисту промислових систем автоматизації використовуються спеціалізовані рішення, що забезпечують безперебійну роботу критичної інфраструктури. Ці системи включають сегментування мережі, контроль доступу до обладнання та регулярне оновлення програмного забезпечення, щоб уникнути уразливостей [7].

Таким чином, основні аспекти інформаційної безпеки "Нафтогаз України" зосереджені на впровадженні сучасних технологій захисту, розбудові системи управління безпекою, навчанні персоналу та співпраці з партнерами. Завдяки комплексному підходу компанія здатна ефективно протистояти сучасним викликам у сфері інформаційної безпеки, що є запорукою її стабільної роботи та безпеки енергетичного сектора України.

Висновок

У процесі дослідження інформаційної безпеки компанії «Нафтогаз України» було виявлено ключові виклики, пов’язані з кіберзахистом у сучасних умовах цифровізації. Аналіз показав необхідність комплексного підходу, який включає впровадження сучасних технологій, розробку ефективних політик і формування культури кібербезпеки. Компанія вже інтегрує міжнародні стандарти, зокрема ISO/IEC 27001, та використовує SIEM-систему для моніторингу загроз. Водночас необхідно оптимізувати процеси реагування,

застосовувати штучний інтелект для прогнозного аналізу та підвищувати рівень обізнаності персоналу.

Розроблена модель зрілості інформаційної безпеки дозволяє оцінювати поточний стан і визначати напрями розвитку. Впровадження дорожньої карти переходу на вищий рівень зрілості сприятиме зниженню ризиків, покращенню координації процесів та підвищенню ефективності витрат. Практичні результати включають скорочення часу на виявлення загроз і зниження витрат на ліквідацію наслідків, що підтверджує ефективність інтеграції новітніх технологій.

Рекомендації для компанії передбачають подальшу автоматизацію процесів, розширення використання штучного інтелекту, посилення взаємодії з підрядниками та регулярні навчання персоналу. Це дозволить зберегти стійкість до кіберзагроз, забезпечити безперебійність операцій та відповідати міжнародним стандартам. Розвиток культури кібербезпеки серед співробітників є критично важливим через вплив людського фактора на ризики.

Інтеграція інформаційної безпеки в бізнес-процеси не лише знизить уразливість до загроз, а й зміцнить довіру клієнтів і партнерів. Використання штучного інтелекту для автоматизації процедур та прогнозування забезпечить стабільність роботи критичної інфраструктури, що має особливе значення для енергетичного сектору. Реалізація дорожньої карти дозволить ефективніше управляти ризиками, мінімізувати наслідки інцидентів і зменшити їх вплив на бізнес-процеси.

Список літератури

1. Kaspersky Lab. “Cyber Threats and Trends in 2022.”
2. National Institute of Standards and Technology (NIST). “Framework for Improving Critical Infrastructure Cybersecurity.”
3. IBM Security Services. “Insider Threats in the Enterprise.”
4. Gartner. “Cybersecurity Predictions for 2023.”
5. ISO. “ISO/IEC 27001: Information Security Management Systems.”
6. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.
7. Офіційний сайт ТОВ ГК “Нафтогаз України”: https://gas.ua/uk/home.