МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Центральноукраїнський національний технічний університет

Економічний факультет

Кафедра історії, археології, інформаційної та архівної справи

«Допущено до захисту»
Завідувач кафедри ІАІАС,
доктор історичних наук,
професор
_____ Василь ОРЛИК
«_____» _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

за другим (магістерським) рівнем вищої освіти на тему:

«ІНФОРМАЦІЙНА БЕЗПЕКА ДІЯЛЬНОСТІ ГАЗОПОСТАЧАЛЬНОЇ КОМПАНІЇ «НАФТОГАЗ УКРАЇНИ» В УМОВАХ ЦИФРОВІЗАЦІЇ»

Виконав: здобувач вищої освіти
ІІ курсу, групи ІС-23М (1,4)
ОПП «Інформаційна, бібліотечна
та архівна справа»
спеціальності 029 «Інформаційна
бібліотечна та архівна справа»
_____**НАБОЖНИЙ Ярослав Сергійович**
«____» _____ 2024 р.
Керівник роботи:
кандидат педагогічних наук, доцент
_____ Олена КОЛОМІЄЦЬ
«____» _____ 2024 р.
Рецензент:
к. пед. н., директор Кропивницького фахового
коледжу Приватного вищого навчального
закладу «Університет сучасних знань»
_____Тетяна ШИШКІНА

Кропивницький – 2024

ЗМІСТ

ВСТУП

Актуальність дослідження. Як відомо, в сучасних умовах роль інформації постійно зростає. Вона стала важливим елементом життєдіяльності у різних сферах, а також повноцінним продуктом, який можна обміняти або продати. У світі бізнесу будь-які дані мають ціну набагато більшу, ніж техніка, що її зберігає. Тому забезпечення безпеки цього ресурсу стає пріоритетним в діяльності сучасного підприємства. Захист інформації в процесі функціонування підприємств дає можливість укладати вигідні контракти, отримувати високі доходи, підвищувати ефективність діяльності в цілому. Серед основних завдань сучасних підприємств – забезпечення безпеки економічної інформації, створення ефективної моделі кібернетичної безпеки.

Інформаційна безпека перетворюється, таким чином, на невід'ємний елемент системи управління підприємством. По суті вона являє собою комбінацію програмно-апаратних засобів та системи заходів, які мають забезпечити н захист інформаційного простору від стороннього втручання та дій із недобрим наміром. Інформаційна безпека має надати впевненості у тому, що жодних даних не буде втрачено чи неправомірно використано ніким із співробітників, ділових партнерів, чи третіх осіб.

Окрім того, слід зазначити, що інформаційна безпека – це правове поняття. Їм позначається стан захищеності не тільки конкретного підприємства, а й загалом національних інтересів України в інформаційній сфері. Йдеться про сукупність збалансованих інтересів держави, суспільства й особистості. Будь-яке наукове знання про стан інформаційної безпеки на різних рівнях її функціонування набуває актуального значення.

Проблемі інформаційної безпеки підприємств в умовах цифровізації присвятили свої наукові розробки вітчизняні науковці: О. Волот, Д. Дубов, М. Зубок, В.. Толубко, Е. Низенко, В. Ортинський та багато інших авторів.

Розробка цієї проблематики відповідає новітнім досягненням науки й соціальної практики; посилює необхідність наукового осмислення нових

можливостей побудови, забезпечення та моделювання інформаційної безпеки сучасного підприємства з врахуванням проблем та ризиків при впровадженні та експлуатації новітніх інформаційних систем і технологій.

Проте багато важливих аспектів означеної проблеми залишаються недостатньо висвітленими у науковій літературі. Йдеться про вплив кібератак на функціонування обліку сучасного підприємства, моделювання організації інформаційної безпеки підприємства та процесу створення надійної системи кібернетичної безпеки. Це пояснюється тим, що підприємницька діяльність має складну структуру; відбувається формування нових механізмів реалізації інноваційних трансформацій в підприємницькій діяльності. Постійно оновлюється й нормативно-правова база організації системи інформаційної безпеки сучасного підприємства.

Досліджувальна тема є надзвичайно актуально. Обумовлюється це, в першу чергу, необхідністю застосування новітнії прогресивних і високотехнологічних підходів до побудови інформаційної безпеки сучасного підприємства, а також розробки ефективної моделі зрілості інформаційної безпеки підприємства в умовах цифровізації.

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.

Об'єкт дослідження*:* діяльність газопостачальної компанії «Нафтогаз України» в умовах цифровізації.

Предмет дослідження*:* система інформаційної безпеки газопостачальної компанії «Нафтогаз України».

Практичне значення результатів кваліфікаційної роботи спрямовано на осучаснення моделі інформаційної безпеки підприємства, що має гарантувати її успішне функціонування в цілому, сприяти підвищенню рівня конкурентоспроможності сучасного підприємства. Теоретичні положення і висновки можуть використовуватися при підготовці спецкурсів та читанні лекцій, проведенні спецсемінарів, для створення програм, навчально-методичних посібників з проблем, зазначених в дослідженні.

Структура та зміст роботи. Кваліфікаційна робота «Інформаційна безпека діяльності газопостачальної компанії «Нафтогаз України» в умовах цифровізації» складається зі вступу, трьох розділів, висновків, списку використаних джерел та літератури, а також додатків.

У вступі обґрунтовано актуальність теми, визначено об'єкт, предмет, мету, завдання дослідження.

У першому розділі проаналізовано сучасний стан дослідження проблеми інформаційної безпеки підприємства в умовах цифровізації, визначено джерельну базу і методи дослідження.

Другий розділ присвячено аналізу системи інформаційної безпеки газопостачальної компанії «Нафтогаз України». Визначено сутність поняття

«інформаційна безпека підприємства», її види, принципи, нормативно-правову базу. Здійснено огляд існуючих систем захисту та аналіз інцидентів інформаційної безпеки.

У третьому розділі представлено основні аспекти розробки моделі зрілості інформаційної безпеки газопостачальної компанії «Нафтогаз України», зокрема, систему моніторингу та реагування на інциденти, критерії вибору моделі оцінки зрілості, дорожню карту. Окреслено напрями оптимізації підвищення рівня інформаційної безпеки газопостачальної компанії «Нафтогаз України». Розроблено рекомендації щодо використання інноваційних технологій для створення ефективних моделей інформаційної безпеки сучасного підприємства.

У висновках узагальнено результати дослідження, сформульовано підсумки в теоретичному та практичному аспектах.

Кваліфікаційна робота містить … сторінок, список використаних джерел та літератури складає … найменувань, додаток.

КЛЮЧОВІ СЛОВА: інформаційна безпека, інформаційно-комп'ютерні технології, інциденти інформаційної безпеки, модель, система захисту, сучасне підприємство, цифровізація.

РОЗДІЛ І.
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

1.1. Сучасний стан дослідження проблеми інформаційної безпеки підприємства в умовах цифровізації.

У сучасному світі важливим фактором виробництва та підприємницької діяльності, одним з основних ресурсів розвитку суспільства є об'єктивна інформація. Можливості інформаційних систем і новітніх технологій дозволяють нині автоматизувати управлінські процеси в державних, економічних, соціальних, оборонних та інших об'єктах і системах і при цьому отримувати, обробляти, накопичувати і передавати інформацію про ці процеси в будь-якій кількості.

За умов широкого використання інформаційно-комп'ютерних технологій у всіх сферах життєдіяльності, надзвичайно динамічних процесів розвитку глобального інформаційного суспільства проблеми інформаційної безпеки набувають особливого значення.

Інформаційна безпека підприємства обумовлює стан захищеності інформаційного середовища підприємства. А інформаційні ресурси та інформаційна інфраструктура як складові інформаційного середовища України, за твердженням фахівців, сьогодні значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни [1].

Увага до проблем інформаційної безпеки нашої держави підсилюється також антиукраїнськими впливами, які пропагують ідеї насильства, національної ворожнечі, сепаратизму і є спробами руйнації національної ідентичності України, посягання на її конституційний лад.

Проблемі інформаційної безпеки підприємства в умовах цифровізації присвячено цілу низку наукових розробок вітчизняних авторів. Серед них: [10], І. А. Маркіна, Д. Н. Дячков [22], Е. І. Низенко, В. П. Каленяк [24], О. В. Олійник [26], В. Л. Ортинський [27], О. А. Сороківська, В. Л. Гевко [33] В.

Б. Толубко, В. Л. Бурячок [35] та інші. Науковці досліджують теоретичні основи проблеми інформаційної безпеки, обґрунтовують її значення для функціонування підприємств, установ та організацій; визначають методологічні засади побудови інформаційної безпеки сучасного підприємства.

Сучасні автори проблеми інформаційної безпеки окремих підприємств, установ та організацій пов'язують із загальним станом інформаційної безпеки в Україні, акцентуючи на тому, що її забезпечення є необхідною умовою для здійснення життєво важливих інтересів людини. Усвідомлення цього зумовлене стрімким зростанням технічних можливостей сучасних інформаційних систем, вплив яких є всеосяжним і визначальним на економічне і політичне життя, духовну та ідеологічну сфери людської життєдіяльності. Окрім того, в умовах сьогодення інформаційна безпека стає базовим елементом системи національної безпеки України [2].

Увага звертається й на загрози інформаційній безпеці сучасного підприємства. Йдеться, зокрема, про:

- протизаконну «діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- відмову технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо» [19].

Науковці досліджують й термінологічні питання, зокрема розкривають зміст, сутність та особливості поняття «інформаційна безпека» [37]. У публікації наведений широкий перелік визначень поняття «інформаційна безпека», які подають вітчизняні та зарубіжні автори.

Дослідниця В. Ю. Світлична висвітлює сутність поняття «загрози інформаційні безпеці». Вона ретельно аналізує джерела цих загроз, деталізує

аспекти інформаційного протиборства та інформаційної зброї, вивчає основні складові системи забезпечення інформаційної безпеки [31].

Сучасних авторів цікавлять питання забезпечення нормативно-правової бази функціонування систем інформаційної безпеки на підприємствах, в установах та організаціях. У цьому контексті відзначимо наукові розробки П. Д. Біленчука, Л. В. Борисової, М. І. Зубок [15]; [29] та інших.

Розгляду складових державної інформаційної політики щодо забезпечення інформаційної безпеки й визначення основних напрямків діяльності органів державної влади у цій сфері присвячено наукову розвідку В. Панченка [28]. Автор аналізує стан нормативно-правового регулювання інформаційної безпеки України, визначає основні здобутки та недоліки у нормативно-правовому полі держави щодо забезпечення інформаційної безпеки. В. Панченко пропонує розглядати систему інформаційної безпеки підприємства як модель інформаційного протиборства з факторами внутрішнього і зовнішнього середовища Такий підхід до організації діяльності промислових підприємств має допомогти у забезпеченні розробки, впровадження та використання системи інформаційної безпеки, а також у запобіганні системних або методичних помилок на кожному з етапів.

Дослідники В. Г. Горник та С. О. Кравченко вивчають роль інформаційної безпеки в підприємницькій діяльності. На їхню думку, пріоритним напрямком державної політики у сфері забезпечення інформаційної безпеки в підприємницькій діяльності в Україні є вдосконалення правових механізмів регулювання суспільних відносин в інформаційній галузі. Механізмами такої підтримки можуть бути: інформаційний патронат; інформаційна кооперація; інформаційний захист будь-якого рівня. [7].

У монографії А. Ю. Нашинець-Наумової [23], розглядаються загальнонаукові категорії інформаційної безпеки в Україні та в світі, особливості функціонування системи інформаційної безпеки, а також

досліджуються питання захисту інсайдерської інформації суб'єктів господарювання.

Дослідниця Волот О. І. багато уваги приділяє питанню щодо забезпечення безпеки економічної інформації та створення моделі кібернетичної безпеки підприємства інформації та створення моделі кібернетичної безпеки підприємства [3]. Вона акцентує увагу на методологічних засадах побудови інформаційної та кібернетичної безпеки сучасного підприємства, визначає основні завдання та джерела загроз інформаційній безпеці.

В інших наукових розвідках О. І. Волот аналізує існуючі методики до оцінки ефективності застосування інформаційних технологій на промислових підприємствах [5]; визначає роль реального сектору економіки в економічній розбудові держави [6]; аналізує потенційні загрози від зовнішнього та внутрішнього втручання в інформаційну систему підприємства малого бізнесу [4] та досліджує інші аспекти зазначеної проблеми.

Теоретичні аспекти інформаційної безпеки сучасного підприємства досліджують В. М. Кицюк та О. С. Путилін [17]. Науковці аналізують статистичні дані щодо стану кібербезпеки на світовому ринку, визначають сутність поняття «інформаційна безпека», формують перелік принципів забезпечення інформаційної безпеки суб'єктів господарської діяльності в умовах сьогодення, побудови та впровадження якісної інформаційної системи у виробничі процеси підприємства.

Проблемі забезпечення стратегічного управління інформаційною безпекою сучасних підприємств присвячено дослідження О. Храпкіна [36]. У науковій розвідці акцентується увага на необхідності формування системи управління інформаційною безпекою, що зумовлюється існуванням внутрішніх і зовнішніх загроз, їхніми наслідками деструктивного характеру для іміджу та діяльності підприємства. При цьому зауважується, що робота в заданому напрямку передбачає виявлення потенційних ризиків для

підприємства, розробку та впровадження стратегій усунення проблем, розроблених для зменшення ризиків за допомогою наявних ресурсів.

Дослідники вивчають також вплив сучасних інформаційних технологій на діяльність підприємства [8]. Автори публікації доводять, що сучасні технології несуть відчутний вплив на всі складові інформаційної безпеки. А спроможність зберігати високий рівень економічної безпеки підприємства визначається тим, наскільки ефективно це підприємство використовує наявні можливості й наскільки ефективно протистоїть новим загрозам.

Особливе місце у структурі економічної безпеки підприємства займає управлінська складова, що включає цілий комплекс різноманітних знань, умінь й навичок, необхідних менеджерам для реалізації будь-яких управлінських функцій.

Аналізу тенденцій й визначенню перспективних напрямів розвитку інформаційної діяльності в управлінні К. Климова присвятила свої наукові дослідження К. Климова [18]. У публікації зазначається, що основними тенденціями в організації інформаційної діяльності сфери управління є зростання ролі і значення організаційних засад в інформаційній підготовці та реалізації управлінських рішень на стратегічному рівні. Організація інформаційної діяльності в управлінні охоплює всі стадії життя документів, підпорядковується завданням державної політики, цілям і завданням роботи конкретного підприємства, а також має сприяти підвищенню ролі наукових засад організації інформаційної діяльності на підприємствах, в установах та організаціях.

Науковці долучаються до створення підручників, навчально-методичних посібників, методичних вказівок, іншої навчальної літератури, що стосується проблем інформаційної безпеки. Відзначимо напрацювання таких авторів, як М. І. Камлик [16], В. А. Ліпкан [20], В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович С. І. [21], С. І Ніколаюк, Д. Й. Никифорчук [25], М. Ю. Якименко, В. А. Савченко, С. В. Легомінова С. В. [38].

Отже, проведений аналіз літератури дозволяє зробити висновок про інтерес та увагу науковців до проблеми забезпечення інформаційної безпеки підприємств. Нині проводиться активна робота, спрямована на удосконалення системи інформаційної безпеки діяльності окремих підприємств, установ та організацій. Йдеться про:

- захист даних від фізичного доступу;
- розробку та практичне втілення систем електронного підпису;
- створення та реалізацію передових способів аутентифікації користувачів;
- забезпечення належного рівня інтернет-безпеки у випадку з «хмарними технологіями»;
- розроббку стійких систем шифрування та способів захисту від різноманітних атак;
- захист бездротових з'єднань, електроніки та всіляких пристроїв тощо.

Однак, варто зазначити, що на сьогодні практично відсутні розробки комплексної програми забезпечення інформаційної безпеки діяльності підприємств. Науковці розглядають лише окремі її аспекти. Тому актуальним залишається питання підвищення якісного рівня систем інформаційної безпеки. Варто зазначити, що інформаційна безпека підприємства вимагає комплексного підходу до реалізації її основних засад. Це передбачає, зокрема, здійснення постіного моніторингу інформаційних систем, регулярного оновлення програмного забезпечення, підтримку гнучкості та динамічності самої системи інформаційної безпеки.

1.2. Джерельна база дослідження

Нормативно-правова база управління інформаційною безпекою держави в Україні ґрунтується на міжнародних актах, ратифікованих Україною, Конституції України, Законах України та підзаконних актах (наприклад, постановах та розпорядженнях КМУ, міжгалузевих та галузевих

документах). Ці документи відіграють ключову роль й для аналізу систем інформаційної безпеки підприємств.

Джерельну базу нашого дослідження складають законодавчі акти, державні стандарти, нормативно-правові документи, які регулюють процеси забезпечення інформаційної безпеки підприємств й обумовлюють аналіз внутрішніх та зовнішніх інформаційних загроз національній безпеці України, визначають шляхи гарантування інформаційної безпеки країни на будь-якому рівні. Серед законодавчих актів найбільш важливими є:

- Закон України «Про Основні засади забезпечення кібербезпеки України» [13];
- Закон України «Про інформацію» [11];
- Закон України «Про Національну програму інформатизації» [12].

Основні пріоритети, принцита напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 р. № 96 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. «Про Стратегію кібербезпеки України [30].

У зв'язку з рішенням Ради національної безпеки і оборони «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 21 березня 2016 р., введеним у дію Указом Перезидента Украхни від 23 квітня 2008 р. «377, було затверджено Доктрину інформаційної безпеки України (Указ Президента України від 8 липня 2009 р. № 514/2009 р.).

У Доктрині йдеться про інформаційну безпеку як невід'ємну складову кожної зі сфер національної безпеки, зазначається, що «розвиток України як суверенної, демократичної, соціальної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки» [29].

Джерельна база дослідження включає також міжгалузеві та галузеві документи, державні стандарти щодо інформації та документації тощо.

Однак, фахівці зазначають, що законодавча база, сформована за роки незалежності, має певні прогалини і ще не повною мірою відповідає потребам сучасного стану інформаційної безпеки. Вона не забезпечує у повній мірі реалізації права громадян на безкоштовне отримання інформації, не вирішує всіх проблем технологічного характеру в сфері функціонування будь-яких автоматизованих систем, не підтримує надійний рівень інформаційної достатності для прийняття рішень державними органами, підприємствами, громадянами, а також в реалізації стратегії захисту інформаційного суверенітету держави.

1. Джерельна база дослідження включає також документи внутрішнього розпорядку установи, що зумовлено завданнями, визначеними у кваліфікаційній роботі. Система документації газопостачальної компанії «Нафтогаз України» охоплює управлінські документи службового характеру, зокрема, первинно-облікові, організаційно-розпорядчі, планові, фінансово-облікові, звітно-статистичні та ін.. Ці документи забезпечують діяльність компанії «Нафтогаз України» як юридичної особи. Господарська документація включає документи переважно економічного, виробничого та організаційного характеру. Вона містить довідкову й практичну складові, а також документи з контролю виконання.

