Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Розрахунок ризиків інформаційної безпеки інфокомунікаційного підприємства
(тема)

Виконала: студентка 2 курсу, групи *ІМІм-20-1*
Спєсівцева А.С.
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
Освітня програма *Інформаційно-мережна інженерія*

Керівник *к.т.н., доц. Золотарьов В.А.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *проф. Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 р.

_____

Не містить відомостей, заборонених до відкритого публікування

Студент _____ Спєсівцева А.С.

Керівник _____ Золотарьов В.А.

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
Тип програми *освітньо-професійна*
Освітня програма *Інформаційно-мережна інженерія*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«08» листопада 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентці Спєсівцевій Анастасії Сергіївні
(прізвище, ім'я, по батькові)

1. Тема роботи: *Розрахунок ризиків інформаційної безпеки інфокомунікаційного підприємства*

затверджена наказом по університету від 08 листопада 2021 р. № *1674 - Ст*
2. Термін подання студентом роботи до екзаменаційної комісії *13 грудня 2021* р.
3. Вихідні дані до роботи: *Об'єкт дослідження – корпоративна мережа інфокомунікаційного підприємства. Дослідити: Визначити й оцінити ризики інформаційній безпеці для типової розподіленої мережі інфокомунікаційного підприємства. Головний акцент при забезпеченні інформаційної безпеки в інфокомунікаційній мережі, що досліджується, зробити на мінімізацію збитків від загроз, спрямованих на порушення цілісності й доступності програмно-апаратного комплексу інфокомунікаційної системи, а не на конфіденційність інфокомунікаційних ресурсів, які обробляються з їхньою допомогою. Розрахувати інформаційні ризики інформаційній безпеці, заснованій на виділенні цінних активів підприємства; ступеню потенційних збитків при реалізації загроз на такі активи; ймовірність реалізації загроз для даної інфокомунікаційної мережі підприємства.*

4. Перелік питань, що потрібно опрацювати в роботі: *Перелік умовних скорочень. Вступ. 1. Інформаційна безпека підприємства: ключові загрози й засоби захисту. 2.Визначення цінностей активів підприємства. 3. Оцінювання ризиків інформаційної безпеки. Висновки. Перелік використаних джерел. Додаток А: слайди презентації*

-

5. Перелік графічного матеріалу із зазначенням комп'ютерних ілюстрацій (слайдів)

Слайди у форматі Power Point: *мета роботи; схематичне розташування розподіленої інформаційної мережі; шкала цінності активів, запропоновані контрзаходи; процес оцінювання та обробки інформаційних ризиків, ступінь вразливості активів.*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	08.11.2021	
2	*Аналіз завдання та літературних джерел.*	12.11.2021	
3	*Написання першого розділу*	18.11..2021.	
4	*Написання другого розділу*	25.11.2021	
5	*Написання третього розділу*	11.12.2021	
6	*Написання вступу та висновків*	12.12.2021	
8	*Оформлення презентаційного матеріалу та підготовка до захисту у ЕК*	13.12.2021	

Дата видачі завдання 08 листопада 2021 р.

Студент _____ Спєсівцева А.С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ к.т.н., доц. Золотарьов В.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 71с., 15рис., 29 посилань, 2 додаток.

Об'єкт дослідження – кооперативна мережа інфокомунікаційного підприємства.

Метою даної роботи є визначення та оцінка ризиків інформаційної безпеки для типової розподіленої інформаційної системи телекомунікаційного підприємства, розташованої в межах трьох контрольованих зон. Основний акцент при забезпеченні інформаційної безпеки у аналізованої інформаційної системі, робиться на мінімізацію збитків від загроз безпеки, спрямованих на цілісність та доступність програмно-апаратного комплексу інформаційної системи, а чи не на конфіденційність інформаційних ресурсів, оброблюваних з допомогою.

Ключові слова: інформаційна безпека, менеджмент ризиків інформаційної безпеки, телекомунікаційне підприємство.

THE ABSTRACT

Explanatory note: 71 p., 15fig., 29 sources, 2 app.

