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 ЕФЕКТИВНОСТІ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ В ОРГАНІЗАЦІЯХ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
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

Іван СЕЛІВАНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБД 41
Іван СЕЛІВАНОВ
Керівник:
к.е.н., доцент Тетяна КАПЕЛЮШНА

Рецензент:
д.т.н., професор Галина ГАЙДУР

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

Селіванову Івану Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Оцінка ефективності заходів захисту інформації від витоку в організаціях ”,
керівник кваліфікаційної роботи Тетяна Капелюшна Вікторівна
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “__“ березня 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека організації, методи та засоби захисту від витоку інформації безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Пояснення важливості забезпечення інформаційної безпеки в організаціях, аналізуючи загрози та шляхи витоку інформації.
4.2. Дослідити сучасні заходи захисту інформації в організації які використовуються для захисту від неавторизованого доступу.
4.3. Надання пропозиції щодо покращення заходів захисту інформації від витоку в організації
Перелік ілюстративного матеріалу: *презентація PowerPoint*

5. Дата видачі завдання “11” березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	виконано
2.	Збір та аналіз літератури.	29.03.2024	виконано
3.	Розгляд заходів захисту інформації в організаціях від витоку критично важливих даних	08.04.2024	виконано
4.	Дослідження та аналіз джерел витоку інформації та заходів захисту інформації в організації	22.04.2024	виконано
5.	Оцінка ефективності заходів для захисту інформації від витоку в організації та надання пропозицій щодо їх покращення	08.05.2024	виконано
6.	Формулювання висновків на основі отриманих результатів дослідження.	20.05.2024	виконано
7.	Оформлення роботи.	22.05.2024	виконано
8.	Оформлення презентації.	03.06.2024	виконано
9.	Отримання рецензії на роботу.	03.06.2024	виконано
10.	Захист в ЕК.	11.06.2024	виконано

Здобувач вищої освіти _____ Іван СЕЛІВАНОВ
(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 Селіванов І.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оцінка ефективності заходів захисту інформації від витоку в організаціях"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **СЕЛІВАНОВ Іван** у кваліфікаційній роботі відповідно до обраної теми, визначив напрями та методи дослідження для опрацювання питань за темою та вирішення поставлених завдань. **СЕЛІВАНОВ Іван** продемонстрував розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Результати дослідження апробовані на конференції, що доводить їх практичну значимість для підприємств.

Вищевикладене дозволяє оцінити виконану кваліфікаційну роботу здобувачем **СЕЛІВАНОВИМ Іваном** на високому рівні та 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. Здобувачка СЕЛІВАНОВ І.С. допускається до захисту даної 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 Селіванова Івана Сергійовича
на тему: “Оцінка ефективності заходів захисту інформації від витоку в організаціях”.

Актуальність. У постіндустріальному суспільстві та розбудові ринкової економіки, інформація стала ресурсом, якому притаманна така сама цінність, як і фінансовому, оскільки її витік призводить до шкоди репутації та збитків на підприємстві. Завдяки аналізу витоків інформації та їх оцінці можливо зрозуміти джерела витоків, вирахувати ефективність заходів захисту інформації, що націлені на протидію витокам. Інформаційні ресурси та інформаційна інфраструктура підлягають постійним атакам з боку зловмисників, частішають кіберінциденти щодо порушення цілісності даних, саме тому захист інформації є пріоритетним завданням у забезпеченні безпеки підприємств та організацій, що підтверджує актуальність обраної теми для дослідження.

Позитивні сторони

1. У роботі проведено аналіз джерел витоку інформації для подальшої їх оцінки та порівняння з пороговими значеннями для прийняття рішень щодо усунення потенційних можливостей її розповсюдження та порушення цілісності, конфіденційності.
2. Розроблено рекомендації для досліджуваного підприємства щодо усунення проблем, що убезпечить підприємство від майбутніх інцидентів витоку інформації.

Недоліки

Варто було б провести ґрунтовнішу оцінку витоків інформації на підприємстві, до прикладу, запропонувати для кожного рівня ефективності захисту інформації окремі рекомендації. Проте, це вказує на горизонт, що відкривається для майбутніх досліджень та суттєво не впливає на оцінку роботи.
Висновок: Кваліфікаційна робота виконана на достатньо високому рівні та, за умови успішного захисту, заслуговує високої оцінки, а здобувач Селіванов Іван Сергійович - присвоєння кваліфікації «Бакалавр кібербезпеки» за освітньою програмою “Управління інформаційною та кібернетичною безпекою”

Рецензент: завідувач кафедри Інформаційної та кібернетичної безпеки, д.т.н, професор — підпис — Галина ГАЙДУР *(Ім’я ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню оцінки ефективності заходів захисту інформації, що спрямовані на усунення її витоку. Робота складається зі вступу, трьох розділів, що містять 3 рисунків, 4 таблиці, 2 схеми висновків і списку використаних джерел із 48 найменувань. Загальний обсяг роботи становить 55 аркушів, з яких 4 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз заходів захисту інформації від витоку в організації

Об'єктом дослідження є організація та її інформаційна інфраструктура

Предметом дослідження - є заходи захисту, які вживаються для запобігання витоку інформації.

Метою дослідження є дослідження сучасних заходів захисту інформації в організації які використовують для захисту від неавторизованого доступу.

Короткий зміст роботи. У роботі вивчено "витоки інформації" компанії, їх вплив і взаємозв'язок з інформаційною безпекою. Проведено аналіз заходів захисту в їх впливу на компанію. Розглянуто шляхи удосконалення заходів захисту від витоку інформації, включаючи виявлення прогалин, розробку технології та їх застосування до загроз організацій. Висновки підкреслюють важливість заходів щодо захисту інформації в компанії .Кінцеві висновки акцентують актуальність теми та її практичну значущість, додається перелік посилань та демонстраційні матеріали.

Галузь застосування. Запропоновані рекомендації до захисту від витоку інформації можуть бути використані для поліпшення систем захисту організацій, у даний час, та протистояти викликам, що виникають в інформаційному полі її діяльності.

КЛЮЧОВІ СЛОВА: ВИТІК ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, ОРГАНІЗАЦІЯ, АНАЛІЗ ВИТОКУ ІНФОРМАЦІЇ,ПОЛІПШЕННЯ СИСТЕМИ ЗАХИСТУ.

ABSTRACT

The qualification work is devoted to the study of assessing the effectiveness of information security measures aimed at eliminating information leakage. The work consists of an introduction, three chapters containing 3 figures, 4 tables, 2 conclusions and a list of references of 48 titles. The total volume of the work is 55 pages, of which 4 pages are occupied by the list of abbreviations and the list of references.

The purpose of the work is to analyze the measures to protect information from leakage in the organization

The object of study is the organization and its information infrastructure

The subject of the study is the protection measures taken to prevent information leakage.

The purpose of the study is to investigate modern information security measures in the organization that are used to protect against unauthorized access.

Summary of the work. The paper examines the “information leakage” of the company, its impact and relationship with information security. An analysis of protection measures in terms of their impact on the company is carried out. Ways to improve information leakage protection measures, including gap identification, technology development, and their application to organizational threats, are considered. The conclusions emphasize the importance of information security measures in the company.The final conclusions emphasize the relevance of the topic and its practical significance, a list of references and demonstration materials are attached.

Scope of application. The proposed recommendations for protection against information leakage can be used to improve the protection systems of organizations, at present, and to confront the challenges arising in the information field of its activities.

KEYWORDS: INFORMATION LEAKAGE, INFORMATION SECURITY, ORGANIZATION, ANALYSIS OF INFORMATION LEAKAGE, IMPROVEMENT OF THE PROTECTION SYSTEM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – Інформаційні технології

ПЗ- Програмне забезпечення

ОС – Операційна система

ІБ – Інформаційна безпека

ІС – Інформаційна система

ВСТУП

Актуальність теми. Актуальність обраної теми визначається швидким розвитком технологій , що в свою чергу призводить до покращення в розробках кібератак, та кіберзагроз .Потенційні загрози для конфіденційності, цілісності та доступності , що стосуються даних стають все складнішими та не передбаченими. Незахищеність даних може призвести до серйозних наслідків для підприємств, таких як витрати на відновлення системи/даних , втрати репутації/клієнтів , юридична тяганина та інші негативні наслідки, що спричинені витоком даних.

Оцінка ефективності заходів захисту інформації покликана за для того щоб допомогти організаціям визначити наскільки ефективно їхні заходи захисту протистоять потенційним загрозам сьогодення.

Оцінка ефективності включає в себе наступні кроки для вирішення потреб у захисті організацій:

1)Аудит існуючих систем захисту – являє собою незалежну оцінку поточного стану системи інформаційної системи безпеки організації, відповідно до критеріїв захисту і надання результатів у вигляді рекомендацій інформаційної безпеки;

2)Оцінку ризиків – процес оцінки та аналізу ризиків, які можуть вплинути на організацію. Включає у себе індифікації загроз, виявлення на вразливостей та розробку стратегії управління ризиками;

3)Аналіз вразливостей системи - полягає у виявленні слабких місць в системах захисту, таких як недостатньо оновлене програмне забезпечення, недоліки у конфігурації систем або відсутність необхідних контрольних механізмів.

Загалом зважаючи на постійне зростання кількості кіберзагроз та швидкий темп змін у технологіях, оцінка ефективності заходів захисту інформації від витоку є невід'ємною частиною стратегії з забезпечення кібербезпеки підприємства будь-якої сучасної організації, що має на меті розвиток у майбутньому часі.

Метою роботи - є аналіз заходів захисту інформації від витоку в організації.

Об’єктом дослідження - є організація та її інформаційна інфраструктура.

Предметом дослідження - є заходи захисту, які вживаються для запобігання витоку інформації.

1. Проаналізувати заходи щодо захисту від витоку інформації.

2.Дослідження основних джерел витоків інформації в організації.

3.Аналіз методів ефективності заходів від витоку інформації та їх оцінка.

Метою дослідження - є дослідження сучасних заходів захисту інформації в організації які використовують для захисту від неавторизованого доступу.

Практичне значення - полягає у покращенні безпеки даних та зниженні ризиків для організацій , його клієнтів і партнерів.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року, тези: «Оцінка ефективності заходів захисту інформації як потреба протидії її витоку в організаціях».