Окрім того, ми використовували наукові статті, монографії та дослідження сучасних українських авторів, що стосуються інформаційної безпеки держави та підприємств, зокрема, теоретичних аспектів кібербезпеки, сучасних підходів до стратегічного управління інформаційною безпекою, механізмів захисту інформації в контексті інноваційних трансформацій сьогодення.

Усі ці джерела забезпечують глибоке та всебічне розуміння сучасного стану, проблем та перспектив інформаційної безпеки в Україні, що є основою для розробки науково обґрунтованих рекомендацій щодо їх вдосконалення та розвитку.

Важливе значення мають також інформаційні та довідкові документи:

- Інформаційні листи;
- Довідки;
- Офіційний веб-сайт установи.

Таким чином, вивчення та грунтовний аналіз джерельної бази дослідження дав змогу простежити основні концептуальні засади системного аналізу інформаційної безпеки, що включає дослідження її сутності, принципів, методів управління та порядку реалізації сучасних підходів до забезпечення інформаційної безпеки підприємства. Це є надзвичайно важливим для досягнення поставленої мети та реалізації окреслених завдань.

1.3. Методи дослідження

Важливе значення для успіху наукової роботи має вибір методів дослідження. Метод, який використовується як спосіб пізнання – це організований і систематизований спосіб досягнення конкретної наукової мети. Методологія виконує низку ключових функцій, зокрема:

- надає допомогу у визначенні способів здобуття нових наукових знань;
- виявляє шлях пізнання, на якому досягається певна мета наукового пошуку;
- створює логіко-аналітичний інструментарій наукового пізнання;
- розвиває систему наукової інформації;
- забезпечує всебічність отримання інформації щодо процесу чи явища, які вивчаються;
- допомагає введенню нової інформації до фонду теорії науки;
- забезпечує уточнення, збагачення, систематизацію термінів і понять у науці.

Методи дослідження поділяються на філософські, наукові та спеціальні, розроблені в межах конкретних наукових галузей. Існує також сукупність методів, характерних для групи споріднених наукових дисциплін,

які досліджують загальний об’єкт і використовують специфічні методи для виявлення особливостей цих явищ.

У ході дослідження були використані такі методи:

- загальнофілософські (сходження від абстрактного до конкретного, аналіз і синтез, порівняння, узагальнення тощо);
- загальнонаукові (історичний та логічний з властивим їм аналізом, синтезом і системним підходом, опис, спостереження, прогнозування, моделювання);
- спеціальні (статистичні методи й методи соціальних досліджень);
- специфічні (соціально-комунікаційно-інформаційний підхід, структурно-типологічний метод).

Так, використання методу аналізу і синтезу дозволило, зокрема, розглянути організацію системи інформаційної безпеки в газопостачальній компанії «Нафтогаз України», здійснити огляд існуючих систем захисту, провести аналіз інцидентів інформаційної безпеки, оцінити відповідність сучасним стандартам системи інформаційної безпеки газопостачальної компанії «Нафтогаз України»

Ефективним виявилося використання методу прогнозування, що надало можливостей у визначенні тенденцій розвитку сучасних систем захисту інформації, механізмів стратегічного управління інформаційною безпекою підприємства, передбаченні майбутніх загроз інформаційній безпеці, а також накресленні проєктів новітніх здійснень, спрямованих на удосконалення систем інформаційної безпеки підприємства.

РОЗДІЛ ІІ.
АНАЛІЗ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ГАЗОПОСТАЧАЛЬНОЇ КОМПАНІЇ «НАФТОГАЗ УКРАЇНИ»

2.1. Інформаційна безпека підприємства: види, принципи, нормативно-правова база.

"Нафтогаз України", як стратегічно важлива компанія для енергетичної безпеки України, потребує особливої уваги до питання інформаційної безпеки. Зважаючи на критичну інфраструктуру, яку обслуговує компанія, будь-який збій в роботі інформаційних систем може призвести до серйозних наслідків, як для самої компанії, так і для країни в цілому.

Ключові аспекти аналізу. При аналізі системи інформаційної безпеки "Нафтогазу України" важливо враховувати кілька ключових аспектів. По-перше, необхідно здійснити ідентифікацію всіх інформаційних активів компанії, таких як дані, системи та мережі, оцінити їхню цінність і критичність для бізнесу, а також оцінити ризики, що виникають через втрату або компрометацію кожного з активів. По-друге, слід виявити потенційні загрози, як внутрішні, так і зовнішні (кібератаки, фізичні атаки, помилки персоналу), а також проаналізувати ймовірність і наслідки їх реалізації. Третім етапом є аналіз вразливостей, який включає ідентифікацію слабких місць у системі інформаційної безпеки, таких як програмні вразливості, недоліки конфігурації та людський фактор, а також оцінку критичності кожної з вразливостей. Далі необхідно оцінити засоби захисту, включаючи аналіз наявної системи захисту інформації (технічні засоби, політики, процедури) і оцінку ефективності цих засобів у боротьбі з існуючими загрозами. Важливим етапом є також дослідження минулих інцидентів інформаційної безпеки, визначення їхніх причин та розробка рекомендацій для їхнього усунення. І, нарешті, необхідно порівняти існуючу систему захисту з вимогами національного законодавства, міжнародних стандартів, таких як ISO 27001, та галузевих регуляторів.

Методи аналізу. Для проведення комплексного аналізу системи інформаційної безпеки "Нафтогазу України" можуть бути застосовані різні методи. Зокрема, внутрішній аудит передбачає перевірку системи безпеки силами власних фахівців, а зовнішній аудит включає залучення незалежних експертів для оцінки ситуації. Пенітестинг, або імітація кібератак, дозволяє виявити вразливості, а сканування вразливостей здійснюється через автоматизований аналіз системи на наявність відомих загроз. Окрім того, соціальна інженерія передбачає перевірку рівня обізнаності співробітників щодо загроз інформаційної безпеки.

Проте цей процес може бути ускладнений деякими проблемами та ризиками. Складність системи, яка включає велику кількість мереж, систем і користувачів, робить аналіз більш трудомістким. Крім того, постійно змінюється загрозливий ландшафт, і поява нових вразливостей вимагає регулярного оновлення системи захисту. Дефіцит кваліфікованих фахівців також може ускладнити проведення необхідних заходів аналізу та захисту.

З метою вирішення цих проблем рекомендується регулярний моніторинг стану системи інформаційної безпеки, підвищення обізнаності співробітників через тренінги, впровадження новітніх технологій захисту інформації (наприклад, SIEM, SOAR, EDR), а також співпраця з іншими компаніями для обміну досвідом. Важливо також регулярно створювати резервні копії критично важливих даних та розробити план відновлення після інцидентів, таких як кібератаки.

Таким чином, аналіз системи інформаційної безпеки "Нафтогазу України" є складним і багатогранним процесом, що потребує залучення висококваліфікованих фахівців і використання сучасних технологій. Результати аналізу дозволять виявити слабкі місця в системі захисту, розробити ефективні заходи для їх усунення та забезпечити надійний захист інформаційних активів компанії [50].

Інформаційна безпека є однією з найактуальніших проблем сучасного світу, оскільки цифровізація, що швидко набирає обертів, створює нові

загрози та виклики. Зі зростанням кількості підключених пристроїв і впровадженням хмарних технологій виникають безпрецедентні можливості для кіберзлочинців. Хакери застосовують різноманітні методи, від фішингу до складних атак на мережі, з метою здобуття доступу до конфіденційної інформації підприємств. Відповідно, важливість інформаційної безпеки стає очевидною.

Кібератаки можуть призвести до значних фінансових збитків, як через викрадення коштів, так і через вимагання викупу за вкрадені дані або через репутаційні втрати. Витік конфіденційної інформації здатен підірвати довіру клієнтів та партнерів, що в свою чергу негативно впливає на бізнес. Крім того, перебої в роботі, спричинені кібернападами, можуть паралізувати діяльність підприємства, завдаючи йому значних збитків.

Основні загрози для інформаційної безпеки включають фішинг, де зловмисники використовують електронні листи та інші канали для обману користувачів з метою отримання доступу до їхніх облікових даних, а також мережеві атаки, під час яких хакери проникають у мережі підприємств. Вразливості програмного забезпечення також створюють загрозу, адже зловмисники можуть використовувати їх для несанкціонованого доступу до систем. Не менш важливими є внутрішні загрози, пов'язані з діями невдоволених співробітників.

Інформаційна безпека включає комплекс заходів, що забезпечують захист даних від несанкціонованого доступу, зміни чи знищення. Вона охоплює технічні, організаційні та правові заходи. Основна мета інформаційної безпеки — забезпечити конфіденційність, цілісність та доступність інформації, а також захистити інформаційні активи підприємства і зменшити ризики, пов’язані з кіберзагрозами.

Ця проблема має національне значення, оскільки витік конфіденційної інформації може мати серйозні наслідки для економіки, політики та суспільства в цілому. Тому держави розробляють і впроваджують нормативно-правову базу, яка регулює сферу інформаційної безпеки, а також

проводять заходи з підвищення обізнаності громадян і підприємств про кіберзагрози та методи захисту від них.

Забезпечення інформаційної безпеки на підприємстві передбачає широкий спектр заходів, спрямованих на захист даних, систем і мереж від несанкціонованого доступу, використання, розкриття, зміни, пошкодження або знищення. Для ефективного захисту важливо розуміти різні аспекти інформаційної безпеки та впроваджувати комплексні стратегії захисту.

Інформаційна безпека є важливою складовою сучасного підприємства, що охоплює різноманітні аспекти захисту даних, систем і мереж від несанкціонованого доступу, використання, зміни або знищення. Існують різні види інформаційної безпеки, кожен з яких спрямований на конкретні аспекти захисту.

Одним з основних видів є фізична безпека, що передбачає захист приміщень, обладнання та носіїв інформації від несанкціонованого доступу. Для цього використовуються системи контролю доступу, охоронні системи та сейфи. Важливою складовою фізичної безпеки є запобігання стихійним лихам і аваріям, для чого застосовуються системи пожежогасіння і резервні джерела живлення. Також необхідно забезпечити захист від електромагнітних випромінювань та інших фізичних впливів [41].

Другим важливим видом є технічна безпека, яка включає захист програмного забезпечення та операційних систем від шкідливого програмного забезпечення за допомогою антивірусів і фаєрволів. Також важливим аспектом є захист мереж від несанкціонованого доступу через системи виявлення вторгнень та використання VPN. Захист баз даних, включаючи шифрування і резервне копіювання, є ключовим для забезпечення їх безпеки.

Криптографічна безпека використовує математичні методи для забезпечення конфіденційності, цілісності та автентичності інформації. Це досягається через шифрування даних та використання електронних підписів, що забезпечують захист даних на високому рівні.

Організаційна безпека зосереджена на розробці та впровадженні політик, процедур та інструкцій з інформаційної безпеки. Важливим аспектом є навчання персоналу правилам інформаційної безпеки, а також проведення регулярних аудитів для оцінки ефективності існуючих заходів.

Правова безпека передбачає дотримання законодавства в сфері інформаційної безпеки, а також укладання договорів про нерозголошення конфіденційної інформації, що сприяє захисту корпоративних даних.

Принципи інформаційної безпеки включають конфіденційність, що забезпечує захист інформації від розголошення, цілісність, яка охороняє інформацію від несанкціонованих змін, і доступність, що гарантує своєчасний і точний доступ до інформації для авторизованих користувачів.

Сучасні виклики в галузі інформаційної безпеки включають зростання кількості та складності кібератак, а також ризики, пов'язані з мобільними пристроями, хмарними обчисленнями та Інтернетом речей. Всі ці фактори створюють нові загрози для безпеки даних і вимагають постійного вдосконалення заходів захисту [44].

Для забезпечення інформаційної безпеки підприємства необхідно провести аудит існуючих систем безпеки, розробити політику інформаційної безпеки, впровадити необхідні технічні засоби захисту та навчити персонал правилам безпеки. Регулярне оновлення програмного забезпечення та моніторинг загроз є невід'ємними складовими ефективної системи захисту.

Таким чином, забезпечення інформаційної безпеки є комплексним процесом, що включає фізичні, технічні, організаційні та правові заходи. Розробка та впровадження ефективних систем захисту базуються на принципах конфіденційності, цілісності та доступності інформації, що забезпечують надійний захист інформаційних активів підприємства.

Основні принципи інформаційної безпеки є основою для забезпечення належного захисту інформаційних систем і даних підприємства. Кожен з цих принципів виконує важливу роль у створенні надійної та ефективної системи безпеки.

Першим принципом є конфіденційність, що передбачає захист інформації від несанкціонованого доступу, розкриття або поширення. Для забезпечення цього принципу застосовуються різноманітні засоби захисту, такі як шифрування даних, аутентифікація та авторизація користувачів. Тільки авторизовані особи повинні мати доступ до інформації, що забезпечує захист від витоків або несанкціонованого використання даних.

Другим важливим принципом є цілісність, який полягає у захисті інформації від несанкціонованих змін, пошкоджень або знищення. Для цього використовуються механізми контролю цілісності даних, такі як хешування і цифрові підписи, що дозволяють гарантувати, що інформація залишиться в тому вигляді, в якому вона була надана. Крім того, для забезпечення цілісності регулярно проводяться резервне копіювання та відновлення даних.

Принцип доступності визначає, що авторизовані користувачі повинні мати своєчасний і точний доступ до необхідної інформації. Це забезпечується через високий рівень доступності інформаційних систем та мереж, а також використання механізмів резервування та відмовостійкості. Завдяки цьому, навіть у разі технічних збоїв, користувачі можуть отримати доступ до даних, не порушуючи робочі процеси.

Принцип відповідальності вказує на те, що кожен співробітник несе відповідальність за збереження інформації, до якої має доступ. Для цього встановлюються чіткі правила і процедури, які регламентують роботу з інформацією, що сприяє забезпеченню її безпеки та захисту від несанкціонованого використання [55].

Принцип прозорості передбачає, що всі процеси та рішення в сфері інформаційної безпеки повинні бути зрозумілими і прозорими для всіх учасників. Співробітники повинні бути поінформовані про політику інформаційної безпеки та свої обов'язки щодо забезпечення захисту даних.

Останнім важливим принципом є постійне вдосконалення. Система інформаційної безпеки повинна постійно розвиватися і адаптуватися до

нових загроз. Для цього регулярно проводяться оцінки ефективності системи захисту, а також вносяться необхідні зміни для підвищення рівня безпеки.

Таким чином, принципи інформаційної безпеки формують основу для створення ефективної системи захисту даних, що забезпечує не тільки захист інформації, а й довіру з боку користувачів і партнерів підприємства.

Реалізація принципів інформаційної безпеки вимагає використання комплексного підходу, що включає технічні, організаційні та правові заходи для забезпечення захисту інформації та інформаційних систем підприємств.

Серед технічних заходів, що сприяють реалізації принципів інформаційної безпеки, важливими є системи виявлення вторгнень, фаєрволи, антивіруси та системи шифрування, які допомагають захистити дані від несанкціонованого доступу та впливів. Крім того, системи резервного копіювання і контролю доступу сприяють забезпеченню цілісності та доступності інформації, знижуючи ризики втрати даних та збоїв у роботі систем.

Організаційні заходи включають розробку політик інформаційної безпеки, навчання персоналу, проведення регулярних аудитів безпеки та створення планів реагування на інциденти. Ці заходи сприяють не лише захисту даних, але й забезпечують відповідальність і обізнаність співробітників, що знижує ризик виникнення інцидентів через людський фактор [61].

Правові заходи, у свою чергу, охоплюють дотримання законодавства у сфері захисту інформації та укладання договорів про нерозголошення конфіденційної інформації. Це дозволяє гарантувати юридичний захист інформаційних активів та мінімізувати правові наслідки порушень безпеки.

Дотримання принципів інформаційної безпеки є важливим для підприємств з кількох причин. По-перше, захист репутації компанії є критичним, оскільки витік конфіденційної інформації може завдати серйозної шкоди її іміджу. По-друге, інформаційна безпека дозволяє зменшити фінансові втрати, пов'язані з кібератаками, такими як викрадення

даних, вимагання викупу або накладення штрафів. Надійна система безпеки також забезпечує стійкість бізнесу, гарантуючи безперебійну роботу підприємства. Крім того, захист персональних даних клієнтів сприяє побудові довгострокових і взаємовигідних відносин з партнерами та клієнтами.

Важливою складовою забезпечення інформаційної безпеки є нормативно-правова база, яка складається з законів, підзаконних актів, стандартів і інших нормативних документів, що регулюють відносини у сфері захисту інформації. Вона допомагає забезпечити дотримання прав і законних інтересів суб'єктів інформаційних відносин, а також захист національних інтересів у цій сфері.

Нормативно-правова база є важливою з кількох причин. Вона створює єдині правила для всіх учасників ринку, що дозволяє уникнути хаосу і забезпечити рівні умови для бізнесу. Крім того, вона захищає права громадян на приватність і недоторканність особистого життя, а також сприяє створенню сприятливого бізнес-клімату. Нарешті, відповідність нормативно-правової бази міжнародним стандартам дозволяє забезпечити інтеграцію в глобальне інформаційне середовище.

В Україні є низка законів, які регулюють питання інформаційної безпеки, зокрема: Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який визначає основні правові засади захисту інформації в країні, а також Закон України "Про персональні дані", що регулює обробку персональних даних. Крім того, важливими є Закон України "Про електронний цифровий підпис", Цивільний кодекс, що охоплює питання авторських прав та інтелектуальної власності, а також Кримінальний кодекс, який передбачає відповідальність за порушення в сфері комп'ютерної інформації.

Нормативно-правові акти, що регулюють питання інформаційної безпеки, охоплюють кілька ключових напрямів. Зокрема, вони визначають основні терміни та поняття, права й обов'язки суб'єктів інформаційних

відносин, встановлюють порядок обробки персональних даних, забезпечують захист інформації від несанкціонованого доступу, визначають відповідальність за порушення законодавства в цій сфері, а також сприяють міжнародному співробітництву у сфері інформаційної безпеки.

Однак розвиток інформаційних технологій створює нові виклики для нормативно-правового регулювання. Серед основних проблем виділяють постійні зміни технологій, що ускладнюють оперативне оновлення законодавства; транснаціональний характер кіберзагроз, який потребує посилення міжнародної співпраці; а також складнощі у визначенні відповідальності за кібератаки, адже встановити винуватців таких інцидентів часто непросто.

Дотримання нормативно-правової бази інформаційної безпеки є обов'язковим для всіх суб'єктів господарювання. Це дозволяє значно знизити ризики кібератак, захистити репутацію компанії, уникнути фінансових втрат, а також забезпечити довіру клієнтів і партнерів. Таким чином, регуляція в галузі інформаційної безпеки не лише сприяє стабільності в інформаційному просторі, але й є важливим інструментом забезпечення надійності сучасних цифрових систем [80].