The goal of this work is to identify and assess information security risks for a typical distributed information system within three controlled areas.

The main emphasis, application of information security in the considered information system is done to minimize damage from security threats, aimed at the integrity and availability of the hardware and software complex of the information system, and not to the confidentiality of information resources processed with their help. The study examined international and national standards in the field of information security, which regulate issues of information security risks management.

KEYWORDS: information security, information security risks' management, telecommunication enterprise.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – база даних
ІБ – інформаційна безпека
ІКМ – інфокомунікаційна мережа
ІС – інформаційна система
ІТ- інформаційні технології
НСД – несанкціонований доступ
ОС – операційна система
ПЗ – програмне забезпечення
СЗІ – система захисту інформації
СМІБ – система менеджменту інформаційної безпеки

ВСТУП

На сьогоднішній день перед кожним підприємством, що дбає про безпеку своїх інформаційних ресурсів, постає питання про організацію системи захисту інформації, яка б дозволила повною мірою забезпечити безпеку функціонування і телекомунікаційного обладнання та циркулюючої інформації в інформаційній системі підприємства. Ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів розрахунку ризиків інформаційної безпеки.

Існує безліч методик оцінки та обробки ризиків, які застосовуються до будь-якої інформаційної системі, незалежно від рівня конфіденційності оброблюваної у ній інформації, проте, зазвичай, для грамотної побудови системи захисту інформації з використанням таких методик потрібен великий обсяг інформації про реалізовані атаках, а також про спроби їх реалізації, що підлягає програмному аналізу з метою виявлення найбільш актуальних загроз інформаційної безпеки (далі – ІБ), то є необхідна своєрідна відправна точка, з якою і слід розпочинати створення системи захисту, про це говорять стандарти BS 7799-3 та NIST 800-30, що не завжди можливо реалізувати практично, зважаючи на обмеженість тимчасових та фінансових ресурсів – це особливо актуально для телекомунікаційних організацій, оскільки обсяги даних у таких підприємствах величезні, а аналіз кожного пакета дуже дорога та трудомістка процедура.

У цій кваліфікаційній роботі пропонується метод розрахунку ризиків для системи, яку можна охарактеризувати великими обсягами даних і невизначеним числом користувачів.

Необхідно відмітити, що існує низка методик оцінки ризиків інформаційної безпеки, що дозволяють однозначно і з високим ступенем обґрунтованості виділити актуальні ризики. Міжнародні та національні стандарти пропонують достатньо вичерпний вибір методів з цього питання, проте їх застосування можливе тільки в умовах невеликого обсягу даних, та малого числа користувачів, а самі методики дуже узагальнені.

Відмінною рисою будь-якого телекомунікаційного підприємства є чутливість до безпеки та надійній роботі всього апаратно-програмного комплексу для забезпечення безперервності функціонування ключових бізнес-

процесів організації, що просто зобов'язує керівників організації створити та підтримувати ефективну систему інформаційної безпеки.

В рамках даної кваліфікаційної роботи запропонований якісний метод оцінки ризиків ІБ, заснований на розбиття інформаційної системи телекомунікаційного підприємства на типові сегменти (що включають не більше трьох контрольованих зон), які мають однакові характеристики з точки зору інформаційної безпеки. А сама методика розрахунку ризиків ґрунтується на сукупності способів та методів визначення та оцінки ризиків, апропонованих рядом міжнародних та українських стандартів у сфері інформаційної безпеки, застосування яких можливо до аналізованої інформаційної системі.

1 ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА: КЛЮЧОВІ ЗАГРОЗИ Й ЗАСОБИ ЗАХИСТУ

Комп'ютерні та інформаційні технології сьогодні охопили усі галузі економіки. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, збереження та правильне розпорядження яким має ключове значення для розвитку бізнесу та зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

1.1 Поняття інформаційної безпеки підприємства

Під інформаційною безпекою підприємства чи компанії розуміють комплекс заходів організаційного та технічного характеру, спрямованих на збереження та захист інформації та її ключових елементів, а також обладнання та системи, що використовуються для роботи з інформацією, її зберігання та передачі. Цей комплекс включає технології, стандарти та методи управління інформацією, які забезпечують її ефективний захист.

