МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОЦІНКА ЗАГРОЗ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ”

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

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

_____ Данiїл СТРІКАНОВ
(*підпис)* *Ім’я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр. УБД 41
Данiїл СТРІКАНОВ

Керівник: Тетяна КАПЕЛЮШНА
К.е.н., доцент

Рецензент:
К.т.н., доцент Юрій ПЕПА

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Стріканову Даніїлу Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оцінка загроз цілісності інформації на підприємствах”

керівник кваліфікаційної роботи КАПЕЛЮШНА Тетяна, к.е.н., доцент
(Ім’я, ПРІЗВИЩЕ,науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “07” березня 2024 р. № 195.

2. Строк подання кваліфікаційної роботи “25” травня 2024р.
3. Вихідні дані до кваліфікаційної роботи: міжнародні стандарти, наукова та технічна література, методики управління ризиками, загрози та вразливості порушень інформаційної безпеки
4. Перелік питань, які мають бути розроблені:
   1. Загрози цілісності інформації на підприємстві.
   2. Проаналізувати загрози цілісності інформації на підприємстві
   3. Надати оцінку загроз та розробити рекомендації для збереження цілісності.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “22“ лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	19.03.2024	
2.	Збір та аналіз літератури.	25.03.2024	
3.	Визначення загроз цілісності інформації на підприємстві	08.04.2024	
4.	Аналіз загроз цілісності інформації на підприємства	22.04.2024	
5.	Проведення оцінки загроз та розробити рекомендації для збереження цілісності	09.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	14.05.2024	
7.	Оформлення роботи.	17.05.2024	
8.	Оформлення презентації.	19.05.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

здобувач вищої освіти _____ Данііл СТРІКАНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Стріканов Д.О до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оцінка загроз цілісності інформації на підприємствах "
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **СТРІКАНОВ Даніїл** за темою роботи опрацював достатній обсяг інформаційно-аналітичних, наукових матеріалів, що дозволило розкрити тему, досягти мети за поставленими завданнями. **СТРІКАНОВ Даніїл** продемонстрував вміння та навички систематизувати матеріал, аналізувати та робити висновки. Крім того, результати дослідження апробовані на конференції, що засвідчує їх значимість до використання на практиці.

Вищезазначене дозволяє відзначити роботу, як завершену, виконану здобувачем освіти **СТРІКАНОВИМ Даніїлом** на високому рівні, та, відповідно, оцінити на високий бал і присвоїти йому кваліфікацію "Бакалавр з кібербезпеки" за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Стріканов Д.О. допускається до захисту роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Стріканова Даніїла
на тему “Оцінка загроз цілісності інформації на підприємствах”

Актуальність. Використання інформації, збільшення обсягів її передачі, діджиталізація суспільства спричинила підвищення інтересу до її отримання та маніпулювання нею у цифровому середовищі. Зростають посягання на інформацію з боку кібершахраїв, а також конкурентів, при чому всі зацікавлені у отриманні вигоди за рахунок володіння нею, тому інтерес до отримання даних, витоку підвищується, актуалізуючи питання забезпечення її цілісності на підприємстві, на що націлено дослідження здобувача.

Позитивні сторони.

1. Послідовне та логічне викладення матеріалу з опрацюванням необхідної кількості джерел за темою засвідчують досягнення мети за сформульованими завданнями у роботі

2. Доцільним внеском у роботі є пропозиції щодо забезпечення цілісності інформації на підприємстві, які запропоновані на підставі попереднього визначення загроз цілісності інформації щодо об’єкту дослідження, а саме: схематично представлена пропозиція щодо ідентифікації потенційних загроз «Датагруп» з подальшим аналізом та управлінням потенційними загрозами і ризиками для забезпечення цілісності інформації на підприємстві.

Недоліки. Доцільно було б детальніше опрацювати питання щодо витоку конфіденційної інформації, з’ясувати причини несанкціонованого доступ до клієнтських даних, розуміти слабкі місця у захисті, проте це суттєво не впливає на загальну позитивну оцінку виконання роботи.

Висновок: Висновок: Кваліфікаційна робота виконана на належному науковому рівні, заслуговує позитивної оцінки, а здобувач Стріканов Даніїл Олегович заслуговує присвоєння кваліфікації “Бакалавр кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою”

Рецензент: _____ Юрій ПЕПА
к.т.н., доцент, завідувач кафедри робототехніки та технічних систем
підпис Ім’я, ПРІЗВИЩЕ

ЗМІСТ

ВСТУП

Актуальність теми. На сьогоднішній день інформаційні ресурси стають визначальним чинником у різних сферах суспільного життя, включаючи науку, техніку, виробництво та послуги. Значна частина цих ресурсів стає доступною для широкого загалу, сприяючи швидкому розповсюдженню знань та інформації.

Проте виникають ситуації, коли доступ до певних джерел інформації обмежений з різних причин. Це ставить перед суспільством виклики, пов’язані з класифікацією цих ресурсів, розробкою стратегій забезпечення їхньої доступності та визначенням ефективності та економічної доцільності заходів з охорони інформації на підприємствах. Такі аспекти вимагають системного аналізу та розробки ефективних стратегій управління інформаційними ресурсами для забезпечення їхньої цілісності та доступності.

У сучасному цифровому світі, де інформація перетворюється на ключовий ресурс, забезпечення цілісності інформації на підприємствах стає найважливішою складовою їхньої діяльності. Захист від загроз цілісності інформації стає стратегічним завданням для бізнесу будь-якої форми і розміру, оскільки від цього залежить не лише ефективність ведення ділових операцій, але і збереження довіри клієнтів, конфіденційності даних та репутації.

З огляду на постійне зростання кількості кіберзагроз і розвиток технологій, які можуть бути використані для порушення цілісності інформації, управління інформаційною безпекою стає завданням, що вимагає постійного аналізу, оновлення та вдосконалення. Така потреба посилюється не тільки з боку зловмисників, а й у зв’язку з конкурентним тиском на ринку та потребою в ефективному управлінні ризиками.

Мета роботи полягає у дослідженні та оцінці загроз цілісності інформації на підприємствах.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Провести огляд теоретичних положень щодо інформації на підприємствах та загроз, що порушують її цілісність.
2. Проаналізувати загрози цілісності інформації та її забезпечення на досліджуваному підприємстві.
3. Визначити методи для проведення оцінки загроз цілісності інформації на досліджуваному підприємстві.
4. Оцінити загрози та запропонувати рекомендації щодо їх упередження та забезпечення цілісності інформації на підприємстві.

Об’єкт та предмет дослідження. Об’єктом дослідження є процес оцінювання загроз цілісності інформації, а предметом – загрози цілісності інформації.

Для досягнення поставлених цілей було використано такі методи: аналіз системної вразливості для ідентифікації та оцінки потенційних загроз цілісності інформації на підприємствах; вивчення теорії інформаційної безпеки для аналізу методів та стратегій захисту інформації від загроз цілісності; методів теорії інформаційного протиборства для виявлення та аналізу потенційних загроз цілісності інформації на підприємствах.

Практичне значення отриманих результатів полягатиме у розробці конкретних і практично застосовних рекомендацій щодо забезпечення цілісності інформації на підприємствах. Ці рекомендації будуть ефективним інструментом для управління ризиками та збереження довіри клієнтів підприємства до його інформаційних ресурсів.

РОЗДІЛ 1
ЗАГРОЗИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

1.1. Інформація, її види, роль на підприємстві в сучасних умовах

В сучасному світі спостерігається стрімке зростання ролі інформації у всіх сферах життєдіяльності. Ця тенденція пов’язана з докорінними трансформаціями, спрямованими на підвищення якості життя людини та досягнення суспільного добробуту. Інформація стає одним із ключових ресурсів, визначаючи конкурентоспроможність та ефективність діяльності у будь-якій галузі.

Інформація – це сукупність даних, які мають певне значення або інтерпретацію. На підприємстві інформація відіграє ключову роль у прийнятті управлінських рішень, плануванні, аналізі результатів діяльності та спілкуванні як всередині організації, так і зовнішньо з клієнтами, партнерами та конкурентами.

Розглянемо термінологічне поняття слова «інформація». Слово «інформація» походить від латинського слова «informatio», що означає пояснення або уявлення про щось. Офіційне визначення терміну «інформація» закріплене у ст.1 Закону України «Про інформацію», де зазначено, що інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [29].

За «Економічним енциклопедичним словником», інформація – це властивість певних матеріальних систем, які можуть бути як живими організмами, так і економічними структурами, включаючи техніко-економічні та техніко-технологічні аспекти [12].

Науковці Клаус Ян Хоффман, Джеймс Глік, Клод Шеннон [39;40;44] визначають інформацію як нематеріальний ресурс, який виникає в результаті інтелектуальної, виробничої і суспільної діяльності людини та її взаємодії з

суспільством. Інформація може існувати у формі фактів, даних, знань, винаходів та їх комбінацій.З іншого погляду, інформація розглядається як властивість матерії відображати явища матеріального світу та сприяти збереженню та стійкості його структур у процесі розвитку.

Інформація має дві аспекти: кількісний та якісний. Згідно цього підходу, інформацію можна розділити на комерційно вигідну (якісну), яку можна монетизувати на ринку, та таку, яка не має комерційної цінності. Це означає, що кількість інформації, що має комерційну цінність, становить якісну основу, що у арифметичному розумінні може бути меншою за обсяг інформації, яка не має комерційної цінності для свого автора чи власника.

Сучасне суспільство переживає епоху, де обсяги інформації зростають геометрично, а її значення перевершує значимість інших ресурсів при управлінні. Оволодіння важливими даними стає ключовим чинником конкурентоспроможності для будь-якого суб'єкта господарювання, надаючи можливість оперативно реагувати на зміни у середовищі та бути на кроком попереду від конкурентів.

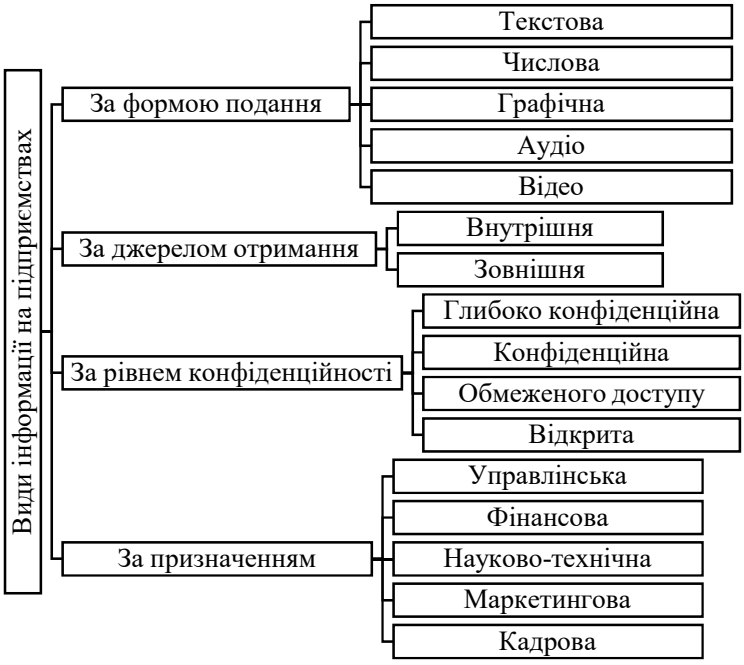

Рис. 1.1. Класифікація інформації на підприємствах

Джерело: складено за даними [18]

Інформацію можна класифікувати за декількома ознаками, включаючи форму представлення, джерело отримання, рівень конфіденційності та призначення.

Одним із ключових видів інформації є внутрішня та зовнішня інформація. Внутрішня інформація стосується даних, що знаходяться всередині підприємства, таких як фінансові звіти, виробничі дані, кадрова інформація тощо. Зовнішня інформація, натомість, охоплює дані, які надходять ззовні, такі як інформація про ринок, конкурентів, законодавство тощо.

Іншим важливим видом є структурована та неструктурована інформація. Структурована інформація має чітку організаційну форму, таку як таблиці, бази даних або документи з чітко визначеними розділами. Неструктурована інформація, навпаки, не має чіткої організації і може включати такі форми, як текстові документи, електронні листи, відео тощо.

Описані вище категорії інформації відображають різноманітність джерел та форматів даних, які використовуються на підприємстві і є важливими для ефективного управління та прийняття стратегічних рішень.

У сучасному світі розповсюдження інформації перетворилося на надзвичайно важливий процес, який безпосередньо залежить від технологічних засобів її передачі. Технологічні досягнення в сфері інформаційних технологій досягли таких висот, що вони суттєво впливають на світогляд споживачів.

З кожним роком зростає значення і роль інформації, а також методів та засобів її поширення, збереження та аналізу для сучасного суспільства. Практично, можливість впливати на свідомість людей через розповсюдження інформації стала не тільки ключовим елементом, а й нематеріальним активом, що може приносити конкретні матеріальні вигоди в умовах сучасного світу.

Це змінює роль інформації у суспільних відносинах. Розвиток інформаційних проектів, мереж та технічних засобів для відтворення інформації стає необхідним для ефективного функціонування суспільства. Це призводить до появи підприємств, які спеціалізуються на створенні комерційних проектів для

задоволення потреб споживачів у доступі до інформації.

Вибір споживача часто визначається сучасними тенденціями, які формуються під впливом інформації. Такі явища, як мода, культурні тенденції та увага до новітніх технологій, є результатом поширення інформації. У цьому контексті, сучасні мережеві технології відіграють значну роль у формуванні ефекту рою у віртуальних мережах, який виявляється через можливість зручного репосту та посилання на цікаву інформацію, що призводить до подвійного впливу на споживача, коли рекламне повідомлення, спочатку замовлене, потім починає активно розповсюджуватися серед звичайних користувачів мережі.

Це зростаюче явище електронної конкурентної боротьби за споживача відображається у виникненні нових інформаційних форм, що впливають на цінову політику та рекламні бюджети. Згідно з висновками вчених Г.А. Жовтяка та Д.О. Серьогіної [11], принципи ціноутворення на ринку доповнюються особливостями конкретного підприємства. Не дивлячись на зростаючі ціни, товар залишається привабливим для споживача завдяки можливостям інформаційно-комунікаційної взаємодії, що посилює його привабливість.

Потреба у передачі інформаційних даних, що мають велике значення, привела до появи блокчейн-платформ, що, за словами К.С. Жадька та інших дослідників[10], забезпечують споживачам нові можливості забезпечення безпеки та конфіденційності. Розвиток блокчейн-технологій визначив нові галузі господарської діяльності, зокрема, майнінг криптовалют, що вплинув на їх обіг, як зазначено С.В. Огіноком [25] та співавторами, і спричинив попит на криптобіржі та інтернет-обмінники, розширивши межі інтернет-торгівлі та зробивши доступ до інформації ще ціннішим для кінцевих споживачів.

Цей технологічний розвиток перевершує засоби фіксації, передачі та відтворення інформації, що робить інформацію ще більш доступною для споживачів на кожному етапі індустріальних революцій. Зростає комерційна цінність інформації, яка раніше не розглядалася як комерційно вигідна. У «Індустрії

4.0» вона може бути монетизована завдяки використанню сучасних технологій та ресурсів. В результаті цих змін змінюється соціальна роль створення, збереження, розповсюдження та відтворення інформації.

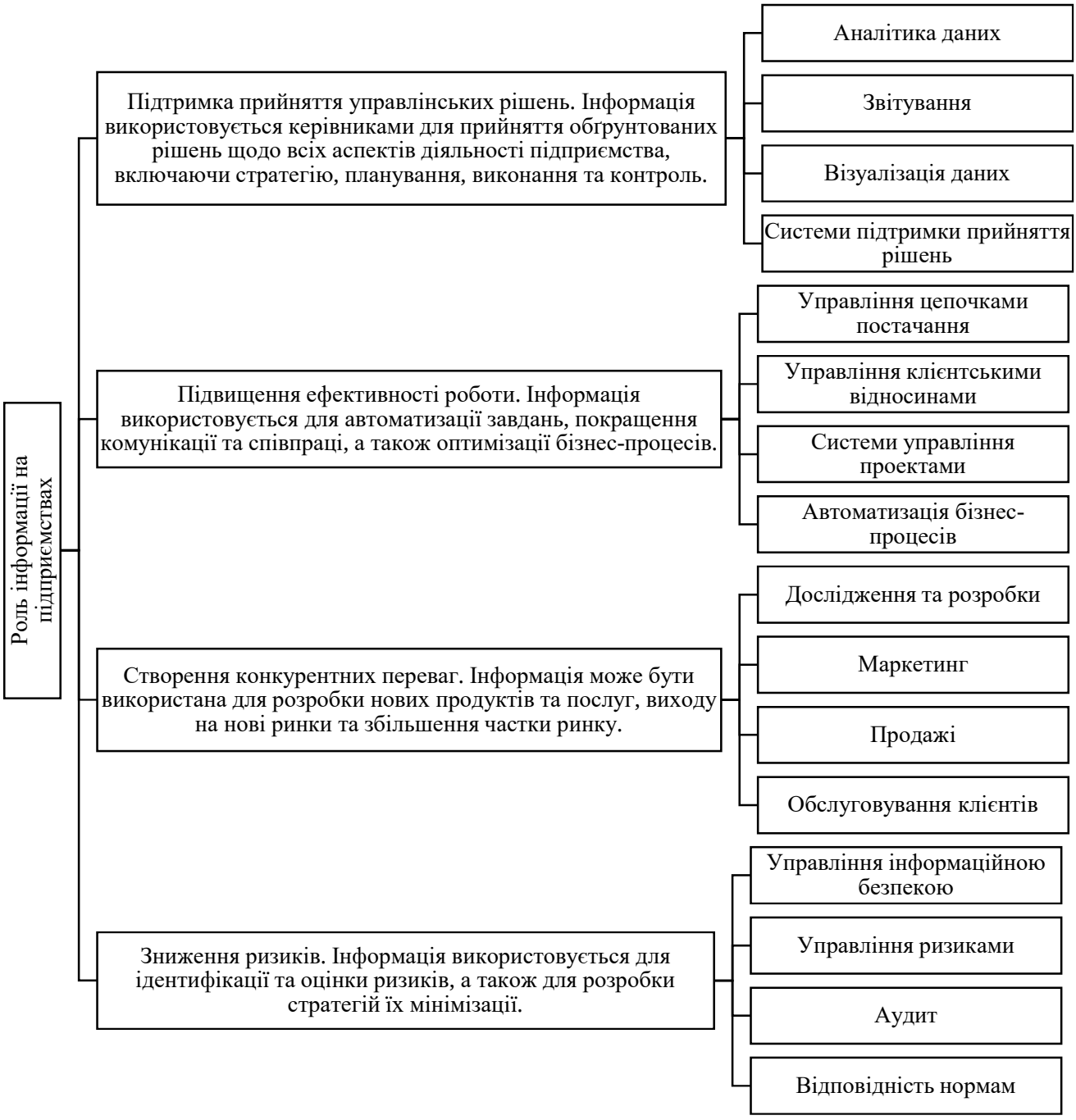

Рис. 1.2. Роль інформації на підприємствах

Джерело: складено автором на основі [10;11;25]

Отже, інформація виступає як ключовий ресурс для прийняття управлінських рішень, планування стратегій, аналізу ринкових тенденцій та взаємодії з клієнтами. Вона допомагає підприємствам збирати, зберігати, обробляти та аналізувати дані для досягнення своїх цілей. Правильне використання інформації може сприяти підвищенню продуктивності, зменшенню витрат та підвищенню конкурентоспроможності підприємства.