РОЗДІЛ 1
ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ ВІД ВИТОКУ

1.1. Інформація як об’єкт захисту в організаціях

У сучасному світі стрімко зростає роль інформації у всіх сферах життя.

Ця тенденція пов'язана з фундаментальними змінами, спрямованими на підвищення якості життя людей і досягнення загального блага. Інформація стала одним із ключових ресурсів, що визначає конкурентоспроможність та ефективність діяльності будь-якої галузі.

Інформація – це сукупність даних, які мають певне значення або інтерпретацію. Тому розглянемо термінологічне поняття слова «інформація». Слово «інформація» походить від латинського слова «informatio», що означає пояснювати або представляти щось. Офіційне визначення терміну «інформація» наведено у статті 1 «Про інформацію» Закону України, згідно з якою інформація — це будь-яка інформація або дані, які можуть зберігатися на матеріальних носіях або в електронній формі [5].

У бізнесі інформація відіграє важливу роль у прийнятті ділових рішень, плануванні, аналізі результатів діяльності та спілкуванні з клієнтами, партнерами та конкурентами як всередині, так і за межами організації.

Інформація - дані, що є одними з найцінніших активів для бізнесу та організацій. Інформація компаній включає в собі такі типи даних: конфіденційні дані клієнтів, стратегічні плани, фінансові дані, інтелектуальну власність, особисті дані співробітників та інші типи інформації, що належать компанії. Захист даних типів інформації має величезне значення для компанії, оскільки має критичну цінність для неї. Типи інформації поділяються на відкриту та з обмеженим доступом.

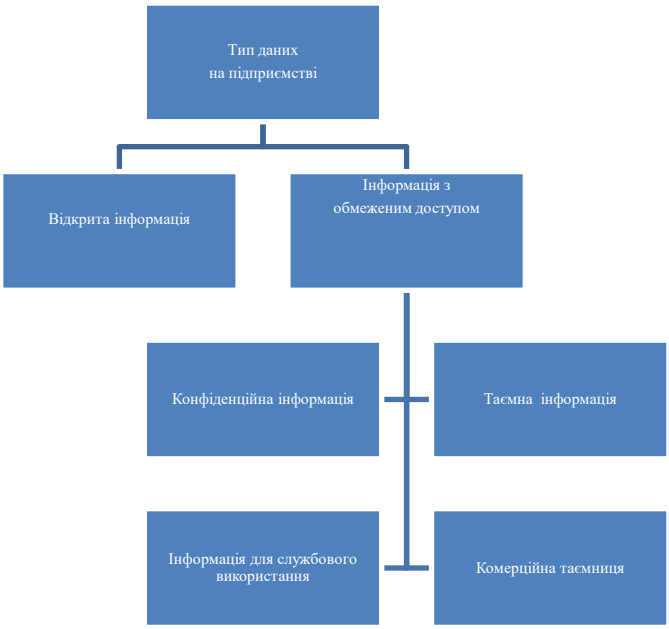

Схема. 1.1Типи даних на підприємстві

На основі жерела:[1]

Нас цікавить з обмеженим доступом, а саме – конфіденційна, адже саме вона, як правило є одним з об'єктів захисту на підприємстві. Вона поділяється на:

1) Конфіденційна інформація - включає особисті дані, комерційні таємниці, медичні записи, фінансову інформацію тощо. Доступ до неї мають лише уповноважені особи, захищається законодавством: Законом України "Про захист персональних даних".

2) Таємна інформація - державні таємниці, військова інформація, інформація, що стосується національної безпеки. Потребує спеціального дозволу для доступу і суворих заходів захисту, регулюється законодавством: Законом України "Про державну таємницю".

3) Інформація для службового користування - інформація, яка не є державною таємницею, але потребує обмеження доступу для службового використання. Часто зустрічається в організаціях, компаніях та урядових установах.

4) Комерційна таємниця - включає будь-яку інформацію, що має комерційну цінність і не є загальнодоступною. Компанії застосовують заходи для захисту такої інформації шляхом підписання угод про конфіденційність. [1]

Організація має піклуватися про захист інформації своє компанії, оскільки тоді можуть статися витоки інформації, кібератаки, внутрішні загрози.

Захист інформації - діяльність із забезпечення доступності, конфіденційності та цілісності важливої інформації, яка обробляється в інформаційних, телекомунікаційних або інформаційно - телекомунікаційних системах, або озвучується на об'єктах інформаційної діяльності, а також із забезпечення використання інформації.

Конфіденційність, доступність та цілісність є властивостями, що характеризують інформацію як об'єкт захисту

Рис.1.1 Тріада інформаційної безпеки

Джерело: [2].

Конфіденційність — властивість інформації, яка характеризує захищеність інформації від не санкціонованого доступу.

Цілісність — властивість інформації, яка характеризує захищеність інформації від несанкціонованого спотворення, або зміни даних в ній.

Доступність — властивість інформації, яка характеризує захищеність інформації від несанкціонованого блокування.[3]

Щоб захистити інформацію ми маємо впровадити політику інформаційної безпеки, вона має здійснюватися шляхом комплексного підходу, політика

інформаційної безпеки має встановлювати відповідальність вищого керівництва, його цілі і принципи щодо дотримання інформаційної безпеки; є дієвим засобом успішного проходження процедури проведення сертифікації у цій сфері. Хоча розробка політики інформаційної безпеки є початковим етапом процедури проведення сертифікації та починається з аналізу ризиків у цій сфері, але вона в числі визначення оптимального рівня ризику. Досягнення такого цього рівня має стати визначальним кроком для розробки системи управління інформаційною безпекою. Наступним кроком є аналіз інформаційних ресурсів, визначення їх цінності та побудова моделі взаємозв'язків між ними. Отримана модель дає можливість вибрати найоптимальніший спосіб для протидії інформаційним ризикам та дотримання плану щодо стратифікації системи управління. На останок нам буде потрібно розробити документації в сфері забезпечення інформаційної безпеки. У результаті зроблених дій ми маємо створити документацію, що має на меті допомогти компанії, але компанія має дотримуватися наведених там правил та настанов у сфері політик інформаційної безпеки.[4]

1.2. Причини витоку інформації в організаціях

Витік інформації, також відомий як витік даних або розкриття інформації, являє собою тип загрози кібербезпеки, при якій конфіденційна інформація випадково або навмисно передається стороннім особам. Це може статися з різних причин, таким як людська помилка, слабкі засоби контролю безпеки, уразливості програмного забезпечення або кібератаки.

Витік інформації може приймати різні форми, такі як:

1.Несанкціонований доступ до конфіденційних файлів або документів, що включає в себе отримання конфіденційних даних особами, що не мають право на доступ. Це може бути здійснено шляхом зламу, використання прогалин у системі

захисту або отримання доступу до таких приміщень як серверна. Ось історія деяких компаній що постраждали:

А) Yahoo

У 2013 році Yahoo зазнала одного з найбільших витоків даних в історії, коли хакери отримали доступ до даних понад 3 мільярдів акаунтів користувачів. Зловмисники отримали особисту інформацію, включаючи імена, електронні адреси, телефонні номери, дати народження та хешовані паролі. Цей інцидент значно вплинув на репутацію компанії та призвів до фінансових втрат

В) Facebook

У 2018 році компанія Facebook повідомила про витік даних, який торкнувся 87 мільйонів користувачів. Інцидент стався через використання додатку Cambridge Analytica, який збирав особисту інформацію користувачів без їхньої згоди. Цей витік викликав великий скандал і призвів до посилення регуляторного нагляду та змін у політиці приватності компанії.

2.Випадковий обмін конфіденційною інформацією з електронної пошти, соціальних мереж або іншими каналами зв'язку. Може статися через не коректне використовування соцмереж, користування поштою. Зловмисники отримують конфіденційну інформацію через працівників компанії шляхом їхньої недбалості. Ось історія деяких компаній що постраждали:

А) British Airways

У 2018 році British Airways повідомила про випадковий витік даних, коли особиста та фінансова інформація близько 380 тисяч клієнтів була ненавмисно розкрита через уразливість у системі онлайн-бронювання. Хоча це не був класичний випадок випадкового обміну інформацією через електронну пошту, витік стався через неналежну конфігурацію системи, що дозволило зловмисникам отримати доступ до конфіденційної інформації.

А) Wells Fargo

У 2017 році банк Wells Fargo випадково надіслав конфіденційну інформацію про 50 тисяч клієнтів адвокатам у справі про позов. Ця інформація включала імена, номери соціального страхування, номери рахунків і транзакції. Інцидент стався через помилку працівника, який відправив файли електронною поштою без належної перевірки.

Б)Coca-Cola

У 2014 році компанія Coca-Cola зазнала інциденту, коли співробітник випадково передав конфіденційну інформацію про понад 70 тисяч працівників, включаючи номери соціального страхування та інші особисті дані. Інцидент стався через втрату зашифрованого пристрою з даними.

В)SolarWinds

У 2020 році компанія SolarWinds зазнала масового кібератаку через уразливості в їх програмному забезпеченні Orion. Хакери, пов'язані з Росією, змогли вбудувати шкідливий код у оновлення програмного забезпечення, що використовувалося тисячами клієнтів, включаючи урядові установи США та великі корпорації. Це дозволило зловмисникам отримати доступ до конфіденційної інформації та мереж багатьох організацій.

4. Неадекватні заходи захисту даних, такі як слабке шифрування або небезпечні методи зберігання. Приймає таку форму коли компанія нехтує заходами щодо захисту системи. Ось історія деяких компаній що постраждали:

А) Equifax - 2017 році компанія зазнала масового витоку даних через уразливість в програмному забезпеченні Apache Struts, яка не була вчасно оновлена. Хакери скористалися цією уразливістю для доступу до конфіденційної інформації, включаючи імена, соціальні номери страхування, дати народження, адреси та номери водійських посвідчень понад 147 мільйонів людей. Цей інцидент викликав значні фінансові та репутаційні втрати для компанії.

Б) Target - у 2013 році компанія постраждала від витоку даних через уразливість у їх системах POS (Point of Sale). Хакери використали цю вразливість

для встановлення шкідливого програмного забезпечення, яке збирало дані кредитних та дебетових карток клієнтів. В результаті було скомпрометовано дані понад 40 мільйонів карток, що призвело до значних фінансових втрат та шкоди репутації.