Забезпечення інформаційної безпеки допомагає захистити інформацію та інформаційну інфраструктуру підприємства від негативних впливів. Такі дії можуть мати випадковий або навмисний, внутрішній або зовнішній характер. Результатом таких втручань може стати втрата важливої інформації, її несанкціонована зміна чи використання третіми особами. Тому інформаційна безпека – це важливий аспект захисту бізнесу та забезпечення його безперервності.

Принципи ефективного впровадження у компанії систем інформаційної безпеки полягають у забезпеченні трьох умов: конфіденційності, цілісності та доступності.

Під конфіденційністю розуміють організацію та підтримку ефективного контролю для забезпечення достатнього ступеня безпеки даних, активів та інформації на різних етапах бізнес-процесів для виключення несанкціонованого

чи небажаного розкриття. Підтримка конфіденційності обов'язково застосовується при збереженні та транзиті інформації у будь-якому форматі.

Цілісність охоплює елементи управління, які забезпечують внутрішню та зовнішню незмінності інформації. Забезпечення цілісності дає змогу виключити можливість спотворення даних на будь-якому з етапів ділових операцій.

Доступність підтримує повноцінний та надійний доступ до інформації для посадових осіб, які мають відповідні повноваження. Ключовим моментом тут є передбачуваність процесів, що протікають у мережному середовищі, щоб користувачі мали можливість доступу до необхідних даних у потрібний час. Одним із важливих факторів доступності інформації є можливість швидкого та повного відновлення системи після збоїв, щоб не допустити його негативного впливу на функціонування компанії.

1.2 Контроль за дотриманням інформаційної безпеки підприємства

Забезпечити повноцінну та надійну інформаційну безпеку підприємства можна лише за умови застосування комплексного та системного підходу. Система інформаційної безпеки має бути побудована з урахуванням усіх актуальних загроз та вразливостей, а також з урахуванням тих загроз, які можуть виникнути в майбутньому. Тому важливо забезпечити підтримку безперервного контролю, який має діяти щодня та цілодобово. Необхідною умовою є забезпечення контролю на кожному з етапів життєвого циклу інформації, починаючи з моменту її надходження до інфраструктури компанії і закінчуючи втратою її актуальності чи знищенням даних.

Існує кілька видів контролю інформаційної безпеки, впровадження яких дозволяє компанії знижувати ризики у цій сфері та підтримувати їх на прийнятному рівні..

Адміністративний контроль інформаційної безпеки - це система, що складається з комплексу встановлених стандартів, принципів та процедур. Цей вид контролю визначає межі для здійснення бізнес-процесів та управління

персоналом. Він включає законодавчі та нормативні акти, прийняту на підприємстві політику корпоративної безпеки, систему найму працівників, дисциплінарні та інші заходи.

Логічний контроль передбачає використання засобів управління (засобів технічного контролю), що захищають інформаційні системи від небажаного доступу. Ці засоби об'єднують спеціальне ПЗ, брандмауери, паролі тощо.

Фізичний контроль зосереджений серед робочих місць і засобах обчислення. У тому числі він передбачає забезпечення ефективного функціонування інженерних систем будівель підприємства, робота яких може вплинути на зберігання та передачу інформації. До таких систем відносяться опалення та кондиціювання, протипожежні системи. Іншою важливою складовою фізичного контролю є системи контролю та управління доступом на об'єкти.

1.3 Інформаційні ризики безпеці підприємства

Інформаційний ризик - імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок виникнення зовнішніх або внутрішніх подій, зміни бізнес-середовища та/або інформаційних технологій чи неадекватних або помилкових внутрішніх процесів щодо: функціонування інформаційних систем та інших інформаційних ресурсів підприємства та управління ними (ризик інформаційно-комунікаційних технологій); збереження конфіденційності, цілісності та доступності інформації підприємства (ризик інформаційної безпеки)

Інформаційна інфраструктура підприємства постійно наражається на численні загрози, які за своїм походженням діляться на кілька видів:

Природні. Загрози, спричинені причинами, що не залежать від людини. До них належать урагани, пожежі, удари блискавки, повені, інші природні катаклізми.