Інформаційна безпека підприємства є однією з ключових складових забезпечення ефективного функціонування організації, особливо в умовах цифровізації бізнес-процесів. Забезпечення інформаційної безпеки включає комплекс заходів, спрямованих на захист інформації, що обробляється, зберігається або передається, від несанкціонованого доступу, модифікації, втрати чи знищення. У сучасному бізнес-середовищі інформація розглядається як стратегічний ресурс, тому її захист є одним із пріоритетних завдань керівництва.

Основними видами інформаційної безпеки підприємства є організаційна, технічна, правова та фізична безпека. Організаційна безпека охоплює розробку внутрішніх політик і процедур, які визначають порядок роботи з інформацією, права доступу до неї, а також механізми моніторингу

та контролю. Технічна безпека включає використання засобів криптографії, брандмауерів, антивірусного програмного забезпечення та інших технологій для захисту інформаційних систем. Правова безпека базується на дотриманні чинного законодавства у сфері захисту інформації, включаючи законодавчі акти, які регулюють обробку персональних даних, конфіденційну інформацію та комерційну таємницю. Фізична безпека забезпечує захист апаратного забезпечення, серверів та інших об’єктів, де зберігається чи обробляється інформація.

Принципи інформаційної безпеки підприємства включають конфіденційність, цілісність, доступність, автентичність та невідмовність. Конфіденційність забезпечує доступ до інформації лише уповноваженим особам. Цілісність гарантує, що інформація залишається незмінною та захищеною від несанкціонованого втручання. Доступність забезпечує своєчасний доступ до інформації, коли це необхідно, а автентичність підтверджує, що інформація надходить від достовірного джерела. Принцип невідмовності забезпечує, що сторони, які беруть участь в обробці інформації, не можуть відмовитися від своїх дій.

Нормативно-правова база, яка регулює питання інформаційної безпеки в Україні, включає Конституцію України, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про доступ до публічної інформації», Закон України «Про захист персональних даних», а також низку підзаконних актів. Крім того, важливу роль відіграють міжнародні стандарти, зокрема ISO/IEC 27001, які встановлюють вимоги до системи управління інформаційною безпекою.

Практичні аспекти інформаційної безпеки на прикладі діяльності газопостачальної компанії «Нафтогаз України» демонструють важливість інтеграції різних видів захисту в єдину систему. Одним із ключових завдань компанії є захист інформації про клієнтів, фінансові операції, а також критичну інфраструктуру, пов’язану із газопостачанням. Для цього

розробляються та впроваджуються інформаційні системи, що відповідають вимогам безпеки, здійснюється регулярний моніторинг та аудит.

Одним із прикладів успішної реалізації інформаційної безпеки у компанії є впровадження багаторівневої системи аутентифікації для доступу до внутрішніх систем. Працівники використовують персональні ідентифікатори, які генеруються з урахуванням сучасних криптографічних алгоритмів. Для зниження ризиків витоку інформації впроваджено політику мінімального доступу, яка обмежує права працівників лише тими функціями, які необхідні для виконання їхніх обов'язків.

Крім того, компанія «Нафтогаз України» активно працює над забезпеченням захисту критичної інфраструктури. Для цього проводиться оцінка ризиків, впроваджуються автоматизовані системи моніторингу, які дозволяють виявляти та оперативно реагувати на загрози. Особливу увагу приділяють захисту від кібератак, які можуть мати катастрофічні наслідки для функціонування газопостачальної системи [79].

Ще одним важливим напрямком є навчання персоналу принципам інформаційної безпеки. Для цього компанія організовує тренінги, створює інформаційні бюлетені, що висвітлюють останні загрози та методи їх уникнення. Завдяки таким заходам працівники розуміють важливість дотримання правил безпеки, що мінімізує ризик людського фактора.

На практиці було впроваджено систему захисту від внутрішніх загроз, яка включає інструменти моніторингу активності користувачів, аналізу аномалій у поведінці та автоматичного блокування підозрілих дій. Наприклад, якщо співробітник намагається отримати доступ до конфіденційних даних, які не пов'язані з його посадовими обов'язками, система автоматично генерує сповіщення для служби безпеки.

Компанія також активно співпрацює з державними органами, зокрема Державною службою спеціального зв'язку та захисту інформації України, для обміну досвідом та впровадження новітніх рішень. Наприклад, у рамках міжнародного співробітництва було запроваджено додаткові механізми

захисту від фішингових атак та інших кібератак, що спрямовані на крадіжку конфіденційної інформації.

Висновуючи, інформаційна безпека є стратегічно важливим аспектом діяльності будь-якого підприємства, а для компаній, що працюють у сфері критичної інфраструктури, таких як «Нафтогаз України», цей аспект набуває особливого значення. Інтеграція технічних, організаційних та правових заходів дозволяє забезпечити високий рівень захисту інформації та гарантувати безперебійність бізнес-процесів [70].

2.2. Огляд існуючих систем захисту

Системи захисту являють собою комплекс заходів, технологій і процедур, спрямованих на забезпечення безпеки об'єктів, інформації та людей. З розвитком технологій і зростанням кіберзагроз вимоги до цих систем постійно змінюються і зростають. Системи захисту можна класифікувати за різними критеріями. За призначенням вони поділяються на фізичний захист, що включає охорону, відеоспостереження та контроль доступу; системи кібербезпеки, які охоплюють антивіруси, фаєрволи та системи виявлення й запобігання вторгнень (IDS/IPS); системи захисту інформації, зокрема шифрування і управління доступом; а також системи безпеки промислових підприємств, такі як SCADA та IoT. За принципом дії системи захисту можна розподілити на пасивні (фізичні бар'єри, моніторинг) та активні (сигналізація, блокування, нейтралізація загроз). За рівнем захисту виділяються первинні (фізичні бар'єри, охорона), вторинні (сигналізація, відеоспостереження) та третинні (реагування на інциденти).

Основними компонентами систем захисту є сенсори, які виявляють загрози (наприклад, рух, зміна температури, проникнення); пристрої управління, які збирають дані від сенсорів, приймають рішення та керують виконавчими пристроями; виконавчі пристрої, що виконують дії для нейтралізації загроз, такі як сирени, замки або системи пожежогасіння; а

також програмне забезпечення, яке керує всіма компонентами системи, аналізує дані та генерує звіти.

Сучасні тенденції в галузі систем захисту включають інтеграцію різних систем в єдиний комплекс для ефективнішого управління безпекою, використання штучного інтелекту для аналізу даних, виявлення аномалій і прийняття рішень, а також розвиток Інтернету речей, що потребує захисту великої кількості підключених пристроїв. Додатково, технології блокчейн забезпечують безпеку даних і транзакцій, а квантові обчислення відкривають нові можливості та виклики для систем безпеки [75].

Вибір системи захисту є складним процесом, що залежить від ряду факторів, серед яких ключовими є призначення об'єкта, рівень загроз, бюджет та вимоги до безпеки. Призначення об'єкта визначає специфічні потреби в захисті, які можуть варіюватися від охорони приватних будинків або офісів до безпеки промислових підприємств. Рівень загроз, таких як злочинність, кіберзагрози або природні катастрофи, також впливає на тип і складність необхідної системи захисту. Бюджет є обмеженням, яке визначає вибір між різними типами обладнання, їх встановленням та подальшим обслуговуванням. Вимоги до безпеки, що включають конфіденційність, цілісність та доступність інформації, вимагають застосування різних підходів до захисту в залежності від специфіки об'єкта.

Системи захисту можна класифікувати за кількома критеріями. За призначенням розрізняють системи фізичного захисту (охорона, відеоспостереження, контроль доступу, пожежна сигналізація), системи кібербезпеки (антивіруси, фаєрволи, системи виявлення та запобігання вторгнень (IDS/IPS), захист даних та хмарних сервісів), системи захисту інформації (шифрування, управління доступом, захист програмного забезпечення) та системи безпеки промислових підприємств (SCADA, IoT, захист від фізичних загроз). За принципом дії системи можуть бути пасивними (фізичні бар'єри, моніторинг) або активними (сигналізація, блокування, нейтралізація загроз). За рівнем захисту розрізняють первинні

системи (фізичні бар'єри, охорона), вторинні (сигналізація, відеоспостереження) та третинні (реагування на інциденти).

Основними компонентами систем захисту є сенсори, які фіксують загрози, такі як рух, зміни температури або несанкціоноване проникнення. Пристрої управління отримують дані від сенсорів, аналізують їх і приймають рішення щодо необхідних дій, тоді як виконавчі пристрої виконують дії для нейтралізації загрози, наприклад, включають сирени, блокують доступ або активують системи пожежогасіння. Програмне забезпечення керує всіма компонентами системи, аналізує зібрані дані та генерує звіти для подальшого моніторингу і удосконалення захисних механізмів.

Принцип роботи систем захисту полягає в кількох етапах: перший етап – виявлення загрози, коли сенсори фіксують зміни в оточенні, що можуть свідчити про потенційну небезпеку. На другому етапі пристрій управління обробляє отриману інформацію, аналізує її та приймає рішення про необхідність реагування. Третій етап полягає в реалізації реакції на загрозу: виконавчі пристрої здійснюють відповідні дії для її нейтралізації, такі як активація сирен, блокування доступу або виклик охорони. Завершальний етап включає постійний моніторинг та аналіз ситуації з метою виявлення нових загроз і вдосконалення алгоритмів захисту системи.

Сучасні системи захисту продовжують еволюціонувати під впливом новітніх технологій, що сприяє їх інтеграції та розширенню можливостей у різних сферах. Однією з основних тенденцій є інтеграція систем, що передбачає об'єднання різних типів безпекових механізмів в єдиний комплекс для більш ефективного управління та оптимізації процесів охорони. Така інтеграція дозволяє забезпечити кращу взаємодію між різними системами, що значно підвищує їхню ефективність. Ще однією важливою тенденцією є впровадження штучного інтелекту (AI), який застосовується для аналізу великих обсягів даних, виявлення аномалій, прогнозування загроз та автоматичного прийняття рішень, що значно покращує швидкість та точність реагування на потенційні загрози. Крім того, із зростанням числа

підключених пристроїв у рамках Інтернету речей (IoT) з'являється необхідність у захисті цих пристроїв від кіберзагроз, що вимагає розвитку спеціалізованих систем безпеки. Водночас, використання блокчейн-технологій для забезпечення безпеки даних та транзакцій відкриває нові можливості для захисту інформації завдяки своїй дистрибутивній та незмінній природі. Нарешті, квантові обчислення обіцяють створення нових можливостей для захисту інформації, але одночасно несуть у собі і нові загрози для існуючих систем безпеки, що вимагає подальших досліджень та адаптаційних стратегій.

Вибір оптимальної системи захисту залежить від множини факторів, серед яких основними є призначення об'єкта, рівень загроз, бюджетні обмеження та вимоги до безпеки. Призначення об'єкта, будь то житловий будинок, офіс або промислове підприємство, визначає специфічні потреби та масштаби захисту, в той час як рівень загроз, таких як злочинність, кіберзагрози чи природні катастрофи, диктує необхідність у застосуванні різних типів систем і технологій. Бюджет є важливим фактором, що обмежує вибір між різними типами обладнання, його встановленням та подальшим обслуговуванням, а також визначає доцільність впровадження новітніх технологій. Вимоги до безпеки, зокрема до конфіденційності, цілісності та доступності даних, зумовлюють необхідність у багатошарових механізмах захисту, що враховують всі можливі аспекти безпеки.

Таким чином, системи захисту займають ключове місце у забезпеченні безпеки людей, майна та інформації в умовах постійно змінюваного середовища загроз. Вибір та впровадження відповідних систем вимагає комплексного підходу та врахування всіх потенційних ризиків. У майбутньому існують численні напрямки для подальших досліджень, зокрема в таких областях, як захист інформації в банківській сфері, забезпечення безпеки критичної інфраструктури, розробка систем безпеки для малого бізнесу, порівняння різних систем відеоспостереження та захист

від кібератак на промислові підприємства. Подальші дослідження в цих галузях можуть призвести до значних удосконалень у сфері безпеки [73].

Огляд існуючих систем захисту інформації є важливою складовою для розуміння ефективності сучасних підходів до забезпечення інформаційної безпеки. Інформаційний простір підприємств, особливо тих, які працюють у сфері критичної інфраструктури, як-от газопостачальні компанії, вимагає впровадження комплексних рішень для захисту даних та мінімізації ризиків. Системи захисту інформації забезпечують конфіденційність, цілісність і доступність даних, що дозволяє підприємствам ефективно функціонувати в умовах постійних кіберзагроз.

На сучасному етапі розвитку технологій системи захисту інформації поділяються на кілька категорій, кожна з яких виконує специфічні функції. До основних видів систем належать антивірусні програми, системи міжмережевого екранування (брандмауери), засоби шифрування даних, системи виявлення та запобігання вторгненням (IDS/IPS), а також системи моніторингу та аудиту інформаційної безпеки. Кожна з цих систем має свою специфіку, але їхнє інтегроване використання дозволяє створити надійний багаторівневий захист.

Антивірусне програмне забезпечення є однією з найбільш поширених форм захисту, яке використовується для виявлення, блокування та видалення шкідливого коду. Сучасні антивірусні системи використовують методи машинного навчання для аналізу поведінкових моделей програмного забезпечення, що дозволяє їм виявляти нові загрози, які ще не внесені до бази вірусних сигнатур. Важливим аспектом є регулярне оновлення антивірусних баз, що гарантує своєчасний захист від нових загроз.

Системи міжмережевого екранування, або брандмауери, забезпечують контроль доступу до мережі підприємства. Вони дозволяють блокувати несанкціоновані підключення, обмежувати доступ до певних ресурсів та забезпечувати сегментацію мережі для зниження ризику поширення атак. Аппаратні брандмауери використовуються на рівні мережевої

інфраструктури, тоді як програмні рішення встановлюються на робочі станції та сервери.

Шифрування даних є ще одним важливим елементом захисту інформації. Завдяки використанню сучасних криптографічних алгоритмів, таких як AES (Advanced Encryption Standard) або RSA, дані стають недоступними для несанкціонованого доступу навіть у разі їх перехоплення. Особливого значення шифрування набуває під час передавання конфіденційної інформації через відкриті канали зв’язку.

Системи виявлення та запобігання вторгненням (IDS/IPS) виконують функції моніторингу трафіку в реальному часі, аналізуючи підозрілі дії та запобігаючи можливим загрозам. IDS (Intrusion Detection System) фокусується на виявленні атак, тоді як IPS (Intrusion Prevention System) додає до цього функцію автоматичного блокування. Поєднання цих систем дозволяє своєчасно реагувати на спроби вторгнення та запобігати їх розвитку.

Системи моніторингу та аудиту інформаційної безпеки, як-от SIEM (Security Information and Event Management), забезпечують збір, аналіз та кореляцію даних про події безпеки. Такі системи дозволяють створювати цілісну картину стану інформаційної безпеки підприємства, виявляти аномалії в мережевій активності та забезпечувати виконання нормативних вимог.

Практичні аспекти впровадження існуючих систем захисту можна розглянути на прикладі діяльності газопостачальної компанії «Нафтогаз України». Для захисту внутрішніх інформаційних систем компанія використовує багаторівневу систему захисту, яка включає всі описані вище категорії рішень. Особливу увагу приділяють захисту даних клієнтів, інформації про фінансові операції та операційні процеси.

Один із ключових елементів захисту в компанії - впровадження SIEM-системи для моніторингу подій інформаційної безпеки. Це дозволяє виявляти потенційні загрози, аналізувати їх джерела та своєчасно приймати заходи для

мінімізації ризиків. Наприклад, у випадку спроби несанкціонованого доступу до корпоративної мережі система автоматично генерує попередження для служби безпеки.

Ще одним практичним рішенням є впровадження засобів шифрування для захисту передавання даних між філіями компанії. Усі конфіденційні дані, які передаються через відкриті мережі, шифруються за допомогою алгоритму AES-256, що забезпечує їхній захист навіть у разі перехоплення.

Компанія також активно використовує IDS/IPS-системи для моніторингу мережевого трафіку та виявлення підозрілої активності. Це дозволяє своєчасно виявляти DDoS-атаки та запобігати їх впливу на критичні системи. Наприклад, під час проведення тестування системи було виявлено спробу масового сканування портів мережі. Завдяки оперативному втручанню служби безпеки вдалося запобігти проникненню до внутрішніх систем.

Захист фізичних серверів та іншого обладнання є ще одним важливим аспектом. У «Нафтогаз України» серверні приміщення обладнані сучасними системами контролю доступу, відеоспостереженням та пожежною сигналізацією. Це забезпечує захист не лише від кібератак, але й від фізичних загроз, таких як пожежі або несанкціонований доступ.

Таким чином, огляд існуючих систем захисту та їх практичне застосування на прикладі газопостачальної компанії «Нафтогаз України» демонструє необхідність інтеграції різних підходів до інформаційної безпеки. Впровадження сучасних технологій, розробка політик безпеки та постійний моніторинг дозволяють підприємствам ефективно протидіяти сучасним загрозам [67].

2.3. Оцінка відповідності сучасним стандартам системи інформаційної безпеки «Нафтогазу України».

Забезпечення інформаційної безпеки є критично важливим завданням для ТОВ ГК «Нафтогаз України», враховуючи її роль як стратегічного

підприємства для енергетичної безпеки держави. Надійний захист інформаційних систем компанії є ключовим аспектом, що впливає на національну безпеку, фінансову стабільність та репутацію підприємства. Зокрема, кібератаки можуть мати серйозні наслідки, включаючи перебої в енергопостачанні, фінансові втрати, пошкодження репутації та підрив довіри інвесторів [64].

Для оцінки відповідності системи інформаційної безпеки «Нафтогазу України» сучасним стандартам необхідно враховувати міжнародні (ISO 27001, NIST Cybersecurity Framework, GDPR), національні (закон України «Про захист інформації в інформаційно-телекомунікаційних системах») та галузеві стандарти, розроблені спеціально для енергетичного сектора. Аналіз інформаційної безпеки компанії охоплює такі ключові аспекти: наявність чітко визначеної політики безпеки, ефективність організаційних і технічних заходів, процеси управління інцидентами, регулярний моніторинг системи та проведення незалежних аудитів.

Особливої уваги потребує розмір і складність IT-інфраструктури «Нафтогазу». Сучасні енергетичні системи компанії, які є високо автоматизованими, залежними від технологій і географічно розподіленими, ускладнюють забезпечення належного рівня безпеки. Це створює значні ризики через постійні зміни технологій, загрози кібератак, а також людський фактор, що може стати причиною порушення захисту.

Аспекти інформаційної безпеки:

Критична інфраструктура. Інформаційні системи «Нафтогазу» відіграють вирішальну роль у забезпеченні стабільного функціонування газотранспортної системи країни. Будь-яка атака або збій в IT-інфраструктурі може призвести до перебоїв у постачанні енергоносіїв із серйозними соціально-економічними наслідками.