1.2. Загрози інформації на підприємстві та їх класифікація

Під системою захисту інформації в інформаційних системах розуміється комплексний набір правових норм, організаційних заходів та технічних, програмних та криптографічних засобів, спрямованих на забезпечення безпеки інформації відповідно до прийнятої політики інформаційної безпеки.

У контексті забезпечення безпеки інформації в інформаційних системах, такі системи цілком доцільно розглядати як єдиний комплекс, складений з трьох взаємопов’язаних компонентів:

Інформація – це компонент, що охоплює саму інформацію, яка потребує захисту, включаючи її конфіденційність, цілісність та доступність.

Технічні та програмні засоби – включає апаратне та програмне забезпечення, яке використовується для збереження, передачі та обробки інформації, а також для захисту її від несанкціонованого доступу або змін.

Обслуговуючий персонал і користувачі – компонент, що охоплює персонал, який відповідає за управління та експлуатацію інформаційних систем, а також користувачів, які мають доступ до інформації.

Забезпечення безпеки інформації в інформаційних системах має передбачати захист усіх цих компонентів від потенційних зовнішніх та внутрішніх загроз.

Вчені під загрозою безпеки інформації розуміють потенційні події, процеси

чи явища, які можуть призвести до нищівного впливу на інформацію, зокрема до її знищення, втрати цілісності, розголошення конфіденційності або обмеження доступності[1].

Загроза інформаційної безпеки – це потенційна можливість виникнення події, що може призвести до порушення конфіденційності, цілісності, доступності інформації або до зниження її цінності[24].

Загроза інформаційної безпеки – це сукупність обставин і факторів, що створюють небезпеку життєве важливим інтересам особистості, суспільства, держави в інформаційній сфері[7].

Рис.1.3. Загрози безпеці інформації у комп'ютерних системах

Джерело: складено автором на основі [1;7;24]

У забезпеченні безпеки інформації в інформаційних системах загрози поділяються на три основні класи: випадкові, навмисні, ненавмисні (рис.1.3).

Випадкові загрози є тими, що виникають не з навмисних дій зловмисників, а випадково у різні моменти часу. Ці загрози, за статистикою, призводять до найбільших втрат інформації, до 80%. Зазвичай вони виявляються у втратах, порушенні цілісності та доступності даних, а іноді можуть створювати передумови для навмисних дій.

Розглянемо основні випадкові загрози:

1. Стихійні лиха та аварії. Фізичне знищення інформаційних систем під час стихійних лих або аварій призводить до втрати даних або неможливості доступу до них.

2. Збої та відмови складних систем. Збої в роботі технічних засобів можуть призвести до знищення або спотворення даних та програм, порушення алгоритмів роботи системи.

3. Помилки під час розробки інформаційних систем. Помилки в програмному забезпеченні можуть призвести до різних наслідків, включаючи порушення безпеки.

4. Алгоритмічні і програмні помилки. Ці загрози виникають в результаті помилок у логіці програм або в їхньому виконанні, що може призвести до некоректної обробки даних чи витоку інформації.

5. Помилки користувачів і обслуговуючого персоналу. Недбале або неохайне виконання обов’язків може призвести до порушення конфіденційності інформації та компрометації системи безпеки[3].

Загалом, хоча ці загрози можуть мати серйозні наслідки, сучасні технології дозволяють ефективно протидіяти їм, включаючи розробку надійного програмного забезпечення, систему резервного копіювання даних та ефективний контроль користувачів та обслуговуючого персоналу.

Навмисні загрози безпеці інформації в наш час є недостатньо дослідженими і

постійно зростають за рахунок нових витоків. Ці загрози можуть класифікуватися за їхньою фізичною суттю і механізмами реалізації.

Серед навмисних загроз, що залишаються актуальними, є:

1.Традиційний шпіонаж та диверсії. Ці методи використовуються для отримання та знищення інформації, включаючи підслуховування, візуальне спостереження, крадіжку документів та програм, підкуп співробітників тощо. Сучасні технології дозволяють впроваджувати нові методи, наприклад, віддалене підслуховування за допомогою лазерного променя або радіосигналів.

2. Несанкціонований доступ до інформації визначається як отримання доступу до даних, що порушує встановлені правила та положення щодо розподілу доступу, використовуючи стандартні засоби комп'ютерної техніки та інформаційних систем. Ці правила визначаються для кожного користувача відповідно до його функціональних обов'язків, і їх виконання забезпечується через систему розподілу доступу.

Несанкціонований доступ до інформації може статися у наступних випадках:

- Відсутність системи розподілу доступу;
- Відмова або порушення роботи інформаційної системи;
- Помилкові дії користувачів або обслуговуючого персоналу;
- Помилки у системі розподілу доступу;
- Фальсифікація прав доступу[18].

Якщо система розподілу доступу відсутня, зловмиснику, який має відповідні навички у роботі з комп'ютерними системами, може бути доступна необмежена кількість інформації у системі. Також можливі несанкціоновані доступи через збої та відмови в роботі інформаційної системи, а також через помилки користувачів чи персоналу. Зловмисник може також використовувати виявлені в системі розподілу доступу помилки для несанкціонованого доступу до інформації. Фальсифікація прав доступу є одним із найбільш ймовірних шляхів несанкціонованого доступу до інформації.

3. Електромагнітне випромінювання і наводки є невід’ємною частиною процесу обробки та передачі інформації за допомогою технічних засобів інформаційних систем. Це явище полягає у випромінюванні електромагнітних хвиль у навколишнє середовище та появі електричних сигналів у лініях зв’язку, сигналізації та інших елементах. Це феномен відомий як побічне електромагнітне випромінювання та наводки[20].

За допомогою спеціального обладнання можна приймати, виділяти та підсилювати сигнали, які потім можна записувати або аналізувати. Електричні сигнали, що наводяться у провідниках, також можуть бути виділені та зафіксовані за допомогою віддаленого обладнання, розташованого на відстані сотень метрів від джерела сигналу.

Зловмисники можуть отримувати інформацію, використовуючи також метод «прочісування» інформаційних сигналів у мережі електроживлення технічних пристроїв інформаційних систем. Це можливо завдяки магнітному зв’язку між трансформаторами підсилювача та випрямляючого трансформатора, або через падіння напруги на внутрішньому опорі джерела живлення під час проходження струмів підсилення інформаційних сигналів. Якщо фільтрація випрямного пристрою недостатня, то інформаційні сигнали можуть бути виявлені у мережі живлення.

Несанкціонована модифікація структур представляє серйозну загрозу безпеці інформації в інформаційних системах, оскільки може торкнутися алгоритмів, програмних та технічних структур системи на будь-якому її етапі життєвого циклу.

Процес внесення несанкціонованих змін у структуру інформаційної системи під час її розробки чи модернізації часто називають "закладкою". Ці втручання, як правило, виконуються у спеціалізованих системах, і вони можуть залишатися непоміченими завдяки високій кваліфікації їхніх авторів і складності сучасних інформаційних систем.

Алгоритмічні, програмні і апаратні «закладки» можуть бути використані для

різноманітних цілей, включаючи безпосередню шкідливу дію на систему або створення можливості для неконтрольованого доступу до неї. Шкідливі ефекти «закладок» можуть спрацьовувати при отриманні відповідних команд ззовні або при настанні певних подій у системі, таких як активація певного режиму роботи чи досягнення певного часу роботи.

«Люки» – це програмні або апаратні «закладки», які призначені для створення можливості неконтрольованого доступу до програми або для використання привілейованих режимів роботи, таких як режими операційної системи. Вони можуть обходити засоби захисту інформації та використовуватися для несанкціонованого отримання доступу до системи.

Шкідливі програми становлять одне з основних джерел загрози безпеці інформації в інформаційних системах, і вони відомі під загальною назвою «віруси». Ці програми поділяються на чотири основні класи (див. рис.1.4), в залежності від їхнього механізму дії.

Перший клас – «логічні бомби», які складаються з програм або їх частин, що перебувають у системі і активуються лише при певних умовах, таких як певна дата або специфічні події.

Другий клас – «черв'яки», це програми, які активуються при кожному завантаженні системи і можуть переміщатися в системі або мережі, розповсюджуючись і створюючи копії, що може призвести до перенавантаження системи.

Третій клас – «троянські коні», це програми, які вносяться в користувацькі програми шляхом явних змін або додавання команд. При наступному виконанні цих програм, окрім зазначених функцій, вони виконують також несанкціоновані дії.

Четвертий клас – «комп’ютерні віруси», які самостійно розповсюджуються шляхом створення копій і виконують негативні дії при відповідних умовах.

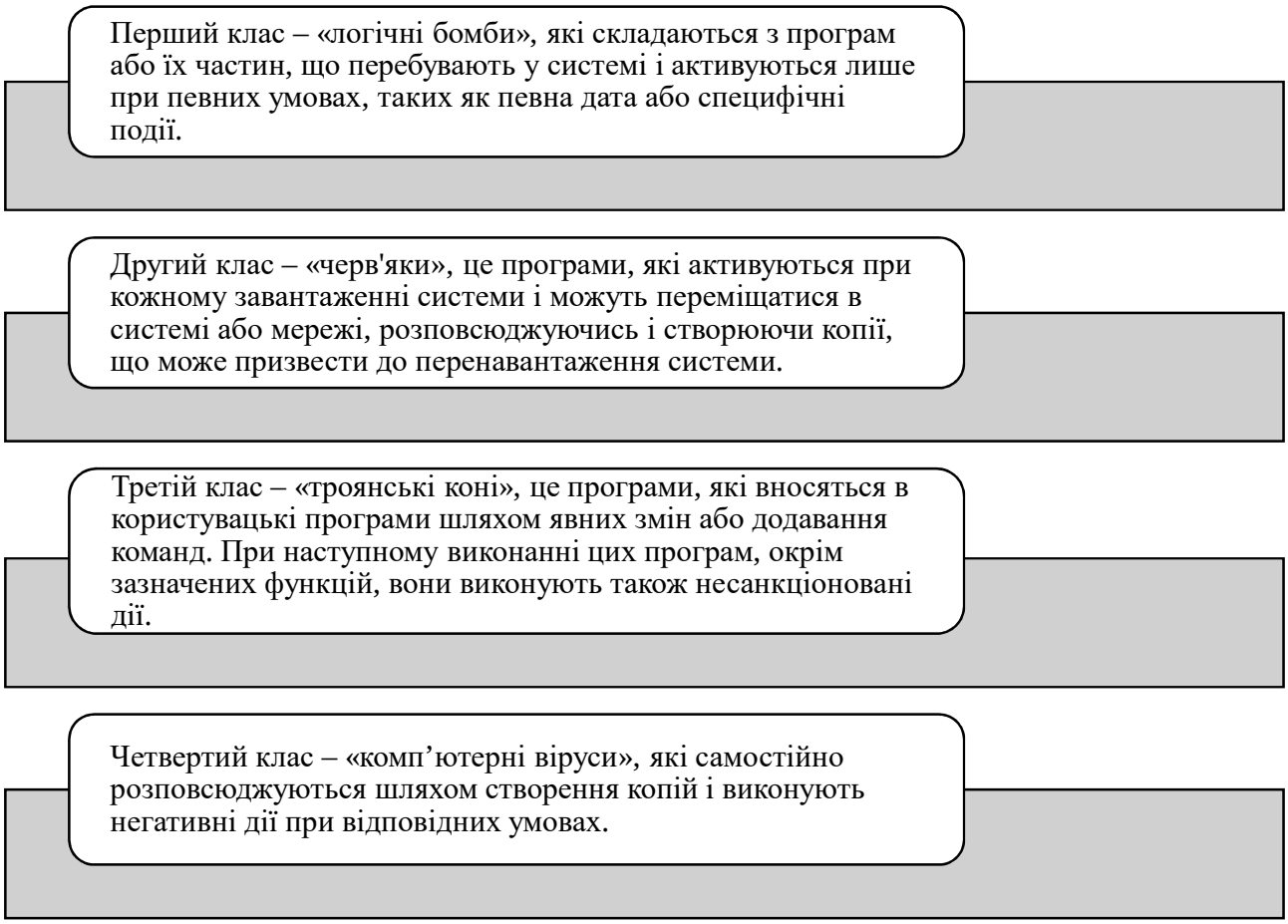

Рис.1.4. Основні класи шкідливих програм, що становлять загрози інформації

Джерело: складено автором на основі [17;31]

Враховуючи те, що властивості вірусів притаманні усім класам шкідливих програм, то часто всі ці програми в побуті називають вірусами.

Загрози інформації на підприємстві можуть бути досить різноманітними та потенційно небезпечними. Їх класифікація (див. рис.1.4) важлива для правильного розуміння та управління ризиками, які вони становлять. Нижче наведено деякі загальні категорії загроз інформації на підприємствах:

1. Кібератаки. Ця категорія включає в себе широкий спектр загроз, таких як віруси, черви, троянці, шпигунське програмне забезпечення та інші форми

зловмисного програмного забезпечення. Кібератаки можуть призвести до незаконного доступу до конфіденційної інформації, її пошкодження або втрати.

2. Соціальний інжиніринг. Цей вид загрози використовує маніпуляцію та обман, щоб отримати доступ до конфіденційної інформації. Наприклад, фішингові атаки, де нападники видають себе за довірених осіб або організації, щоб отримати доступ до облікових записів або інших конфіденційних даних.

3. Внутрішня загроза – загрози, які виникають зсередини самого підприємства. Це можуть бути навмисні або ненавмисні дії співробітників, які призводять до витоку конфіденційної інформації або її недоступності.

4. Фізичні загрози – загрози, пов’язані з фізичним доступом до обладнання або інфраструктури підприємства. Наприклад, крадіжки комп’ютерів або інших пристроїв, пожежі, повені або інші природні катастрофи.

5. Ненавмисні помилки. Ця категорія включає помилки, які роблять співробітники, наприклад, випадкове видалення даних або надсилання конфіденційної інформації не тим людям.

6. Відмови обладнання та програмного забезпечення. Навіть найсучасніші системи можуть вийти з ладу, що може призвести до втрати даних або простою в роботі.

7. Стихійні лиха. Пожежі, повені та інші стихійні лиха можуть серйозно пошкодити обладнання та інфраструктуру, що призведе до втрати даних та простою в роботі.

8. Застарілі технології. Використання застарілих технологій може зробити підприємства більш уразливими до кібератак та інших загроз.

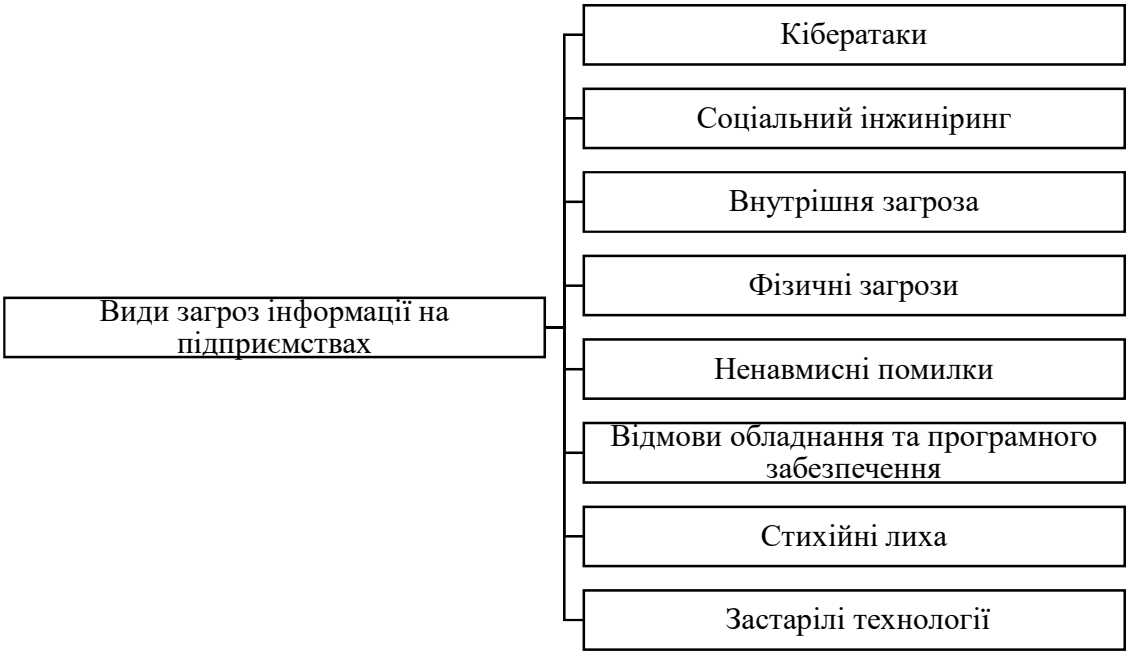

Рис.1.5. Категорії загроз інформації на підприємствах

Джерело: складено на основі [18;20]

Класифікація цих загроз (рис.1.5) допомагає підприємствам розуміти їхню природу та вплив, що вона може мати, та розробляти відповідні заходи забезпечення інформаційної безпеки.

Аналізуючи загрози безпеки інформації на підприємстві та їх класифікацію, стає очевидним, що ретельне розуміння цих загроз дозволяє підприємствам адекватно реагувати на них. Класифікація загроз на випадкові, навмисні, ненавмисні надає базову рамку для аналізу ризиків.

Випадкові загрози, такі як стихійні лиха та аварії, можуть призвести до фізичного знищення інформаційних систем, тоді як навмисні загрози, такі як традиційний шпіонаж та викрадання даних, можуть використовуватися для цілеспрямованого нападу на підприємство.

Ретельний моніторинг і вдосконалення заходів безпеки є ключем до запобігання та виявлення таких загроз. Додатково, освіта персоналу стосовно

безпеки даних і впровадження ефективних процедур можуть допомогти зменшити наслідки інформаційних загроз на підприємстві.

1.3. Цілісність інформації: сутність, загрози, забезпечення, захист

Цілісність інформації є одним із ключових аспектів безпеки даних та інформаційних систем. Вона визначається як стан, коли дані залишаються недоторканими, невикривленими та невиробленими.

Сутність інформації означає, що дані зберігаються та передаються без будь-яких неправомірних або непередбачуваних змін у їх змісті, форматі чи значенні. Однак загрози цілісності інформації можуть виникати з різних джерел та мати різні характеристики. Ці загрози включають в себе можливість зміни або викривлення даних, введення помилкових або шкідливих даних, а також непередбачені помилки чи дефекти програмного забезпечення.

Збереження цілісності інформації стає набагато складнішим у відкритих мережевих середовищах, де дані можуть бути відкриті для доступу зовнішнім користувачам.