В) Marriott International - у 2018 році Marriott International виявила витік даних, який тривав з 2014 року і був пов'язаний з уразливістю у системах бронювання, що використовувалися їх дочірньою компанією Starwood. Хакери отримали доступ до конфіденційної інформації про 500 мільйонів гостей, включаючи імена, адреси, номери телефонів, електронні адреси, номери паспортів та інформацію про готельні номери. Інцидент викликав значні фінансові втрати та шкоду репутації [1].

Фактори витоку інформації в організаціях можна поділити на такі групи:

- Персонал

Кожен співробітник є потенційною загрозою інформаційній безпеці, і компанія, в якій вони розташовані, не може бути захищена від цього фактора витоку.

Працюючи з даними, людина зберігає робочі файли на різних носіях, переносить їх на альтернативні електронні листи та спілкується з друзями, які можуть далі поширювати цю інформацію протягом усього робочого часу. Дії HR поділяються на навмисні та ненавмисні.

У разі навмисного витоку інформації зловмисники вчиняють такі злочини, як: продаж даних, вимагання тощо. Ненавмисні дії відбуваються внаслідок ігнорування працівниками нормативної документації компанії щодо інформаційної безпеки. Плинність працівників відбувається частіше, коли умови праці недостатньо високі, коли в компанії відбуваються різного роду скорочення чи реструктуризація тощо. Головний офіс переїхав до нової будівлі. У цьому випадку підвищується ризик витоку інформації через недбалість недобросовісних працівників або співробітників, які допомагають у переїзді.

- Співпраця

Вона є важливою частиною розвитку компанії, але цей процес може бути дуже ризикованим. Коли ви співпрацюєте над проектами з іншими компаніями, більше людей мають доступ до ваших даних, тому часто неможливо повністю захистити ваші дані.

- Використання складних систем обробки інформації

Великі компанії часто використовують складні багаторівневі системи захисту та передачі даних, що, як це не парадоксально звучить, може призвести до некомпетентності Зростає ризик витоку інформації з боку людських ресурсів. Наприклад, один адміністратор бази даних змінює деякі правила обмеження доступу, а інший адміністратор не враховує це і випадково надає доступ до сервера бази даних співробітнику, якому не слід було надавати його.

- Збої програмного забезпечення

На жаль, навіть найновіші та найдосконаліші програми, включаючи програмні засоби захисту вашої інформації, можуть виходити з ладу. На жаль, ніхто не застрахований від помилок програмного забезпечення, а помилки програмного забезпечення надзвичайно поширені. Важливо підтримувати постійну працездатність програмних компонентів вашої системи захисту, тому що в разі несправності важлива інформація може бути перехоплена третіми особами. Крім того, ви завжди повинні зберігати резервну копію своїх даних на інших захищених носіях, оскільки помилки програмного забезпечення можуть призвести до видалення інформації з вашого пристрою.

- Помилки в роботі технічних заходів

Пристрої можуть виходити з ладу з різних причин, що може призвести до витоку інформації. Наприклад, через сервісний центр, куди привозять несправну техніку.

- Проблеми з роботою сервера

Великі компанії часто використовують хмарні обчислення, оскільки це полегшує доступ до інформації для працівників і прискорює обробку всієї

інформації. На жаль, останнім часом кількість хакерських атак на сервери зросла. Крім того, проблеми з нашими серверами можуть виникнути через погодні умови або інші непередбачені події [19, 20, 21]

Таблиця 1.1

Причини витоку інформації в компаніях

Назва компанії	Причина	Характеристика
Сінево	Атака на систему Хакерським угрупуванням “XakNet Team”.	Отримання та оприлюднення даних клієнтів компанії, з них - 226 тисяч унікальних адрес, 437 унікальних номерів.
Київстар	Напад на систему Російського хакерського угрупування «Солнцепек».	У ході атаки було знищено більше 10 тисяч комп’ютерів, та більше 4 тисяч серверів. Під час своїх дій хакери дібралися до хмарного сховку з даними і резервним копіюванням.
Facebook	Через використання додатку Cambridge Analytica.	Даний додаток збирав особисту інформацію користувачів без їхньої згоди.
Target	Уразливість системах POS (Point of Sale).	Хакери використали вразливість компанії, для встановлення шкідливого програмного забезпечення, яке збирало дані клієнтів.
Equifax	Неадекватні заходи захисту даних (слабке шифрування).	Масовий витік даних через уразливість в програмному забезпеченні, через не своєчасне оновлення системи захисту.
Wells Fargo	Обмін конфіденційною інформацією з електронної пошти.	Витік стався через помилку працівника, який відправив файли електронною поштою без належної перевірки.
Yahoo	Несанкціонований доступ до конфіденційних файлів.	Хакери отримали доступ до даних понад 3 мільярдів акаунтів користувачів

На основі джерел[19, 20, 21]

Наша країна також не виняток з точки зору нападів кіберзлочинних на організації , які бажають отримати бажану інформацію, з цілью отримати викуп за неї, або найчастіше використовують для оприлюднення внутрішньої інформації, яка належить тій чи іншій організації.

Розглянемо випадок хакерської атаки на компанію "Київстар" 12 грудня цього року. У наслідок атаки не працював зв'язок, домашній та мобільний інтернети. За кіберзлочин взяла відповідальність - Російське хакерське угруповання «Солнцепек». А така почалась приблизно о 8.05 ранку. Багато хто думав що це звичайний збій системи, але вже за короткий проміжок часу стало відомо, що хакери здійснили атаку на ядро мережі та інфраструктуру організації. У ході атаки було знищено більше 10 тисяч комп'ютерів, та більше 4 тисяч серверів. Під час своїх дій хакери дібралися до хмарного сховку з даними і резервним копіюванням.

У результаті цієї атаки на найбільшого мобільного оператора було позбавлено зв'язку близько половини населення України. Атака на ядро мережі була серйозним ударом по операторам, оскільки саме воно обробляло весь трафік, який передавався через мобільну мережу. Це також вплинуло на роботу банків, таких, як "Ощадбанк". Оскільки вони мали POS-термінали та банкомати, оскільки працювали з сервісами компанії "Київстар". Також зауважмо що ця атака спонукала користувачів мобільних "Київстар" переходити на інших операторі, тим самим компанія втрачала клієнтську базу, але люди були готові стояти в чергах, а інші компанію навіть змогли наживитися на цьому кіберзлочині, оскільки зміна сім-карти вартувала великих коштів для тих хто в день кібератаки змінював оператора зв'язку [37,38].

Також 10.01.2023 було скоєне ще одна атака на IT-інфраструктуру української мережі медичних лабораторій "Сінево" (synevo.ua). Злочинці з хакерського угруповання "XakNet Team" отримали данні персональні дані клієнтів та пацієнтів організації – ПІБ клієнтів та замовників послуг, адреси електронних поштових скриньок (приблизно 226 тисяч унікальних адрес), телефонні номери(приблизно у 437 унікальних номерів), та іншу приватну інформацію.

Це угруповання не вперше атакує інфраструктуру нашої країни, раніше розповсюджували облікові записи “Міністерства Фінансів України”, дані “Агентства розвитку інфраструктури фондового ринку України”[39].

1.3 Заходи захисту інформації від витоку в організаціях

Враховуючи сучасний технологічний розвиток і збільшення кількості кібератак, захист інформації стає все більш важливим для бізнесу. Витік інформації може призвести до серйозних наслідків, у тому числі до фінансових втрат, шкоди репутації та юридичних проблем. Тому організації повинні впроваджувати комплексні заходи захисту інформації, які включають технічні, організаційні та фізичні заходи. Нижче наведено основні заходи, які можуть допомогти зменшити ризик витоку даних.

1.Навчання та обізнаність працівників:

А) Регулярне навчання - воно допомагає працівникам краще розуміти потенційні загрози та навчитися уникати типових помилок. Навчання може охоплювати такі теми, як фішингові атаки, безпечне використання програмного забезпечення та правила обробки конфіденційної інформації.

Б) Інструкції з безпеки - розробка та впровадження чітких інструкцій з безпеки є ключовим елементом захисту інформації. Розробники політики повинні встановити правила обробки конфіденційних даних, вимоги до пароля, процедури реагування на інциденти тощо. Співробітники повинні бути ознайомлені з цією політикою та дотримуватися її.

В) Інформаційні кампанії - постійне нагадування співробітникам про важливість дотримання правил безпеки за допомогою інформаційних бюлетенів, плакатів і внутрішньої комунікації може допомогти підтримувати високий рівень обізнаності та обізнаності з проблемами кібербезпеки.

2.Технічні заходи захисту:

А) Шифрування даних- конфіденційність може бути забезпечена за допомогою сучасних процедур шифрування для захисту даних як під час передачі, так і в стані спокою. Шифрування гарантує, що навіть якщо дані перехоплено, зловмисник не зможе отримати до них доступ.

Б) Антивірусне програмне забезпечення- для захисту від зловмисного програмного забезпечення важливо встановлювати та регулярно оновлювати антивірусне програмне забезпечення. Антивірусні програми виявляють і видаляють віруси, троянські програми та інше шкідливе програмне забезпечення, яке може загрожувати безпеці ваших даних.

В) Брандмауер- налаштування брандмауера для контролю трафіку може запобігти неавторизованому доступу до вашої мережі. Вони блокують підозрілий трафік і захищають вашу внутрішню мережу від зовнішніх загроз.

Г) Система запобігання вторгнень (IDS/IPS)- ви можете захистити свою мережу від атак, встановивши систему виявлення та запобігання вторгненням, яка відстежує та блокує підозрілу активність. Системи IDS/IPS аналізують трафік і виявляють аномалії, які можуть свідчити про спробу зловмисника зламати систему.

3.Контроль доступу:

А) Зведення до мінімуму прав доступу- надання працівникам доступу лише до інформації, необхідної для виконання роботи, зменшує ризик витоку даних. Принцип найменшого доступу гарантує, що кожен працівник має доступ лише до тих ресурсів, які йому справді потрібні.