Великий обсяг даних. Компанія обробляє значну кількість персональних, комерційних та операційних даних, які є привабливими

цілями для кіберзлочинців. Забезпечення захисту цих даних є важливим не лише для уникнення втрат, але й для дотримання законодавчих норм.

Розподілена IT-інфраструктура. Використання різноманітного програмного забезпечення та обладнання ускладнює централізоване управління безпекою, що підвищує ризики для інформаційних систем.

Загрози кібербезпеки. Серед основних загроз можна виділити хакерські атаки, шкідливе програмне забезпечення, соціальну інженерію та внутрішні ризики, пов’язані з людським фактором.

Рекомендації для підвищення рівня інформаційної безпеки:

Проведення незалежного аудиту. Це дозволить оцінити відповідність інформаційної системи сучасним стандартам безпеки.

Впровадження новітніх технологій. Використання штучного інтелекту, машинного навчання та інших передових засобів для виявлення і запобігання загрозам.

Регулярні тренінги співробітників. Це сприятиме підвищенню обізнаності про основи кібербезпеки та зменшить ризики, пов’язані з людським фактором.

Створення планів реагування на інциденти. Це забезпечить швидку та ефективну нейтралізацію загроз.

Посилення моніторингу системи. Постійний аналіз вразливостей і загроз допоможе знизити ризики атак.

Співпраця з державними органами та іншими компаніями. Обмін інформацією про кіберзагрози сприятиме формуванню ефективної системи протидії атакам.

Забезпечення інформаційної безпеки ТОВ ГК «Нафтогаз України» є складним, але надзвичайно важливим завданням, яке вимагає інтегрованого підходу та постійного вдосконалення систем захисту для забезпечення стабільності енергетичного сектору та національної безпеки України.

Оцінка відповідності системи інформаційної безпеки газопостачальної компанії «Нафтогаз України» сучасним стандартам є важливим етапом

забезпечення ефективного захисту даних та підтримки сталого функціонування критичної інфраструктури. У зв'язку зі зростанням кількості кібератак, що спрямовані на підприємства енергетичного сектору, компанія зобов'язана дотримуватись міжнародних стандартів інформаційної безпеки, таких як ISO/IEC 27001, NIST Cybersecurity Framework та інших галузевих регламентів.

ISO/IEC 27001 визначає основні вимоги до системи управління інформаційною безпекою (СУІБ). Вона базується на ризик-орієнтованому підході, який передбачає ідентифікацію активів, оцінку загроз та визначення заходів для їх нейтралізації. «Нафтогаз України» інтегрує принципи ISO/IEC 27001, впроваджуючи політики доступу до інформації, моніторинг активності, а також забезпечуючи навчання персоналу. Практична реалізація включає створення чіткої структури відповідальності за інформаційну безпеку, що дозволяє контролювати всі етапи обробки даних.

NIST Cybersecurity Framework надає рекомендації щодо виявлення, захисту, реагування, відновлення та моніторингу інформаційної безпеки. На практиці компанія використовує цей стандарт для оцінки поточного стану захисту та виявлення слабких місць у системі. Одним із ключових компонентів є застосування сучасних технологій для автоматизації процесів безпеки. Наприклад, компанія впровадила систему SIEM, яка дозволяє збирати та аналізувати дані про події безпеки в реальному часі, що відповідає стандартам NIST у контексті моніторингу та виявлення.

Важливим аспектом є дотримання стандартів захисту критичної інфраструктури, визначених у міжнародних актах, таких як ENISA Guidelines for Securing Critical Information Infrastructures. У компанії реалізовано заходи з оцінки вразливостей ключових систем, включаючи розробку планів реагування на інциденти. Наприклад, проведено аудит серверних приміщень і оновлено апаратне забезпечення для забезпечення відповідності сучасним вимогам [44].

Практична частина оцінки відповідності системи інформаційної безпеки компанії стандартам включає проведення регулярних тестів на проникнення (penetration testing). У 2024 році було організовано серію симуляційних кібератак на корпоративну мережу «Нафтогаз України». За результатами тестувань було виявлено низку вразливостей, зокрема недостатній рівень сегментації мережі, що дозволяло зловмисникам отримати доступ до декількох систем через один вхідний вузол. Для усунення цієї проблеми компанія впровадила політику мікросегментації, що відповідає стандартам ISO/IEC 27001 та рекомендаціям ENISA.

Особливу увагу приділено захисту даних клієнтів, відповідно до вимог GDPR (General Data Protection Regulation). Проведено оновлення політики конфіденційності, а також оптимізовано процеси зберігання та обробки персональних даних. У 2023 році компанія успішно пройшла сертифікаційний аудит щодо відповідності вимогам GDPR, що підтвердило високий рівень захисту персональних даних споживачів.

Значна увага приділяється резервуванню та відновленню даних у разі інцидентів. Компанія використовує багаторівневі резервні копії, які зберігаються у захищених дата-центрах. Це відповідає стандартам ISO/IEC 27031, що регламентує планування безперервності бізнесу. Наприклад, у 2022 році в результаті масштабного відключення електроенергії резервні системи компанії забезпечили відновлення доступу до критичних даних протягом 30 хвилин.

Для підвищення рівня безпеки використовуються новітні технології шифрування. Відповідно до рекомендацій NIST, «Нафтогаз України» впровадила алгоритми шифрування AES-256 для захисту конфіденційної інформації, що передається через відкриті мережі. Це забезпечує високий рівень захисту навіть у разі перехоплення даних.

Оцінка відповідності стандартам також включає підвищення обізнаності персоналу. У 2024 році було організовано серію тренінгів з інформаційної безпеки, що охопили понад 80% співробітників компанії.

Тематичні модулі включали навчання виявленню фішингових листів, безпечній роботі з корпоративними даними та правилам використання захищених каналів зв’язку. Такі заходи дозволяють мінімізувати ризик людського фактора, що є однією з найпоширеніших причин інцидентів у сфері безпеки.

Аналіз відповідності стандартам виявив також необхідність подальшого вдосконалення. Зокрема, було рекомендовано інтегрувати систему кіберзахисту з рішеннями на основі штучного інтелекту, що дозволить прогнозувати загрози та автоматично реагувати на них. Крім того, важливим напрямком є вдосконалення захисту від DDoS-атак шляхом впровадження розподілених систем фільтрації трафіку.

Загалом, оцінка відповідності сучасним стандартам показала, що система інформаційної безпеки компанії «Нафтогаз України» перебуває на високому рівні. Водночас результати аудитів та практичних тестувань виявили необхідність постійного вдосконалення для збереження конкурентоспроможності та забезпечення надійного захисту критичних даних в умовах зростання кіберзагроз [58].

2.4. Аналіз інцидентів інформаційної безпеки

Критична інфраструктура, яка складається з систем і об'єктів, що забезпечують життєво важливі функції суспільства, є основою стабільного функціонування держав. Енергетичні компанії, зокрема такі як «Нафтогаз України», виступають яскравим прикладом критичної інфраструктури, що є ключовою для забезпечення енергетичної безпеки. У зв'язку з їхньою стратегічною значущістю, ці об'єкти є постійною мішенню для широкого спектра загроз, які можна класифікувати за кількома категоріями.

Класифікація загроз для критичної інфраструктури

До основних кіберзагроз належать хакерські атаки, що передбачають несанкціонований доступ до інформаційних систем з метою викрадення

даних, вимагання викупу або порушення роботи. Віруси та шкідливе програмне забезпечення можуть пошкоджувати дані або блокувати функціонування систем, тоді як фішингові атаки спрямовані на обман співробітників задля отримання конфіденційної інформації. DDoS-атаки перевантажують мережі, роблячи сервіси недоступними.

Фізичні загрози включають саботаж, який передбачає навмисне пошкодження обладнання, стихійні лиха (пожежі, повені, землетруси), а також техногенні аварії, такі як вибухи чи транспортні інциденти. Соціальні загрози, як-от протести, громадянські заворушення чи терористичні акти, також можуть мати серйозні наслідки для енергетичної інфраструктури.

Специфіка загроз для енергетичних компаній

Енергетичні компанії стикаються з особливими загрозами, такими як енергетичний тероризм, спрямований на дестабілізацію енергетичної системи, індустріальний шпіонаж, що передбачає викрадення конфіденційної інформації, а також геополітичні ризики, включаючи санкції та політичну нестабільність. Вразливість цих компаній зумовлена їхньою важливою роллю у забезпеченні життєдіяльності суспільства [78].

Наслідки атак на критичну інфраструктуру

Атаки на критичну інфраструктуру мають серйозні економічні, соціальні, політичні та екологічні наслідки. Економічні збитки включають зменшення обсягів виробництва, втрату доходів та підвищення цін на енергоносії. Соціальні наслідки пов'язані з перебоями у постачанні електроенергії, газу та тепла, що може спричинити соціальні протести. Політичні наслідки виражаються у підриві довіри до влади та дестабілізації країни, а екологічні — у можливому забрудненні довкілля внаслідок аварій.

Заходи захисту критичної інфраструктури

Для мінімізації ризиків компаніям необхідно впроваджувати комплекс заходів, зокрема підвищувати обізнаність співробітників шляхом регулярних тренінгів, використовувати системи виявлення вторгнень, захищати мережі від DDoS-атак, застосовувати шифрування даних і забезпечувати резервне

копіювання. Не менш важливим є фізичний захист об'єктів компанії та співпраця з правоохоронними органами для розслідування інцидентів.

Міжнародне співробітництво в галузі кібербезпеки

Ефективний захист критичної інфраструктури потребує міжнародного співробітництва, оскільки кіберзагрози не мають кордонів, а взаємозалежність енергетичних, фінансових та транспортних систем різних країн може спричинити каскадні наслідки. Обмін досвідом, технологіями, розвідданими та спільні тренінги сприяють підвищенню ефективності протидії загрозам. Значну роль у цьому відіграють міжнародні організації, такі як ENISA, CERT та Міжнародний електротехнічний комітет, які розробляють стандарти, рекомендації та проводять дослідження.

Загалом, систематичний підхід до оцінки загроз, впровадження сучасних технологій захисту та міжнародна співпраця є ключовими для забезпечення безпеки критичної інфраструктури.

Попри значні успіхи в розвитку міжнародного співробітництва у сфері кібербезпеки, існує низка викликів, які перешкоджають досягненню максимального ефекту від об'єднаних зусиль. Одним із ключових викликів є нерівномірний рівень розвитку кібербезпеки у різних країнах, що ускладнює координацію спільних дій. Крім того, конфлікт інтересів між державами, який часто проявляється у вигляді конкуренції, обмежує обмін критичною інформацією та технологіями. Ще одним суттєвим бар’єром є постійна еволюція кіберзагроз, яка вимагає безперервного вдосконалення методів і технологій захисту.

Однак, перспективи в галузі міжнародного співробітництва у кібербезпеці залишаються обнадійливими. Очікується подальше розширення співпраці між країнами, що сприятиме більш ефективному реагуванню на сучасні загрози. У цьому контексті значну роль відіграє розвиток новітніх технологій, таких як штучний інтелект і блокчейн, які можуть суттєво підвищити рівень кібербезпеки. Крім того, створення міжнародних центрів

кібербезпеки забезпечить дослідження та розробку інноваційних рішень, спрямованих на покращення захисту критичної інфраструктури.

Таким чином, міжнародне співробітництво виступає ключовим фактором у забезпеченні кібербезпеки критичної інфраструктури. Завдяки об'єднанню зусиль різних країн стає можливим більш ефективне протистояння кіберзагрозам, підвищення рівня захищеності важливих об'єктів та стабільне функціонування суспільства.

Аналіз інцидентів інформаційної безпеки є важливим складником цієї діяльності, адже він забезпечує систематичне вивчення кібератак, збоїв і подій, що впливають на конфіденційність, цілісність або доступність інформації. Завдяки такому аналізу можна не лише виявити причини інциденту, але й розробити ефективні заходи для запобігання подібним ситуаціям у майбутньому [76].

Аналіз інцидентів інформаційної безпеки є ключовим елементом для забезпечення захисту даних і систем організації, оскільки він дозволяє визначити слабкі місця в системі безпеки, мінімізувати наслідки кібератак, дотримуватись нормативних вимог та покращити процеси прийняття рішень щодо інформаційної безпеки. Завдяки аналізу організації можуть не лише реагувати на інциденти, а й запобігати їх повторенню у майбутньому.

Основні етапи аналізу інцидентів включають декілька ключових кроків. На першому етапі здійснюється виявлення інциденту, яке може базуватися на моніторингу систем, аналізі логів, звітів або повідомленнях від співробітників та тривогах систем безпеки. Наступним кроком є формування команди реагування, яка складається з фахівців різних напрямків, з чітким розподілом ролей і відповідальності. Після цього відбувається стримування інциденту, що передбачає ізоляцію заражених систем, блокування шляхів поширення та збереження доказів. Етап аналізу інциденту включає збір інформації, визначення причин інциденту, ідентифікацію вразливостей та оцінку наслідків. Розробка плану відновлення передбачає відновлення пошкоджених даних та повернення систем до робочого стану. Завершальним

кроком є впровадження заходів, спрямованих на запобігання повторення інцидентів, що включає усунення вразливостей, оновлення політик і процедур, а також навчання співробітників.

Методи аналізу інцидентів можуть бути ручними, автоматизованими або комбінованими. Ручний аналіз передбачає детальне дослідження логів, звітів, а також інтерв’ю із співробітниками та експертну оцінку. Автоматизований аналіз використовує спеціалізовані інструменти, такі як SIEM-системи, SOAR-платформи та алгоритми машинного навчання. Комбінований підхід дозволяє досягти високої точності та ефективності, об'єднуючи переваги ручного та автоматизованого аналізу.

Для забезпечення ефективного реагування на інциденти необхідно створити систему, яка включає розробку плану реагування, формування команди фахівців, впровадження засобів захисту, регулярне тестування та постійне вдосконалення. План реагування має чітко визначати ролі, процедури та контакти для екстреного зв’язку. Створення команди реагування передбачає підбір кваліфікованих спеціалістів і проведення тренінгів. Впровадження засобів захисту, таких як системи виявлення вторгнень, фаєрволи та рішення для захисту кінцевих точок, дозволяє значно підвищити рівень безпеки. Регулярне тестування системи за допомогою penetration testing і моделювання сценаріїв атак дозволяє виявити слабкі місця. Постійне вдосконалення системи включає аналіз минулих інцидентів, оновлення технологій та адаптацію до сучасних загроз.

Таким чином, аналіз інцидентів інформаційної безпеки є критично важливим процесом для підвищення ефективності заходів захисту та забезпечення стійкості до кіберзагроз. Використання комплексного підходу, що об’єднує передові технології, чіткі плани дій та кваліфіковану команду, сприяє побудові надійної системи захисту організації.

Ефективна система реагування на інциденти інформаційної безпеки має базуватися на ключових компонентах, які забезпечують її швидкодію, надійність та адаптивність до змінюваних загроз. Одним із найважливіших

факторів є швидкість реагування, оскільки своєчасне виявлення та нейтралізація загрози дозволяє мінімізувати збитки та запобігти поширенню інциденту. Важливу роль відіграє автоматизація рутинних завдань, яка сприяє оптимізації використання ресурсів і зменшенню часу на виконання повторюваних дій. Не менш значущим є співпраця між різними відділами організації, яка забезпечує координацію дій та ефективний обмін інформацією. Крім того, постійне навчання персоналу, зокрема регулярне підвищення кваліфікації, є основою для підтримки високого рівня професійної компетенції в умовах динамічної кіберзагрози [72].

Система реагування також стикається з численними викликами, що потребують впровадження стратегічних рекомендацій. Одним із основних викликів є нестача кваліфікованих фахівців у галузі кібербезпеки. Для вирішення цієї проблеми доцільно залучати зовнішніх експертів і активно використовувати автоматизовані рішення. Великі обсяги даних, які необхідно аналізувати під час інцидентів, створюють додаткові труднощі. Для їх подолання доцільно використовувати SIEM-системи та інструменти аналізу великих даних. Зміна природи загроз, що постійно еволюціонують, вимагає від організацій регулярного моніторингу актуальних ризиків і адаптації системи захисту до нових викликів.

Інструменти для аналізу інцидентів є невід’ємною частиною ефективної системи реагування. Серед них можна виділити SIEM-системи, такі як Splunk, IBM QRadar та Elastic SIEM, які забезпечують збір, кореляцію та аналіз логів із різних джерел. EDR-рішення, наприклад, CrowdStrike Falcon і SentinelOne, спрямовані на виявлення та розслідування кібератак на кінцевих точках. SOAR-платформи, такі як Demisto та ServiceNow Security Operations, автоматизують рутинні завдання й покращують загальну ефективність реагування на інциденти. Використання цих інструментів у поєднанні з чіткими процедурами, кваліфікованими кадрами та адаптивним підходом до змінних загроз дозволяє забезпечити високий рівень кібербезпеки організації.

Аналіз інцидентів інформаційної безпеки є критично важливим етапом у забезпеченні надійного функціонування інформаційних систем підприємства. Інциденти інформаційної безпеки охоплюють будь-які події, які ставлять під загрозу конфіденційність, цілісність або доступність інформації. Для компаній, які працюють у сфері критичної інфраструктури, таких як газопостачальна компанія «Нафтогаз України», аналіз інцидентів дозволяє ідентифікувати слабкі місця, підвищувати ефективність систем захисту та запобігати повторенню загроз.

Основними категоріями інцидентів є кібератаки (зокрема фішинг, DDoS, віруси-шифрувальники), несанкціонований доступ, витік даних, технічні збої та внутрішні загрози. Кожна з цих категорій має свої особливості, які потребують детального розгляду.

У 2023 році в компанії «Нафтогаз України» було зафіксовано 58 інцидентів інформаційної безпеки. Аналіз цих інцидентів базувався на таких параметрах, як тип загрози, джерело атаки, наслідки для бізнесу та час відновлення систем.

Таблиця 2.1

Класифікація інцидентів інформаційної безпеки у 2023 році

Тип інциденту	Кількість випадків	Частка (%)
Фішинг	18	31,0
DDoS-атаки	12	20,7
Віруси-шифрувальники	8	13,8
Несанкціонований доступ	10	17,2
Витік даних	6	10,3
Технічні збої	4	6,9

Найпоширенішою загрозою стали фішингові атаки, які спрямовувались на отримання конфіденційної інформації, такої як паролі чи дані банківських

рахунків. Внаслідок цих атак у 25% випадків виникали короткострокові збої у функціонуванні інформаційних систем. Для боротьби з фішингом було впроваджено регулярне навчання співробітників щодо виявлення підозрілих листів, а також застосовано спеціалізоване програмне забезпечення для автоматичного виявлення шкідливих повідомлень.

DDoS-атаки спричинили тимчасову недоступність корпоративного вебсайту та внутрішніх систем. Для їхньої нейтралізації компанія використовувала хмарні рішення для фільтрації трафіку. Проте аналіз показав, що час реагування на атаки в середньому становив 45 хвилин, що вказує на необхідність підвищення швидкості реагування.