Забезпечення цілісності інформації вимагає впровадження різноманітних заходів технічного та організаційного характеру. До таких заходів відносяться використання методів контролю цілісності даних, застосування криптографічних методів, регулярна перевірка та аудит систем, а також освіта персоналу стосовно питань безпеки інформації.

Загалом, забезпечення цілісності інформації є невід'ємною складовою системи захисту даних і вимагає постійного моніторингу та вдосконалення підходів до безпеки.

Загрози цілісності інформації можуть мати різноманітні форми і проявлятися з різних джерел. Одна з таких загроз полягає в недбалому або зловмисному

втручанні в дані під час їх передачі через мережу. Це може призвести до їх зміни або викривлення. Іншою загрозою є введення помилкових або шкідливих даних в систему, що може виникнути через недостатній контроль прийому даних або вразливості програмного забезпечення. Наприклад, зловмисники можуть впровадити в систему програми-шкідливі «троянці», які змінюють або видаляють дані, що може спричинити порушення цілісності.

Крім того, випадкові помилки або дефекти програмного забезпечення також можуть призвести до порушення цілісності даних, оскільки вони можуть призвести до непередбачуваних змін у даних або їх втрати. Такі загрози стають особливо серйозними в умовах швидкого розвитку технологій та зростання складності інформаційних систем, тому необхідно постійно вдосконалювати методи захисту та вживати заходів для попередження таких ситуацій.

Цілісність інформації є ключовим аспектом інформаційної безпеки, оскільки вона визначає, що інформація залишається точною, цілісною і недоступною для несанкціонованих змін чи втрати. У цьому підрозділі ми детально розглянемо сутність цілісності інформації, загрози, які загрожують її цілісності, а також методи забезпечення та захисту цілісності інформації.

Отже, цілісність інформації визначається як стан, у якому інформація залишається недоторканною і не зазнає несанкціонованих змін, модифікацій або втрат. Це означає, що інформація має залишатися вірною, достовірною та незмінною протягом усього її життєвого циклу.

Загрози цілісності інформації включають в себе всі види небажаних подій або дій, спрямованих на зміну, викривлення або втрату інформації. Ці загрози можуть бути викликані як зовнішніми, так і внутрішніми факторами, включаючи кібератаки, випадкові помилки, а також зловмисні дії співробітників.

Для забезпечення цілісності інформації необхідно використовувати широкий спектр технологій, політик і процедур. Це включає в себе регулярні резервні копії, застосування криптографічних методів, встановлення прав доступу та моніторинг

системи. Існує ряд методів (див. рис.1.6), які можна використовувати для забезпечення цілісності інформації, включаючи:

– Контроль доступу – обмеження доступу до інформації авторизованим користувачам.

– Шифрування – захист даних від несанкціонованого доступу та зміни за допомогою шифрування.

– Резервне копіювання – створення резервних копій даних, які можна використовувати для відновлення у разі втрати чи пошкодження.

– Контроль журналів – відстеження доступу до даних та внесених змін.

– Аудит – регулярний перегляд систем та процесів для виявлення потенційних загроз тощо.

Методи забезпечення цілісності інформації	Контроль доступу – обмеження доступу до інформації авторизованим користувачам.
	Шифрування – захист даних від несанкціонованого доступу та зміни за допомогою шифрування.
	Резервне копіювання – створення резервних копій даних, які можна використовувати для відновлення у разі втрати чи пошкодження.
	Контроль журналів – відстеження доступу до даних та внесених змін.
	Аудит – регулярний перегляд систем та процесів для виявлення потенційних загроз тощо.

Рис.1.6. Методи забезпечення цілісності інформації

Джерело: створено автором на основі [5;8]

Захист цілісності інформації полягає в запобіганні, виявленні та відновленні від будь-яких загроз, що можуть поставити під загрозу її цілісність. Це може включати в себе встановлення сучасних систем виявлення вторгнень, моніторинг

активності користувачів та швидке відновлення після інцидентів.

Забезпечення цілісності інформації включає в себе різноманітні заходи, спрямовані на збереження інформації у відповідному та недоторканому стані. Це може включати регулярне оновлення програмного забезпечення, встановлення ефективних систем захисту, які перешкоджають несанкціонованому доступу та змінам інформації, а також впровадження проактивних стратегій, які попереджають можливі загрози.

Щодо захисту цілісності інформації, основною метою є запобігання будь-яким несанкціонованим змінам чи втратам інформації. Це досягається шляхом використання сучасних методів аутентифікації та авторизації, моніторингу систем на предмет виявлення надмірної активності, регулярного аудиту інформаційних систем, а також реалізації стратегій екстреного відновлення після інцидентів.

Забезпечення та захист цілісності інформації на підприємствах вимагає комплексного підходу, що враховує як технологічні, так і організаційні аспекти. Він має бути постійною пріоритетною задачею для керівництва та IT-відділів підприємства з метою запобігання великим втратам даних та інших негативних наслідків, пов’язаних із порушенням цілісності інформації.

Важливо зосередитися на практичних аспектах впровадження методів забезпечення цілісності інформації у контексті конкретного підприємства. Нижче представлено ключові моменти, які слід врахувати, а саме:

1) Аналіз ризиків. Проведення ретельного аналізу ризиків для ідентифікації притаманних підприємству загроз цілісності інформації. Це допоможе визначити пріоритетні напрямки для впровадження заходів захисту.

2) Впровадження політики та стандартів. Розробка та впровадження чіткої політики безпеки інформації, яка описує правила та процедури захисту цілісності даних. До політики також повинні додаватися стандарти, що визначають конкретні технічні та організаційні вимоги щодо захисту інформації.

3) Використання технічних засобів захисту. Впровадження технічних

засобів захисту, таких як програмне забезпечення для шифрування, антивірусні програми, брандмауери та системи контролю доступу.

4) Застосування організаційних заходів. Реалізація організаційних заходів, таких як навчання персоналу з питань інформаційної безпеки, проведення регулярних аудитів та тестування на проникнення.

5) Підтримка актуального стану систем. Забезпечення постійного оновлення програмного забезпечення, операційних систем та обладнання для виправлення відомих загроз.

Захист цілісності інформації на підприємстві потребує комплексного підходу, який включає не лише впровадження заходів безпеки, а й постійний моніторинг та удосконалення цих заходів. При цьому важливо врахувати такі ключові аспекти:

– Створення культури інформаційної безпеки. Важливо сформувати на підприємстві культуру інформаційної безпеки, коли всі співробітники усвідомлюють важливість захисту інформації та знають, як правильно використовувати системи та дані.

– Регулярний моніторинг та тестування. Необхідно проводити регулярний моніторинг систем та даних для виявлення потенційних загроз та уразливостей. Також слід проводити регулярні тестування на проникнення для перевірки ефективності заходів безпеки.

– Управління інцидентами. Розробка та впровадження чіткої процедури реагування на інциденти інформаційної безпеки. Це допоможе мінімізувати збитки та швидко відновити роботу у разі виникнення інформаційних інцидентів.

– Постійне навчання та удосконалення. Важливо забезпечувати постійне навчання та удосконалення знань та навичок персоналу з питань інформаційної безпеки. Це допоможе їм залишатися в курсі нових загроз та ефективно захищати інформацію[16].

Крім загальних методів, описаних вище, для забезпечення цілісності

інформації на підприємствах рекомендується вжити таких заходів, як:

– Впровадження системи управління інформаційною безпекою (СУІБ) на основі міжнародних стандартів, таких як ISO 27001. СУІБ дозволяє систематизувати підхід до захисту інформації, визначити чіткі ролі та відповідальність, а також встановити контрольні процедури.

– Використання технологій захисту даних, таких як криптографічні алгоритми, електронний цифровий підпис та електронний документообіг. Ці технології дозволяють забезпечити автентичність, цілісність та конфіденційність даних та ін.

– Важливо підкреслити, що захист цілісності інформації – це неперервний процес, який потребує постійної уваги та зусиль.

– Цілісність інформації – це один із трьох китів інформаційної безпеки, поряд з конфіденційністю та доступністю. Вона гарантує, що інформація залишається актуальною, тобто відповідає своєму автентичному стану, не була несанкціоновано змінена, видалена чи пошкоджена[20].

Отже, загрози цілісності інформації, такі як зловмисні атаки, віруси та помилки користувачів, відображають постійно зростаючу складність сучасного інформаційного середовища. Забезпечення цілісності інформації вимагає комплексного підходу, що включає в себе технологічні, організаційні та правові заходи. Важливо визначити критичні активи та інформаційні ресурси підприємства для ефективного захисту. Організації повинні активно вдосконалювати свої заходи захисту відповідно до зростаючих загроз і використовувати сучасні технології та стандарти безпеки, такі як ISO/IEC27001[48], для забезпечення цілісності інформації. Крім того, навчання персоналу та постійне аудитування процесів захисту інформації є важливими компонентами стратегії забезпечення цілісності інформації на підприємстві. Результативне впровадження заходів захисту допомагає підприємствам не лише запобігти втратам даних, але й зберегти свою

репутацію та впевненість клієнтів у безпеці їхньої інформації.

Висновки до першого розділу

У першому розділі були розглянуті теоретичні засади цілісності інформації, загрози, які їй можуть нашкодити та методи забезпечення та захисту.

Зокрема, було визначено, що цілісність інформації – це одна з трьох основних властивостей інформаційної безпеки, яка гарантує, що інформація залишається необхідною, тобто відповідає своєму автентичному стану.

Було ідентифіковано основні категорії загроз цілісності інформації на підприємствах, до яких належать кібератаки, соціальний інжиніринг, внутрішні загрози, фізичні загрози, ненавмисні помилки, відмови обладнання та програмного забезпечення, стихійні лиха та застарілі технології.

Для забезпечення цілісності інформації рекомендується використовувати такі методи, як контроль доступу, шифрування, резервне копіювання, контроль журналів та аудит.

Захист цілісності інформації – це комплексне завдання, яке потребує використання різних методів та підходів. Важливо мати чітку політику безпеки інформації та впроваджувати відповідні технічні та організаційні заходи.

Крім того, важливо постійно підвищувати знання співробітників про загрозу цілісності інформації та навчити їх правильно використовувати системи та дані.

Важливо пам’ятати, що цілісність інформації – це не статична властивість, а постійний процес, який потребує постійної уваги та зусиль.

Враховуючи специфіку підприємства, рекомендується провести детальний аналіз загроз цілісності інформації та на його основі розробити індивідуальні рекомендації щодо удосконалення системи захисту.

Впровадження заходів, описаних у цьому розділі, допоможе підприємствам забезпечити цілісність інформації та захистити її від різноманітних загроз.

РОЗДІЛ 2
АНАЛІЗ ЗАГРОЗ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

2.1. Загальний огляд підприємства та його інформаційного середовища

ПРАТ «ДАТАГРУП», код ЄДРПОУ 31720260, було зареєстровано 29.10.2001. Розмір статутного капіталу компанії складає 210 709 275,00.

Керівником підприємства ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ДАТАГРУП» є Шелема Михайло Васильович.

Організаційно-правова форма фірми - АКЦІОНЕРНЕ ТОВАРИСТВО. Основний вид діяльності (КВЕД) – 61.10 Діяльність у сфері проводового електрозв'язку.

Контактна інформація компанії ПРАТ «ДАТАГРУП»

Телефон: +380445380008 +380445380037

Підприємство зареєстрована за юридичною адресою Україна, місто Київ, вул. Бродських Сім'ї[26].

«ДАТАГРУП» – це всеукраїнський постачальник послуг зв'язку для бізнесу та дому. Для компанії немає неможливого в сегментах передачі даних і доступу в інтернет, телефонії, відео-конференцій і відеоспостереження, супутникового зв'язку і хмарних рішень.

Телеком-рішення компанії забезпечують надійний зв'язок не тільки для корпоративного, міжоператорського і домашнього сегментів. Нам довіряють розробку і впровадження інновацій представники державного сектора і оборонних структур. Сьогодні ми забезпечуємо електронними комунікаційними послугами абонентів у більш ніж 90 населених пунктах України.

Компанія зростаємо і розвивається разом з клієнтами – за 20 років плідної співпраці добре вивчили потреби і побажання всіх сегментів і стали одним з

провідних гравців на ринку електронних комунікаційних послуг України. Сьогодні у компанії розробляють оптимальні рішення для підвищення ефективності бізнесу і комфорту користувачів.

Датагруп – це український провайдер телекомунікаційних послуг, який пропонує широкий спектр послуг, включаючи:

– Інтернет-доступ. Датагруп пропонує фіксований та мобільний інтернет-доступ для приватних та бізнес-користувачів.

– Телефонія. Датагруп пропонує фіксовану та мобільну телефонію для приватних та бізнес-користувачів.

– Телебачення. Датагруп пропонує кабельне та IPTV-телебачення для приватних користувачів.

– Хмарні послуги. Датагруп пропонує широкий спектр хмарних послуг, включаючи хостинг, віртуальні машини, резервне копіювання даних та багато іншого.

– Центри обробки даних. Датагруп володіє та оперує мережею центрів обробки даних по всій Україні[26].

Датагруп – це один із провідних постачальників телекомунікаційних послуг в Україні. Датагруп має розгалужену мережу, яка охоплює всю Україну. Мережа компанії включає:

1) Оптична волоконна мережа. Датагруп володіє однією з найдовших оптичних волоконних мереж в Україні.

2) Центри обробки даних. Датагруп володіє та оперує мережею центрів обробки даних по всій Україні.

3) Системи безпеки. Датагруп використовує найсучасніші системи безпеки для захисту своїх мереж та даних.

Датагруп використовує інформаційні системи для автоматизації багатьох бізнес-процесів.

Датагруп має широкий спектр інформаційних активів, включаючи[26]:

– Дані про клієнтів. Датагруп зберігає велику кількість даних про своїх клієнтів, включаючи їхні імена, адреси, номери телефонів та інформацію про їх рахунки.

– Фінансові дані. Датагруп зберігає фінансові дані про свої доходи, витрати та активи.

– Дані про співробітників. Датагруп зберігає дані про своїх співробітників, включаючи їх імена, адреси, номери телефонів та інформацію про їхню заробітну плату.

– Інтелектуальна власність. Датагруп має значну кількість інтелектуальної власності, включаючи патенти, авторські права та торгові марки.

– Інформаційні активи. Датагруп є цінними для компанії та потребують захисту від загроз.

– Датагруп займається обслуговуванням доступу до банківських сервісів.

Компанія «ДАТАГРУП» є провідним оператором зв’язку та інтернет-провайдером в Україні. Вона пропонує широкий спектр послуг зв’язку для корпоративних та приватних клієнтів. Інформаційне середовище «ДАТАГРУП» включає в себе інформаційні системи, бази даних, мережеві засоби та інші інфраструктурні компоненти, які використовуються для надання послуг зв’язку.

2.2. Аналіз загроз інформації та її цілісності на підприємстві

Загрози цілісності інформації на підприємстві «ДАТАГРУП» можуть включати технічні атаки на інфраструктуру мережі, програмні помилки, витоки конфіденційної інформації, а також вплив зовнішніх чинників, таких як природні лиха та регуляторні зміни в сфері телекомунікацій.

Аналізуючи інформацію зі звіту компанії «ДАТАГРУП», можна виокремити деякі потенційні загрози цілісності інформації на даному підприємстві[26].

Кібератаки та витоки даних – кібератаки, спрямовані на інформаційні системи «ДАТАГРУП». Ці атаки можуть призвести до витоку конфіденційної інформації та порушення цілісності даних.

Технічні помилки та вразливості в інформаційних системах, які можуть бути використані для атак з метою порушення цілісності даних.

Підприємство може бути під загрозою від природних катастроф, таких як повені, пожежі або землетруси, які можуть спричинити фізичне знищення інфраструктури та втрату даних.

Зміни в законодавстві або регуляторні обмеження можуть мати вплив на збереження та обробку даних на підприємстві, що вплине на їхню цілісність.

Аналіз цих потенційних загроз допоможе підприємству «ДАТАГРУП» розробити ефективні стратегії захисту та управління ризиками для забезпечення цілісності своєї інформації.

Основними завданнями забезпечення інформаційної безпеки Датагруп є:

Захист інформаційних активів Датагруп від зовнішніх та внутрішніх навмисних та ненавмисних загроз. Це включає захист від кібератак, внутрішніх загроз, людських помилок, фізичних загроз, стихійних лих та інших загроз.

Впровадження та забезпечення ефективного функціонування системи управління інформаційною безпекою. Це включає розробку та впровадження політик та процедур інформаційної безпеки, проведення навчання співробітників, моніторинг та аудит систем безпеки та реагування на інциденти інформаційної безпеки.

Попередження, виявлення та усунення загроз безпеки Датагруп, причин та умов, які призводять до матеріальних втрат. Це включає використання засобів захисту інформації, моніторинг мереж та систем, розслідування інцидентів інформаційної безпеки та впровадження заходів щодо попередження повторення

подібних інцидентів.

Забезпечення безперервної та надійної роботи інформаційних систем Датагруп. Це включає резервне копіювання даних, відновлення після збоїв, управління ризиками та планування спадкоємності.

Створення умов для зменшення негативного впливу наслідків порушення вимог інформаційної безпеки Датагруп. Це включає розслідування інцидентів інформаційної безпеки, визначення причин та умов, що призвели до інциденту, та впровадження заходів щодо попередження повторення подібних інцидентів.

Управління інформаційною безпекою Датагруп на основі ризик-орієнтованого підходу, ідентифікація та оцінювання ризиків. Це включає ідентифікацію потенційних загроз, оцінку їх ймовірності та впливу, а також впровадження заходів щодо зниження ризиків.

Координація діяльності всіх працівників Датагруп, визначення ролей та обов’язків щодо управління та забезпечення інформаційної безпеки Датагруп. Це включає призначення відповідальних осіб за інформаційну безпеку, розробку та впровадження політик та процедур інформаційної безпеки, а також проведення навчання співробітників.

Навчання та підвищення кваліфікації працівників Датагруп у сфері інформаційної безпеки. Це включає проведення тренінгів, семінарів та інших заходів з питань інформаційної безпеки, а також розповсюдження інформаційних матеріалів.

Забезпечення мінімізації комплаєнс-ризиків, сприяння мінімізації ризиків операційної діяльності Датагруп. Це включає дотримання законодавства та нормативних актів у сфері інформаційної безпеки, а також впровадження заходів щодо зниження ризиків, пов’язаних з операційною діяльністю компанії[14].

Підприємство «Датагруп» здійснює систематичний аналіз загроз та забезпечує цілісність інформації на основі комплексного підходу до управління інформаційною безпекою. Однією з ключових структур управління є комітет із

захисту інформації, який регламентується відповідним положенням та має за собою голову – заступника голови правління, що відповідає за інформаційну безпеку. Комітет визначає та впроваджує політику і стратегію інформаційної безпеки, а також забезпечує контроль за впровадженням нових проектів та стратегічних завдань у цій сфері.

Окремою складовою управління інформаційною безпекою є підрозділ ризик-менеджменту, який відповідає за розробку ризик-апетиту та моніторинг показників ризиків. Цей підрозділ забезпечує контроль над наближенням показників ризику до встановлених лімітів та вживає заходів для попередження їх порушень.