Б) Двофакторна автентифікація (2FA)- її реалізація підвищує безпеку під час входу у вашу систему. 2FA вимагає додаткової перевірки на додаток до вашого пароля, що робить доступ до вашої системи більш безпечним.

В) Періодичні перевірки доступу- періодичні перевірки та оновлення прав доступу допомагають належним чином контролювати доступ до конфіденційної інформації.

4.Керування вразливими місцями:

А) Оновлення програмного забезпечення- регулярне встановлення операційної системи та оновлень програмного забезпечення та виправлень допомагає усунути вразливості, якими можуть скористатися зловмисники під час атак. Тако ж своєчасне оновлення знижує ризик експлойтів.

Б) Оцінка вразливості- виконання регулярних тестів на вразливість для виявлення та усунення вразливостей у вашій системі допомагає переконатися, що ваша система захищена. Тести на проникнення та сканери вразливостей можуть допомогти виявити потенційні загрози.

В) Використання надійного програмного забезпечення- використання програмного забезпечення від перевірених постачальників, які регулярно випускають оновлення безпеки, зменшує ризик використання вразливого програмного забезпечення.

5. Політика безпеки:

А) Політика керування паролями- встановлення вимог до складності паролів, їх регулярна зміна та використання менеджера паролів можуть допомогти забезпечити надійний захист облікового запису. Складні паролі важко зламати, а їх регулярне оновлення знижує ризик злому.

Б) Резервне копіювання даних- регулярне резервне копіювання важливих даних і зберігання їх у безпечному місці може допомогти запобігти втраті інформації. Резервне копіювання дозволяє швидко відновити дані в разі аварії.

В) Політика використання персональних пристроїв (BYOD)- встановлення правил використання працівниками персональних пристроїв у корпоративних цілях, включаючи вимоги безпеки, може допомогти зменшити ризик витоку даних через персональні пристрої.

6.Фізична безпека:

А) Контроль доступу до об’єктів- встановлення системи контролю доступу

для обмеження фізичного доступу до серверних приміщень та архівів забезпечує захист даних від несанкціонованого фізичного доступу.

Б) Безпека пристрою- використання замків та інших заходів безпеки на ноутбуках та інших портативних пристроях може захистити їх від крадіжки. Фізична безпека вашого пристрою зменшує ризик втрати даних у разі крадіжки.

В) Охорона будинків- встановлення системи відеоспостереження та сигналізації для забезпечення безпеки вашого приміщення допоможе запобігти несанкціонованому доступу та виявити спроби злому [23,24,25]

Таблиця 1.2

Заходи захисту інформації від витоку в організаціях

Захисний захід	Характеристика
Навчання та обізнаність працівників	Допоможе працівникам краще розуміти потенційні загрози та навчитися уникати типових помилок.
Розробка новітніх інструкції з безпеки	Впровадження чітких інструкцій безпеки, які включатимуть - обробки конфіденційних даних, вимоги до складання паролів, та інше.
Система запобігання вторгнень (IDS/IPS)	Данні системи спеціалізуються на виявленні та запобігання вторгненням, вони відстежують та блокують підозрілу активність у системі.
Обмеження прав доступу	Надання працівникам доступу лише до інформації, необхідної для виконання роботи.
Керування вразливими місцями	До цього заходу входять - виконання регулярних тестів на вразливість, використання програмного забезпечення від перевірених постачальників, оновлень програмного забезпечення.

Продовження таблиці 1.2

Запровадження політики безпеки	Включає встановлення вимог до складності паролів, копіювання важливих даних, встановлення правил використання працівниками персональних пристроїв
Контроль доступу до об’єктів	Має на меті встановлення системи контролю доступу для обмеження фізичного доступу до серверних приміщень та архівів.

Узагальнено з джерел[23,24,25]

Висновки до першого розділу

Усі підрозділи цієї теми підкреслюють важливість захисту інформації в організаціях. Інформація є критично важливим активом і має бути належним чином захищена від різних загроз, таких як порушення даних, кібератаки та несанкціонований доступ. Для ефективного захисту інформації організації повинні прийняти комплексний підхід, який включає технічні, організаційні та процесуальні заходи безпеки.

Постійне вдосконалення та впровадження новітніх методів захисту має вирішальне значення для запобігання витоку даних і підтримки довіри клієнтів і партнерів. Організації повинні розуміти, що інформація є критично важливим ресурсом, і вони відповідають за забезпечення її безпеки для підтримки конфіденційності, цілісності та доступності даних.

РОЗДІЛ 2

АНАЛІЗ ДЖЕРЕЛ ВИТОКУ ТА ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЇ

2.1 Загальна характеристика підприємства

Фірму ТОВ «ДОЛЯ І КО. ЛТД», код ЄДРПОУ 01043342, було зареєстровано 09.04.1992. Розмір статутного капіталу фірми складає 200 000,00.

Керівником компанії ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДОЛЯ І КО. ЛТД" є ТАТАРІНЦЕВА ЛАРИСА АНАТОЛІЇВНА, ТАТАРІНЦЕВА ЛАРИСА АНАТОЛІЇВНА, ТАТАРІНЦЕВ АНДРІЙ ЛЕОНІДОВИЧ.

Організаційно-правова форма компанії ТОВ ДОЛЯ І КО. ЛТД" - ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ.

Основний вид діяльності (КВЕД) – 26.30 Виробництво обладнання зв'язку.

Контактні відомості організації «ТОВ ДОЛЯ І КО. ЛТД»

Телефон: 0444557777 0444557777

Установа ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДОЛЯ І КО. ЛТД" зареєстрована за юридичною адресою Україна, **5, місто Київ, ПРОВУЛОК ПАМВИ БЕРИНДИ.[7]

«ДОЛЯ І КО. ЛТД» - компанія що спеціалізується на інтеграції професійних засобів зв’язку та є постачальником комплексних рішень у сфері цивільного захисту та громадської безпеки.

На ринку послуг має 31 рік успішного досвіду роботи як системного інтегратора інфраструктурного радіообладнання та розробника засобів захищеного зв'язку. Компанія є частиною критичної інфраструктури країни, оскільки співпрацює у різних сферах життєдіяльності країни.

Ключових замовників є Міністерство оборони України, СБУ, Державна прикордонна служба України, Національна поліція Україна, Управління держаної охорони України.

Сьогодні у організації розробляють оптимальні, та нові рішення що допоможуть компаніям підвищити свою ефективність на ринку та бути конкурентноспроможними.

ДОЛЯ І КО. ЛТД – це українська компанія інтегратор, що пропонує телекомунікаційні послуги у великих обсягах, включаючи:

- PTT Over Cellular (Широкосмуговий PTT-зв'язок для професійного користування).

Це технологія, що використовує широкосмугові мобільні та Wi-Fi мережі для миттєвого з'єднання через натискання однієї кнопки Push-to-Talk. Технологія здобула популярність завдяки здатності забезпечити швидкий зв'язок на великих відстанях при відсутності витрат на розгортання і технічне обслуговування інфраструктури та радіообладнання у порівнянні з мережами LMR. [12]

- Будівництво систем професійного радіозв’язку та оповіщення. Проектування, будівництво, налаштування та супровід систем спеціалізованого технологічного та оперативного радіозв’язку.[13]

- Діагностика та ремонт обладнання. Гарантійне та післягарантійне обслуговування, діагностика та ремонт радіообладнання і засобів зв'язку. [14]

- Криптографічний та технічний захист інформаці. Послуги з розробки засобів криптографічного та технічного захисту інформації, володіння нормативною базою у сферах криптографічного та технічного захисту інформації КЗІ та ТЗІ, та практичний досвід реалізації власних проєктів робить спеціалістів відділу інформаційної безпеки компанії «ДОЛЯ І КО.ЛТД» експертами своєї справи. Відповідність українським стандартам використання криптографічних алгоритмів та протоколів і міжнародним нормам дозволяє нам успішно конкурувати з іноземними компаніями.[11]

- Навчання персоналу замовника. Індивідуальні програми професійного навчання персоналу замовника роботі з обладнанням, також експлуатація телекомунікаційної системи та її окремих складових вимагає навичок та знань, і спеціалісти авторизованого тренінг-центра «ДОЛЯ І КО. ЛТД» готові їх надати. Як компанія, що сфокусована на комплексному вирішенні завдань, ми не тільки постачаємо та налаштовуємо обладнання нашим замовникам, але й розробляємо учбові програми, розраховані на різні рівні підготовки персоналу. [10]

- Реєстрація та супровід. Консалтингові послуги та супровід при отриманні дозволів на користування радіочастотним ресурсом України. Компанія «ДОЛЯ І КО. ЛТД» представляє інтереси замовників, що не надають телекомунікаційних послуг, та супроводжує на різних етапах взаємодії з радіочастотними регуляторами України. Їхня мета — спрощення процесу отримання дозвільних документів для замовників та надання кваліфікованої допомоги із повним супроводом та підготовкою до кожного етапу взаємодії з органами влади. [9]

- Технічний аудит. Виконується у телекомунікаційної системи — являє собою комплексну перевірка роботи інфраструктури зв'язку та її складових. Проводиться для оцінки загального стану системи радіозв’язку та її оптимізації. Періодичне проведення аудиту необхідне для вчасного виявлення можливих несправностей системи, оцінки пов’язаних з ними ризиків й того, наскільки наявна інфраструктура відповідає сучасним бізнес-вимогам замовника, і чи готова вона до змін у майбутньому. [8]

Рисунок. 2.1 Послуги ІКТ компанії «ДОЛЯ І КО. ЛТД»

Компанія також пропонує такі стандарти/технології [6]:

1.DMR- Digital Mobile Radio (Цифровий Рухомий Радіозв'язок) – це відкритий стандарт для цифрового радіозв'язку. Розроблений і описаний ETSI(Європейський інститут телекомунікацій стандартів) в 2005 році.

2.TETRA- інфраструктурне обладнання для облаштування IP-інфраструктури різного рівня масштабованості у сферах громадської безпеки, нафтової промисловості, транспорту, комунікаційних служб та комерції.

3.MIMO- (Multiple Input Multiple Output), метод просторового кодування сигналу, що дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві, або більше антен і така ж кількість антен для прийому інформації.