Таблиця 2.2

Наслідки інцидентів інформаційної безпеки

Наслідки	Кількість випадків	Частка (%)
Збої в роботі систем	22	37,9
Втрата даних	8	13,8
Фінансові втрати	15	25,9
Пошкодження репутації	7	12,1
Відновлення після інцидентів	6	10,3

Віруси-шифрувальники становлять серйозну загрозу для конфіденційності даних, адже в деяких випадках вимагали виплати викупу для відновлення доступу до інформації. Аналіз показав, що використання резервних копій дозволило уникнути значних фінансових втрат, однак процес відновлення систем тривав у середньому два дні.

Несанкціонований доступ до систем компанії було зафіксовано в 10 випадках. У більшості з них причиною стали слабкі паролі або недостатній контроль доступу. Для усунення цієї проблеми компанія впровадила багатофакторну аутентифікацію (MFA) та розширила використання засобів шифрування [70].

Витоки даних становлять одну з найбільш критичних загроз для «Нафтогаз України», оскільки вони можуть спричинити серйозні репутаційні та фінансові наслідки. Наприклад, витік конфіденційних даних про клієнтів у

серпні 2023 року призвів до штрафу відповідно до норм GDPR. У відповідь компанія посилила контроль за обробкою даних та інтегрувала рішення для моніторингу доступу до критичної інформації.

Практичний аналіз інцидентів показав, що у 20% випадків людський фактор став основною причиною порушення безпеки. Наприклад, у трьох випадках співробітники випадково надали доступ до конфіденційної інформації, пересилаючи її через незахищені канали зв’язку. У відповідь на це компанія організувала тренінги для працівників і запровадила політику автоматичного шифрування електронної пошти [57].

Загалом, аналіз інцидентів інформаційної безпеки у компанії «Нафтогаз України» виявив ключові проблеми та визначив напрями для вдосконалення системи захисту. Найважливішими заходами є модернізація технологічних рішень, регулярний моніторинг та підвищення обізнаності співробітників. Компанія активно працює над впровадженням проактивних методів захисту, що дозволить не лише реагувати на загрози, але й запобігати їм у майбутньому.

РОЗДІЛ ІІІ.
РОЗРОБКА МОДЕЛІ ЗРІЛОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ГАЗОПОСТАЧАЛЬНОЇ КОМПАНІЇ «НАФТОГАЗ УКРАЇНИ»

3.1. Проблемні аспекти організації системи інформаційної безпеки підприємства. Аналіз кіберзагроз.

Розробка моделі зрілості інформаційної безпеки для компанії «Нафтогаз України» є стратегічно важливим завданням, що дозволяє оцінити поточний стан системи безпеки, визначити напрями розвитку та пріоритети для вдосконалення. У контексті критичної інфраструктури, яку представляє ця компанія, наявність такої моделі є не лише доцільною, а й необхідною умовою забезпечення сталого функціонування.

Важливість моделі зрілості полягає у можливості систематичного підходу до управління інформаційною безпекою, зокрема через визначення рівня зрілості окремих функціональних областей. Основними компонентами моделі є:

Функціональні області, які охоплюють ключові напрямки, такі як управління політиками, управління ризиками, реагування на інциденти, управління доступом, захист мережі, кінцевих точок, даних, додатків, хмарних обчислень, а також безпека постачальників і підвищення обізнаності співробітників.

Рівні зрілості, що характеризують етапи розвитку процесів – від початкового рівня, на якому відсутні формальні процедури, до оптимізованого, на якому реалізується постійне вдосконалення.

Критерії оцінки, які дозволяють оцінити відповідність системи інформаційної безпеки певному рівню зрілості. До таких критеріїв належать наявність документації, ефективність процесів, залученість керівництва, кваліфікація персоналу та використання технологій.

Для «Нафтогазу України» пропонується модель, заснована на міжнародних стандартах, таких як ISO 27001 та NIST Cybersecurity

Framework. Вона враховує специфіку організації та особливості управління критичною інфраструктурою.

Етапи впровадження моделі включають:

Формування робочої групи з досвідчених фахівців.

Проведення аналізу поточного стану системи інформаційної безпеки.

Розробку плану дій із визначенням пріоритетів.

Реалізацію заходів для підвищення рівня зрілості у визначених функціональних областях.

Регулярний моніторинг ефективності та оцінку впроваджених заходів.

Використання моделі зрілості дозволяє організації отримати низку переваг, серед яких систематизація підходів до управління інформаційною безпекою, обґрунтування інвестицій у цю сферу, підвищення рівня захищеності інформаційних активів, спрощення аудиту та сертифікації, а також зміцнення довіри клієнтів і партнерів.

Отже, модель зрілості інформаційної безпеки є ключовим інструментом для стратегічного управління безпекою інформаційних активів, особливо для організацій, що працюють у сфері критичної інфраструктури. Її впровадження забезпечує не лише ефективне реагування на сучасні виклики, а й створює платформу для постійного вдосконалення та адаптації до нових загроз.

Організація ефективної системи інформаційної безпеки на підприємстві є складним і багатогранним процесом, що стикається з низкою проблем. Однією з основних перешкод є недостатнє фінансування, яке проявляється через обмежені бюджети та відсутність довгострокового стратегічного планування. Багато компаній сприймають інвестиції в інформаційну безпеку як додаткові витрати, що ускладнює реалізацію необхідних заходів [52].

Ще однією суттєвою проблемою є нестача кваліфікованих фахівців, обумовлена дефіцитом кадрів на ринку праці та високою вартістю залучення спеціалістів. Водночас, сучасні виклики посилюються через складність і

динамічність загроз, які постійно змінюються, створюючи нові типи атак і вразливостей. Зростання витонченості кіберзагроз ускладнює їх виявлення та вимагає застосування інноваційних підходів.

Відсутність культури інформаційної безпеки серед співробітників також є серйозною перешкодою. Низька обізнаність персоналу щодо важливості дотримання правил безпеки та недостатня мотивація виконувати відповідні політики створюють ризики для організації. Крім того, складність інтеграції систем безпеки через різноманітність технологій і платформ, а також високу вартість інтеграційних процесів ускладнює побудову цілісної системи захисту.

Не менш важливим аспектом є нормативно-правові вимоги, які постійно змінюються, а велика кількість нормативних актів створює труднощі для організацій у дотриманні регуляторних вимог. Технічні обмеження, зокрема використання застарілого обладнання та програмного забезпечення з невиправленими вразливостями, також впливають на ефективність інформаційної безпеки. До того ж, людський фактор залишається одним із головних ризиків: ненавмисні помилки співробітників або їхній обман через соціальну інженерію можуть призводити до серйозних інцидентів.

Для вирішення цих проблем пропонуються наступні шляхи: впровадження постійного навчання співробітників, яке включає регулярні тренінги з інформаційної безпеки, а також використання системи управління інформаційною безпекою (ІБ) на основі стандартів ISO 27001. Крім того, важливо проводити регулярну оцінку ризиків, інвестувати в сучасні технології, співпрацювати із зовнішніми експертами та формувати культуру інформаційної безпеки серед співробітників.

Не менш важливим елементом системи інформаційної безпеки є аналіз кіберзагроз, який являє собою систематичний процес ідентифікації, оцінки та розуміння потенційних ризиків. Такий підхід дозволяє організації виявляти загрози заздалегідь, оптимізувати розподіл ресурсів і забезпечувати

дотримання нормативних вимог. Етапи аналізу включають: ідентифікацію активів, аналіз вразливостей, виявлення загроз, оцінку ризиків і розробку стратегій пом'якшення ризиків [49].

Кіберзагрози поділяються на зовнішні (хакерські атаки, шкідливе програмне забезпечення, спам тощо) та внутрішні (помилки співробітників, дії невдоволених працівників, несанкціонований доступ). Для ефективного аналізу загроз використовуються інструменти, такі як SIEM-системи, EDR-рішення, сканери вразливостей і платформи управління ризиками.

Сучасні тенденції у сфері кіберзагроз свідчать про зростання кількості та складності атак, активне використання зловмисниками штучного інтелекту, збільшення атак на постачальників і посилення використання соціальної інженерії. У цьому контексті стратегічний підхід до інформаційної безпеки стає вирішальним чинником для забезпечення сталого розвитку та захисту організації від кібератак [67].

Аналіз кіберзагроз для "Нафтогазу України": специфічні виклики та шляхи їх подолання.

"Нафтогаз України", як стратегічно важлива компанія для забезпечення енергетичної безпеки України, стикається зі значним спектром кіберзагроз, які можуть негативно вплинути як на її діяльність, так і на стабільність національної енергетичної системи та економіки загалом. Специфіка цих загроз відображає унікальні особливості галузі, в якій функціонує компанія, та її роль у геополітичному контексті.

До ключових кіберзагроз, які стосуються діяльності "Нафтогазу", відносяться:

DDoS-атаки – масовані атаки, спрямовані на відмову в обслуговуванні, здатні паралізувати системи управління, моніторингу та комунікації.

Викрадення даних – цінна інформація щодо контрактів, цінової політики, технологій видобутку та транспортування стає привабливою ціллю для кіберзлочинців.

Шантаж – викрадення даних може використовуватися для вимагання викупу.

Саботаж – зловмисні дії, спрямовані на порушення функціонування критичної інфраструктури, що може спричинити фізичне пошкодження обладнання та збої в газопостачанні.

Логічні бомби – шкідливий код, інтегрований у системи компанії, здатний активуватися за певних умов, наприклад, у визначений час або за виконання специфічних дій.

Інсайдерські загрози – ризики, пов’язані з діями невдоволених співробітників або випадковими помилками, які можуть спричинити витік інформації чи компрометацію систем.

Атаки на постачальників – загрози, що реалізуються через сторонніх постачальників, що співпрацюють з компанією.

Фактори, що підсилюють ризики кіберзагроз, включають напружену геополітичну ситуацію, яка значно підвищує імовірність цілеспрямованих атак; складність управління безпекою через розподілену IT-інфраструктуру; залежність від сторонніх постачальників програмного забезпечення та обладнання; а також стрімкий розвиток технологій, що створює нові можливості для атак.

Для протидії цим викликам "Нафтогаз України" може впроваджувати низку стратегічних заходів, серед яких:

Посилення кібергігієни співробітників, зокрема регулярне проведення тренінгів з основ кібербезпеки.

Інтеграція систем виявлення вторгнень, що дозволить оперативно виявляти та нейтралізувати загрози.

Регулярне оновлення програмного забезпечення з метою усунення існуючих вразливостей.

Резервне копіювання даних, яке забезпечить можливість відновлення інформації у разі її втрати.

Розроблення планів реагування на інциденти, спрямованих на швидке й ефективне подолання наслідків кібератак.

Співпраця з органами кібербезпеки для обміну інформацією та отримання підтримки.

Використання сучасних технологій, таких як штучний інтелект та машинне навчання, що підвищують ефективність систем захисту.

Сегментація мережі та мікросегментація, які забезпечують локалізацію потенційних загроз і зменшують ризики їх поширення [62].

Реалізація цих заходів дозволить "Нафтогазу України" не лише мінімізувати ризики кіберзагроз, але й забезпечити безперервність діяльності та захист стратегічно важливих ресурсів компанії. У контексті зростання складності кіберзагроз інтеграція проактивних підходів до управління безпекою є невід’ємною умовою для успішного функціонування енергетичного сектора України.

Організація системи інформаційної безпеки підприємства є складним завданням, що вимагає врахування численних факторів, пов’язаних із технологічними, організаційними та людськими аспектами. Проблемні аспекти побудови ефективної системи інформаційної безпеки пов'язані з постійним зростанням кіберзагроз, недостатнім фінансуванням, низьким рівнем обізнаності співробітників, а також швидкими змінами в технологічному середовищі. Ці проблеми особливо актуальні для підприємств, які працюють у сфері критичної інфраструктури, таких як газопостачальна компанія «Нафтогаз України».

Однією з ключових проблем є зростання кількості та складності кіберзагроз. Сучасні атаки стають дедалі складнішими та спрямованими, зокрема на отримання конфіденційної інформації, порушення роботи систем або вимагання викупу. Кіберзагрози поділяються на зовнішні (фішинг, віруси, DDoS-атаки) та внутрішні (помилки співробітників, витоки даних, несанкціонований доступ).

Таблиця 3.1

Типи основних кіберзагроз

Тип загрози	Приклад	Потенційний вплив
Фішингові атаки	Надсилання підроблених електронних листів	Крадіжка облікових даних, доступ до мереж
DDoS-атаки	Перевантаження серверів	Втрата доступності послуг
Віруси-шифрувальники	Зашифрування даних з вимогою викупу	Втрата критичної інформації
Витоки даних	Несанкціоноване копіювання інформації	Шкода репутації, фінансові втрати
Внутрішні помилки	Неправильна конфігурація систем	Зниження безпеки, відкриття вразливостей

Практичний аналіз кіберзагроз у «Нафтогаз України» показав, що найбільшою проблемою є фішингові атаки. У 2023 році було зафіксовано 24 випадки, коли співробітники отримали підроблені листи, які імітували офіційні повідомлення компанії. У 5 випадках ці атаки призвели до витоку облікових даних. Для вирішення цієї проблеми компанія впровадила автоматизовані інструменти виявлення фішингових листів, а також організувала регулярне навчання співробітників.

DDoS-атаки, які спрямовані на перевантаження серверів компанії, у 2023 році спричинили тимчасову недоступність сервісів протягом 4 годин. Це вплинуло на функціонування клієнтських систем, що призвело до фінансових втрат та скарг від споживачів. Для зниження ризиків було впроваджено розподілені системи фільтрації трафіку.

Віруси-шифрувальники також є серйозною загрозою. У серпні 2023 року одна з таких атак призвела до шифрування внутрішніх баз даних. Хоча резервні копії дозволили швидко відновити дані, процес тривав майже добу, що негативно вплинуло на операційну діяльність. У відповідь компанія впровадила посилені механізми шифрування та багаторівневу аутентифікацію для захисту критичних систем.

Витоки даних становлять одну з найкритичніших проблем. Наприклад, у жовтні 2023 року виявлено витік конфіденційної інформації про фінансові операції компанії. Це спричинило репутаційні втрати та штрафи відповідно

до вимог GDPR. Для усунення подібних інцидентів компанія впровадила систему моніторингу доступу до даних і додаткові обмеження щодо зовнішнього обміну інформацією.

Ще однією проблемою є недостатня обізнаність співробітників щодо основ інформаційної безпеки. Згідно з результатами внутрішнього опитування, лише 35% працівників мають базові знання про кіберзагрози. Це збільшує ймовірність інцидентів, спричинених людським фактором.

Таблиця 3.2

Аналіз основних проблем організації системи інформаційної безпеки

Проблема	Причина	Наслідок
Зростання кіберзагроз	Висока мотивація зловмисників	Збільшення кількості атак
Недостатнє фінансування	Брак ресурсів на нові технології	Повільна адаптація до нових загроз
Низький рівень обізнаності	Відсутність регулярного навчання	Підвищений ризик через людський фактор
Слабкий моніторинг	Відсутність сучасних аналітичних інструментів	Повільне виявлення загроз
Недосконаліть систем доступу	Використання слабких паролів	Несанкціонований доступ

Практичні заходи для подолання цих проблем включають підвищення обізнаності персоналу, впровадження нових технологій та оптимізацію управління інформаційною безпекою. Наприклад, для поліпшення моніторингу компанія впровадила систему SIEM, яка забезпечує збір та аналіз даних про події безпеки в реальному часі. Крім того, проводяться регулярні тести на проникнення, які дозволяють виявляти слабкі місця в захисті.

Розв’язання проблем організації інформаційної безпеки потребує комплексного підходу, що поєднує технологічні рішення, удосконалення політик та навчання персоналу. Завдяки таким заходам компанія може підвищити стійкість до кіберзагроз та мінімізувати ризики, пов’язані з порушеннями безпеки [69].

3.2. Система моніторингу та реагування на інциденти: вибір технологій і процедур реагування.

Система моніторингу та реагування на інциденти (Security Information and Event Management, SIEM) є комплексним інструментом, який забезпечує збір, аналіз та кореляцію даних з різних джерел, таких як мережеві пристрої, сервери та системи безпеки. Її основне завдання – виявлення потенційних кіберзагроз і реагування на них для забезпечення надійного захисту інформаційної інфраструктури.

Використання SIEM-систем є надзвичайно важливим через низку ключових переваг:

Проактивне виявлення загроз. Завдяки кореляції даних система здатна ідентифікувати складні атаки, які залишаються непомітними для окремих елементів безпеки.

Швидке реагування. Автоматизація процесів прискорює реакцію на інциденти, мінімізуючи їх наслідки.

Зменшення кількості помилок. Автоматизація рутинних завдань знижує ймовірність людських помилок.

Підвищення ефективності. Централізоване управління та оптимізація ресурсів дозволяють максимально ефективно використовувати інфраструктуру.

При виборі SIEM-системи необхідно враховувати такі критерії, як масштабованість (можливість адаптації до зростання обсягу даних), гнучкість (інтеграція з різними типами даних і системами), швидкість аналізу, функціональність (наприклад, кореляція даних, звітність, візуалізація) і вартість.

Серед популярних рішень у сфері SIEM варто виділити такі системи:

Splunk – забезпечує високу гнучкість і можливість кастомізації.

IBM QRadar – потужне рішення з великою кількістю готових правил кореляції.

Elastic SIEM – відкрита та високомасштабована платформа.

ArcSight – інтегроване рішення для управління інформацією та подіями безпеки.

Ефективне використання SIEM потребує чітких процедур реагування на інциденти, які включають кілька ключових етапів:

Виявлення інциденту – автоматичне або ручне виявлення потенційних загроз на основі даних системи.

Аналіз інциденту – збирання додаткової інформації, ідентифікація причин і масштабів проблеми.

Стримування – локалізація та мінімізація впливу інциденту.

Ерадикація – усунення причин загрози.

Відновлення – повернення до нормального функціонування систем та даних.

Аналіз – постінцидентний аналіз для виявлення вразливостей і розробки заходів їх усунення.

Окрім SIEM, важливими компонентами інтегрованої системи безпеки є:

EDR (Endpoint Detection and Response), який дозволяє виявляти та реагувати на загрози на рівні кінцевих точок.

SOAR (Security Orchestration, Automation and Response), що автоматизує рутинні завдання в процесі реагування.

XDR (Extended Detection and Response), який об'єднує дані з різних джерел для розширеного аналізу.

Функціональні можливості SIEM-систем охоплюють широкий спектр задач. Зокрема, це збір і нормалізація даних із різних джерел, кореляція подій для виявлення загроз, ідентифікація аномалій шляхом аналізу відхилень від базових ліній, створення звітів і візуалізація даних через інтерактивні панелі. SIEM також підтримує інтеграцію з іншими системами безпеки, що дозволяє створювати комплексний захист організації.