Працівники «Датагруп» мають знати та виконувати вимоги нормативно-правових актів з питань інформаційної безпеки, сприяти попередженню та виявленню інцидентів, а також вживати всіх можливих заходів безпеки для запобігання втратам і збиткам[14].

Партнери та постачальники «Датагруп» також зобов’язані виконувати договірні вимоги та внутрішні нормативні документи компанії з питань інформаційної безпеки та сприяти розслідуванню інцидентів, що виникають під час виконання договорів.

Управління захистом інформації на «Датагруп» відповідає за впровадження та підтримку засобів захисту ресурсів, розробку та впровадження вимог щодо налаштувань безпеки інформаційних систем, а також забезпечує ефективність функціонування систем управління ключовими даними.

Забезпечення інформаційної безпеки на підприємстві «Датагруп» базується на наступних фундаментальних засадах:

Мінімальність повноважень. Доступ до інформаційних ресурсів обчислювальної мережі «Датагруп» має бути обмежений лише необхідними повноваженнями для виконання службових завдань. Це забезпечує обмеження ризиків в разі можливого несанкціонованого доступу[14].

Явне санкціонування дій. Дії працівників «Датагруп», що не передбачені

внутрішніми розпорядчими чи нормативними документами, заборонені. Це сприяє уникненню неправомірної діяльності та зменшує ризики безпеки.

Законність. Система управління інформаційною безпекою на «Датагруп» враховує вимоги чинного законодавства України та міжнародних нормативних вимог у галузі інформаційної безпеки.

Узгодженість. Цілі та завдання інформаційної безпеки на "Датагруп" відповідають стратегічним цілям та завданням компанії.

Єдність. Управління інформаційною безпекою є невід'ємною частиною управління підприємством «Датагруп».

Ефективність. Засоби захисту інформаційних ресурсів впроваджуються відповідно до їх критичності та рівня ризику, заснованого на оцінці ризику та управлінні ним.

Практичність. Засоби захисту інформаційних ресурсів мають бути практичними і підтримувати баланс між працездатністю та захищеністю інформаційних систем.

Безперервність. Інформаційна безпека є неперервним процесом, спрямованим на протидію загрозам та управління ризиками на підприємстві «Датагруп».

Відповідальність. Керівництво, працівники, постачальники та інші треті сторони, які мають доступ до інформаційних ресурсів «Датагруп», повинні дотримуватися вимог нормативно-правових актів та нести персональну відповідальність за їх виконання.

Принцип постійного удосконалення. Забезпечення інформаційної безпеки передбачає постійний контроль, виявлення та усунення негативних факторів та постійне покращення системи захисту.

Комплексність та системність. Інформаційна безпека забезпечується на різних рівнях та включає в себе всі аспекти управління операційною діяльністю та інформаційними технологіями «Датагруп».

Загрози, які були виявлені впродовж 2021-2023 рр. на ведено у таблиці 2.1.

Таблиця 2.1

Виявлені загрози у ПрАТ «Датагруп» у 2021-2023 роках[14]

Роки	Загрози	Інформація
2021	1.Кібератака на мережеву інфраструктуру	Напад на системи маршрутизації та комутації даних.
	2. Фішингові атаки	Спроби отримати доступ до конфіденційної інформації через маскування як легітимний запит.
	3. Витік конфіденційної інформації	Несанкціонований доступ до клієнтських даних через слабкість у захисті
2022	1.DDoS-атаки	Збої в роботі мережевих сервісів через масовані атаки з перевантаження мережевого трафіку
	2.Витік конфіденційної інформації	Несанкціонований доступ до конфіденційної інформації через внутрішні джерела.
	3. Соціальний інжиніринг	Використання маніпуляції та обману для отримання конфіденційних даних
2023	1. Витік даних через необережне використання USB-пристроїв	Втрата чутливої інформації через використання зовнішніх пристроїв.
	2. Фізичний доступ до серверних приміщень	Потенційний доступ до конфіденційних даних через фізичні засоби.
	3. Відмова відповідності регулятивним вимогам	Порушення правил і вимог щодо обробки та зберігання конфіденційної інформації.

Так, у таблиці 2.1 наведено огляд потенційних загроз, які стали відомі на підприємстві «Датагруп» протягом трьох останніх років. Ці загрози включають кібератаки, витік конфіденційної інформації, фішингові атаки, DDoS-атаки, а також ризики, пов'язані з необережним використанням зовнішніх пристроїв та фізичним доступом до серверних приміщень. Аналіз цих загроз важливий для розроблення ефективних заходів безпеки, спрямованих на захист цілісності інформації підприємства. Наявність високоякісних заходів безпеки допоможе зменшити ризики та забезпечити надійний захист від потенційних загроз. Однак важливо постійно вдосконалювати заходи безпеки, враховуючи постійно зростаючий характер кіберзагроз та вдосконалювання методів атак.

2.3. Забезпечення цілісності інформації на підприємстві

Для забезпечення цілісності інформації «ДАТАГРУП» використовує сучасні методи захисту даних, включаючи шифрування, мережеві фаєрволи, системи виявлення вторгнень та регулярне навчання персоналу з питань кібербезпеки. Крім того, компанія дотримується відповідних стандартів та регуляторних вимог щодо захисту інформації.

ДАТАГРУП отримала Атестат від Державної служби спеціального зв’язку та захисту інформації України (див. Додаток А) та гарантує високий рівень захисту вузла інтернет-доступу для своїх клієнтів[26]. Підтвердженням наявності комплексної системи захисту інформації оператора є Атестат відповідності КСЗІ ІТС захищеного вузла інтернет-доступу, який відповідає вимогам нормативних документів, що регулюють технічний захист інформації в Україні. Відповідно до вимог РНБО державним органам, підприємствам, установам і організаціям державної форми власності заборонено укладати договори й закуповувати послуги доступу до мережі Інтернет у постачальників електронних комунікаційних послуг, у яких відсутні документи, що підтверджують відповідність системи захисту інформації встановленим вимогам щодо захисту інформації.

ДАТАГРУП має сертифікат відповідності вимогам стандарту ISO 27001 (див. Додаток Б), який підтверджує, що організована в компанії система управління інформаційною безпекою (СУІБ) відповідає всім вимогам міжнародного стандарту ISO/IEC 27001:2013 у наступних сферах діяльності[26]:

- управління інформаційними активами з питань надання клієнтам хмарних сервісів,
- надання доступу до мережі Інтернет та каналів зв'язку,
- надання послуг контакт-центру,
- розробки та підтримки програмного забезпечення.

Відповідність вимогам стандарту ISO 27001 гарантує ефективний менеджмент і підтверджує високу якість надаваних послуг із забезпечення конфіденційності, цілісності та доступності інформації. Це особливо важливо для замовників різних електронних та комунікаційних послуг та IT послуг, які працюють з персональними даними клієнтів, зокрема банків.

Цільова аудиторія:

1. Споживачі, визначені у «Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям», затвердженому постановою Кабінету Міністрів України від 11 жовтня 2002 року № 1519, та які є бюджетними установами відповідно до пункту 12 частини першої статті 2 Бюджетного кодексу України.

2.Державні органи отримують доступ до Інтернету через систему захищеного доступу до Інтернету Державного центру кіберзахисту, через постачальників електронних комунікаційних мереж, які мають захищені вузли доступу до Інтернет із створеними комплексними системами захисту інформації (КСЗІ) з підтвердженою відповідністю. (п.9 Постанови КМУ №518 від 19.06.2019)

3.Об’єкти критичної інформаційної інфраструктури повинні підключатися до Інтернету через тих постачальників електронних комунікаційних мереж, які мають захищені вузли доступу до Інтернет із створеними комплексними системами захисту інформації (КСЗІ) з підтвердженою відповідністю.

4.Інші юридичні особи та фізичні особи-підприємці для забезпечення захищеного доступу до мережі Інтернет[14].

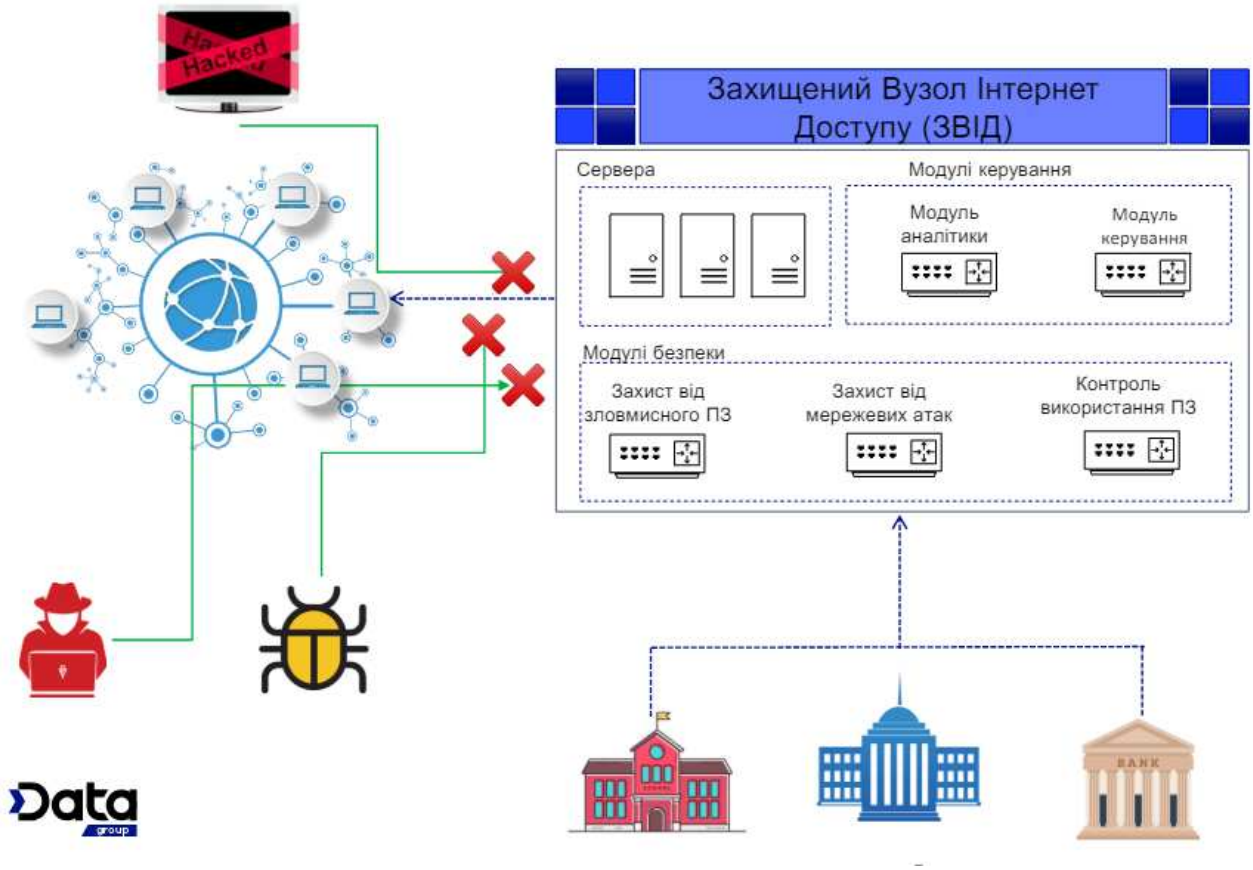

Рис.2.1. Захищений Вузол Інтернет Доступу (ЗВІД) [14]

Наприклад, працівникам Компанії А необхідно передати інформацію в Компанію Б через мережу Інтернет, то Компанія А може бути певна, що інформація не буде перехоплена або модифікована на шляху, який захищає ЗВІД.

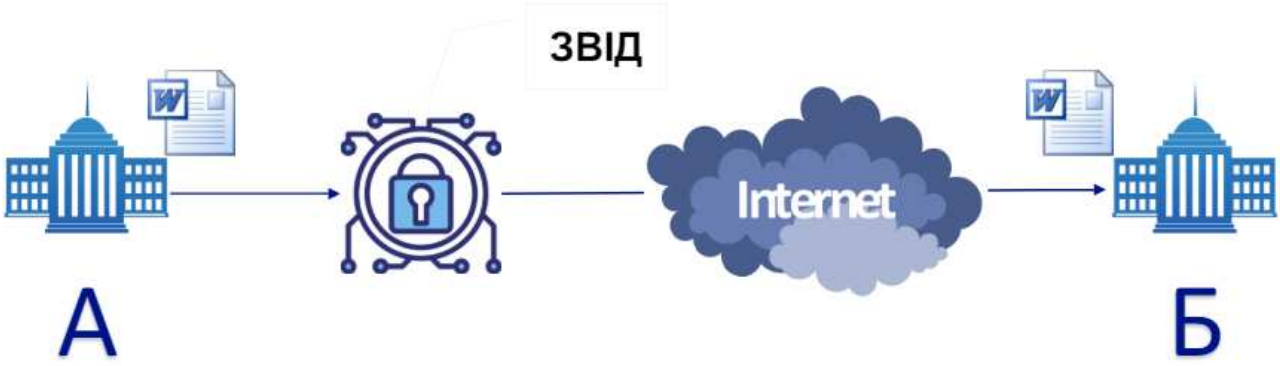

Рис.2.2. Як працює ЗВІД для споживачів[14]

Компанія «Датагруп», як провідний оператор зв’язку для бізнесу, успішно розробила та впровадила сучасну хмарну інфраструктуру (IaaS) в Європі. Недавно оголошено про повноцінний запуск цього сервісу в Франкфурті-на-Майні, де він уже демонструє високу ефективність.

Публічна хмара Євроклауд із центром у сучасному німецькому дата-центрі, що відповідає високим вимогам рівня сертифікації TIER IV і має необхідні сертифікати міжнародного стандарту ISO, заслуговує на визнання.

Компанія «Датагруп» є одним з провідних постачальників хмарних рішень в Україні та виступає в ролі зручного клауд-агрегатора для своїх клієнтів. Вона пропонує широкий спектр хмарних рішень – як локальні, так і міжнародні, що враховують індивідуальні потреби бізнесу клієнтів.

Крім того, компанія надає конвергентні рішення для клієнтів державного сектора, що підтверджені високим ступенем захищеності атестатом КСЗІ (ДССЗЗІУ) та ISO:27001.

На європейському ринку компанія співпрацює з партнерськими Cloud провайдерами Deac (Латвія), а також з глобальними міжнародними гігантами: Microsoft AZUR, Google Cloud.

Використання сервісу побудови віртуальної інфраструктури на базі публічної хмари Євроклауд дозволяє клієнтам вирішувати низку стратегічно важливих завдань, таких як: мінімізація ризиків втрати даних через бойові дії в Україні, швидке розширення хмарної інфраструктури з урахуванням бізнес-потреб та оптимізація капітальних витрат на ІТ-інфраструктуру.

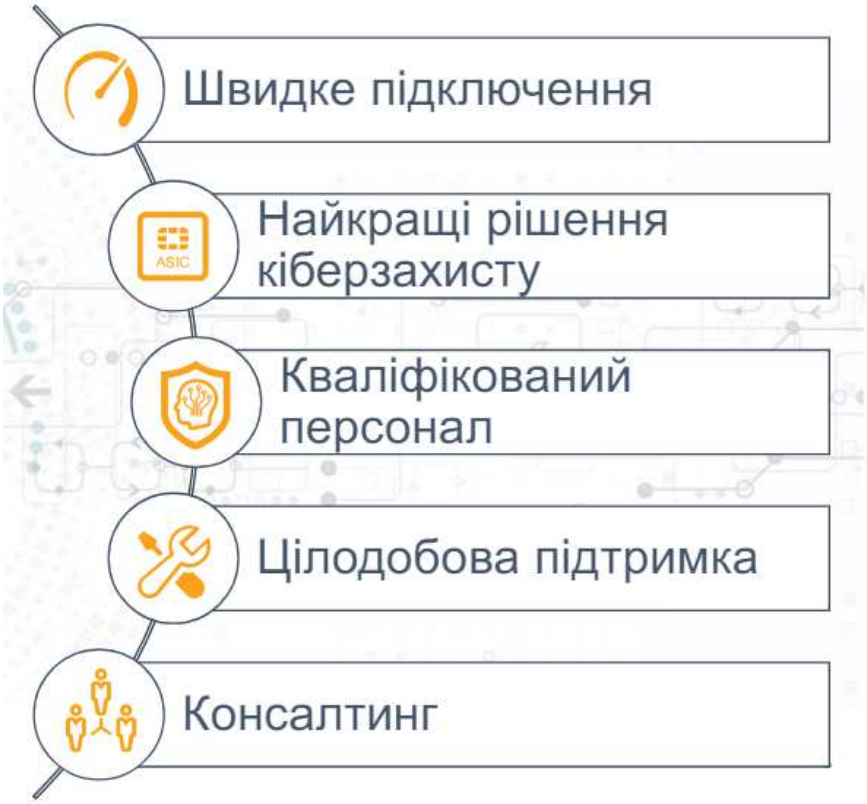

Рис.2.3. Переваги «ЗВІД – ДАТАГРУП»

Джерело: Datagroup Presentation[14]

Основні цілі забезпечення інформаційної безпеки на підприємстві «Датагруп» включають наступні властивості інформації:

1. Конфіденційність – ця властивість інформації гарантує, що доступ до неї можуть отримати лише авторизовані користувачі та процеси. Інформація залишається недоступною для несанкціонованих осіб та процесів.

2. Цілісність – інформація зберігає свою цілісність, що означає, що вона не може бути модифікована несанкціонованими користувачами або процесами. Дані залишаються непорушеними і не зазнають втручання без відповідного дозволу.

3. Спостережність – дає можливість фіксувати діяльність користувачів та процесів, що використовують інформацію, а також забезпечує можливість

однозначно ідентифікувати осіб, які здійснювали певні дії. Це дозволяє встановлювати відповідальність за вчинені дії та запобігати порушенням політики безпеки.

4. Недоступність – властивість системи, що забезпечує безперервну доступність інформації для авторизованих користувачів та процесів. Система забезпечує доступ до ресурсів у відповідності з встановленими правилами безпеки без зайвої затримки, забезпечуючи продуктивну діяльність підприємства.

Вказані цілі допомагають забезпечити безпеку інформації на підприємстві «Датагруп» та запобігти можливим загрозам її цілісності та конфіденційності.

Забезпечення інформаційної безпеки в Датагруп передбачає створення наступного ряду послідовних рівнів захисту інформаційних ресурсів та персоналу (див. рис.2.4):

1. Організаційно-правовий рівень. Визначення нормативно-правових вимог і зобов’язань персоналу, користувачів інформаційних ресурсів та контрагентів Датагруп щодо інформаційної безпеки.

2. Фізичний рівень захисту. Запобігання несанкціонованому фізичному доступу, пошкодженню та вторгненню до приміщень Датагруп та обладнання.

3. Рівень прикладного програмного забезпечення. Забезпечення безпеки взаємодії з користувачем інформаційних систем.

4. Рівень системи управління базами даних. Зберігання та оброблення даних з врахуванням вимог безпеки.

5. Рівень операційної системи. Забезпечення безпечного та надійного обслуговування програмного забезпечення та систем управління базами даних.