4.APCO 25 – (Terrestrial Trunked Radio), відкритий стандарт цифрового транкінгового радіозв'язку, розроблений Європейським інститутом телекомунікаційних стандартів ETSI, для заміни застарілого стандарту MPT 1327.

5.LITE – комплекс інфраструктурних рішень та пристроїв для забезпечення широкополосного бездротового зв'язку в службах громадської безпеки та груп екстреного реагування в кризових ситуаціях.

6.PMR 446 – являє собою не ліцензований УВЧ (UHF) діапазон радіозв'язку доступний для персональних та ділових потреб у більшості країн Європейського союзу та в Україні. Як і у більшості країн союзу, в Україні можливе використання даного рішення, за умов включення абонентських станцій до переліку радіоелектронних засобів.

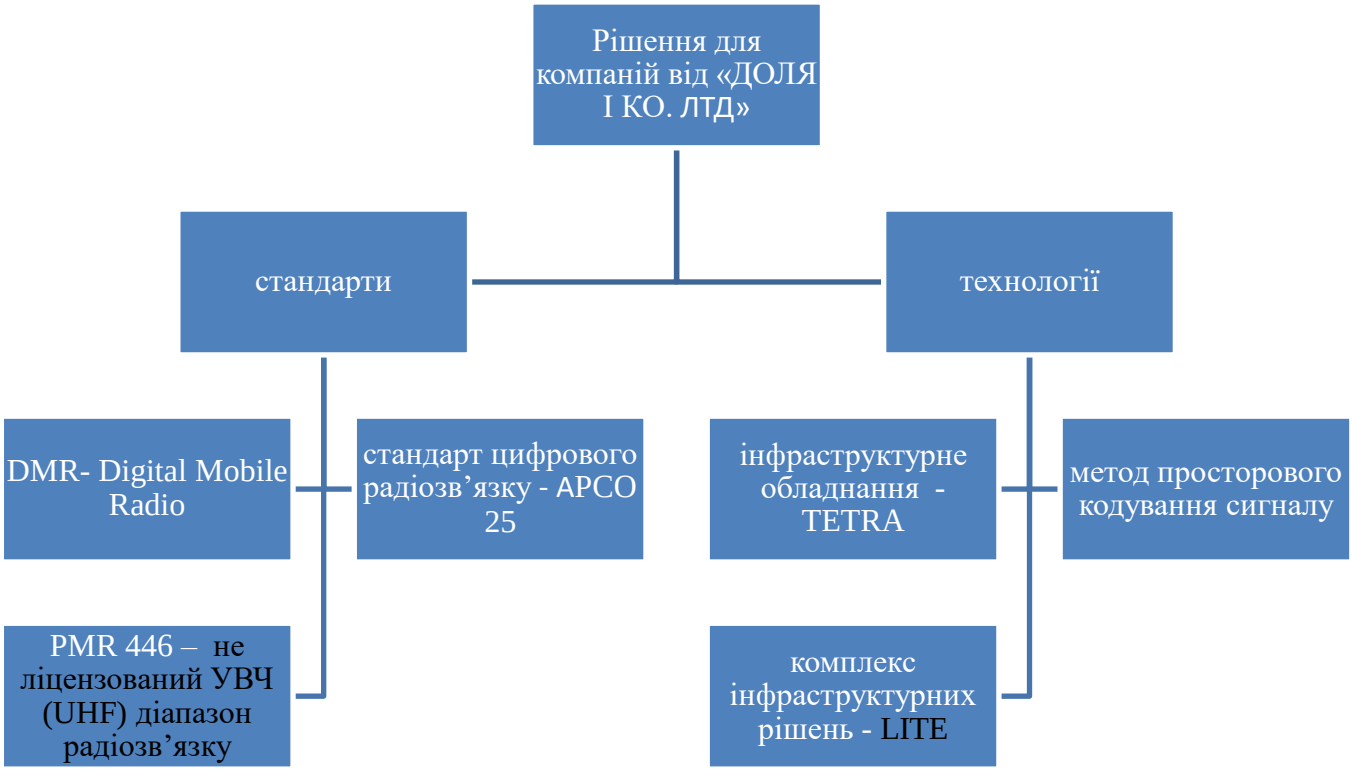

Схема. 2.1 .Пропоновані компанією «ДОЛЯ І КО. ЛТД»

стандарти та технології

2.2 Аналіз джерел витоку інформації в організації

На даний час існує безліч джерел витоку інформації, це пов'язано зі швидким розвитком інтернет систем, автоматизації процесів та розвитку штучного інтелекту. Тому зараз компанії мають бути більш прискіпливішими та не мають економити на системах захисту своєї компанії, бо якщо не вкластися вчасно в захист, під час атак, або несанкціонованого доступу до баз даних компанії як правило втрачають більше, а інколи доходить до летальних випадків, при яких компанія може стати банкротом.

Нашим об’єктом дослідження, щодо аналізу джерел витоку інформації в організації стала компанія «ДОЛЯ І КО. ЛТД». Проаналізуємо на її прикладі, а точніше на тих джерелах витоку інформації що вона має. Розглянемо такі джерела: випадкові та інсайдерські витоки, злам системи, фізичні та хмарні витоки, і також витоки в соціальні мережі.

Випадкові витоки в компанії є, це факт і ніхто не буде з цим сперечатися. Нажаль з цим багато хто може не погодитися керівництво або працівники, бо саме вони є причиною даного типу витоків. Витоки даного типу являють собою не обережність з боку працівників компанії.

Перебуваючи на підприємстві з моєї точки зору, під час робочого процесу робітники працюють як правило мовчки, говорячи лише по справі в загальному не розкриваючи подробиць своїх проектів. Це наштовхнуло мене на думку, я проаналізував певні ситуації і зробив висновок, щодо до того, що працівники усвідомлюють всю важливість захисту інформаційного поля в якому працюють.

Наступними розглянемо інсайдерський тип витоку інформації. Він являє собою розкриття інформації передчасно, прикладом є розкриття нового продукта чи технології перед офіційний релізом. У даній компанії за час перебування у її стінах за мною не було помічено таких порушень, ні співробітники ні онлайн джерела на це не вказували.

Злам системи один з найстрашніших факторів та одночасно брежів у захисті системи компанії. Він являє собою збій усієї системи, кмітливі та завзяті хакери часто намагалися заволодіти інформацією, що находиться в хмарному чи електронному сховку компанії. ДОЛЯ І КО. ЛТД має одні з найкращих та найновітніших рішень та систем управління, для захисту серверів своєї компанії. Тому запевняю вас працюючи там, ви зможете працювати та не перейматися за станом своєї захищеності.

Фізичні витоки. Витоки що йдуть від: викрадення пристроїв, або агентів що засилають компанії конкуренти. Даний тип страшний тим, що він дуже не передбачуваний. Його можна легко отримати утилізуючи папери на яких міститься, наприклад бухгалтерський обіг коштів, або надати доступ до таких кімнат – серверна, прибиральнику чи звичайному працівнику технічного чи ремонтного відділу.

Навіть були не поодинокі випадки коли компанія конкурент засилають шпигунів. Такі люди як правило не помітні, вони маскуються під звичайними працівниками або тих яким потрібна робота. Наші так названі шпигуни проходять співбесіди потів влаштовуються на певну позицію у гілці заяв після успішної співбесіди. Тим самим вони на даний час можуть зливати інформацію про те, що відбувається в середині компанії. Тому компанія дбає про те, щоб таке не сталось. Вона має спеціальну систему перепусток, завдяки чому працівники компанії можуть пересуватися в межах їм дозволеної території.

Витоку з хмар у компанії «ДОЛЯ І КО. ЛТД» є малоймовірними. Цьому сприяє високий рівень безпеки. Оскільки компанія сертифікована такими сертифікатами ISO 27001, ISO 9001, ISO 42001, що підтверджують дотримання стандартів безпеки. компанія впровадила надійні механізми управління доступом та моніторингу. Всі підходи до отримання конфіденційної інформації контролюються та реєструються у системі, що дозволяє вчасно виявляти та запобігати будь-якій підозрілій діяльності. Використання сучасних інструментів для аналізу поведінки

користувачів допомагає виявляти відхилення від норми і знижувати ризик зловживання доступом такі, як – Exabeam, інструмент надає розширені можливості для аналізу поведінки користувачів, використовуючи машинне навчання та автоматизацію. Система створює поведінкові базові лінії для кожного користувача і виявляє відхилення від норми в системі хмари.

Перейдемо до витоків в соціальних мережах. Такий тип витоку спостерігається часто і компанія що розглядається також частково відноситься до них. Працівники звичайно не мають права встановлювати соціальні додатки та інші веб-додатки без дозволу системного адміністратора , оскільки вони можуть тим самим зливати інформацію до мережі. У компанії суворо ставляться до дотримання конфіденційності тому завантажувати суворо заборонено без дозволу керівників інформаційного відділу. Також порти від носіїв та дисководів є вирізаними, це зроблено насамперед для того, «шпигуни» не нашкодили системі вірусами та іншим вірусним програмним забезпеченням. Працівники коли їх беруть на посаду у даній кампанії вони підписують лист про не розголошення, такий метод є частково працюючим, оскільки він скорегований на те, що працівники будуть дбайливими до своєї репутації та не за хочуть мати чорний піар про себе та проблеми щодо подальшого працевлаштування.

На рисунку 2.2 виділені основні джерела витоку інформації в компанії «ДОЛЯ І КО. ЛТД». Червони позначено найчастіші джерела витоку інформації, синім - джерела через які рідко відбувається витік інформації, а жовтим джерела що найбільш захищені, тому через них витік інформації є найменшим вірогідним.