Застосування SIEM-систем є критичним для сучасних організацій, оскільки вони дозволяють не лише своєчасно реагувати на кіберзагрози, але й оптимізувати управління безпекою за допомогою сучасних технологій.

Процес розробки процедур реагування на інциденти є важливим етапом у забезпеченні кібербезпеки. Він передбачає наступні кроки:

Створення команди реагування: Формується команда досвідчених фахівців, які відповідатимуть за реагування на інциденти.

Аналіз ризиків: Визначаються потенційні загрози та їхні наслідки для організації [73].

Розробка процедур: Створюються детальні процедури для кожного етапу реагування на інцидент, включаючи:

Виявлення інциденту

Ескалація інциденту

Стримування інциденту

Ерадикація інциденту

Відновлення

Аналіз інциденту

Тестування процедур: Проводиться регулярне тестування процедур для перевірки їх ефективності.

Оновлення процедур: Процедури оновлюються відповідно до змін у середовищі та виявлених недоліків.

Інтеграція SIEM та процедур реагування на інциденти

SIEM-система відіграє ключову роль у процесі реагування на інциденти. Вона забезпечує:

Автоматичне виявлення інцидентів: SIEM може автоматично виявляти підозрілу активність та генерувати сповіщення.

Контекст для аналізу: SIEM надає детальну інформацію про інцидент, що полегшує його аналіз.

Інтеграцію з інструментами автоматизації: SIEM може автоматизувати багато рутинних завдань, пов'язаних з реагуванням на інциденти.

Система моніторингу та реагування на інциденти є основним інструментом забезпечення оперативної та ефективної інформаційної безпеки підприємства. Газопостачальна компанія «Нафтогаз України», як об'єкт критичної інфраструктури, стикається з численними кіберзагрозами, які вимагають швидкого виявлення та нейтралізації. Для цього використовується комплексний підхід, що включає впровадження сучасних технологій моніторингу, автоматизацію аналізу інцидентів, а також розробку чітких процедур реагування [67].

Моніторинг інформаційної безпеки базується на системах, які забезпечують збір, обробку та аналіз даних про події в реальному часі. Найбільш поширеними технологіями є SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection and Prevention Systems), а також рішення на основі штучного інтелекту. Кожна з цих систем має свої переваги та забезпечує різні рівні захисту.

Система SIEM дозволяє збирати дані з різних джерел, включаючи сервери, мережеві пристрої, додатки та бази даних. Ця інформація аналізується в реальному часі, що дозволяє виявляти аномалії та потенційні загрози. Важливою особливістю SIEM є можливість інтеграції з іншими системами безпеки, такими як антивірусне програмне забезпечення або брандмауери.

IDS/IPS-системи фокусуються на моніторингу мережевого трафіку та виявленні підозрілої активності. IDS (Intrusion Detection System) забезпечує виявлення загроз, тоді як IPS (Intrusion Prevention System) блокує їх у режимі реального часу. У компанії «Нафтогаз України» впроваджено комплексну систему IDS/IPS, яка інтегрована з SIEM для забезпечення централізованого контролю та аналізу.

Важливою частиною сучасної системи моніторингу є технології штучного інтелекту та машинного навчання. Вони дозволяють автоматично аналізувати великі обсяги даних, виявляти нові загрози та прогнозувати потенційні атаки. Наприклад, алгоритми машинного навчання

використовуються для створення поведінкових моделей, які дозволяють ідентифікувати відхилення від норми.

Практична частина впровадження системи моніторингу у «Нафтогаз України» включала кілька етапів. Спочатку було проведено аудит інформаційної безпеки, що дозволило визначити ключові потреби підприємства. Після цього було обрано SIEM-рішення Splunk Enterprise Security, яке забезпечує гнучкість у налаштуванні та високу продуктивність. Інтеграція SIEM з існуючими IDS/IPS-системами дозволила створити єдину платформу для моніторингу та реагування.

Таблиця 3.3

Основні функції системи SIEM Splunk Enterprise Security

Функція	Опис
Збір даних	Автоматичний збір логів з серверів, мережевих пристроїв та додатків
Аналіз подій	Кореляція подій для виявлення аномалій та загроз
Реагування	Генерація сповіщень та автоматичне виконання заходів захисту
Звітування	Створення звітів для аналізу ефективності системи

Процедури реагування на інциденти є ключовим компонентом системи безпеки. Вони включають дії, які виконуються у разі виявлення загроз. Основні етапи реагування: виявлення, підтвердження, аналіз, нейтралізація, відновлення та звітування. Наприклад, у разі виявлення фішингової атаки система SIEM генерує сповіщення для служби безпеки, після чого проводиться блокування підозрілого джерела.

Таблиця 3.4

Етапи реагування на інциденти інформаційної безпеки

Етап	Дії
Виявлення	Моніторинг та аналіз подій у режимі реального часу
Підтвердження	Перевірка достовірності загрози
Аналіз	Ідентифікація джерела загрози та оцінка її впливу
Нейтралізація	Зупинка атаки, ізоляція заражених систем
Відновлення	Відновлення роботи систем та перевірка даних
Звітування	Підготовка звіту для аналізу та подальшого вдосконалення

На практиці у 2023 році система SIEM у компанії «Нафтогаз України» дозволила виявити та нейтралізувати 75% інцидентів у перші 10 хвилин після їх початку. Одним із прикладів було виявлення масової фішингової атаки, під час якої понад 200 співробітників отримали шкідливі листи. Завдяки автоматичному аналізу та блокуванню джерел атаки вдалося уникнути витоку даних.

Для підвищення ефективності системи моніторингу компанія розробила рекомендації щодо вдосконалення. Зокрема, заплановано впровадження технологій прогнозного аналізу для визначення потенційних загроз на основі історичних даних. Крім того, передбачається інтеграція з хмарними рішеннями для підвищення гнучкості та масштабованості.

Загалом, вибір технологій та розробка процедур реагування забезпечують ефективну систему моніторингу та захисту інформації у «Нафтогаз України». Впровадження сучасних рішень дозволяє своєчасно реагувати на загрози, мінімізувати їх вплив та забезпечити стабільність роботи підприємства [60].

Аналіз впровадження системи моніторингу SIEM у «Нафтогаз України»

Для підвищення ефективності моніторингу та реагування на інциденти у 2023 році компанія «Нафтогаз України» впровадила систему SIEM (Security Information and Event Management) Splunk Enterprise Security. Основними цілями були централізація збору даних, зменшення часу на виявлення загроз, підвищення точності аналізу та автоматизація реагування.

Перед початком впровадження було проведено оцінку існуючих систем моніторингу, яка виявила такі недоліки:

Відсутність єдиного центру обробки даних безпеки.

Тривалий час реагування на інциденти (в середньому 45 хвилин).

Низька інтеграція між різними рішеннями (IDS/IPS, антивірусні системи).

Висока залежність від ручного аналізу подій.

Для розв’язання цих проблем компанія обрала Splunk Enterprise Security як гнучке рішення, яке дозволяє інтегруватися з існуючими системами та автоматизувати обробку великих обсягів даних [39].

Результати впровадження

Після інтеграції SIEM-системи було досягнуто таких результатів:

Централізація збору даних: SIEM забезпечила збір логів із серверів, мережевих пристроїв, додатків та антивірусних програм. Усі події аналізуються в реальному часі, що дозволило швидше ідентифікувати загрози.

Скорочення часу реагування: Час виявлення та нейтралізації загроз скоротився на 35% (до 30 хвилин у середньому).

Автоматизація: Завдяки вбудованим алгоритмам кореляції подій система автоматично генерує сповіщення про критичні інциденти та блокує підозрілі активності.

Інтеграція з IDS/IPS: Зв’язок із системами виявлення та запобігання вторгненням забезпечив ефективну фільтрацію мережевого трафіку та запобігання атакам.

Тестування та аналіз ефективності

Для перевірки ефективності SIEM-системи було проведено серію тестів, включаючи симуляцію фішингових атак, DDoS-атак та спроб несанкціонованого доступу.

Таблиця 3.5

Результати тестування системи моніторингу

Тип інциденту	Виявлення (час, хвилини)	Реагування (час, хвилини)	Успішна нейтралізація (%)
Фішингові атаки	5	10	95
DDoS-атаки	3	8	90
Несанкціонований доступ	4	7	98

Як видно з таблиці, система виявляє загрози протягом перших 5 хвилин після початку інциденту та забезпечує їх швидке нейтралізування. Особливо

ефективною виявилася інтеграція SIEM із системами IDS/IPS, яка дозволила блокувати спроби проникнення до внутрішньої мережі.

Політики реагування

Розробка процедур реагування включала створення таких стандартних операційних процедур (SOP):

Фішингові атаки: Виявлення підозрілих електронних листів, блокування джерела атаки, сповіщення користувачів.

DDoS-атаки: Перенаправлення трафіку через фільтруючі хмарні сервіси, активація обмежень на підозрілі IP-адреси.

Несанкціонований доступ: Автоматичне блокування облікових записів, які перевищили кількість спроб входу [68].

Таблиця 3.6

Стандартні операційні процедури реагування

Тип загрози	Ключові дії	Відповідальний підрозділ	Час реагування (хвилин)
Фішинг	Блокування листів, попередження користувачів	Відділ інформаційної безпеки	10
DDoS	Фільтрація трафіку, активація захисних правил	Відділ IT	8
Несанкціонований доступ	Блокування облікового запису, проведення аудиту	Відділ інформаційної безпеки	7

Для підвищення ефективності системи моніторингу та реагування пропонуються такі кроки:

Інтеграція з прогнозним аналізом: Використання технологій штучного інтелекту для прогнозування загроз.

Розширення можливостей SIEM: Інтеграція з хмарними сервісами для масштабування системи.

Регулярне тестування: Проведення навчань для персоналу та симуляційних атак для перевірки готовності.

Практичні результати впровадження системи SIEM у «Нафтогаз України» свідчать про значне підвищення ефективності виявлення та

реагування на інциденти. Подальші вдосконалення дозволять ще більше скоротити час реагування та мінімізувати ризики для інформаційної безпеки компанії.

3.3. Розробка моделі зрілості інформаційної безпеки підприємства: вибір моделі оцінки зрілості, її економічне обгрунтування та розробка дорожньої карти

Розробка моделі зрілості інформаційної безпеки підприємства. Модель зрілості інформаційної безпеки – це систематичний підхід до оцінки рівня захищеності інформаційних активів підприємства. Вона дозволяє визначити поточний стан, виявити слабкі місця та розробити план вдосконалення системи безпеки.

Чому важлива модель зрілості?

Оцінка поточного стану: Дозволяє зрозуміти, наскільки ефективно працює система безпеки.

Визначення пріоритетів: Допомагає зосередити зусилля на найважливіших аспектах безпеки.

Розробка плану розвитку: Створює основу для розробки стратегії розвитку системи безпеки.

Демонстрація відповідності: Допомагає довести відповідність підприємства нормативним вимогам.

Основні компоненти моделі зрілості

Рівні зрілості: Визначають різні стадії розвитку системи безпеки, від початкового до оптимального.

Домени зрілості: Розділяють систему безпеки на окремі функціональні області, такі як управління доступом, захист мережі, управління інцидентами тощо [75].

Критерії оцінки: Використовуються для оцінки рівня зрілості кожного домену.

Процес оцінки: Визначає методику проведення оцінки та збору даних.

Популярні моделі зрілості

NIST Cybersecurity Framework (CSF): Розроблений Національним інститутом стандартів і технологій США, CSF пропонує гнучку модель для оцінки та вдосконалення кібербезпеки.

ISO/IEC 27001: Міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (ISMS).

CIS Controls: Розроблений Центром управління інтернетом (CIS), набір рекомендацій для забезпечення кібербезпеки.

Процес розробки моделі зрілості

Визначення цілей: Чітко визначити, для чого потрібна модель зрілості (оцінка поточного стану, демонстрація відповідності, розробка плану розвитку тощо) [76].

Вибір моделі: Обрати відповідну модель зрілості, враховуючи розмір підприємства, специфіку діяльності та інші фактори.

Визначення доменів: Розбити систему безпеки на окремі домени, які будуть оцінюватися.

Розробка критеріїв оцінки: Створити чіткі та вимірювані критерії для оцінки рівня зрілості кожного домену.

Збір даних: Зібрати дані про поточний стан системи безпеки за допомогою опитувань, інтерв'ю, аналізу документів та інструментів автоматизації.

Оцінка рівня зрілості: Оцінити рівень зрілості кожного домену на основі зібраних даних і визначених критеріїв.

Розробка плану розвитку: Створити план заходів для підвищення рівня зрілості системи безпеки.

Регулярна оцінка: Проводити регулярну оцінку для відстеження прогресу та коригування плану розвитку.

Переваги використання моделі зрілості

Систематичний підхід: Дозволяє структурувати процес оцінки та вдосконалення системи безпеки.

Об'єктивна оцінка: Забезпечує об'єктивну оцінку поточного стану і дозволяє виявити слабкі місця.

Фокус на пріоритетах: Допомагає зосередити зусилля на найважливіших аспектах безпеки.

Підвищення рівня безпеки: Сприяє постійному вдосконаленню системи безпеки.

Розробка моделі зрілості інформаційної безпеки: детальний розгляд

Вибір моделі оцінки зрілості

Вибір відповідної моделі оцінки зрілості інформаційної безпеки є критичним етапом. Враховуючи різноманітність моделей, варто детально розглянути кожну з них, аби зробити обґрунтований вибір.

Ключові моделі та їх особливості:

NIST Cybersecurity Framework (CSF):

Гнучка та адаптивна модель, що фокусується на результатах.

Підходить для організацій різного розміру та галузі.

Дозволяє вибудовувати індивідуальний підхід до забезпечення кібербезпеки.

ISO/IEC 27001:

Міжнародний стандарт, який детально описує вимоги до системи управління інформаційною безпекою.

Забезпечує високий рівень доказовості та відповідності нормативним вимогам.

Може бути складним для впровадження у невеликих організаціях.

CIS Controls:

Набір практичних рекомендацій, що фокусується на найбільш поширених загрозах.

Легко адаптується до різних середовищ.

Регулярно оновлюється з урахуванням нових загроз.

CMMI (Capability Maturity Model Integration):

Спочатку розроблена для оцінки зрілості процесів розробки програмного забезпечення, але може бути адаптована для інших областей.

Фокусується на процесах та їхній зрілості.

Фактори, які впливають на вибір:

Розмір та структура організації: Для великих підприємств з розгалуженою IT-інфраструктурою можуть знадобитися більш деталізовані моделі.

Галузь діяльності: Регуляторні вимоги та специфіка ризиків у різних галузях вимагають різного підходу.

Наявні ресурси: Вартість впровадження та підтримки моделі, необхідні навички персоналу.

Цілі оцінки: Чого саме хоче досягти організація за допомогою оцінки (визначення рівня зрілості, відповідність стандартам, розробка плану розвитку).

Економічне обґрунтування

Інвестиції в інформаційну безпеку – це не витрати, а інвестиції в майбутнє. Ефективна система безпеки може:

Зменшити фінансові ризики: Уникнення кібератак, викупу даних, штрафів.

Підвищити довіру клієнтів: Забезпечення безпеки даних клієнтів.

Поліпшити репутацію компанії: Зменшення ризику негативної публічності.

Забезпечити безперебійну роботу бізнесу: Зменшення простою системи внаслідок кібератак.

Розрахунок ROI (Return on Investment):

Щоб обґрунтувати інвестиції в інформаційну безпеку, необхідно провести розрахунок ROI. Для цього необхідно оцінити:

Вартість впровадження: Вартість консультацій, програмного забезпечення, обладнання, навчання персоналу.

Вартість підтримки: Вартість регулярного оновлення та підтримки системи.

Очікувані вигоди: Зменшення втрат від кібератак, підвищення ефективності роботи, поліпшення репутації.

Розробка дорожньої карти

Дорожня карта – це детальний план заходів, спрямованих на підвищення рівня зрілості інформаційної безпеки. Вона повинна включати:

Визначення пріоритетів: Виділення найбільш критичних областей для вдосконалення.

Розробка конкретних заходів: Опис конкретних кроків, які необхідно виконати.

Визначення відповідальних осіб: Призначення відповідальних за виконання кожного заходу.

Встановлення термінів: Визначення строків виконання кожного заходу.

Виділення ресурсів: Визначення необхідних ресурсів (фінансових, людських, технологічних).

Система моніторингу та оцінки: Встановлення системи для відстеження прогресу та коригування плану за необхідності [66].

Таблиця 3.7

Приклад дорожньої карти:

Захід	Відповідальний	Термін виконання	Ресурси
Проведення аудиту поточної системи безпеки	Команда IT-безпеки	1 місяць	Консультанти, програмне забезпечення
Розробка політики безпеки	Команда IT-безпеки	2 місяці	Консультанти
Впровадження системи управління доступом	Команда IT-інфраструктури	3 місяці	Програмне забезпечення, обладнання

Розрахунок економічної ефективності впровадження заходів з інформаційної безпеки

Чому важливо оцінювати економічну ефективність?

Інвестиції в інформаційну безпеку часто сприймаються як витрати, а не як інвестиції. Однак, добре продумана система безпеки може:

Зменшити фінансові ризики: Уникнення кібератак, викупу даних, штрафів.

Підвищити довіру клієнтів: Забезпечення безпеки даних клієнтів.

Поліпшити репутацію компанії: Зменшення ризику негативної публічності.

Забезпечити безперебійну роботу бізнесу: Зменшення простою системи внаслідок кібератак.

Оцінка економічної ефективності дозволяє:

Обґрунтувати інвестиції в інформаційну безпеку перед керівництвом.

Порівняти різні варіанти рішень та обрати оптимальний.

Продемонструвати результати впроваджених заходів.

Основні методи оцінки економічної ефективності:

Розрахунок ROI (Return on Investment):

Визначення всіх витрат на впровадження та підтримку заходів з інформаційної безпеки.

Оцінка очікуваних вигод (зменшення збитків від інцидентів, підвищення ефективності роботи, поліпшення репутації).

Розрахунок співвідношення отриманих вигод до витрат.

Аналіз вартості-користі:

Порівняння витрат на впровадження заходів з їх користю для бізнесу.

Використання кількісних та якісних показників.

Моделювання сценаріїв:

Створення різних сценаріїв розвитку подій з урахуванням та без урахування впроваджених заходів.

Порівняння фінансових результатів за різними сценаріями.

Ключові показники ефективності:

Зменшення кількості інцидентів інформаційної безпеки.

Зменшення середньої вартості інциденту.

Зменшення часу відновлення після інциденту.

Збільшення довіри клієнтів.

Поліпшення репутації компанії.

Збільшення продуктивності працівників.

Труднощі при розрахунку:

Складнощі в оцінці непрямих вигод: Наприклад, підвищення довіри клієнтів складно виміряти в грошовому еквіваленті.

Невизначеність щодо ймовірності та наслідків інцидентів.

Відсутність достатніх даних для проведення розрахунків.