6. Рівень мережі. Забезпечення безпеки взаємодії між вузлами інформаційної системи Датагруп[14].

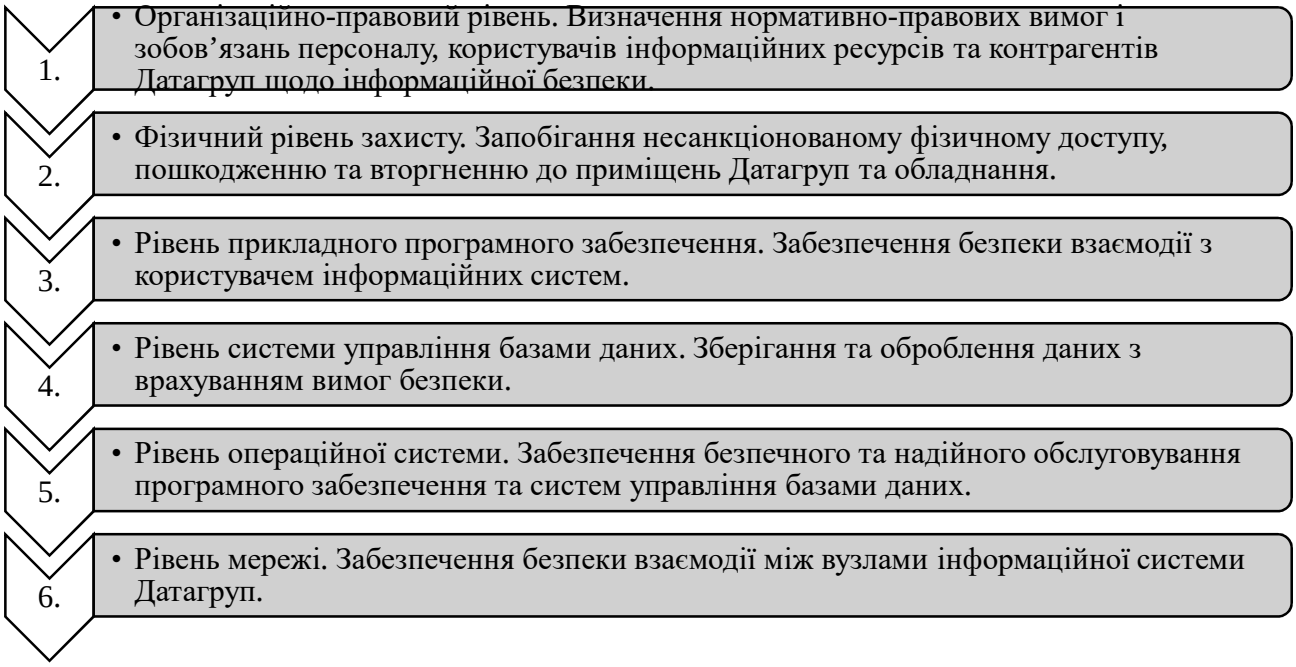

Рис. 2.4. Рівні захисту інформаційних ресурсів на підприємстві Датагруп

Джерело: складено автором на основі даних підприємства[14]

Ця схема ілюструє послідовні рівні захисту інформаційних ресурсів на підприємстві Датагруп, що охоплюють організаційно-правовий рівень, фізичний рівень захисту, рівень прикладного програмного забезпечення, рівень системи управління базами даних, рівень операційної системи та рівень мережі.

Кожен рівень відповідає за певний аспект безпеки та виконує конкретні заходи для забезпечення цілісності інформаційних ресурсів на підприємстві.

Принципи інформаційної безпеки повинні бути вбудовані у всі аспекти управління операційною діяльністю та інформаційними технологіями Датагруп для забезпечення найвищого рівня захисту даних та інформаційних ресурсів.

Усвідомлення та забезпечення цілісності інформації є критичним завданням для ефективної функціональності підприємства. Ретельне впровадження описаних заходів дозволяє забезпечити надійний та стійкий рівень захисту інформації, що є важливим аспектом успішної діяльності підприємства.

Висновки до другого розділу

Встановлено, що підприємство «Датагруп» є провідним українським постачальником послуг зв’язку для бізнесу та дому. Заснована в 2001 році, компанія пропонує широкий спектр телекомунікаційних послуг, включаючи інтернет-доступ, телефонію, телебачення, хмарні послуги та центри обробки даних. «Датагруп» володіє великою мережею центрів обробки даних по всій Україні.

За двадцять років своєї діяльності компанія набула довіру клієнтів та стала одним з провідних гравців на ринку електронних комунікаційних послуг України, розвиваючи оптимальні рішення для підвищення ефективності бізнесу та комфорту користувачів.

В ході загального огляду підприємства та його інформаційного середовища було виявлено ключові складові та особливості, що впливають на цілісність інформації. Це дозволило визначити основні напрямки дослідження загроз цілісності інформації на підприємстві.

Аналіз загроз інформації та її цілісності на підприємстві показав, що існують різноманітні потенційні загрози, що можуть порушити цілісність інформаційних ресурсів. Визначення цих загроз дозволяє розробити ефективні заходи захисту та запобігання можливим інцидентам.

Забезпечення цілісності інформації на підприємстві вимагає комплексного підходу, який включає в себе не лише технічні заходи захисту, але й організаційні та процедурні аспекти. Впровадження такого підходу дозволить забезпечити стабільність та надійність інформаційного середовища підприємства.

Результати аналізу дають підстави для подальшого удосконалення системи захисту інформації та забезпечення цілісності даних на підприємстві з метою зменшення ризиків інцидентів та підвищення рівня довіри стейкхолдерів.

РОЗДІЛ 3
ОЦІНКА ЗАГРОЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

3.1. Методи оцінки загроз цілісності інформації підприємства

Цілісність інформації є однією з ключових складових захисту даних на підприємствах. Для забезпечення цілісності інформації необхідно регулярно оцінювати загрози, які можуть вплинути на її стан. Існують різні методи для оцінки загроз цілісності інформації, які можна застосувати в залежності від специфіки підприємства. Оцінка ризику є частиною основних елементів управління ризиками, визначених у ISO 31000, якими є:

− спілкування та консультації;

− встановлення контексту;

− оцінка ризику (ідентифікація ризику, аналіз ризику);

− запобігання ризику;

− моніторинг та огляд.

«Оцінка ризику – це загальний процес ідентифікації ризику, аналізу та оцінки ризику» (ISO 31010) [42]. Ризик можна оцінити на будь-якому рівні операцій або цілей компанії. Існує 31 метод оцінки ризику, перерахований у Додатку B ISO/IEC 31010. Нижче розглянемо основні з них:

1. Аналіз ризиків (Risk Assessment)

Аналіз ризиків є одним з найбільш поширених методів оцінки загроз. Він включає в себе ідентифікацію потенційних загроз, вразливостей, а також оцінку можливих наслідків і ймовірності їх виникнення. Для проведення аналізу ризиків використовуються різні методики, зокрема:

Кількісний аналіз ризиків – оцінка вартісного еквівалента можливих втрат від

реалізації загроз.

Якісний аналіз ризиків – суб’єктивна оцінка загроз на основі експертних суджень і досвіду.

2. SWOT-аналіз.

SWOT-аналіз (Strengths, Weaknesses, Opportunities, Threats) дозволяє виявити сильні і слабкі сторони підприємства, а також можливості та загрози, які можуть впливати на цілісність інформації. Цей метод допомагає зрозуміти, де саме знаходяться вразливості і які заходи можуть бути ефективними для їх усунення.

3. Метод дерева відмов (Fault Tree Analysis, FTA)

Метод дерева відмов використовується для візуалізації та аналізу можливих причин відмов системи. Він допомагає визначити основні фактори, які можуть вплинути на цілісність інформації, і оцінити їх ймовірність.

4. Метод аналізу впливу на бізнес (Business Impact Analysis, BIA).

BIA дозволяє оцінити потенційний вплив різних загроз на бізнес-процеси підприємства. Цей метод допомагає визначити критичні процеси і системи, від яких залежить цілісність інформації, і розробити стратегії їх захисту.

5. Аудит інформаційної безпеки.

Аудит інформаційної безпеки включає в себе перевірку і оцінку існуючих засобів захисту інформації на підприємстві. В рамках аудиту проводяться такі заходи:

– Огляд політик і процедур безпеки.

– Тестування систем і мереж на наявність вразливостей.

– Оцінка відповідності стандартам і нормативам (наприклад, ISO/IEC 27001).

6. Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

Методологія OCTAVE дозволяє підприємству самостійно провести оцінку ризиків і визначити заходи для їх мінімізації. Вона включає в себе три фази:

1) Ідентифікація критичних активів та загроз.

2) Оцінка вразливостей і розробка плану дій.

3) Впровадження заходів з управління ризиками[34].

7. Методи кількісного та якісного аналізу загроз

Кількісні методи – оцінка ймовірності виникнення загроз і потенційних збитків у числовому вигляді.

Якісні методи – використання експертних оцінок, сценарного аналізу і SWOT-аналізу для визначення загроз і їх впливу на підприємство.

Далі розглянемо більш детально кожен з наведених вище методів оцінки загроз.

Аналіз ризиків (Risk Assessment) є систематичним процесом, який використовується для виявлення, оцінки і управління ризиками, що можуть вплинути на цілісність інформації на підприємстві. Оцінка ризиків включає кілька основних етапів, кожен з яких важливий для ефективного управління ризиками.

Етапи аналізу ризиків включають:

1.Ідентифікація ризику

Мета – виявити всі можливі ризики, які можуть вплинути на цілісність інформації.

Методи: огляд документації, експертні опитування, аналіз минулих інцидентів, брейнштормінг.

Приклад. На підприємстві можна використовувати аналіз журналів доступу до систем, щоб ідентифікувати можливі загрози несанкціонованого доступу до інформації.

2.Аналіз ризику

Мета – оцінити ймовірність виникнення і можливі наслідки ідентифікованих ризиків.

Методи: кількісний аналіз (наприклад, обчислення очікуваних збитків) і якісний аналіз (наприклад, побудова матриці ризиків).

Приклад. Використання моделі «Ймовірність-Наслідки» для оцінки ризиків несанкціонованого доступу до конфіденційної інформації на підприємстві.

3.Оцінка ризику

Мета – визначити рівень ризиків і пріоритетність їх усунення або зменшення.

Методи: встановлення допустимих рівнів ризику, класифікація ризиків за рівнем критичності.

Приклад. Встановлення критичного рівня ризику для доступу до фінансових даних, що вимагає негайного впровадження додаткових заходів захисту.

4.Запобігання ризику

Мета – розробка і впровадження заходів для усунення або мінімізації ризиків.

Методи: впровадження політик безпеки, технічних засобів захисту, навчання персоналу.

Приклад. Встановлення багатофакторної аутентифікації для доступу до критичних систем підприємства.

5.Моніторинг та огляд

Мета – постійний контроль за рівнем ризиків і ефективністю впроваджених заходів.

Методи: регулярні аудити, моніторинг систем безпеки, перегляд політик безпеки.

Приклад. Щоквартальні перевірки систем безпеки і оновлення політик доступу до інформації на підприємстві.

Далі розглянемо детальніше метод оцінки SWOT-аналіз, який є стратегічним інструментом, що дозволяє оцінити внутрішні та зовнішні фактори, які впливають на цілісність інформації підприємства. Цей метод допомагає ідентифікувати сильні та слабкі сторони організації, а також можливості та загрози, які можуть впливати на інформаційну безпеку.

Визначимо основні етапи проведення SWOT-аналізу:

1)Ідентифікація сильних сторін (Strengths)

Мета – визначити внутрішні переваги підприємства, які сприяють забезпеченню цілісності інформації[32].

Приклад. На ПРАТ «Датагруп» сильними сторонами можуть бути наявність кваліфікованого персоналу з кібербезпеки, використання сучасних технологій захисту даних, наявність розроблених політик і процедур інформаційної безпеки.

2)Ідентифікація слабких сторін (Weaknesses)

Мета – виявити внутрішні недоліки, які можуть становити загрозу для цілісності інформації.

Приклад. Відсутність регулярних тренінгів для персоналу з кібербезпеки, недостатнє фінансування заходів інформаційної безпеки, застаріле програмне забезпечення.

3)Виявлення можливостей (Opportunities)

Мета – визначити зовнішні фактори, які можуть бути використані для покращення інформаційної безпеки.

Приклад. Впровадження нових технологій захисту даних, участь у міжнародних програмах з кібербезпеки, співпраця з іншими підприємствами для обміну досвідом.

4)Виявлення загроз (Threats)

Мета – визначити зовнішні фактори, які можуть негативно вплинути на цілісність інформації.

Приклад. Зростання кіберзлочинності, регуляторні зміни, які вимагають додаткових заходів захисту, поява нових вразливостей в програмному забезпеченні.

Приклад проведення SWOT-аналізу на ПРАТ «Датагруп» наведено нижче:

-Сильні сторони:

Сучасні технології шифрування даних.

Досвідчений персонал з кібербезпеки.

Впроваджені політики інформаційної безпеки.

-Слабкі сторони:

Недостатнє фінансування на навчання персоналу.

Відсутність регулярних аудитів інформаційної безпеки.

-Можливості:

Впровадження нових технологій, таких як блокчейн, для захисту даних.

Партнерство з іншими компаніями для обміну найкращими практиками.

-Загрози:

Зростання кількості кібератак.

Регуляторні вимоги, які постійно змінюються.

Метод дерева відмов (Fault Tree Analysis, FTA) є графічним методом аналізу, який використовується для ідентифікації та оцінки потенційних причин відмов системи. Цей метод допомагає виявити основні фактори, які можуть призвести до порушення цілісності інформації, і визначити їх взаємозв’язки.

Етапи проведення методу дерева відмов включають:

1)Визначення верхнього рівня події (Top Event).

Мета – визначити основну подію, яка представляє собою порушення цілісності інформації.

Приклад. Втрата цілісності конфіденційних даних на сервері підприємства.

2)Ідентифікація основних подій (Basic Events).

Мета – визначити основні причини, які можуть призвести до виникнення верхнього рівня події.

Приклад. Неавторизований доступ до сервера, помилки в програмному забезпеченні, фізичне пошкодження обладнання.

3)Побудова логічних воріт (Logical Gates)

Мета – визначити логічні взаємозв’язки між основними подіями.

Приклад. Використання «AND» та «OR» воріт для побудови взаємозв'язків між подіями.

4)Аналіз і оцінка ризиків.

Мета – оцінити ймовірність виникнення основних подій і їх вплив на верхню

подію.

Методи. Кількісний аналіз (наприклад, обчислення ймовірності відмови) і якісний аналіз (визначення критичних подій).

Приклад використання методу дерева відмов на ПРАТ «Датагруп» може включати:

Визначення верхнього рівня події – втрата цілісності даних клієнтів.

Ідентифікація основних подій:

– Неавторизований доступ до бази даних.

– Збій в системі резервного копіювання.

– Зловмисне програмне забезпечення.

Побудова логічних воріт:

– Використання «AND» воріт для поєднання подій, які повинні статися одночасно для втрати цілісності даних.

– Використання «OR» воріт для подій, будь-яка з яких може призвести до втрати цілісності.

Аналіз і оцінка ризиків:

– Кількісний аналіз ймовірності кожної події.

– Якісний аналіз впливу кожної події на загальну безпеку даних[32].

Отже, метод дерева відмов дозволяє виявити основні причини, які можуть призвести до порушення цілісності інформації, і визначити їх взаємозв'язки. Це допомагає підприємству розробити ефективні заходи для запобігання таким подіям і забезпечення високого рівня інформаційної безпеки.

Один із методів, який також використовується для оцінки загроз, є метод аналізу впливу на бізнес (Business Impact Analysis, BIA). Цей метод дозволяє виявити критичні бізнес-процеси та оцінити потенційні наслідки від їх порушення, що допомагає в розробці ефективних заходів для забезпечення безперервності бізнесу.

Метод аналізу впливу на бізнес (Business Impact Analysis, BIA). BIA є систематичним процесом, який використовується для виявлення і оцінки наслідків переривання бізнес-процесів. Цей метод дозволяє визначити критичні бізнес-функції, ресурси, необхідні для їх виконання, і час, який необхідний для їх відновлення після інциденту. BIA допомагає організаціям зрозуміти, які процеси є найбільш важливими для їх виживання та розвитку, і які ресурси потрібно захищати найпершими[33].

Етапи проведення BIA наступні:

1.Підготовка до аналізу

Мета – визначити цілі та обсяг аналізу, призначити відповідальних осіб.

Приклад. Створення робочої групи з представників різних відділів компанії для проведення BIA, встановлення чітких цілей і задач аналізу.

2.Визначення критичних бізнес-процесів

Мета – виявити процеси, які є ключовими для безперервної роботи організації.

Приклад. Визначення процесів, таких як обробка замовлень, підтримка клієнтів, бухгалтерія, які є критичними для діяльності компанії.

3.Оцінка впливу на бізнес

Мета – оцінити наслідки для організації у випадку порушення критичних процесів.

Приклад. Аналіз фінансових втрат, втрати репутації, зниження продуктивності у випадку збою в обробці замовлень.

4. Визначення ресурсів та залежностей

Мета – визначити ресурси, необхідні для виконання критичних процесів, та їх залежності.

Приклад. Визначення необхідного програмного забезпечення, обладнання, персоналу для забезпечення безперервної роботи обробки замовлень.

5.Визначення максимально допустимого простою (Maximum Acceptable

Outage, MAO)

Мета – встановити максимально допустимий час простою для кожного критичного процесу.

Приклад. Встановлення, що обробка замовлень не може бути перервана більш ніж на 4 години без суттєвих фінансових втрат.

6.Розробка планів відновлення

Мета – розробити стратегії для відновлення критичних процесів у випадку їх порушення.

Приклад. Створення планів резервного копіювання даних, альтернативних каналів зв’язку, резервних робочих місць для забезпечення безперервної роботи.

Опишемо приклад проведення BIA нижче:

Визначення критичних бізнес-процесів.

Наприклад, для компанії, яка займається електронною комерцією, критичними можуть бути такі процеси, як управління інвентарем, обробка замовлень та підтримка клієнтів. Ці процеси необхідно визначити як пріоритетні для аналізу впливу.

Оцінка впливу на бізнес.

Припустимо, що через технічний збій система обробки замовлень виходить з ладу на один день. Це може призвести до значних фінансових втрат через втрату потенційних продажів, зниження рівня задоволеності клієнтів та втрату репутації.

Визначення ресурсів та залежностей.

Для забезпечення роботи системи обробки замовлень необхідні надійні сервери, безперебійний доступ до інтернету, програмне забезпечення для управління замовленнями та кваліфікований персонал, який може оперативно реагувати на технічні проблеми.

Визначення MAO.

Максимально допустимий час простою для системи обробки замовлень може бути встановлений як 4 години. Це означає, що у випадку порушення роботи

системи, її необхідно відновити протягом цього часу, щоб мінімізувати негативні наслідки.

Розробка планів відновлення.

Стратегії для відновлення можуть включати регулярне резервне копіювання даних, наявність запасних серверів, планування відновлювальних заходів та проведення навчань для персоналу з відновлення роботи після інциденту.