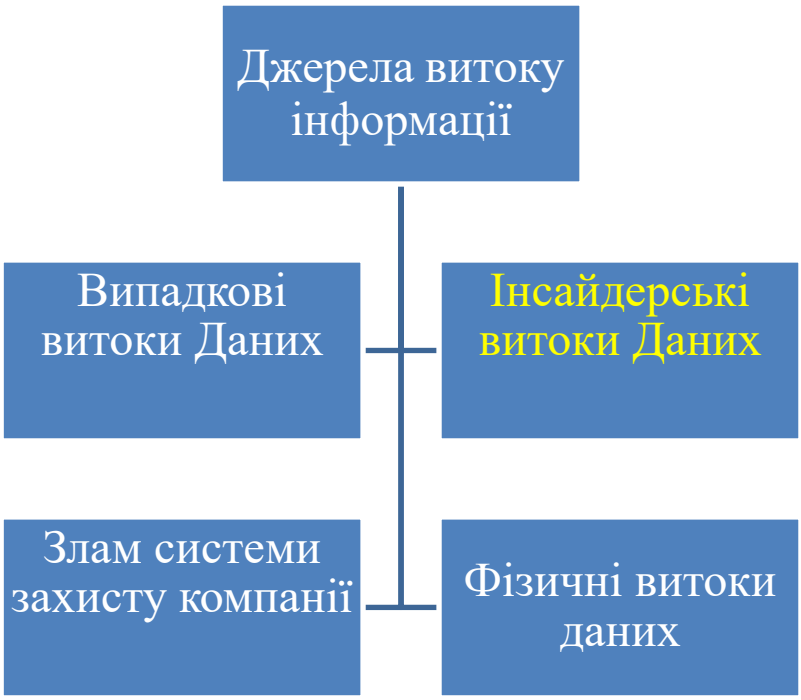

Рис. 2.2 Джерела витоку інформації у компанії «ДОЛЯ І КО. ЛТД»

2.3. Аналіз заходів захисту інформації від витоку в організаціях

Вибрати просто заходи, що до захисту системи не є 100% захистом будь-якої організації. Ми маємо чітко розуміти чим кожний крок у забезпеченні нашого захисту є особливий для нас. Також маємо не забувати, що кожний з кроків забезпечення по одинці має слабкі сторони, тому їх як правило об'єднують у КСЗІ (Комплексна Система Захисту Інформації), оскільки комплексне рішення буде виконувати задану задачу краще, а ніж поодинокі заходи.

Для початку розберемо які заходи найчастіше використовують компанії:

1) Запровадження політики запобігання втраті даних:

Надійна політика запобігання втраті даних закладає основу захисту. Це дозволяє компаніям знати, хто має доступ до їхніх даних, а що залишається заблокованим. Розглянемо це, це як контрольно-пропускний пункт безпеки в аеропорту.

Ви аналізуєте інформацію, щоб виявити делікатні аспекти, такі як фінанси, дані клієнтів і комерційні таємниці. Предмети, які можуть завдати шкоди у разі втрати, ці цифрові охоронці використовують інноваційні технології для виявлення ризикованого вмісту на основі ключових слів, типів файлів і шаблонів даних.

Вона також легко інтегрується з електронною поштою, хмарним сховищем і мережею, це гарантує, що всі канали повністю захищені. Тому вам потрібно створити політики DLP, щоб захистити дані вашої організації.

2) Використання водяних знаків і криміналістичне відстеження:

Це ще одна стратегія безпеки, яка представлена собою приховування секретних кодів у ваших даних. Це саме те, що роблять цифрові водяні знаки та криміналістичне відстеження.

Розглянемо це, як невидиме чорнило, яке вбудовує ідентифікатори в конфіденційні файли, позначаючи їхній вміст як ваш власний, отже коли дані зберігаються десь, де вони не належать, прихований водяний знак діє як відбиток їх джерела.

Криміналістичне відстеження працює аналогічно. Він залишає невидимий цифровий слід у ваших даних, дозволяючи відстежувати їх переміщення та виявляти витоки. По суті, ці невидимі маркери забезпечують важливі можливості відстеження, але залишаються непоміченими. Це дає значуще розуміння того, як дані переміщуються за лаштунками. Якщо щось піде не так, ви зможете швидко визначити зв'язок.

3) Посилення цифрового периметра, для цього ви можете розглянути:

А) Endpoint Security: встановлюючи антивірусне програмне забезпечення та програмне забезпечення для захисту від шкідливих програм, а також регулярно встановлюючи виправлення та оновлення.

Б) Безпека мережі: заблокуйте мережеву безпеку за допомогою створення брандмауерів, шифрування та моніторингу вторгнень, залиште точку входу незахищеною.

В) Керування ідентифікацією та доступом: ви також можете контролювати, хто має доступ до вашої конфіденційної інформації. Також не завадить розглянути можливість створення надійних паролів і багатофакторної автентифікації, а також надання доступу на основі ролі.

4) Проводження регулярних оцінки ризиків:

Необхідні регулярні перевірки безпеки, щоб виявити прогалини та забезпечити захист даних. Ці аудити включають ретельну оцінку існуючої політики безпеки, процедур і систем для виявлення вразливостей.

Наприклад, ви можете виконати тестування проникнення в мережу, щоб виявити вразливості, якими можуть скористатися хакери. Або зімітувати фішингову атаку, щоб оцінити рівень обізнаності вашої команди щодо кібербезпеки. Крім того, досліджуючи журнали та елементи керування доступом, ви можете визначити, чи здійснюється незаконний доступ до конфіденційних систем.

У той же час можна замислитися про стороннє управління ризиками. Проводження перевірки, переглядаючи політики, процедури, відповідність, навчання, обробку даних і заходи безпеки. Це гарантуватиме дотримання третіми сторонами стандартів безпеки під час обробки даних і знижує ризик зовнішніх атак через сторонні посилання.

5) Створення комплексного плану реагування на інциденти:

Незважаючи на всі ваші зусилля, витоки даних все одно можуть статися, тому дуже важливо мати надійний план реагування на інциденти. Це дозволяє вашій команді швидко й ефективно реагувати на катастрофу.

Комплексний план реагування на інцидент повинен містити такі деталі: ролі контактів і груп реагування на надзвичайні ситуації, протоколи ескалації, які вказують, коли вище керівництво або органи влади повинні бути повідомлені, та процедури документування інцидентів для підтримки криміналістики та відповідності і також стратегії реагування. Наприклад - ізоляція скомпрометованих систем, скасування доступу та ініціювання резервного копіювання відновлює. План

комунікацій для керування обміном повідомленнями з клієнтами та членами команди. Механізми тестування, приклади: симуляція інциденту [15,16,18].

Табл.2.1

Переваги та недоліки заходів захисту на підприємстві «ДОЛЯ І КО. ЛТД»

Заходу для захисту	Переваги	Недоліки
Шифрування даних	Навіть якщо дані будуть викрадені, без ключа шифрування вони залишаться нерозбірливими	необхідність безпечного зберігання та управління ключами шифрування
Суворе управління доступом	Мінімізація можливості несанкціонованого доступу співробітниками	вимагає регулярного перегляду прав доступу та адаптації до змін у складі персоналу
Багаторівнева аутентифікація	навіть якщо пароль буде зламано, додаткові рівні аутентифікації захистять від несанкціонованого доступу	вимагає впровадження та підтримки додаткових технологій
Моніторинг активності користувачів	дозволяє швидко реагувати на підозрілу активність	може викликати занепокоєння серед співробітників щодо порушення їхньої приватності
Фізичні заходи безпеки	запобігає крадіжці або пошкодженню обладнання	фізичні заходи не захищають від внутрішніх загроз або віддалених атак

Продовження таблиці 2.1

Регулярні аудити безпеки	забезпечує відповідність внутрішнім та зовнішнім стандартам безпеки	без належних дій на основі результатів аудитів, вони можуть бути неефективними
Використання захищених мереж	Технології такі, як - IDS/IPS дозволяють вчасно виявляти та реагувати на мережеві атаки	налаштування та управління можуть бути складними і потребувати спеціалізованих знань, та спеціалістів що знаються на системі захисту

У нашій країні компанії, як і компанії в усьому іншому світі потерпають від витоку даних. Тому на прикладі однієї з компанії ми розглянемо які заходи вони використовують та проаналізуємо їх. У нашому досліді ми поглянемо на українське підприємство «ДОЛЯ І КО. ЛТД», що є однією з провідних постачальників над новітніх систем зв’язку та інтегрованих систем захисту передачі інформації на базі радіостанцій, докладніше про компанії у пункті 2.1 цієї роботи.

У таблиці 2.3., що наведена вище, коротко представлені заходи захисту даної компанії від витоку інформації. Розглядається шифрування даних, що знаходяться в компанії. Достатньо суворе управління доступом до системи компанії. Багаторівнева аутентифікація для входу у систему, наприклад робочого пк. Моніторинг активності усіх користувачів у мережі, та внутрішньо на серверах компанії. Фізичні заходи захисту, Проводження аудиту безпеки та використання захищених джерел, як правило стосується виходу до інтернету.

Шифрування. Це буде стосуватися програмування радіостанцій, на підприємстві їх шифрують таким типом шифру: AES-256. Цей шифр являє собою

симетричний алгоритм шифрування, який використовує ключ довжиною 256 біт., та є одним з найнадійнішим стандартом для шифрування.

На черзі у нас таке собі суворе управлінням доступом до тих чи інших приміщень. Воно впроваджено з метою забезпечити захист інформації на території підприємства. Реалізовано магнітними чіп-картою яка запрограмована адміністратором з інформаційної безпеки для кожного працівника компанії окремо, з погодженням керівництва.

Багаторівнева аутентифікація – з цим ми стикаємося кожний раз коли заходимо на комп'ютер. На нашому робочому столі будуть певні обмеження, якщо не провести цей крок.

Моніторинг активності користувачів, це перегляд усієї активності певного робітника підприємства, будь то камери спостереження чи огляд активності за комп'ютером.

Фізичні заходи безпеки – вони розгорнуті чипування та пломбуванням речей компанії, від столів та стільців до запчастин, у нашому випадку це будуть запчастини та технічне приладдя.

Регулярні аудити безпеки – розглядаються певні строки, чи дні у які до компанії запрошують аудиторів, для проведення аудиту з безпеки системи підприємства.

Використання захищених мереж – це стосується інтернет мереж, тому уся мережа інтернету має надійний пароль, що складається з 12-14 символів з використання спец символів, великих літр та цифр.

Висновки до другого розділу

Компанія «ДОЛЯ І КО. ЛТД» застосовує комплексний підхід до захисту інформації від витоків, включаючи технічні, організаційні та фізичні заходи. Незважаючи на наявність різноманітних джерел потенційних витоків, такі заходи, як шифрування, багаторівнева автентифікація, моніторинг активності користувачів,

чіткі політики та регулярні навчання співробітників, значно знижують ризик несанкціонованого доступу до конфіденційної інформації. Однак постійний розвиток технологій та зміна загроз вимагають регулярного перегляду та оновлення цих заходів для забезпечення високого рівня безпеки.