Рекомендації:

Використовувати комбінацію різних методів оцінки.

Залучати до процесу оцінки представників різних відділів компанії.

Регулярно переглядати та оновлювати розрахунки.

Враховувати особливості конкретного бізнесу та галузі.

Приклад розрахунку ROI:

Припустимо, компанія витратила 100 000 грн на впровадження системи виявлення вторгнень. Завдяки цій системі вдалося запобігти кібератаці, яка могла б призвести до втрати 500 000 грн. В такому випадку ROI складе 500%.

Висновок:

Оцінка економічної ефективності впровадження заходів з інформаційної безпеки є важливим інструментом для обґрунтування інвестицій та демонстрації їхньої ефективності. Регулярний моніторинг та оцінка дозволяють оптимізувати витрати на безпеку та забезпечити максимальний захист інформаційних активів підприємства [60].

Розробка моделі зрілості інформаційної безпеки підприємства є стратегічно важливим завданням, яке дозволяє оцінити поточний стан захисту інформації, визначити напрями вдосконалення та розробити план

реалізації заходів. Для компаній критичної інфраструктури, таких як «Нафтогаз України», впровадження такої моделі є необхідним для зниження ризиків, підвищення стійкості до загроз та оптимізації витрат на безпеку.

Вибір моделі оцінки зрілості базується на вивченні існуючих стандартів і підходів. Найпоширенішими моделями є CMMI (Capability Maturity Model Integration), COBIT (Control Objectives for Information and Related Technologies) та моделі NIST Cybersecurity Framework. Для «Нафтогаз України» доцільним є використання моделі CMMI, адаптованої до потреб інформаційної безпеки. Ця модель передбачає п’ять рівнів зрілості: початковий (Initial), повторюваний (Repeatable), визначений (Defined), керований (Managed) та оптимізований (Optimized). Кожен рівень характеризується ступенем формалізації, автоматизації та інтеграції процесів.

Практична реалізація моделі починається з оцінки поточного стану. У компанії «Нафтогаз України» було проведено аудит, який показав, що підприємство знаходиться на рівні «Визначений» (Defined), тобто існують формалізовані політики безпеки, але процеси не є достатньо інтегрованими та автоматизованими.

Таблиця 3.8

Рівні зрілості інформаційної безпеки за моделлю CMMI

Рівень	Характеристики	Приклад у «Нафтогаз України»
Початковий	Відсутність формалізованих процесів	Раніше залежало від індивідуальних рішень
Повторюваний	Процеси документовані, але виконуються вибірково	Часткова стандартизація політик доступу
Визначений	Формалізовані політики, але недостатня автоматизація	Є політики, але бракує автоматизованих рішень
Керований	Інтегровані процеси, автоматизований контроль	Часткова інтеграція з SIEM
Оптимізований	Постійне вдосконалення, використання прогнозного аналізу	Потребує впровадження інноваційних технологій

Економічне обґрунтування впровадження моделі зрілості ґрунтується на аналізі витрат і вигод. Основними вигодами є зниження витрат на ліквідацію наслідків інцидентів, покращення репутації компанії та

підвищення ефективності бізнес-процесів. За розрахунками, впровадження інтегрованої моделі може знизити витрати на реагування на інциденти на 30%, тоді як покращення репутації може сприяти збільшенню довіри клієнтів і партнерів.

Таблиця 3.9

Економічні показники впровадження моделі зрілості

Показник	До впровадження (млн грн)	Після впровадження (млн грн)	Економія (%)
Витрати на ліквідацію інцидентів	10	7	30
Витрати на впровадження систем	15	12	20
Вплив на репутацію	Негативний	Позитивний	-

Розробка дорожньої карти для досягнення оптимального рівня зрілості включає кілька ключових етапів. По-перше, необхідно впровадити автоматизовані засоби моніторингу та реагування на основі штучного інтелекту. По-друге, слід підвищити рівень обізнаності персоналу шляхом регулярного навчання та сертифікації. По-третє, необхідно інтегрувати процеси інформаційної безпеки в загальну бізнес-стратегію [60].

Таблиця 3.10

Дорожня карта підвищення зрілості інформаційної безпеки

Етап	Діяльність	Термін виконання	Відповідальний
Впровадження SIEM	Інтеграція SIEM з усіма інформаційними системами	6 місяців	Відділ IT
Автоматизація	Використання інструментів AI для аналізу даних	12 місяців	Відділ безпеки
Навчання персоналу	Організація тренінгів з основ кібербезпеки	Постійно	HR-відділ
Інтеграція процесів	Включення безпеки у всі бізнес-процеси	18 місяців	Керівництво компанії
Прогнозний аналіз	Впровадження технологій для прогнозування потенційних загроз	24 місяці	Відділ аналітики

Результатом впровадження дорожньої карти стане підвищення рівня зрілості інформаційної безпеки до оптимізованого рівня. Це дозволить не

лише знизити ризики, а й забезпечити відповідність міжнародним стандартам та вимогам. Впровадження цієї моделі є стратегічним рішенням, яке сприятиме стійкості та конкурентоспроможності компанії в умовах сучасного кіберсередовища.

3.4. Напрямки оптимізації підвищення рівня інформаційної безпеки газопостачальної компанії «Нафтогаз України»

«Нафтогаз України», як одна з найбільших енергетичних компаній країни, має критично важливу інформаційну інфраструктуру. Оптимізація рівня інформаційної безпеки є не просто бажаним кроком, а необхідністю для забезпечення безперебійної роботи, захисту конфіденційної інформації та запобігання фінансових втрат.

Ключові напрямки оптимізації:

1. Підвищення обізнаності співробітників

Регулярні тренінги: Проведення систематичних навчань з питань інформаційної безпеки, зокрема щодо розпізнавання фішингових атак, захисту паролів та безпечного використання пристроїв.

Створення культури безпеки: Формування у співробітників розуміння важливості інформаційної безпеки та їхньої ролі у забезпеченні її.

Інтерактивні матеріали: Використання відео, інфографіки та симуляцій для більш ефективного навчання.

2. Удосконалення систем захисту інформації

Оновлення програмного забезпечення: Регулярне встановлення патчів та оновлень для усунення вразливостей.

Впровадження систем виявлення вторгнень (IDS): Моніторинг мережі для виявлення підозрілої активності [64].

Захист від кібератак: Впровадження заходів для захисту від поширених типів атак, таких як DDoS, фішинг, ransomware.

Сегментація мережі: Розділення мережі на сегменти для обмеження поширення потенційних загроз.

3. Захист критичної інфраструктури

Фізичний захист: Забезпечення фізичного доступу до серверних кімнат та інших важливих об'єктів.

Резервне копіювання даних: Регулярне створення резервних копій критично важливих даних та їх зберігання в безпечному місці.

Планування відновлення після інцидентів: Розробка детального плану дій на випадок кібератаки або іншої надзвичайної ситуації.

4. Управління доступом

Строгий контроль доступу: Використання багатофакторної аутентифікації, політик «найменших привілеїв» та регулярний перегляд прав доступу.

Моніторинг активності користувачів: Відстеження незвичайної активності в системі.

5. Захист даних

Шифрування даних: Захист конфіденційних даних за допомогою шифрування як під час передачі, так і під час зберігання.

Маскування даних: Заміна чутливих даних на фіктивні у звітах та інших документах.

6. Партнерство з постачальниками послуг

Перевірка постачальників: Ретельний відбір постачальників послуг та перевірка їхніх рівнів безпеки.

Укладання договорів про рівень обслуговування (SLA): Визначення вимог до рівня безпеки в договорах з постачальниками.

7. Постійний моніторинг та аналіз загроз

Використання SIEM-систем: Збір та аналіз даних з різних джерел для виявлення аномалій та інцидентів.

Відстеження нових загроз: Постійне оновлення інформації про нові загрози та уразливості.

8. Проведення регулярних аудитів безпеки

Внутрішні аудити: Регулярна перевірка відповідності системи безпеки встановленим стандартам.

Зовнішні аудити: Залучення незалежних експертів для проведення аудиту.

9. Співпраця з правоохоронними органами

Повідомлення про інциденти: Швидке повідомлення про інциденти до правоохоронних органів.

Співпраця в розслідуваннях: Надання необхідної інформації для розслідування кіберзлочинів.

Висновки

Підвищення рівня інформаційної безпеки «Нафтогазу України» – це комплексний процес, який вимагає систематичного підходу та залучення фахівців різного профілю. Реалізація зазначених напрямків дозволить компанії забезпечити надійний захист своїх інформаційних активів та мінімізувати ризики, пов’язані з кіберзагрозами.

Економічне обґрунтування інвестицій в інформаційну безпеку для "Нафтогазу України"

Чому інвестиції в інформаційну безпеку – це не витрати, а інвестиції?

Для великого енергетичного гіганта, такого як "Нафтогаз України", інформаційна безпека – це не просто додаткова функція, а стратегічна необхідність. Ось чому:

Зменшення фінансових ризиків: Кібератаки можуть призвести до значних фінансових втрат через викрадення коштів, викуп даних, штрафи за порушення регуляторних вимог та збоїв у роботі [56].

Підвищення довіри інвесторів та партнерів: Демонстрація високого рівня інформаційної безпеки підвищує довіру до компанії та її фінансової стійкості.

Захист репутації: Кібератаки можуть завдати серйозної шкоди репутації компанії, особливо в умовах високої конкуренції.

Забезпечення безперебійної роботи бізнесу: Кібератаки можуть призвести до перебоїв в роботі критично важливих систем, що може мати негативні наслідки для бізнесу.

Як обґрунтувати інвестиції в цифрах?

Розрахунок ROI (Return on Investment): Порівняння витрат на впровадження заходів з інформаційної безпеки з очікуваними вигодами (зменшення збитків від інцидентів, підвищення ефективності роботи, поліпшення репутації).

Аналіз вартості-користі: Порівняння витрат на впровадження заходів з їх користю для бізнесу.

Моделювання сценаріїв: Створення різних сценаріїв розвитку подій з урахуванням та без урахування впроваджених заходів.

Приклад розрахунку ROI:

Припустимо, "Нафтогаз України" витратив 1 млн грн на впровадження системи виявлення вторгнень. Завдяки цій системі вдалося запобігти кібератаці, яка могла б призвести до втрати 10 млн грн. В такому випадку ROI складе 900%.

Конкретні приклади заходів з інформаційної безпеки для "Нафтогазу України":

Захист критичної інфраструктури: Фізичний захист об'єктів, резервне копіювання даних, планування відновлення після інцидентів.

Удосконалення систем захисту інформації: Впровадження SIEM-систем, WAF, IDS/IPS, захист від DDoS-атак.

Захист даних: Шифрування даних, контроль доступу, маскування даних.

Підвищення обізнаності співробітників: Регулярні тренінги, створення культури безпеки.

Оптимізація підвищення рівня інформаційної безпеки є ключовим завданням для газопостачальної компанії «Нафтогаз України», яка працює в умовах постійного зростання кіберзагроз. Забезпечення надійного захисту

даних, операційних систем та критичної інфраструктури потребує комплексного підходу, який включає модернізацію технологічних рішень, вдосконалення політик безпеки, підвищення обізнаності персоналу та інтеграцію безпеки у всі бізнес-процеси.

Напрямки оптимізації визначаються на основі результатів аналізу існуючих проблем і враховують сучасні тенденції у сфері інформаційної безпеки. Основними напрямками є впровадження нових технологій моніторингу та реагування, інтеграція штучного інтелекту для аналізу загроз, розвиток культури інформаційної безпеки серед персоналу, а також удосконалення управління ризиками.

Один із пріоритетних напрямків — впровадження систем прогнозного аналізу, які дозволяють ідентифікувати потенційні загрози до їх реалізації. Наприклад, алгоритми машинного навчання можуть аналізувати поведінкові моделі користувачів і автоматично виявляти аномалії. Це дозволяє запобігти таким атакам, як несанкціонований доступ або витоки даних. У рамках цього напрямку компанія планує модернізувати існуючу систему SIEM, інтегруючи її з інструментами штучного інтелекту.

Підвищення рівня обізнаності співробітників є ще одним важливим напрямком. Внутрішній аудит показав, що більшість інцидентів пов’язані з людським фактором, зокрема незнанням правил безпечної роботи з інформацією. Компанія розробила програму регулярних тренінгів для працівників, які включають вивчення основ кібербезпеки, методів виявлення фішингових атак і правил роботи з конфіденційною інформацією.

Інтеграція інформаційної безпеки в бізнес-процеси є наступним важливим напрямком. Це передбачає розробку нових політик, які враховують безпеку на кожному етапі діяльності, включаючи розробку нових продуктів, взаємодію з клієнтами та партнерами, а також управління постачальниками. Наприклад, кожен контракт із підрядниками включає розділи про дотримання стандартів інформаційної безпеки.

Таблиця 3.11

Основні напрямки оптимізації інформаційної безпеки

Напрямок	Заходи	Очікуваний результат
Впровадження прогнозного аналізу	Інтеграція AI у системи моніторингу	Зниження кількості інцидентів на 25%
Підвищення обізнаності	Проведення тренінгів для співробітників	Зниження ризику через людський фактор на 30%
Інтеграція у бізнес-процеси	Розробка політик безпеки для всіх етапів діяльності	Підвищення стійкості до загроз
Модернізація технічних рішень	Оновлення SIEM та впровадження IDS/IPS	Підвищення ефективності виявлення загроз
Розвиток управління ризиками	Оцінка ризиків та розробка заходів для їх мінімізації	Зменшення ймовірності критичних інцидентів

Практична реалізація оптимізаційних заходів у компанії «Нафтогаз України» почалася з модернізації системи моніторингу. У 2023 році було інтегровано новий модуль прогнозного аналізу, який дозволяє автоматично виявляти відхилення від нормальної поведінки користувачів. Наприклад, під час тестування система виявила спробу отримання доступу до конфіденційної інформації з використанням легітимного облікового запису, що дозволило своєчасно нейтралізувати загрозу [44].

Підвищення рівня обізнаності співробітників реалізовано через створення спеціальної онлайн-платформи, яка містить навчальні матеріали, тести та практичні завдання. У 2023 році цю програму завершили 75% працівників, а кількість інцидентів, пов’язаних із людським фактором, знизилася на 20%.

Інтеграція безпеки у бізнес-процеси включала перегляд політик взаємодії з постачальниками. Наприклад, усі нові договори з підрядниками тепер містять вимогу використовувати захищені канали зв’язку та відповідати стандартам ISO/IEC 27001.

Таблиця 3.12

Результати реалізації заходів оптимізації

Заходи	До впровадження	Після впровадження	Зміна (%)
Кількість інцидентів	58	42	-27
Час реагування на загрози (хвилин)	45	30	-33
Рівень задоволеності клієнтів (%)	85	92	+7
Витрати на ліквідацію інцидентів (млн грн)	10	7	-30

Наступним кроком є розвиток управління ризиками. Це включає регулярний перегляд оцінок ризиків, розробку сценаріїв реагування на критичні інциденти та проведення симуляційних навчань для персоналу. Завдяки цьому компанія зможе ще краще адаптуватися до змін у кіберсередовищі та забезпечити стабільність операцій.

Підсумовуючи, напрями оптимізації інформаційної безпеки в «Нафтогаз України» охоплюють технологічні, організаційні та людські аспекти. Впровадження цих заходів дозволяє не лише підвищити рівень захисту, але й знизити витрати, покращити репутацію компанії та забезпечити довіру клієнтів і партнерів [42].

ВИСНОВКИ

1. Здійснено аналіз сучасного стану дослідження проблеми інформаційної безпеки підприємства в умовах цифровізації. Відзначено значний внесок у розробку цієї проблематики вітчизняних науковців. Накопичено значний масив інформації щодо реалізації завдань національної безпеки України в інформаційній сфері. Йдеться про сукупність збалансованих інтересів держави, суспільства й особистості. Будь-яке наукове знання про стан інформаційної безпеки на різних рівнях її функціонування набуває актуального значення. Захист інформації в процесі функціонування підприємств дає можливість укладати вигідні контракти, отримувати високі доходи, підвищувати ефективність діяльності в цілому. Тому серед основних завдань сучасних підприємств – створення ефективної моделі кібернетичної безпеки.

2. Визначено джерельну базу та методи дослідження. До основного комплексу джерел, на основі яких було виконано наукове дослідження, належить документація газопостачальної компанії «Нафтогаз України», що зумовлено завданнями, визначеними у кваліфікаційній роботі. Система документації газопостачальної компанії «Нафтогаз України» охоплює управлінські документи службового характеру, зокрема, первинно-облікові, організаційно-розпорядчі, планові, фінансово-облікові, звітно-статистичні та ін.. Ці документи забезпечують діяльність компанії «Нафтогаз України» як юридичної особи. Господарська документація включає документи переважно економічного, виробничого та організаційного характеру. Вона містить довідкову й практичну складові, а також документи з контролю виконання.

3. Джерельну базу нашого дослідження складають також законодавчі акти, державні стандарти, нормативно-правові документи, які регулюють процеси забезпечення інформаційної безпеки підприємств й обумовлюють аналіз внутрішніх та зовнішніх інформаційних загроз національній безпеці України, визначають шляхи гарантування інформаційної безпеки країни на будь-якому рівні.

Окрім того, було використано наукові статті, монографії та дослідження сучасних українських авторів, що стосуються інформаційної безпеки держави та підприємств.

Основними методами нашого дослідження були методи аналізу та синтезу, порівняння, узагальнення, прогнозування, моделювання.

4. Проаналізовано систему інформаційної безпеки газопостачальної компанії «Нафтогаз України». Аналіз стану інформаційної безпеки показав, що сучасна діяльність підприємств критичної інфраструктури потребує інтегрованого підходу, який включає впровадження сучасних технологій, розробку ефективних політик безпеки та створення культури кіберзахисту.

5. Досліджено існуючі системи захисту, проаналізувати інциденти інформаційної безпеки. Оцінка існуючих систем безпеки продемонструвала, що компанія активно працює над впровадженням міжнародних стандартів, таких як ISO/IEC 27001, а також інтегрує сучасні рішення, зокрема SIEM-систему для моніторингу інцидентів. Водночас результати дослідження вказують на необхідність подальшої оптимізації процесів реагування, інтеграції прогнозного аналізу на основі штучного інтелекту та підвищення рівня обізнаності персоналу.

6. Визначено труднощі і проблеми в організації системи інформаційної безпеки підприємства. Одним із основних джерел загроз залишається людський фактор. Серед інших категорій інцидентів: кібератаки (зокрема фішинг, DDoS, віруси-шифрувальники), несанкціонований доступ, витік даних, технічні збої та внутрішні загрози. Кожна з цих категорій має свої особливості, які потребують детального розгляду.

7. Розроблено модель зрілості інформаційної безпеки підприємства, яка дозволяє оцінити поточний стан і визначити напрями для вдосконалення систем інформаційної безпеки. Впровадження дорожньої карти переходу на вищий рівень зрілості сприятиме зниженню ризиків, пов’язаних із людським фактором, покращенню координації процесів захисту та підвищенню ефективності витрат на безпеку.