Одним із ефективних методів є аудит інформаційної безпеки, який дозволяє систематично оцінити захищеність інформаційних ресурсів підприємства та визначити можливі вразливості.

Розглянемо метод аудиту інформаційної безпеки (Information Security Audit).

Аудит інформаційної безпеки є систематичним процесом перевірки та оцінки політик, процесів і систем, які забезпечують захист інформації в організації. Основною метою аудиту є виявлення вразливостей, оцінка ризиків і розробка рекомендацій щодо покращення заходів безпеки.

Етапи проведення аудиту інформаційної безпеки включають:

1)Підготовка до аудиту

Мета – визначити обсяг і цілі аудиту, розробити план проведення перевірок.

Приклад. Встановлення цілей аудиту, таких як перевірка відповідності політик безпеки стандартам, оцінка ефективності існуючих заходів безпеки.

2) Огляд документації

Мета – перевірка наявних політик, процедур і стандартів безпеки.

Приклад. Аналіз політик управління доступом, процедур резервного копіювання, стандартів реагування на інциденти.

3) Оцінка фізичної безпеки

Мета – оцінка заходів фізичного захисту інформаційних ресурсів.

Приклад. Перевірка контролю доступу до серверних кімнат, наявність систем відеоспостереження, заходів захисту від пожеж.

4)Оцінка технічних заходів безпеки

Мета – перевірка технічних засобів захисту інформації.

Приклад. Аналіз налаштувань брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень.

5)Оцінка процедур управління ризиками

Мета – оцінка ефективності процедур управління ризиками.

Приклад. Перевірка наявності планів реагування на інциденти, регулярності проведення аналізу ризиків, процедур управління змінами.

6) Проведення тестувань та перевірок

Мета – проведення практичних тестів для виявлення вразливостей.

Приклад. Виконання пенетраційних тестів, аналіз журналів безпеки, перевірка наявності оновлень програмного забезпечення.

7) Аналіз результатів та підготовка звіту

Мета – оцінка отриманих даних та розробка рекомендацій.

Приклад. Виявлення слабких місць в системі безпеки, розробка плану заходів для покращення безпеки, підготовка звіту з висновками та рекомендаціями.

Розглянемо приклад проведення аудиту інформаційної безпеки з етапами.

Підготовка до аудиту. Визначення цілей аудиту – перевірка відповідності політик безпеки міжнародним стандартам, таким як ISO / IEC 27001[47]. Розробка плану – складання графіка перевірок, визначення відповідальних осіб.

Огляд документації. Аналіз наявних політик – перевірка відповідності політик управління доступом стандартам безпеки. Оцінка процедур – перевірка регулярності оновлення політик безпеки та їх впровадження на практиці.

Оцінка фізичної безпеки. Перевірка доступу – контроль доступу до серверних кімнат, наявність систем відеоспостереження. Захист від пожеж – перевірка наявності систем пожежогасіння, регулярність проведення навчань з пожежної безпеки.

Оцінка технічних заходів безпеки. Аналіз налаштувань – перевірка налаштувань брандмауерів, антивірусних програм. Оновлення систем – перевірка

регулярності оновлення програмного забезпечення.

Оцінка процедур управління ризиками. Планування – наявність планів реагування на інциденти, процедур управління змінами. Регулярність – перевірка регулярності проведення аналізу ризиків, оновлення процедур.

Проведення тестувань та перевірок. Пенетраційні тести – виконання тестів для виявлення вразливостей. Аналіз журналів: перевірка журналів безпеки для виявлення підозрілих активностей.

Аналіз результатів та підготовка звіту. Виявлення вразливостей – ідентифікація слабких місць у системі безпеки. Розробка рекомендацій – підготовка звіту з конкретними рекомендаціями для покращення безпеки.

Отже,аудит інформаційної безпеки дозволяє організаціям оцінити поточний стан безпеки інформаційних систем, виявити вразливості та розробити заходи для їх усунення. Регулярне проведення аудиту допомагає забезпечити високий рівень захисту інформації, мінімізувати ризики та підвищити загальну стійкість організації до загроз.

Один із комплексних методів, що дозволяє це зробити, є методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Ця методологія спрямована на оцінку загроз, вразливостей та активів організації, щоб забезпечити ефективний захист інформаційних ресурсів.

OCTAVE є ризик-менеджмент методологією, розробленою для допомоги організаціям у визначенні, оцінці та управлінні ризиками інформаційної безпеки. Вона надає структурований підхід до оцінки загроз, вразливостей і критичних активів, допомагаючи розробити стратегії для покращення захисту інформаційних систем[34].

Етапи методології OCTAVE включають наступні:

-Визначення критичних активів

Мета – виявити та класифікувати активи, які є критичними для функціонування організації.

Приклад: визначення баз даних клієнтів, фінансових систем, виробничих систем як критичних активів.

-Ідентифікація загроз і вразливостей

Мета – виявити можливі загрози та вразливості, які можуть вплинути на критичні активи.

Приклад: аналіз потенційних загроз, таких як кібератаки, внутрішні зловживання, фізичні загрози.

- Оцінка ризиків

Мета – оцінити ризики на основі ймовірності їх реалізації та можливих наслідків.

Приклад: визначення ризиків на основі аналізу загроз і вразливостей, оцінка ймовірності та впливу.

- Розробка стратегій зниження ризиків

Мета – розробити заходи для зниження ризиків до прийнятного рівня.

Приклад: впровадження технічних заходів, таких як шифрування даних, політики безпеки, навчання персоналу.

- Проведення оцінки та моніторинг

Мета – регулярно оцінювати та оновлювати заходи безпеки для забезпечення їх ефективності.

Приклад: проведення регулярних аудиторських перевірок, моніторинг систем безпеки, оновлення політик та процедур.

Розглянемо на прикладі проведення OCTAVE. Отже цей метод може включати такі послідовні дії:

а) Визначення критичних активів.

Для підприємства критичними активами можуть бути інформаційні системи, які обробляють фінансові транзакції, особисті дані клієнтів, системи управління ризиками та інші важливі активи.

б) Ідентифікація загроз і вразливостей

Аналіз потенційних загроз для підприємства може включати в себе кіберзлочинність, фізичні загрози (наприклад, крадіжка обладнання), внутрішні загрози (наприклад, зловживання доступом персоналу).

в) Оцінка ризиків.

Ризики оцінюються на основі ймовірності реалізації загроз та їх потенційних наслідків. Наприклад, ризик витоку даних клієнтів може бути оцінений як високий через можливі фінансові та репутаційні втрати.

г) Розробка стратегій зниження ризиків.

Для зниження ризиків можуть бути впроваджені такі заходи, як багатофакторна аутентифікація, регулярні оновлення програмного забезпечення, навчання співробітників з питань інформаційної безпеки.

д) Проведення оцінки та моніторинг.

Підприємство має регулярно проводити аудиторські перевірки, моніторити активність у системах безпеки, оновлювати політики безпеки на основі змін у зовнішньому середовищі та внутрішніх процесах.

Методи кількісного та якісного аналізу загроз є невід’ємною частиною процесу оцінки загроз на підприємстві, оскільки вони дозволяють отримати повне уявлення про стан безпеки інформаційних ресурсів та розробити ефективні заходи для їх захисту.

Кількісний та якісний аналіз загроз використовуються для визначення й оцінки ризиків, що впливають на інформаційну безпеку. Обидва підходи мають свої особливості та переваги, і часто використовуються разом для досягнення більш точних результатів.

Кількісний аналіз загроз базується на використанні числових даних та статистичних методів для оцінки ризиків. Він дозволяє визначити ймовірність настання певних подій та їх потенційний вплив на організацію в числових значеннях, а саме:

1.Збір даних.

Мета – зібрати дані про минулі інциденти, вразливості та загрози.

Приклад. Аналіз журналів подій, звітів про інциденти безпеки, статистичних даних про кібератаки.

2.Оцінка ймовірності.

Мета – визначити ймовірність настання певних загроз.

Приклад. Використання статистичних моделей для оцінки ймовірності проникнення в систему через вразливість.

3.Оцінка впливу.

Мета – визначити потенційний вплив загроз на організацію.

Приклад. Оцінка фінансових втрат, можливих збитків репутації, витрат на відновлення систем після атаки.

4.Використання математичних моделей.

Мета – розрахунок ризиків за допомогою математичних моделей.

Приклад. Використання методів Монте-Карло для моделювання ризиків, побудова сценаріїв на основі ймовірностей.

Якісний аналіз загроз базується на експертних оцінках та суб’єктивному аналізі інформації. Він дозволяє отримати глибше розуміння контексту та особливостей загроз, які важко кількісно оцінити. Розглянемо основні етапи проведення оцінки загроз з використанням якісного аналізу:

1.Ідентифікація загроз

Мета – виявити можливі загрози на основі експертних знань та досвіду.

Приклад. Використання методів брейнстормінгу, опитувань, інтерв’ю з фахівцями з інформаційної безпеки.

2.Оцінка серйозності загроз

Мета – визначити рівень серйозності загроз.

Приклад. Класифікація загроз за рівнем впливу на бізнес-процеси, критичністю для організації.

3.Визначення ймовірності реалізації загроз

Мета – оцінити ймовірність реалізації загроз на основі експертних оцінок.

Приклад. Аналіз минулих інцидентів, вивчення тенденцій у сфері інформаційної безпеки.

4.Розробка рекомендацій

Мета – розробити рекомендації щодо зниження ризиків.

Приклад. Впровадження нових політик безпеки, навчання персоналу, підвищення рівня контролю доступу.

Розглянемо приклади використання методів кількісного та якісного аналізу.

Кількісний аналіз. Для оцінки загроз, наприклад, у банківській установі можна використовувати дані про кількість спроб кіберзлочинів за останні п’ять років, вартість відновлення після інцидентів та частоту успішних атак. На основі цих даних можна розрахувати ймовірність успішної атаки та можливі фінансові втрати.

Якісний аналіз. Для оцінки загроз у тій самій установі можна провести опитування серед експертів з інформаційної безпеки, щоб визначити найбільш критичні вразливості та можливі сценарії атак. Наприклад, фахівці можуть вказати на слабкі місця в системі управління доступом або недоліки в політиках безпеки, які потребують негайного вирішення.

Комбіноване використання кількісного та якісного аналізу загроз дозволяє отримати повне уявлення про ризики, з якими може зіткнутися організація. Кількісний аналіз надає об’єктивні дані для прийняття рішень, тоді як якісний аналіз дозволяє врахувати контекст та специфіку загроз, що не завжди піддаються кількісній оцінці. Разом ці методи забезпечують комплексний підхід до управління ризиками інформаційної безпеки[32].

Розглянуті методи оцінки загроз цілісності інформації є фундаментальними інструментами для забезпечення інформаційної безпеки на підприємствах. Кожен з них має свої особливості та переваги, що дозволяє ефективно виявляти, аналізувати та управляти ризиками. Аналіз ризиків допомагає ідентифікувати і кількісно

оцінити загрози, SWOT-аналіз забезпечує стратегічне розуміння сильних і слабких сторін, а метод дерева відмов і методологія OCTAVE надають детальне бачення можливих сценаріїв загроз. Аудит інформаційної безпеки та BIA дозволяють систематично оцінювати поточний стан безпеки та вплив потенційних загроз, тоді як кількісний і якісний аналізи забезпечують комплексний підхід до управління ризиками.

3.2. Оцінка загроз цілісності інформації на підприємстві

Використання зазначених методів дозволяє отримати повне уявлення про поточний стан інформаційної безпеки та визначити найбільш ефективні заходи для забезпечення цілісності інформації. Наступний етап нашого дослідження присвячений конкретній оцінці загроз для ПРАТ «Датагруп», що є провідним постачальником послуг зв’язку в Україні. Розглянемо детально інформаційне середовище підприємства, виявимо потенційні загрози та запропонуємо рекомендації щодо їх мінімізації.

Для того щоб оцінити загрози цілісності інформації на підприємстві «Датагруп», необхідно провести комплексний аналіз потенційних небезпек, які можуть вплинути на цілісність інформаційних ресурсів компанії. Основні напрямки аналізу включатимуть оцінку внутрішніх та зовнішніх загроз, їхню вірогідність та потенційні наслідки для цілісності інформації.

У зовнішніх загроз можуть входити кібератаки, злам систем безпеки, віруси та шкідливі програми, а також несанкціонований доступ до інформації з боку конкурентів чи зловмисників. Внутрішні загрози можуть виникати внаслідок недбалого ставлення до захисту інформації з боку співробітників, випадкових помилок або зловмисних дій зсередини самої компанії.

Підприємство «Датагруп» має ретельно аналізувати свої існуючі системи

захисту і виявити їхні слабкі місця, які можуть стати точками входу для потенційних загроз. Важливо також визначити критичні для бізнесу активи та інформаційні ресурси, щоб зосередити зусилля на їхньому захисті.

У таблиці 3.1 наведено перелік загроз цілісності інформації на підприємстві «Датагруп».

Таблиця 3.1

Загрози цілісності інформації «Датагруп» та методи їх виявлення

Загроза	Метод виявлення	Пропозиції з усунення
Невідповідність доступу	Аналіз журналів доступу, аудит користувачів, тестування на проникнення	Впровадження принципів найменшого привілею, використання багатофакторної автентифікації, регулярний перегляд прав доступу
Програмне забезпечення-вимагач	Аналіз мережевого трафіку, моніторинг активності системи, резервне копіювання даних	Впровадження політики кібербезпеки, навчання співробітників, оновлення програмного забезпечення, використання антивірусного програмного забезпечення
Внутрішні порушення	Аналіз поведінки користувачів, моніторинг активності системи, тестування на проникнення	Проведення тренінгів з кібербезпеки, впровадження політики кібербезпеки, моніторинг активності співробітників
Відмов обладнання	Моніторинг стану обладнання, резервне копіювання даних, планування аварійного відновлення	Регулярне обслуговування обладнання, використання резервного обладнання, впровадження плану аварійного відновлення
Стихійні лиха	Планування аварійного відновлення, резервне копіювання даних, страхування	Впровадження плану аварійного відновлення, резервне копіювання даних у безпечному місці, страхування майна та даних
Несанкціоноване розголошення інформації	Аналіз журналів доступу, моніторинг активності системи, навчання співробітників	Впровадження політики кібербезпеки, навчання співробітників, використання шифрування даних
Людська помилка	Навчання співробітників, тестування на проникнення, моніторинг активності системи	Проведення тренінгів з кібербезпеки, впровадження політики кібербезпеки, моніторинг активності співробітників
Втрата чи крадіжка носіїв інформації	Шифрування даних, контроль доступу до носіїв інформації, резервне копіювання даних	Використання шифрованих носіїв інформації, контроль доступу до носіїв інформації, резервне копіювання даних

Джерело: складено автором на основі даних підприємства

Для здійснення ефективного контролю над загрозами цілісності інформації «Датагруп» має розглянути використання сучасних інструментів моніторингу та детекції загроз, регулярно проводити аудит безпеки, а також надавати періодичне навчання співробітникам з питань інформаційної безпеки.

Враховуючи постійно зростаючі загрози в галузі інформаційної безпеки, «Датагруп» повинен постійно оновлювати свої підходи до захисту інформації та вдосконалювати свої системи з урахуванням новітніх технологій та найкращих практик у цій області.

Розглянемо приклад використання аналізу ризиків (Risk Assessment) на ПРАТ «Датагруп».

Ідентифікація ризику. Виявлено, що однією з основних загроз є несанкціонований доступ до інформаційних систем через віддалені робочі місця співробітників.

Аналіз ризику. Визначено, що ймовірність несанкціонованого доступу висока, оскільки багато співробітників працюють віддалено, і не всі використовують захищені канали зв’язку. Можливі наслідки включають втрату конфіденційної інформації клієнтів і фінансові збитки.

Оцінка ризику. Ризик класифікований як високий, і необхідні негайні дії для його зменшення.

Запобігання ризику. Впровадження VPN для віддалених співробітників, обов’язкове використання двофакторної аутентифікації.

Моніторинг та огляд. Регулярний аудит використання VPN і перевірка дотримання політик безпеки.

Ролі і відповідальності в процесі аналізу ризиків наступні:

– Менеджери з безпеки інформації – відповідальні за організацію і проведення аналізу ризиків.

– IT-відділ – впровадження технічних засобів для зменшення ризиків.

– Персонал – дотримання встановлених політик і процедур безпеки.

В рамках SWOT-аналізу можна виявити внутрішні та зовнішні фактори, що впливають на цілісність інформації на підприємстві «Датагруп». Сильні сторони можуть включати високий рівень експертизи у сфері інформаційної безпеки та доступ до передових технологій. Слабкі сторони можуть охоплювати відсутність повноцінної культури безпеки серед персоналу та нестабільність програмних платформ. Можливості включають розробку нових систем захисту інформації, тоді як загрози можуть бути пов’язані зі зростаючими кіберзагрозами та зміною регуляторного середовища.

SWOT-аналіз є інструментом стратегічного планування, який допомагає визначити сильні та слабкі сторони підприємства, а також можливості та загрози, що впливають на його діяльність. На прикладі ПРАТ «Датагруп», SWOT-аналіз може допомогти ідентифікувати наступне:

Сильні сторони – широкий спектр послуг, висока якість обслуговування, сильна брендова репутація.

Слабкі сторони – можливі проблеми з безпекою даних, недостатня інвестиційна активність у захист інформації, обмежені можливості для розширення інфраструктури.

Можливості – зростання попиту на послуги зв’язку, впровадження новітніх технологій у сфері телекомунікацій, партнерські угоди з іншими компаніями.

Загрози – кібератаки на інфраструктуру, конкуренція на ринку, зміни у законодавстві з питань інформаційної безпеки.

Метод дерева відмов (Fault Tree Analysis, FTA). FTA може бути корисним для ідентифікації потенційних причин відмов у системах безпеки, які можуть призвести до порушення цілісності інформації на підприємстві. Наприклад, можуть виявитися такі можливі відмови, як недостатнє оновлення програмного забезпечення або некомпетентність персоналу у використанні захисних заходів[30].

Метод дерева відмов використовується для ідентифікації потенційних відмов

у системі та їхніх причин. На прикладі ПРАТ «Датагруп», FTA може бути використаний для аналізу можливих відмов в інформаційних системах та їхніх наслідків для цілісності даних. Наприклад, FTA може показати, що відмова в системі збереження даних може призвести до втрати конфіденційної інформації клієнтів.

Метод аналізу впливу на бізнес (Business Impact Analysis, BIA). BIA допомагає визначити вплив відсутності або порушення цілісності інформації на різні аспекти діяльності підприємства «Датагруп». Це може охоплювати втрати фінансових ресурсів, пошкодження репутації бренду, порушення взаємовідносин з клієнтами та інші негативні наслідки.

Метод аналізу впливу на бізнес використовується для визначення впливу можливих відмов на діяльність підприємства. На прикладі ПРАТ «Датагруп», BIA може допомогти визначити, як втрата доступу до критичних інформаційних ресурсів може вплинути на її функціонування і призвести до фінансових втрат та втрати репутації.