РОЗДІЛ 3

ОЦІНКА ЕФЕКТИВНОСТІ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ В ОРГАНІЗАЦІЯХ ТА ПРОПОЗИЦІЇ ЩОДО ЇХ ПОКРАЩЕННЯ

3.1. Методи оцінки ефективності заходів захисту інформації від витоку

Що ж тепер поговоримо про методи оцінки ефективності заходів. Які можемо запровадити для ефективного захисту нашої організації. Для оцінки інформаційної безпеки часто використовують методи:

1. Рентабельності витрат на здійснення заходів щодо захисту інформації;

2. Методи оцінки шкоди від загрози хакерських атак;

3.Методи нечітких множин;

4. Витратний метод (оцінка витрат на забезпечення інформаційної безпеки в загальній величині витрат);

5. Експертний метод (оцінюють ймовірність подолання системи захисту інформації).

При цьому експертним шляхом оцінюють ймовірність подолання системи захисту інформації, імовірність доставки одиниці інформації до споживача, час доставки й апаратурну складність. Ще використовують показники частки працівників інформаційних секціях у загальній кількості працівників та частки витрат на забезпечення інформаційної безпеки в загальній величині витрат організації.

Крім того, деякі науковці аналізують такі показники:

– продуктивність інформації;

– коефіцієнт інформаційної озброєності;

– коефіцієнт захищеності інформації [40; 41].

Перелік параметрів оцінювання рівня захисту інформації та ступінь їх кращості визначають такою методичною умовою: кількість оцінюваних параметрів повинна бути достатньо обмеженою з метою забезпечення оперативності

управлінських рішень, які приймають. Формування та групування параметрів спирається на аналіз широкого комплексу проблем економічного і соціального характеру, тому множина вхідних чинників повинна задовольняти умови дієвості та мінімальності. За критерієм повноти необхідно визначити кількість параметрів, яка охоплювала б усі аспекти діяльності підприємства, про те вилучення хоча б одного з них не змінювало би результат. Далі на основі сформованої множини за критерієм повноти необхідно виділити групу з максимальним ступенем результативності за критерієм дієвості. Потім критерієм мінімальності потрібно зменшити кількість параметрів, виключивши ті, які є оберненими, або дублюють один одного.

На основі аналізу праць науковців [42 – 44] визначено ключові чинники, які визначають рівень захисту інформації на підприємстві. Можна встановити функціональну залежність між рівнем захисту інформації та факторами впливу на нього у вигляді схеми. Тому, було складено структурно-логічну схему захисту

інформації на підприємстві (схема.3.1).

Пропонується взяти множину вхідних параметрів lc (c = ,1 C); сукупність показників, що розраховують на основі оцінювальних параметрів xi (i = ,1 n); функцію перетворення вхідних параметрів на оцінювальні показники F1: L → X множину функцій, на основі яких здійснюють ідентифікацію рівня ефективності політики інформаційної безпеки F2 = F (f1,…,f i);множину вихідних параметрів

E= (ej), j=1,J.

На множинах X параметрів xi сформована сукупність функцій перетворення: F1 – функція ефективності роботи технічного забезпечення; F2 – функція ефективності кадрового складника; F3 – функція ефективності керування інформаційними потоками, F4 – функція ефективності програмного забезпечення.

Як було зазначено вище, використання окремих показників (рентабельності, захищеності інформації), а також методів експертних оцінок не дозволяє ефективно ідентифікувати рівень захисту інформації на підприємстві. Для ефективного оцінювання захисту інформації підприємств необхідно використовувати сучасні

математичні апарати, які дозволять поєднати не тільки різні за змістом показники і моделі, але й різні за своєю природою – кількісні та якісні параметри. Саме таким інструментом виступає апарат нечітких множин [45]. Важливою перевагою нечітких моделей є їхня прозорість, яка дозволяє їм успішно конкурувати з різними індуктивними методами обробки даних [46].

3.2 Оцінка ефективності заходів захисту інформації від витоку в організації

Впровадження комплексних заходів захисту інформації включає оцінку та підвищення ефективності різних аспектів діяльності підприємства.

Розглянемо за допомогою яких показників ми зможемо проводити оцінювання рівня захисту інформації організації. Розглянемо на прикладі складеної таблиці.

Таблиця 3.1

Показники моделі оцінювання рівня захисту інформації підприємства

Показник ефективності	Коефіцієнт	Значення	Критерій
Ефективність роботи технічного забезпечення підприємства	коефіцієнт технічного захисту інформації(1)	0,8	Н - 0 С – 0,2 В - 1
Ефективність роботи персоналу з інформацією підприємства	коефіцієнт надійності персоналу (2)	0,2	Н – 0 – 0,3 С – 0,5 В - 1

Продовження таблиці 3.1

Ефективність керування інформаційними потоками підприємства	коефіцієнт надійності захисту інформації (3)	0,4	Н - 0 – 0,1 С – 0,5 В - 1
Ефективність програмного забезпечення підприємства	коефіцієнт забезпечення програмними засобами для захисту інформації (4)	0,65	Н - 0 – 0,3 С – 0,5 В - 0,6 – 1

Нижче наведено пояснення до обраних показників та залежності, за якими необхідно їх розраховувати:

1)Ефективність роботи технічного забезпечення підприємства:

технічних заходів = кількості усіх інформаційних атаки/кількість інформаційних атак, що були відбиті за допомогою технічного зв'язку.

2) Ефективність роботи персоналу з інформацією підприємства:

Коефіцієнт надійності персоналу = Числу загальних працівників – число звільнених працівників з причин витоку інформації / на загальну кількість працівників.

3) Ефективність керування інформаційними потоками підприємства:

Коефіцієнт надійності захисту інформації = Загальний обсяг інформації / обсяг інформації що підлягає захисту.

4) Ефективність програмного забезпечення підприємства:

Коефіцієнт забезпечення програмними засобами для захисту інформації = кількість наявних засобів захисту / кількість затребуваних засобів захисту.

Розрахунок показників для оцінки рівня захисту -

1) коефіцієнт технічного захисту інформації $X_{(11)}$:

$$К_{т.з.} = l_3/l_4, \qquad \text{формула 3.1}$$

де l_4 – кількість інформаційних атак, на які не відреагував технічний захист;

2) коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства $X_{(22)}$:

$$К_{н.п.} = l_7 - l_8 / l_7, \quad \text{формула 3.2}$$

де $l7$ – загальна чисельність звільнених працівників; $l8$ – чисельність працівників, звільнених через витік інформації;

3) коефіцієнт надійності захисту інформації $X_{(36)}$:

$$К_{н.зі.} = l_{17} / l_{18}, \quad \text{формула 3.3}$$

де 17 l – обсяг інформації, наданої з надійних джерел %, 18 l – загальний обсяг наданої інформації %;

4) коефіцієнт забезпечення програмними засобами для захисту інформації $X_{(42)}$:

$$К_{з.п.з.з.і} = l_{19} / l_{20}, \quad \text{формула 3.4}$$

Де l_{19} - кількості наявних програмних засобів, l_{20} – необхідні програмні засоби.

На останньому етапі формуємо групи показників та встановлюємо числові межі для трьох термів (табл.3.1). Залежно від необхідності врахування жорстких меж зміни низького та високого рівня параметрів обираємо для кожного з них одну з трьох функцій (графіків)

3.3. Пропозиції щодо покращення заходів захисту інформації від витоку в організації

У епоху цифрових технологій захист конфіденційної інформації є головним пріоритетом для компаній у всьому світі. Порушення даних, навмисне чи випадкове, може мати значні фінансові, репутаційні та правові наслідки.

У цьому пункті розглянемо рекомендаційні заходи, які організація може застосувати для запобігання витоку інформації.

Досліджувана компанія «ДОЛЯ І КО. ЛТД» має такі результати з даними нашого дослідження - коефіцієнт технічного захисту інформації - 0,8%; коефіцієнт надійності персоналу - 0,2%; коефіцієнт надійності захисту інформації - 0,4%; коефіцієнт забезпечення програмними засобами для захисту інформації - 0,65%. Тому я пропоную наступні заходи для покращення захисту інформації опираючись на наступні висновки з дослідження:

1. Коефіцієнт технічного захисту інформації є досить високим, аж цілих - 0,8%, що свідчить про значну ефективність технічного забезпечення. Проте є можливості для покращення, а саме - інвестування в нові технології такі, як системи запобігання вторгненням, або засоби захисту від загроз на основі штучного інтелекту;

2. Коефіцієнт надійності персоналу є нажаль є найнижчим з усіх розглянутих і становить - 0,2%, що свідчить про суттєві ризики, пов'язані з людським фактором.

Збільшити цей показник можуть пропозиції, що стосуються: навчання та проведення курсів з підвищенням обізнаності для персоналу та керівників щодо ІБ, та впровадити більш чіткі політики з безпеки та захисту інформації.

3. Коефіцієнт надійності захисту інформації згідно з нашим дослідженням становить - 0,4% вказує на наявність значних проблем у керуванні інформаційними потоками. Пропозиціями будуть: впровадження сигментування мережі , що допоможе обмежити доступ до інформації тільки тим співробітникам, які потребують її для виконання службових обов’язків, також впровадити більш жорсткий контроль доступу що буде базуватися на ролях – посад працівників компанії.

4. Коефіцієнт забезпечення програмними засобами для захисту інформації складає - 0,65%, це вказує на хороший рівень захисту. Проте є декілька рекомендацій що допоможуть вийти на новий рівень захисту та отримати більші показники. Будуть рекомендовані наступні дії: використовувати сучасні системи виявлення атак (IDS/IPS), які в свою чергу допоможуть своєчасно виявляти та

реагувати на потенційні загрози для компанії. Розгорнувши системи IDS компанія отримує можливість моніторингу мережевий трафік на активність, чи ознаки порушень в системі безпеки. Розрізняють два головних типа IDS – мережевий (для виявлення підозрілих шаблонів або аномалій), та хост версію (для виявлення виявлення несанкціонованого доступу чи зловмисних дій). Та IPS – система запобігань вторгнень, яка по суті є більш розширеною версією IDS. Її особливостями є -блокування трафіку та переустановлення з'єднання. Також можна додати використання лише перевіреного та оновленого програмного забезпечення, а також через певний термін його перевіряти на справність.