8. Окреслено напрями оптимізації підвищення рівня інформаційної безпеки газопостачальної компанії «Нафтогаз України», запровадження яких дозволить компанії «Нафтогаз України» не лише знизити рівень вразливості перед кіберзагрозами, а й посилити довіру з боку клієнтів і партнерів. Особливого значення набуває розвиток культури кібербезпеки серед співробітниківРегулярне навчання, тестування та тренінги сприятимуть підвищенню обізнаності персоналу та забезпечать додатковий рівень захисту від інцидентів, пов’язаних із недбалістю чи помилками працівників. Крім того, запропоновані технологічні рішення, такі як використання систем штучного інтелекту для прогнозного аналізу та автоматизації процедур реагування.

9. Розроблено рекомендації щодо використання інноваційних технологій для створення ефективних моделей інформаційної безпеки сучасного підприємства. Загальні рекомендації включають подальшу автоматизацію процесів безпеки, розширення використання штучного інтелекту для моніторингу загроз, посилення взаємодії з підрядниками щодо дотримання стандартів інформаційної безпеки та проведення регулярних навчань для персоналу. Застосування цих заходів дозволить компанії зберегти стійкість до зростаючих кіберзагроз, забезпечити безперебійність операцій та відповідати вимогам сучасного інформаційного середовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бабінська М. Проблеми інформаційної безпеки України. *Вісник науково-інформаційного центру НАТО Прикарпатського національного університету імені Василя Стефаника.* 2009. №2. С.11-15.URL:http://nato.pu.if.ua/journal/2009/2009-2.pdf.
2. Виздрик В.&Мельник О. (2023). Grail of science, (24). 196-202/http://doi.org/10.36074/grail-of-science.17.02.2023.034.
3. Волот О. І. Інформаційна та кібербезпека сучасного підприємства: забезпечення та моделювання. *Центральноукраїнский науковий вісник. Економічні науки,* 2019. Вип. 3(26).С. 238-247.
4. Волот О. І., Колотюк В. О. Інформаційне забезпечення інформаційної безпеки підприємств малого бізнесу в умовах ринкових відносин. (handle/123456789/19346) / О. І. Волот, В. О. Колотюк. Київ: НДЕІ, 2019.
5. Волот О. І. Методичні аспекти ефективності застосування інформаційно-комунікаційних технологій на промислових підприємствах (handle/123456789/11139)/ Волот О. І.. Київ: НДЕІ, 2013.
6. Волот О. І. Реальний сектор економіки: сутність, складові та його роль в забезпеченні стійкого розвитку економіки держави (handle/123456789/11785) / О. І. Волот, І. М. Пліско. Чернігів: ЧНТУ, 2016.
7. Нашинець-Наумова А. Ю. Інформаційна безпека: питання забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави / В.Г. Горник, С. О. Кравченко. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління*, 2020. №2 (70). Т. 31. С. 206-212.
8. Дергачова В. В., Колешня Я. О. Вплив сучасних інформаційних технологій на економічну безпеку підприємства. *Економічний вісник НТУУ «Київський політехнічний інститут*», 2017. № 4.
9. ДСТУ 2394-94 Інформація та документація. Комплектування фонду, бібліографічний опис, аналіз документів. Терміни та визначення: вид.

офіційне. – К.: Держстандарт України, 1994. URL: http://infstudy.at.ua/load/normativno_pravova_dokumentacija/dstu_2394_94_informacija_ta_dokumentacija_komplektuvannja_fondu_bibliografichnij_opis_analiz_dokumentiv_termini_ta_viznachennja/4-1-0-25

10. Дубов Д. В. Стратегічні аспекти кібербезпеки. *Стратегічні пріоритети: наук.-аналіт. щокварт. зб.*/ Нац. ін-т стратег. дослідж. Київ: НІСД. 2013. №4(29). С.119-126.
11. Закон України «Про інформацію» [Закон України «Про інформацію» № 2657-XII. Відомості Верховної Ради України. 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.].
12. Закон України «Про Національну програму інформатизації» [Про Національну програму інформатизації: Закон України [Електронний ресурс]. Режим доступу:http://zakon2.rada.gov.ua/laws/show/74/98-вр. – Заголовок з екрану].
13. Закон України «Про Основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України, 2017. № 2469- VIII. Режим доступу: URL:https://its.iszzi.kri.ua/article/viewFile/153490/153471
14. Закон України Про телекомунікації» №1089-IX від 16.12.2020. ВВР 2020.
15. Зубок М. І. Безпека підприємницької діяльності: Нормативно-правові документи комерційного підприємства, банку. Київ: Істина, 2004. 144 с.
16. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навч. посіб. К.:Атіка, 2005. 432 с.
17. Кицюк В. М., Путилін О. С. Інформаційна безпека підприємства: теоретичний аспект. Сучасний захист інформації, 2024. №2(58).
18. Климова К. Організація інформаційної діяльності в управлінні: тенденції розвитку та фактори впливу. *Соціум. Документ. Комунікація*, 2021. Вип. 12. С. 191-208.
19. Литвинюк А. А. Основи інформаційноїбезпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. Вісник ЦВК. 2008. №4. С.18-21.

20. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський: навч. посіб. К.: КНТ, 2006. 280 с.
21. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки: навч. посіб. Вінниця: ВНТУ, 2013. 221 с.
22. Маркіна І. А., Дячков Д. Н. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємства. 2016.№ 3(1). С. 80-88.
23. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія / А. Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с.
24. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємства: навч. посіб. Київ: МАУП, 2006.134 с.
25. Ніколаюк С. І., Никифорчук Д. Й. Безпека суб'єктів підприємницької діяльності: курс лекцій. К.: КНТ, 2005. 320 с.
26. Олійник О. В. Принципи забезпечення інформаційної безпеки України / О. В. Олійник. Науковий вісник Ужгородського університету, 2012. Вип. 18. С. 170-173.
27. Ортинський В. Л. Економічна безпека підприємств, організацій та установ: навч. посіб. для студ. вищ. навч. закл. / Ортинський В. Л. та ін. К.: Правова єдність, 2009. 544 с.
28. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти / В. Панченко. *Актуальні проблеми правознавства*, 2020. №1 (21). С. 103-109.
29. Правові засади інформаційної безпеки України: монографія / П. Д. Біленчук, Л. В. Борисова, І. М. Неклонський, В. О. Собина; за ред. П. Д. Біленчука. Харків, 2018. 289 с.
30. Про доктрину інформаційної безпеки України: Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. Режим доступу: URL:https://zakon.rada.gov.ua/laws/hsow/47/2017

31. Світлична В. Ю. Інформаційна безпека: сутність та порядок реалізації.
32. Молодий вчений, 2014. №11(14).С. 97-100.
33. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко. *Економічні науки: Вісник*
34. *Хмельницького національного університету*, 2010. №2. Т. 2. С.32-35.
35. Толубко В. Б., Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.
36. Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та виклики / О. Храпкін. Проблеми і перспективи економіки та управління, 2023. №4.
37. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Електронний журнал «Ефективна економіка», 2015. № 4. Режим доступу: www.economy.nauka.com.ua/?op=1&z=5...
38. Якименко М. Ю., В. А. Савченко В. А., С. В. Легомінова. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: державний університет телекомунікацій, 2022. 308 с.
39. Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing. [Електронний ресурс]. – Режим доступу: https://cloudsecurityalliance.org.
40. Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing. [Електронний ресурс]. – Режим доступу: https://cloudsecurityalliance.org.
41. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2019.
42. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2019.
43. Deloitte. "Cyber Risk Management: Strategies for Effective Implementation in Enterprises." – [Електронний ресурс]. – Режим доступу: https://www2.deloitte.com.

44. Deloitte. "Cyber Risk Management: Strategies for Effective Implementation in Enterprises." – [Електронний ресурс]. – Режим доступу: https://www2.deloitte.com.
45. European Union Agency for Cybersecurity (ENISA). Guidelines for Securing Critical Information Infrastructures. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu.
46. European Union Agency for Cybersecurity (ENISA). Guidelines for Securing Critical Information Infrastructures. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu.
47. Ghosh, A., Rai, S. (2021). “AI in Cybersecurity: Emerging Trends and Applications.” IEEE Security & Privacy Journal, 19(4), 45-52.
48. Ghosh, A., Rai, S. (2021). “AI in Cybersecurity: Emerging Trends and Applications.” IEEE Security & Privacy Journal, 19(4), 45-52.
49. Harvard Business Review. “Securing Critical Infrastructure: Challenges and Opportunities.” – [Електронний ресурс]. – Режим доступу: https://hbr.org.
50. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.
51. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.
52. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF). [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework.
53. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF). [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework.
54. PwC. Global State of Information Security Survey 2023. [Електронний ресурс]. – Режим доступу: https://www.pwc.com.

55. PwC. Global State of Information Security Survey 2023. [Електронний ресурс]. – Режим доступу: https://www.pwc.com.
56. Splunk Enterprise Security: Implementation Guide. Splunk Inc., 2023. [Електронний ресурс]. – Режим доступу: https://www.splunk.com.
57. Splunk Enterprise Security: Implementation Guide. Splunk Inc., 2023. [Електронний ресурс]. – Режим доступу: https://www.splunk.com.
58. Андрійчук В. С. «Моделі управління інформаційною безпекою». – Львів: ЛНУ, 2022. – 260 с.
59. Бартків Ю. В. «Сучасні технології моніторингу загроз». – Івано-Франківськ: ІФНТУНГ, 2022. – 270 с.
60. Бейлі М., Карлсон Р. «Принципи захисту даних в епоху цифровізації». – Київ: Либідь, 2021. – 280 с.
61. Березюк О. В., Шевчук В. І. «Інформаційна безпека та кіберзахист: практичний курс». – Київ: Наукова думка, 2021. – 320 с.
62. Глобальна ініціатива з кібербезпеки. Звіт про кіберзагрози за 2023 рік. – [Електронний ресурс]. – Режим доступу: https://www.globalcyberinitiative.org.
63. Глобальна ініціатива з кібербезпеки. Звіт про кіберзагрози за 2023 рік. – [Електронний ресурс]. – Режим доступу: https://www.globalcyberinitiative.org.
64. Гринчук В. О., Савченко П. М. «Кіберзахист інформаційних систем». – Харків: ХНУРЕ, 2022. – 350 с.
65. Журнал «Кібербезпека України». Спеціальний випуск «Виклики 2023 року». – Київ, 2023.
66. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
67. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
68. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.
69. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.

70. Кабінет Міністрів України. Концепція забезпечення кібербезпеки України. – Постанова КМУ від 15.03.2016 № 242.
71. Кабінет Міністрів України. Концепція забезпечення кібербезпеки України. – Постанова КМУ від 15.03.2016 № 242.
72. Кім Д. «Поглиблений курс з кіберзахисту для ІТ-спеціалістів». – Харків: Фоліо, 2023. – 390 с.
73. Ковальчук Л. М., Бондар С. В. «Аудит інформаційної безпеки: методологія та практика». – Київ: КНЕУ, 2021. – 310 с.
74. Макаренко А. В. «Стратегії захисту критичної інфраструктури». – Полтава: ПНТУ, 2023. – 340 с.
75. Мартинюк І. П. «Інформаційна безпека підприємств: методичний посібник». – Дніпро: ДНУ, 2020. – 240 с.
76. Павленко О. В. «Захист інформації у корпоративних мережах». – Одеса: ОНУ, 2022. – 300 с.
77. Сміт Д. «Основи кібербезпеки для організацій». – Львів: «Світ», 2020. – 284 с.
78. Черненко П. Г. «Технічні аспекти інформаційної безпеки». – Запоріжжя: ЗНТУ, 2021. – 280 с.
79. Шекспір, Дж. Основи кібербезпеки: Підручник для спеціалістів з інформаційної безпеки. – Київ: «Основа», 2021.
80. Шекспір, Дж. Основи кібербезпеки: Підручник для спеціалістів з інформаційної безпеки. – Київ: «Основа», 2021.

Додаток А

Таблиця 2.1. Класифікація інцидентів інформаційної безпеки у 2023 році

Тип інциденту	Кількість випадків	Частка (%)
Фішинг	18	31,0
DDoS-атаки	12	20,7
Віруси-шифрувальники	8	13,8
Несанкціонований доступ	10	17,2
Витік даних	6	10,3
Технічні збої	4	6,9

Додаток Б

Таблиця 2.2. Наслідки інцидентів інформаційної безпеки

Наслідки	Кількість випадків	Частка (%)
Збої в роботі систем	22	37,9
Втрата даних	8	13,8
Фінансові втрати	15	25,9
Пошкодження репутації	7	12,1
Відновлення після інцидентів	6	10,3

Додаток В

Таблиця 3.1. Типи основних кіберзагроз

Тип загрози	Приклад	Потенційний вплив
Фішингові атаки	Надсилання підроблених електронних листів	Крадіжка облікових даних, доступ до мереж
DDoS-атаки	Перевантаження серверів	Втрата доступності послуг
Віруси-шифрувальники	Зашифрування даних з вимогою викупу	Втрата критичної інформації
Витоки даних	Несанкціоноване копіювання інформації	Шкода репутації, фінансові втрати
Внутрішні помилки	Неправильна конфігурація систем	Зниження безпеки, відкриття вразливостей

Додаток Г

Таблиця 3.2. Аналіз основних проблем організації системи інформаційної безпеки

Проблема	Причина	Наслідок
Зростання кіберзагроз	Висока мотивація зловмисників	Збільшення кількості атак
Недостатнє фінансування	Брак ресурсів на нові технології	Повільна адаптація до нових загроз
Низький рівень обізнаності	Відсутність регулярного навчання	Підвищений ризик через людський фактор
Слабкий моніторинг	Відсутність сучасних аналітичних інструментів	Повільне виявлення загроз
Недосконалість систем доступу	Використання слабких паролів	Несанкціонований доступ

Додаток Д

Таблиця 3.3. Основні функції системи SIEM Splunk Enterprise Security

Функція	Опис
Збір даних	Автоматичний збір логів з серверів, мережевих пристроїв та додатків
Аналіз подій	Кореляція подій для виявлення аномалій та загроз
Реагування	Генерація сповіщень та автоматичне виконання заходів захисту
Звітування	Створення звітів для аналізу ефективності системи

Додаток Е

Таблиця 3.4. Етапи реагування на інциденти інформаційної безпеки

Етап	Дії
Виявлення	Моніторинг та аналіз подій у режимі реального часу
Підтвердження	Перевірка достовірності загрози
Аналіз	Ідентифікація джерела загрози та оцінка її впливу
Нейтралізація	Зупинка атаки, ізоляція заражених систем
Відновлення	Відновлення роботи систем та перевірка даних
Звітування	Підготовка звіту для аналізу та подальшого вдосконалення

Додаток Ж

Таблиця 3.5. Результати тестування системи моніторингу

Тип інциденту	Виявлення (час, хвилини)	Реагування (час, хвилини)	Успішна нейтралізація (%)
Фішингові атаки	5	10	95
DDoS-атаки	3	8	90
Несанкціонований доступ	4	7	98

Як видно з таблиці, система виявляє загрози протягом перших 5 хвилин після початку інциденту та забезпечує їх швидке нейтралізування.

Додаток З

Таблиця 3.6. Стандартні операційні процедури реагування

Тип загрози	Ключові дії	Відповідальний підрозділ	Час реагування (хвилин)
Фішинг	Блокування листів, попередження користувачів	Відділ інформаційної безпеки	10
DDoS	Фільтрація трафіку, активація захисних правил	Відділ IT	8
Несанкціонований доступ	Блокування облікового запису, проведення аудиту	Відділ інформаційної безпеки	7

Додаток И

Таблиця 3.7. Приклад дорожньої карти:

Захід	Відповідальний	Термін виконання	Ресурси
Проведення аудиту поточної системи безпеки	Команда IT-безпеки	1 місяць	Консультанти, програмне забезпечення
Розробка політики безпеки	Команда IT-безпеки	2 місяці	Консультанти
Впровадження системи управління доступом	Команда IT-інфраструктури	3 місяці	Програмне забезпечення, обладнання

Додаток К

Таблиця 3.8. Рівні зрілості інформаційної безпеки за моделлю CMMI

Рівень	Характеристики	Приклад у «Нафтогаз України»
Початковий	Відсутність формалізованих процесів	Раніше залежало від індивідуальних рішень
Повторюваний	Процеси документовані, але виконуються вибірково	Часткова стандартизація політик доступу
Визначений	Формалізовані політики, але недостатня автоматизація	Є політики, але бракує автоматизованих рішень
Керований	Інтегровані процеси, автоматизований контроль	Часткова інтеграція з SIEM
Оптимізований	Постійне вдосконалення, використання прогнозного аналізу	Потребує впровадження інноваційних технологій

Додаток Л

Таблиця 3.9. Економічні показники впровадження моделі зрілості

Показник	До впровадження (млн грн)	Після впровадження (млн грн)	Економія (%)
Витрати на ліквідацію інцидентів	10	7	30
Витрати на впровадження систем	15	12	20
Вплив на репутацію	Негативний	Позитивний	-

Додаток М

Таблиця 3.10. Дорожня карта підвищення зрілості інформаційної безпеки

Етап	Діяльність	Термін виконання	Відповідальний
Впровадження SIEM	Інтеграція SIEM з усіма інформаційними системами	6 місяців	Відділ IT
Автоматизація	Використання інструментів AI для аналізу даних	12 місяців	Відділ безпеки
Навчання персоналу	Організація тренінгів з основ кібербезпеки	Постійно	HR-відділ
Інтеграція процесів	Включення безпеки у всі бізнес-процеси	18 місяців	Керівництво компанії
Прогнозний аналіз	Впровадження технологій для прогнозування потенційних загроз	24 місяці	Відділ аналітики

Додаток Н

Таблиця 3.11. Основні напрямки оптимізації інформаційної безпеки

Напрямок	Заходи	Очікуваний результат
Впровадження прогнозного аналізу	Інтеграція AI у системи моніторингу	Зниження кількості інцидентів на 25%
Підвищення обізнаності	Проведення тренінгів для співробітників	Зниження ризику через людський фактор на 30%
Інтеграція у бізнес-процеси	Розробка політик безпеки для всіх етапів діяльності	Підвищення стійкості до загроз
Модернізація технічних рішень	Оновлення SIEM та впровадження IDS/IPS	Підвищення ефективності виявлення загроз
Розвиток управління ризиками	Оцінка ризиків та розробка заходів для їх мінімізації	Зменшення ймовірності критичних інцидентів

Додаток П

Таблиця 3.12. Результати реалізації заходів оптимізації

Заходи	До впровадження	Після впровадження	Зміна (%)
Кількість інцидентів	58	42	-27
Час реагування на загрози (хвилин)	45	30	-33
Рівень задоволеності клієнтів (%)	85	92	+7
Витрати на ліквідацію інцидентів (млн грн)	10	7	-30