Аудит інформаційної безпеки. Проведення аудиту інформаційної безпеки може допомогти виявити потенційні слабкі місця в системах захисту інформації на підприємстві. Регулярні аудити можуть забезпечити перевірку дотримання встановлених політик і процедур безпеки та виявлення нових загроз. Аудит інформаційної безпеки включає перевірку систем та процесів на предмет відповідності стандартам безпеки та виявлення можливих слабких місць. На прикладі ПРАТ «Датагруп», аудит може виявити потенційні проблеми у захисті даних та ідентифікувати шляхи їх вирішення.

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). OCTAVE може бути використана для ідентифікації критичних для бізнесу активів та вразливостей, що можуть бути використані зловмисниками для порушення цілісності інформації на підприємстві. Методологія OCTAVE використовується для оцінки загроз цілісності інформації на підприємстві, зокрема

ідентифікації критичних активів та вразливостей. На прикладі ПРАТ «Датагруп», методологія OCTAVE може допомогти визначити найбільш критичні для бізнесу активи та розробити стратегії їх захисту[34].

Методи кількісного та якісного аналізу загроз. Кількісний та якісний аналіз загроз використовується для оцінки впливу різних загроз на цілісність інформації. Кількісний аналіз вимірює загрози за допомогою числових показників, таких як ймовірність виникнення події та потенційні втрати в результаті цієї події. На прикладі ПРАТ «Датагруп», кількісний аналіз може включати визначення імовірності кібератак на сервери компанії та обчислення фінансових збитків у разі їхнього успішного здійснення.

З іншого боку, якісний аналіз спрямований на оцінку характеру та можливих наслідків загроз, а також на визначення ефективності заходів з їх протидії. Наприклад, в контексті ПРАТ «Датагруп», якісний аналіз може допомогти визначити, які типи кіберзагроз найбільш ймовірні для компанії та які заходи з безпеки є найбільш ефективними для їх запобігання.

Обидва ці методи аналізу допомагають підприємству оцінити свої поточні системи захисту інформації, ідентифікувати слабкі місця та розробити стратегії для їх вдосконалення. На основі отриманих даних та результатів аналізу ПРАТ «Датагруп» може приймати обґрунтовані рішення з метою підвищення рівня безпеки своїх інформаційних ресурсів.

Порядок проведення аналізу загроз і вжиття заходів захисту на підприємстві «Датагруп» вимагає взаємодії різних підрозділів, таких як менеджери з безпеки інформації, ІТ-відділ та персонал. Кожен з них має свої ролі і відповідальності у процесі аналізу ризиків та розробки стратегій захисту.

Розглянемо додатково кілька методів оцінки загроз цілісності інформації на підприємстві ПРАТ «Датагруп»:

1. Попередній аналіз небезпек (PHA) є систематичним процесом ідентифікації потенційних загроз цілісності інформації на підприємстві «Датагруп». В цьому

методі учасники визначають можливі небезпеки та їх потенційні наслідки для інформаційних ресурсів. Наприклад, можуть бути виявлені такі небезпеки, як кібератаки на інфраструктуру підприємства, випадкові помилки персоналу або зловмисний доступ до конфіденційної інформації. Після ідентифікації небезпек проводиться оцінка їх впливу на цілісність інформації, що дозволяє розробити стратегії запобігання та захисту.

2. Метод Delphi використовується для прогнозування потенційних загроз цілісності інформації на підприємстві «Датагруп» шляхом експертної оцінки. Експерти з інформаційної безпеки, IT-спеціалісти та інші зацікавлені сторони можуть брати участь у процесі. Вони надають свої прогнози щодо можливих загроз і їхнього впливу на цілісність інформації на підприємстві. Після збору думок експертів, їхні оцінки аналізуються та узагальнюються, щоб зробити прогнози щодо потенційних загроз та розробити стратегії управління ризиками[44].

3.Метод аналізу застосунків (Application Analysis) – це метод аналізу застосунків, що використовується для оцінки впливу різних програмних та апаратних застосунків на цілісність інформації на підприємстві «Датагруп». Цей метод включає аналіз конкретних програм, сервісів та технологій, які використовуються в компанії, з метою визначення їхнього потенційного впливу на безпеку інформації. Наприклад, оцінюються ризики, пов'язані з використанням різних програмних продуктів або технічних засобів, а також їхній потенційний вплив на цілісність даних та інформаційних ресурсів.

Описані методи допоможуть підприємству «Датагруп» ідентифікувати, оцінити та управляти ризиками, пов’язаними з цілісністю інформації, забезпечуючи ефективний захист її активів та даних від потенційних загроз.

3.3. Рекомендації щодо забезпечення цілісності інформації на підприємстві

Зважаючи на сферу діяльності ПРАТ «Датагруп» як провайдера послуг зв'язку для бізнесу та дому, рекомендації щодо забезпечення цілісності інформації повинні бути адаптовані до специфіки цієї галузі.

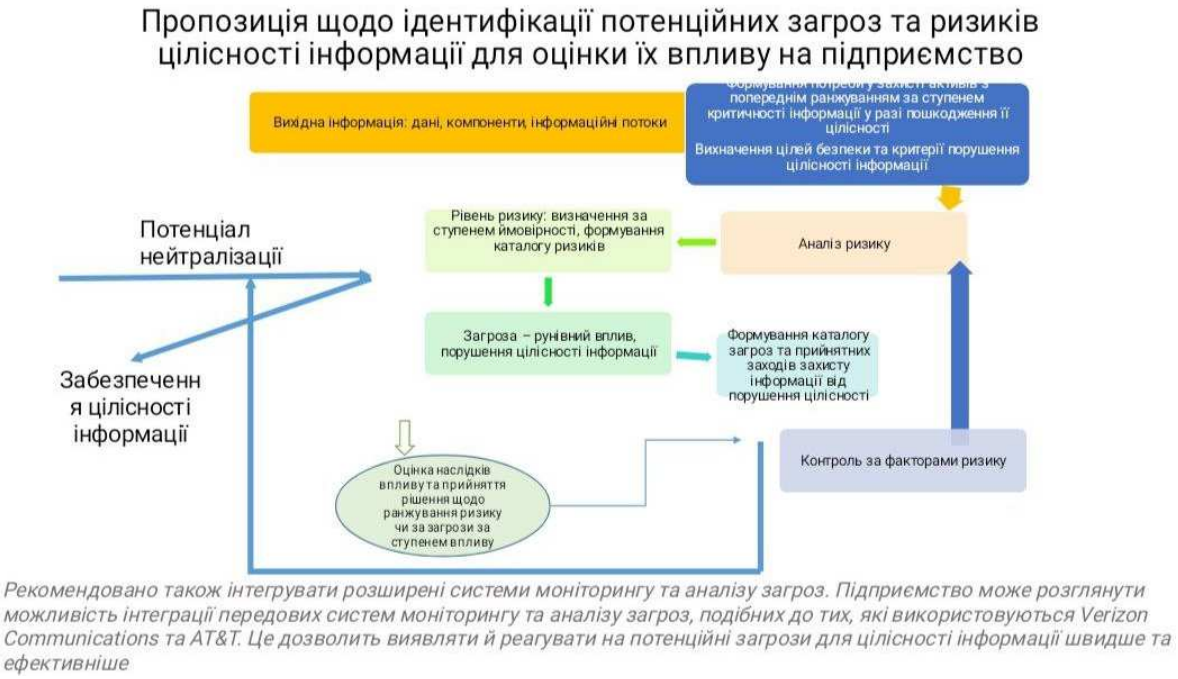

Рис. 3.1. Пропозиція щодо ідентифікації потенційних загроз Датагруп

Джерело: складено автором на основі даних підприємства[14]

Схема, представлена пропозиція щодо ідентифікації потенційних загроз «Датагруп» на рис. 3.1, визначає процес ідентифікації, аналізу та управління потенційними загрозами і ризиками для забезпечення цілісності інформації на підприємстві. Вона включає кілька ключових етапів, які забезпечують комплексний підхід до захисту інформаційних активів.

1. Вихідна інформація. Основними елементами вихідної інформації є

дані, компоненти та інформаційні потоки. Ці елементи становлять базу, на основі якої проводиться подальший аналіз загроз та ризиків.

2. Формування потенційної загрози. На цьому етапі формується перелік загроз, які можуть вплинути на цілісність інформації. Це здійснюється шляхом попереднього ранжування загроз за ступенем критичності інформації у разі її пошкодження. Далі визначаються цілі безпеки та критерії порушення цілісності інформації.

3. Аналіз ризику. Процес аналізу ризику включає визначення рівня ризику за ступенем ймовірності та формування каталогу ризиків. Цей аналіз дозволяє оцінити, наскільки ймовірні ті чи інші загрози, і які ризики вони несуть для цілісності інформації.

4. Визначення загрози. Загрози оцінюються за рівнем впливу на інформаційні активи підприємства та порушення цілісності інформації. Це дозволяє визначити, які загрози є найбільш критичними і потребують негайної уваги.

5. Формування каталогу загроз. На основі проведеного аналізу формується каталог загроз. Для кожної загрози розробляються і приймаються заходи захисту інформації від порушення цілісності. Це можуть бути як технічні, так і організаційні заходи.

6. Оцінка наслідків впливу. На цьому етапі здійснюється оцінка наслідків впливу загроз та прийняття рішень щодо ранжування ризику чи загроз за ступенем впливу. Це дозволяє підприємству розставити пріоритети в управлінні ризиками і зосередити зусилля на найбільш критичних загрозах.

7. Контроль за факторами ризику. Постійний контроль за факторами ризику включає моніторинг та аналіз ризиків. Це дозволяє оперативно реагувати на зміну ситуації та своєчасно оновлювати стратегії захисту інформації.

8. Забезпечення цілісності інформації. Весь процес спрямований на забезпечення цілісності інформації шляхом ефективного управління ризиками та нейтралізації потенційних загроз. Підприємство має постійно вдосконалювати свої

методи захисту і впроваджувати нові технології для покращення безпеки інформаційних активів.

Рекомендується також інтегрувати розширені системи моніторингу та аналізу загроз. Підприємство може розглянути можливість інтеграції передових систем моніторингу та аналізу загроз, подібних до тих, які використовуються Verizon Communications та AT&T. Це дозволить виявляти і реагувати на потенційні загрози для цілісності інформації швидше та ефективніше.

Розглянемо ключові аспекти та рекомендації:

1.Розробка комплексних стратегій безпеки. ПРАТ «Датагруп» повинно розробити та впровадити комплексні стратегії безпеки, які охоплюватимуть усі аспекти їхньої діяльності. Це може включати захист мережі зв'язку, захист баз даних, кібербезпеку та фізичну безпеку інфраструктури.

2.Вдосконалення систем моніторингу та виявлення загроз. ПРАТ «Датагруп» повинно вдосконалити системи моніторингу та виявлення загроз для реагування на потенційні атаки або порушення цілісності даних в реальному часі. Це може включати впровадження системі інтелектуального аналізу відхилень, які автоматично виявляють незвичайну активність на мережі.

3.Навчання та підвищення свідомості співробітників. ПРАТ «Датагруп» повинно проводити регулярне навчання та тренінги з питань інформаційної безпеки для всіх співробітників. Це допоможе забезпечити, що всі працівники розуміють потенційні загрози і знають, як їм діяти у разі виявлення підозрілої активності або атаки.

4.Захист від кіберзагроз. Оскільки сфера телекомунікацій підвищується загрозами кібербезпеки, ПРАТ «Датагруп» повинно активно захищати свої мережі та системи від кібератак. Це включає в себе встановлення вогнепровідних систем, захист від DDoS-атак та використання сучасних методів шифрування даних.

5.Регулярне проведення аудитів безпеки. ПРАТ «Датагруп» повинно

регулярно проводити аудити безпеки, щоб перевірити ефективність їхніх заходів безпеки, виявити слабкі місця та вжити заходів для їх вдосконалення. Це допоможе попередити можливі порушення цілісності інформації та забезпечити високий рівень безпеки даних.

6.Забезпечення дотримання вимог законодавства. ПРАТ «Датагруп» повинно бути уважним до вимог законодавства про захист персональних даних та конфіденційності інформації. Вони повинні розробляти та впроваджувати політики та процедури, які відповідають цим вимогам і забезпечують високий рівень захисту даних клієнтів та корпоративної інформації.

Наведені рекомендації є лише загальними орієнтирами, і ПРАТ «Датагруп» повинно розглянути їхні специфічні потреби та унікальні вимоги в процесі розробки та впровадження стратегій безпеки і захисту інформації.

Зважаючи на широкий спектр діяльності підприємств у сфері телекомунікацій та інформаційної безпеки, деякі відомі компанії здійснюють успішні практики забезпечення цілісності інформації, зокрема:

1)Verizon Communications Inc. Ця американська телекомунікаційна компанія використовує передові технології та стратегії безпеки для захисту інформації своїх клієнтів. Вони активно впроваджують рішення кібербезпеки, такі як мережеві файерволи, системи виявлення вторгнень та системи шифрування даних для забезпечення цілісності інформації[46].

2)AT&T Inc. [35] Інша провідна американська телекомунікаційна компанія, AT&T, активно інвестує в інформаційну безпеку та захист мережі. Вони використовують сучасні методи аналізу загроз, які допомагають виявити потенційні ризики для цілісності інформації та вживати заходів для їх запобігання.

3)Cisco Systems, Inc. Ця компанія спеціалізується на розробці мережевого обладнання та програмного забезпечення для телекомунікаційних систем. Вони надають комплексні рішення з кібербезпеки, які включають в себе системи ідентифікації та аутентифікації, мережеві файерволи та системи моніторингу, що

допомагають підприємствам забезпечити цілісність їхньої інформації[37].

Описані приклади демонструють, як великі телекомунікаційні компанії використовують різноманітні технології та стратегії безпеки для забезпечення цілісності інформації своїх клієнтів. Вони активно впроваджують сучасні методи аналізу загроз, розвивають захист від кібератак та постійно вдосконалюють свої системи безпеки, щоб відповідати зростаючим вимогам у сфері інформаційної безпеки.

Можна сформулювати кілька рекомендацій для ПРАТ «Датагруп» на основі описаних вище прикладів, а саме:

Інтеграція розширених систем моніторингу та аналізу загроз. Підприємство може розглянути можливість інтеграції передових систем моніторингу та аналізу загроз, подібних до тих, які використовуються Verizon Communications та AT&T. Це дозволить виявляти й реагувати на потенційні загрози для цілісності інформації швидше та ефективніше.

Впровадження прогресивних методів шифрування даних. Враховуючи постійні кіберзагрози, які ставлять під загрозу цілісність інформації, ПРАТ «Датагруп» може вдосконалити свої методи шифрування даних, використовуючи передові технології, такі як квантове шифрування, яке забезпечує максимальний рівень захисту від кібератак.

Регулярне оновлення програмного забезпечення та апаратури. ПРАТ «Датагруп» повинно регулярно оновлювати своє програмне забезпечення та апаратуру, включаючи мережеве обладнання, сервери та програми для захисту від вразливостей і кіберзагроз.

Описані рекомендації можуть допомогти підприємству «Датагруп» покращити свої практики забезпечення цілісності інформації та знизити ризик від кіберзагроз.

Додаткові рекомендації з застосуванням новітніх методів захисту цілісності інформації можуть включати наступні:

-Використання методу FAIR (Factor Analysis of Information Risk).

Метод FAIR дозволяє кількісно оцінити ризики, пов’язані з цілісністю інформації, і визначити потенційні втрати. ПРАТ «Датагруп» може використовувати цей метод для ідентифікації та категоризації ризиків, пов’язаних з цілісністю даних, що допоможе у прийнятті обґрунтованих рішень щодо заходів безпеки[38].

- Впровадження методу TARA (Threat and Risk Assessment) – рис. 3.1.

Метод TARA дозволяє ідентифікувати потенційні загрози та ризики для цілісності інформації та оцінювати їх вплив на підприємство.

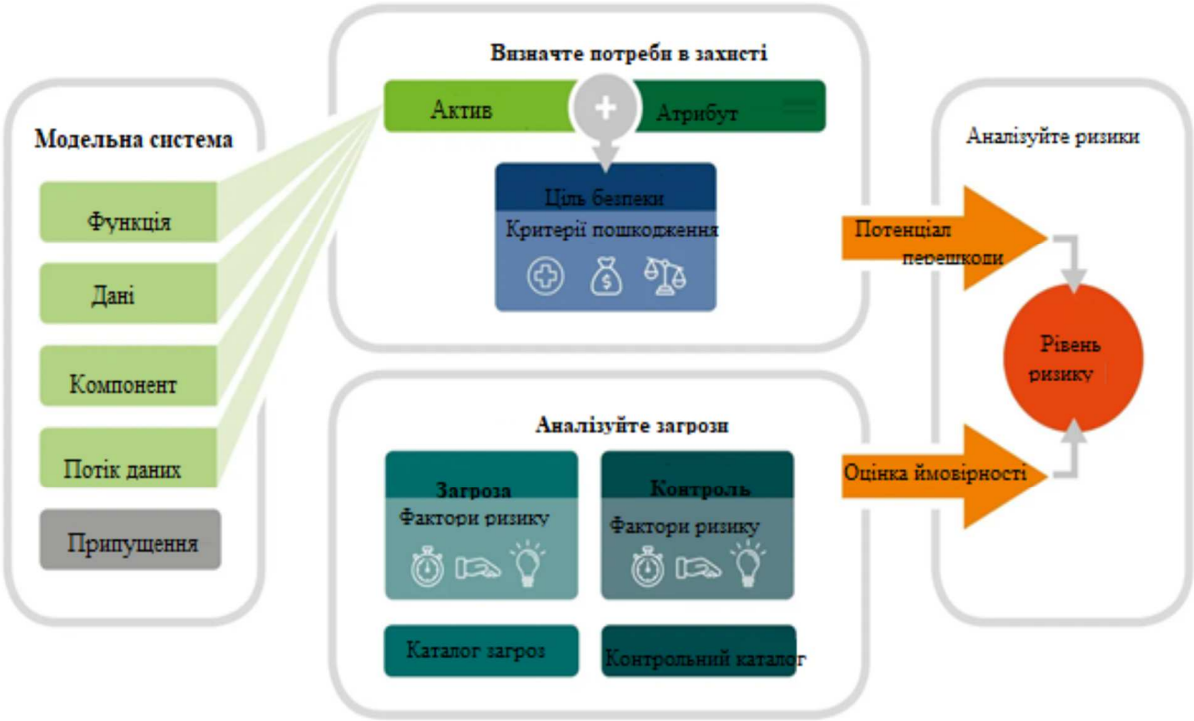

Рис. 3.2. Основні етапи аналізу загроз та метод оцінки ризиків (TARA)

Джерело: складено автором на основі[45]

Схема аналізу загроз TARA складається з наступних етапів:

1) Визначення обсягу аналізу – на цьому етапі визначається, які активи інформаційної системи будуть аналізуватися.

2) Ідентифікація загроз – ідентифікуються можливі загрози для визначених активів.

3) Аналіз загроз – аналізуються ідентифіковані загрози для визначення їх характеристик та впливу на активи.

4) Оцінка ризиків – оцінюється ймовірність виникнення кожної загрози та серйозність її наслідків.