Висновок до третього розділу

Захист від витоку інформації вимагає багатостороннього підходу, що поєднує технології, політики та обізнаність працівників. Впроваджуючи запропоновані заходи, організації можуть значно зменшити ризик витоку даних та захистити свої цінні інформаційні активи. Реалізація запропонованих заходів допоможе значно підвищити рівень захисту інформації та мінімізувати ризики витоків даних.

ВИСНОВКИ

Метою даної роботи був аналіз заходів захисту інформації від витоку в організації. Об'єктом дослідження стала організація та її інформаційна

інфраструктура, а предметом – заходи захисту, які вживаються для запобігання витоку інформації. У процесі дослідження були досягнуті наступні ключові результати.

У ході виконанні роботи було проведено всебічний аналіз заходів захисту інформації від витоку в організації. Він включав вдосконалення технічного забезпечення, зокрема модернізацію фаєрволів, впровадження сучасних систем виявлення/запобігання вторгнень (IDS/IPS) та використання шифрування. Крім того, підвищення ефективності роботи персоналу досягалося через регулярні тренінги, симуляції фішингових атак та впровадження чітких політик безпеки. Також було оптимізовано керування інформаційними потоками, включаючи класифікацію даних, впровадження DLP-систем та регулярний аудит доступу. Підвищення ефективності програмного забезпечення здійснювалося шляхом інтеграції безпеки у процес розробки, регулярних оновлень та вибору надійного ПЗ.

Під час дослідження у роботи було визначено основні джерела витоків інформації в організації. Виявлено, що основні джерела витоків інформації включають людський фактор, що охоплює помилки персоналу та недостатню обізнаність про загрози; вразливості в технічному забезпеченні, такі як застаріле обладнання та неоновлене програмне забезпечення; недостатнє керування інформаційними потоками та правами доступу до даних; використання ненадійного програмного забезпечення та відсутність належного контролю за оновленнями.

В процесі дослідження теми було розглянуто ефективність заходів захисту інформації від витоку була оцінена за декількома критеріями. Технічні заходи, такі як використання сучасних фаєрволів, шифрування даних та впровадження SIEM-систем, показали високу ефективність у зниженні ризиків. Навчальні програми для персоналу та симуляції атак значно підвищили обізнаність співробітників і знизили ймовірність успішних соціальних інженерних атак. Класифікація даних та впровадження систем запобігання витоку даних (DLP) покращили контроль за

інформаційними потоками. Інтеграція безпеки у процес розробки програмного забезпечення та регулярні оновлення допомогли знизити вразливості у ПЗ.

Практичне значення цього дослідження полягало у покращенні безпеки даних та зниженні ризиків для організацій, їх клієнтів і партнерів. Використання отриманих результатів дозволяє організаціям підвищити рівень захисту своєї інформаційної інфраструктури, запобігти потенційним витокам інформації та забезпечити стабільну роботу системи. Також реалізація запропонованих заходів під час дослідження допоможе значно підвищити рівень захисту інформації та мінімізувати ризики витоків даних на підприємстві.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Витік інформації (Vulnerability Assessment as a Service (VAaaS)

Tests systems and applications for vulnerabilities to address weaknesses).URL: https://cqr.company/ua/web-vulnerabilities/information-leakage/

2. Методи захисту інформації в телекомунікаційних системах. URL: https://www.google.com/url?sa=i&url=https%3A%2F%2Fppt-

online.org%2F498294&psig=AOvVaw0eUIYWjT6bv2MWIc9_Q5t8&ust=1717252062953000&source=images&cd=vfe&opi=89978449&ved=0CBQQjhxqFwoTCNC0i8uMuIYDFQAAAAAdAAAAABBI

3. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. навчальний посібник URL:

https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content

4. ATESTATOR quality control center (Політика інформаційної безпеки) URL: https://atestor.ua/uk/poleznye-stati/politika-informaciinoyi-bezpeki/

5. 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

6. Стандарти/Технології компанії Доля. І КО.URL: https://dolya.ua/ua/ctandarti-tehnologii/

7. Сайт YOU control URL: https://youcontrol.com.ua/catalog/company_details/01043342/

8. Технічний аудит телекомунікаційної системи — URL: https://dolya.ua/ua/technical-audit/

9. Консалтингові послуги та супровід при отриманні дозволів на користування радіочастотним ресурсом України URL: https://dolya.ua/ua/registration/

10. Навчання персоналу замовника послуг URL:

https://dolya.ua/ua/training/

11. Криптографічний та технічний захист інформації URL: https://dolya.ua/ua/information-security/

12. Широкополосний PTT-зв'язок для професійного користування URL:https://dolya.ua/ua/ptt-over-cel ular/

13. Будівництво систем професійного радіозв’язку та оповіщення URL: https://dolya.ua/ua/system-integration/

14. Діагностика та ремонт обладнання URL: https://dolya.ua/ua/service-maintenance/

15. Best Practices To Prevent Data Leaks In Your CompanyURL: https://www.cyberdb.co/6-best-practices-to-prevent-data-leaks-in-your-company/

16. Data Leak Prevention Strategies in 2024 URL: https://www.upguard.com/blog/data-leak-prevention-tips

17. Аудит безпеки | Security is part of reputation - Secure crowds URL: https://securecrowds.com.ua/audyt-bezpeky/

18. How to Prevent Data Leakages URL: https://www.infosecurity-magazine.com/next-gen-infosec/prevent-data-leakages/

19. «Технології захисту інформації» URL http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf

20. Система запобігання витоку інформації на підприємстві URL: https://dspace.nau.edu.ua/bitstream/NAU/55920/1/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%D0%BD%D0%B0_%D0%A0%D0%BE%D0%B1%D0%BE%D1%82%D0%B0_%D0%9A%D0%BE%D0%BD%D0%B4%D1%80%D0%B0%D1%82%D0%B5%D0%BD%D0%BA%D0%BE.pdf

21. Інформаційна безпека організації як фактор посилення бренду URL: https://journals.kymu.kyiv.ua/index.php/economy/article/download/48/45

22. Методи захисту інформації для підприємства – Resit URL: https://resit.com.ua/zachist-informacii-na-pidpriemstvi/

23. Pentest, 20 років на ринку IT послуг для бізнесу URL: TechExpert https://techexpert.ua/ru/our-services/pentest/

24. Про затвердження Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій URL: https://zakon.rada.gov.ua/go/v0755388-13

25. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.URL:
https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-1.1-005-07.pdf
26. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111 p. URL:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html
27. «Тестування комп’ютерних систем на проникнення» URL:
https://dspace.univd.edu.ua/bitstreams/0b2a7012-166d-4809-a20f-7e1e8dcfeb6e/download
28. Тестування на проникнення URL:
https://audit3a.com/uk/penetration-test/
29. ISO/IEC 27001 URL:
https://kr-labs.com.ua/books/2ef522.pdf
30.Моніторинг та реакція на інциденти - SYSOFT URL:
https://sysoft.pp.ua/services/monitoring-ta-reakciya-na-incidenti
31. 24/7 Реагування на Інциденти | CQR URL:
https://cqr.company/ua/service/reaguvannya-na-incidenty/
32. Якісний аналіз ризиків підприємницької діяльності URL:
ihttp://www.tsatu.edu.ua/et/wp-content/uploads/sites/33/prezentacija-do-temy-ocinjuvannja-ryzyku.pdf
33. Методи аудиту інформаційної безпеки інформаційних систем URL:
https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/4900/1/1.pdf
34. Messier, Ric. "What Is Penetration Testing?." Apress (2016). URL:
http://dx.doi.org/10.1007/978-1-4842-1857-0_1
35. Engebretson, Patrick. "What Is Penetration Testing?." Elsevier (2011).
URL: http://dx.doi.org/10.1016/b978-1-59749-655-1.00001-5
36. GEO-ENVIRONMENTAL APPLICATIONS OF PENETRATION

TESTING. CRC Press (2020). URL:
http://dx.doi.org/10.1201/9781482295047-16

37. Зірка, яку погасили.
URL: https://www.epravda.com.ua/publications/2023/12/12/707628/

38. Слово І Діло URL:
https://www.slovoidilo.ua/2024/01/18/novyna/suspilstvo/nazvana-suma-zbytkiv-kyyivstar-masshtabnoyi-kiberataky-hrudni 38

39. ANTIRAID - Персональні дані мережі медичних лабораторій “Сінево” потрапили у мережу інтернет URL:
https://antiraid.com.ua/news/personalni-dani-merezhi-medychnykh-laboratorij-sinevo-potrapyly-u-merezhu-internet/?doing_wp_cron=1716364419.5145139694213867187500

40. Ілляшенко С. М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. / С. М. Ілляшенко. – К. : Центр навчальної літератури, 2004. – 220 с.

41. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія / Н. Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

42. Дудикевич В. Б. Ієрархічна модель захисту даних в інформаційних технологіях / В. Б. Дудикевич, Г. В. Микитин, Ю. Р. Гарасим // Проблеми і перспективи Роозвитку ІТ-індустрії : зб. тез. доп. ІІ Міжнар. наук.- практ. конф. – Харків : Вид-во ХНУРЕ, 2010. – С. 212 – 213.

43. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія / Н. Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

44. Ілляшенко С. М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. / С. М. Ілляшенко. – К. : Центр навчальної літератури, 2004. – 220 с.

45. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі : монографія / А. П. Ротштейн. – Вінниця : Універсум-Вінниця, 1999. – 320 с.

46. Штовба С. Д. Порівняння критеріїв навчання нечіткого класифікатора / С. Д. Штовба // Вісник ВПІ. –2007. – № 6. – С. 84 – 91.

47. Корченко А. Г. Побудова систем захисту інформації на нечітких множинах. Теорія та практичнірішення / А. Г. Корченко. - К.: "МК-Прес", 2006. - 320 с

48. Сергєєва Л. Н. Нелінійна економіка: моделі та методи / Л. Н. Сергєєва. − Запоріжжя: Поліграф, 2003.- 217 с.