5) Приоритезація ризиків, тобто ризики пріоритезуються за їх важливістю.

6) Розробка заходів з управління ризиками – на цьому етапі розробляються заходи з управління ризиками, які допоможуть знизити ймовірність виникнення загроз або серйозність їх наслідків.

TARA (Threat Assessment and Risk Assessment) – це методологія аналізу загроз та оцінки ризиків, яка використовується для ідентифікації, аналізу та пріоритезації загроз інформаційної системи.

ПРАТ «Датагруп» може використовувати цей метод для систематичного аналізу загроз та ризиків, що допоможе виявити слабкі місця в системах безпеки та розробити ефективні заходи їх запобігання.

Доцільність застосування TARA на ПрАТ «Датагруп» полягає у наступному. ПрАТ «Датагруп» – це великий постачальник послуг зв’язку, який володіє розгалуженою мережею та значними інформаційними активами. Це робить компанію мішенню для різних кіберзагроз.

Наведемо конкретний приклад: загроза – несанкціонований доступ до інформації.

1)Аналіз загрози.

Характеристика – зловмисник може отримати несанкціонований доступ до конфіденційної інформації компанії, наприклад даних клієнтів або фінансової інформації. Несанкціонований доступ до інформації може призвести до витоку

даних, фінансових втрат, пошкодження репутації компанії та інших негативних наслідків.

2)Оцінка ризиків.

Ймовірність – висока, оскільки компанія володіє значним обсягом інформації, яка може бути цікавою для зловмисників.

Серйозність – висока, оскільки наслідки несанкціонованого доступу до інформації можуть бути дуже серйозними для компанії.

Пріоритезація ризиків – висока.

3)Заходи з управління ризиками:

- впровадження багатофакторної автентифікації;
- шифрування даних;
- регулярний перегляд прав доступу до інформації;
- навчання співробітників з питань кібербезпеки;
- впровадження системи моніторингу інформаційної системи

4)Розрахунок ризиків. Для розрахунку ризиків можна використовувати різні методи, наприклад, метод множення ймовірності та серйозності наслідків.

Наприклад:

Ймовірність – 0,8

Серйозність – 0,9

Ризик – 0,72 (0,8 · 0,9)

Цей розрахунок показує, що ризик несанкціонованого доступу до інформації є дуже високим.

Використання методології TARA дозволить компанії «Датагруп» об’єктивно оцінити кіберзагрози та розробити ефективні заходи з їх управління, що допоможе знизити фінансові втрати та пошкодити репутації компанії.

Застосування алгоритмів машинного навчання для виявлення аномальної активності. Використання алгоритмів машинного навчання дозволяє виявляти

аномальну або незвичайну активність, що може бути ознакою порушення цілісності інформації.

ПРАТ «Датагруп» може використовувати ці алгоритми для постійного моніторингу мережі та реагування на потенційні загрози в реальному часі.

Додатково компанії «Датагруп» рекомендується провести комплексне обстеження інформаційної системи та впровадити комплексну систему захисту інформації.

Застосування технології блокчейн для забезпечення цілісності даних. Технологія блокчейн може бути використана для створення надійної та нескладної системи збереження даних, яка гарантує їхню цілісність. ПРАТ «Датагруп» може розглянути можливість використання блокчейн-технології для збереження та обміну чутливою інформацією, такою як клієнтські дані та транзакції.

Такі рекомендації спрямовані на покращення захисту цілісності інформації на ПРАТ «Датагруп» та допоможуть підприємству ефективно впоратися з сучасними кіберзагрозами.

Описані рекомендації вказують на важливість впровадження комплексної стратегії захисту інформації на підприємстві.

Наочність і ефективність заходів захисту можуть бути покращені завдяки використанню сучасних технологій та методів, таких як Threat and Risk Assessment (TARA) та Factor Analysis of Information Risk (FAIR), які дозволяють ідентифікувати, оцінювати та управляти ризиками для цілісності інформації. Додатково, рекомендації передбачають постійне оновлення заходів захисту відповідно до змін у технологічному ландшафті та появі нових загроз.

Важливо також розглядати варіанти резервного копіювання та відновлення даних, що дозволяє швидко відновити цілісність інформації після інцидентів. Безперечно, ефективне впровадження цих рекомендацій допоможе підприємству підтримувати високий рівень цілісності своєї інформації, забезпечуючи надійну захищеність даних та впевненість клієнтів у безпеці їхньої інформації.

Висновки до третього розділу

Аналіз ризиків є важливим інструментом для забезпечення цілісності інформації на підприємстві. Він дозволяє виявити, оцінити і зменшити ризики, що можуть вплинути на безпеку інформації, забезпечуючи надійний захист даних. Для ПРАТ «Датагруп» регулярне проведення аналізу ризиків є необхідним для підтримки високого рівня інформаційної безпеки.

Оцінка загроз цілісності інформації на підприємствах є важливим етапом у забезпеченні інформаційної безпеки. Використання різних методів дозволяє отримати комплексне уявлення про потенційні ризики і розробити ефективні заходи для їх мінімізації. Для ПРАТ «Датагруп», як великого постачальника послуг зв'язку, важливо застосовувати всі вищезгадані методи для забезпечення високого рівня цілісності інформації.

SWOT-аналіз дозволяє отримати всебічне розуміння ситуації з інформаційною безпекою на підприємстві. Він допомагає визначити внутрішні та зовнішні фактори, які впливають на цілісність інформації, і розробити стратегії для мінімізації ризиків.

BIA є важливим інструментом для управління ризиками та забезпечення безперервності бізнесу. Він допомагає організаціям виявляти критичні процеси, оцінювати потенційні наслідки їх порушення та розробляти ефективні плани відновлення. Це дозволяє підприємствам підвищити свою стійкість до інцидентів та забезпечити безперервність своєї діяльності навіть у випадку несприятливих подій.

Методологія OCTAVE є важливим інструментом для комплексної оцінки ризиків інформаційної безпеки. Вона допомагає організаціям виявляти критичні активи, оцінювати загрози та вразливості, розробляти ефективні стратегії для зниження ризиків. Регулярне застосування OCTAVE дозволяє підвищити рівень захисту інформаційних ресурсів і забезпечити безперервність бізнес-процесів.

ВИСНОВКИ

На основі проведеного дослідження теоретичних та практичних аспектів оцінки загроз цілісності інформації на підприємствах можна зробити певні висновки.

Теоретичний аналіз показав, що сучасні підприємства стикаються з різноманітними загрозами, які можуть вплинути на цілісність їхньої інформації.

Інформація – це набір даних або фактів, які мають певний смисловий зміст та використовуються для прийняття рішень, розв’язання проблем, передачі повідомлень та спілкування. Вона може бути представлена у будь-якій формі, включаючи текст, зображення, звуки або відео, та зберігатися у різних форматах, таких як паперові документи, електронні файли чи бази даних. Інформація надає можливість отримувати, обробляти та передавати знання, що дозволяє людям та організаціям діяти більш ефективно та продуктивно.

Зокрема, визначено різні види загроз та їх класифікацію, що дозволяє краще розуміти сутність проблеми і вживати відповідних заходів безпеки. Особлива увага була приділена аналізу цілісності інформації, визначенню загроз, а також методам її забезпечення та захисту.

Так, у ході теоретичного аналізу було визначено, що загрози цілісності інформації на підприємствах є різноманітними та постійно змінюються в залежності від технологічного прогресу, соціальних та економічних трансформацій. Вони можуть бути класифіковані за різними критеріями, включаючи джерело походження, методи атаки та потенційні наслідки для інформаційних ресурсів.

Однією з основних категорій загроз є зовнішні загрози, такі як кібератаки, віруси, фішингові атаки та інші види зловмисного програмного забезпечення, що намагаються нанести шкоду інформаційним системам ззовні. Внутрішні загрози включають недбале ставлення до безпеки з боку персоналу, зловживання даними

або недбалість у збереженні та обробці інформації. Також до категорій загроз можуть відноситися природні катастрофи, технічні неполадки, а також випадкові помилки та недоліки в програмному забезпеченні. Крім того, загрози можуть бути класифіковані за їхнім впливом на конфіденційність, цілісність та доступність інформації, допомагаючи підприємствам краще розуміти природу потенційних ризиків та розробляти ефективні стратегії захисту.

Результати дослідження свідчать про необхідність постійного вдосконалення систем безпеки для забезпечення цілісності інформації на підприємствах. Також виявлено, що реалізація рекомендацій забезпечить ефективний захист інформації в умовах сучасних викликів та загроз.

Аналіз загроз інформації та її цілісності на підприємстві виявив різноманітні потенційні небезпеки, які можуть вплинути на безпеку та стійкість інформаційних ресурсів. Основні загрози включають кібератаки, несанкціонований доступ до даних, втрату чи зміну інформації, а також внутрішні проблеми, такі як людський фактор і технічні недоліки.

Для забезпечення цілісності інформації на підприємстві «Датагруп» було розроблено комплексний план заходів, включаючи оновлення систем захисту, впровадження нових технологій та методів шифрування даних, а також підвищення обізнаності персоналу щодо правил і процедур безпеки.

Виявлено, що необхідно посилити контроль за доступом до систем, регулярно оновлювати програмне забезпечення та здійснювати аудит інформаційної безпеки. Були запропоновані також заходи щодо підвищення стійкості мережі та резервного копіювання даних для запобігання втратам в разі аварій.

Визначено, що важливо регулярно оновлювати політики безпеки, впроваджувати системи моніторингу та виявлення вразливостей, а також здійснювати навчання персоналу з питань кібербезпеки. Крім того, рекомендується встановлення системи реагування на інциденти та постійне вдосконалення процедур відновлення після інцидентів для забезпечення швидкого відновлення

роботи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Архипов О.Є. Вступ до теорії ризиків: інформаційні ризики: монографія. Київ: Нац. акад. СБУ. 2015. 248 с.

2. Аудит інформаційної безпеки: підручник //тРомака В.А. та ін. Львів: СПОЛОМ, 2015. 363 с.

3. Бєлкіна І.А., Антонюк О.П., Діагностика безпеки цілісності інформаційного підприємства як соціально-економічної системи // Науковий вісник Міжнародного гуманітарного університету. №11. 2015. С.310-312.

4. Білоус АЯ., Репін М. В. Мінімізація ризиків на підприємстві шляхом впровадження системи екологічного менеджменту. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 31(70). № 1. 2020. С. 51–55.

5. Віннікова І.І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними // Східна Європа: Економіка, бізнес та управління. 2018. Вип. 5 (16). С. 110-114.

6. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кібер-ризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. №3. С. 101-115.

7. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

8. Дзюба Л.Ф., Чмир О.Ю. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики //Вісник ЛДУБЖД, №26, 2022. С.47-54.

9. ДСТУ IEC/ ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. [Чинний від 2014-07-01]. Вид. офіц. Київ, Мінекономрозвитку України 2015. 73 с.

10. Жадько К.С., Носова, Т.І., Горященко Ю.Г. Проблеми впровадження

передових світових технологій в умовах цифрового бізнесу // Новий погляд: економіка та управління. №1, 2022. С. 51-60.

11. Жовтяк Г.А., Серьогіна Д.О. Теоретико-методичні підходи до ціноутворення у системі маркетингу. Східна Європа: економіка, бізнес та управління. №1 (34), 2022. С.83-86.

12. Економічний енциклопедичний словник: у 2 т., Т.1 / Мочерний С.В. [та ін..]; за ред. С.В. Мочерного. Львів: світ, 2005. 616 с.

13. Закон України «Про доступ до публічної інформації». URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

14. ЗВІД. Datagroup Presentation. URL: https://www.datagroup.ua/storage/editor/files/zakhishcheniy-vuzol-internet-dostupu-datagrup.pdf

15. Інформаційна безпека. Підручник. Під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

16. Інформаційні технології в освіті та практиці: збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 20 грудня 2019 року / упорядник Т.В. Магеровська. Львів: ЛьвДУВС, 2019. 246 с.

17. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків: Вид. ХНЕУ, 2018. 196 с.

18. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Том 31 (70). № 5. 2020. С.69-74.

19. Комерціалізація інновацій: захист інтелектуального капіталу, маркетинг та комунікації: монографія / за заг. ред. канд. екон. наук, доц. Л. Ю. Сагер, канд. екон. наук, доц. Л. О. Сигиди. Суми: Сумський державний університет, 2022. 363 с.

20. Літвінчук І.С., Корчомний Р.О., Коршун Н.В., Ворохоб М.В. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2020.

№2(10), С. 98-112.

21. Наказ Міністерства юстиції України від 28 березня 2016 року №897/5 «Про затвердження Переліку інформації, що підлягає оприлюдненню у формі відкритих даних, розпорядником якої є Міністерство юстиції України». URL: https://ips.ligazakon.net/document/MUS26483?an=1&hide=true

22. Наказ Міністерства юстиції України від 31 січня 2023 року №423/5 «Про відновлення оприлюднення інформації у формі відкритих даних, розпорядником якої є Міністерство юстиції України». URL: https://minjust.gov.ua/n/22679

23. Наказ Містерства юстиції України від 04.05.2023 № 1638/5 «Про внесення зміни до наказу Міністерства юстиції України від 31 січня 2023 року № 423/5» URL: https://nais.gov.ua/files/general/2023/05/12/20230512102623-19.pdf

24. Нечаєва І.А., Дьордій Є.А. Управління ризиками підприємства в секторі ІТ-послуг як інструмент підвищення його конкурентоспроможності. Ефективна економіка. 2018. № 12. URL : http://www.economy. nayka.com.ua/?op=1&z=6797.

25. Огінок С.В., Янко, К.В. Етапи розвитку ринку криптовалют. Економіка і суспільство, №35. 2022. URL: http://www.economyandsociety.in.ua/ index.php/journal/article/view/1086/1043.

26. Офіційний сайт DATAGROUP. URL: https://www.datagroup.ua/en/pro-kompaniyu#about-info

27. Постанова Кабінету Міністрів України від 21 жовтня 2015 р. № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних». URL: https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text

28. 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.

29. Про інформацію: Закон України від 02.09.1992 р. № 2657-XII. Верховна Рада України. Отримано з https://zakon.rada.gov.ua/laws/show/2657-12#Text.

30. Рой Я.В., Мазур Н.П., Складанний П.М. Аудит інформаційної безпеки – основа ефективного захисту підприємства // Кібербезпека: освіта, наука, техніка. 2018.№ 1 (1). С. 86-93.

31. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану // Науковий вісник Ужгородського Національного Університету, 2023. С.121-127.

32. Черняк Т.Г. Оцінка ризиків інформаційної безпеки Інтернет речей. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. С. 53-55.

33. Яцків Н.Г., Вівчар Д.В., Черняк Т.Г. Аналіз підходів до оцінки ризиків. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. С. 104-106.

34. Alberts, Christopher, Dorofee, Audrey. OCTAVE Criteria Version 2.0. Carnegie Mellon Software Engineering Institute, 2001. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51849

35. AT&T Inc. URL: https://www.att.com/

36. Blockchain for Distributed Systems Security. URL: https://ieeexplore.ieee.org/document/7784455

37. Cisco Systems, Inc. URL: https://www.cisco.com/#tabs-35d568e0ff-item-194f491212-tab

38. FAIR (Factor Analysis of Information Risk). URL: https://www.fairinstitute.org/

39. Gleick, James. The Information: A History, a Theory, a Flood. Pantheon Books, 2011. URL: https://www.pantheonbooks.com/books/9780375423727

40. Hoffman, Martin L. Empathy and Moral Development: Implications for Caring and Justice. Cambridge University Press, 2001. URL: https://www.cambridge.org/core/books/empathy-and-moral-development/99D98C64569DB9B4EE20C8A6A4E2A141

41. IEC 61025:2006. Fault Tree Analysis (FTA). IEC, 2006. URL: https://webstore.iec.ch/publication/5107

42. ISO 31000:2018. Risk management – Guidelines. ISO, 2018. URL: https://www.iso.org/standard/65694.html

43. ISO/SAE 21434. Road vehicles – Cybersecurity engineering. URL: https://www.iso.org/ru/standard/70918.html

44. Shannon, Claude E. A Mathematical Theory of Communication. Bell System Technical Journal, vol. 27, no. 3, 1948, pp. 379-423, 623-656. URL: https://academic.oup.com/book/36500/chapter/321209428

45. Threat and Risk Assessment (TARA) Methodology and Data Standard. URL: https://www.nist.gov/publications/threat-and-risk-assessment-tara-methodology-and-data-standard

46. Verizon Communications Inc. URL: https://www.verizon.com/

47. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/standard/27001

ДОДАТКИ

Додаток А

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«22» грудня 2020 р. за № 22361
Дійсний до «22» грудня 2025 р.

Товариство з обмеженою відповідальністю «НікС»
(найменування державного органу/організації/підприємства/установи, яким видано Атестат)

засвідчує, що комплексна система захисту інформації

**захищеного вузла інтернет-доступу
приватного акціонерного товариства «ДАТАГРУП»
(шифр «КСЗІ-ЗВІД-ДАТАГРУП»),**
(найменування ІТС)

що належить **приватному акціонерному товариству «ДАТАГРУП»**
(найменування державного органу (організації, підприємства, установи) -

м. Київ, вул. Смоленська, буд. 31/33,
власника (розпорядника) ІТС, код ЄДРПОУ, місцезнаходження)

забезпечує захист інформації відповідно до вимог нормативних документів із технічного захисту інформації.

Експертний висновок на 43 аркушах додається до цього Атестата та є його невід'ємною частиною.

Вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Директор ТОВ «НікС» (підпис) **Дмитро ШАТАРСЬКИЙ** (власне ім'я, прізвище)

Додаток Б

IMS®

СЕРТИФІКАТ

На систему менеджменту згідно з
ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT)

Відповідно до процедур IMC справжнім сертифікатом підтверджується, що

ПрАТ «ДАТАГРУП»
вул. Смоленська, 31-33
03005, м. Київ
Україна

DATA GROUP НАДІЙНІСТЬ ТА ЗРУЧНІСТЬ

застосовує систему менеджменту згідно із зазначеним стандартом для наступної офери діяльності:

Надання доступу до мережі інтернет та каналів зв'язку; надання послуг контакт-центру; розробка та підтримка програмного забезпечення; надання послуг Центру обробки даних: послуги обробки та зберігання даних, хмарні послуги, послуги оренди та зберігання даних програмного забезпечення, послуги розміщення обладнання

З урахуванням заяви про застосовність версія 1.0 від 22.05.2018 р.

Реєстраційний номер сертифіката: 44 121 21 00 11
Звіт про аудит № 210011

Чинний від: 29.09.2021
Чинний до: 28.09.2024
Первинна сертифікація 2021

S. Dawydenko

Керівник сертифікаційного органу
ТОВ «Інтернешнл Менеджмент Сістемс»

м. Київ, 29.09.2021

Сертифікація проведена відповідно до затвердженої у IMC методики аудиту та сертифікації і підлягає періодичним наглядовим аудитам.

ТОВ «Інтернешнл Менеджмент Сістемс» вул. Пушкінська, 21 01004, Київ www.ims-cert.com

IAF

SO139
ДСТУ ISO/IEC 17021