Штучні. Комплекс загроз інформаційної безпеки, створених людиною. Штучні загрози, у свою чергу, поділяють на навмисні та ненавмисні. До навмисних загроз відносять дії конкурентів, хакерські атаки, шкідництво ображених працівників і т. д. Ненавмисні загрози виникають в результаті дій, вчинених через брак компетентності або необережності.

Внутрішні. Загрози, що виникають усередині інформаційної інфраструктури підприємства.

Зовнішні. Загрози, що мають походження поза інформаційної інфраструктури підприємства.

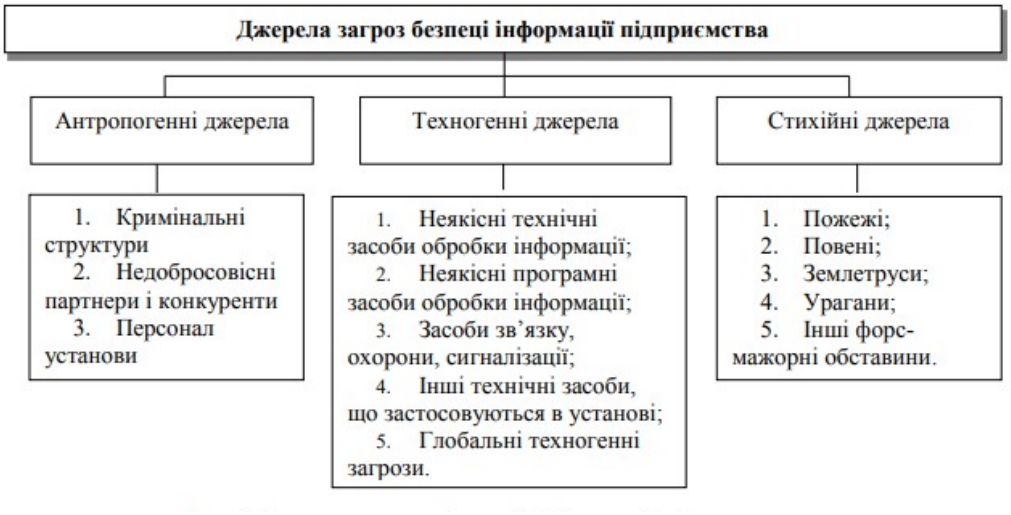

Рисунок 1.1 – Джерела загроз безпеці інформації підприємства

Залежно від характеру впливу загрози інформаційної безпеки поділяються на пасивні та активні. Пасивні загрози — це чинники впливу, які можуть змінювати зміст і структуру інформації. Активні загрози можуть вносити такі зміни. До них відносять, наприклад, вплив шкідливого ПЗ.

Головну небезпеку становлять штучні навмисні небезпеки. З огляду на дедалі більшу комп'ютеризацію всіх сфер бізнесу та зростання кількості електронних транзакцій ці загрози також бурхливо розвиваються. У пошуках способів отримання секретних відомостей та заподіяння шкоди компаніям зловмисники активно використовують сучасні технології та програмні рішення. Їхні дії можуть завдавати значної шкоди, у тому числі у вигляді прямих

фінансових втрат або втрати інтелектуальної власності. Тому інформаційна безпека підприємства також має будуватись на базі передових технологій з використанням актуальних засобів захисту даних.

1.4 Методи й засоби захисту інформації на підприємстві

Залежно від способів реалізації, засоби захисту інформаційної безпеки бувають наступних типів:

Організаційні. Комплекс заходів та засобів організаційно-правового та організаційно-технічного характеру. До перших відносять законодавчі та нормативні акти, локальні нормативні документи організації. Другий тип – це заходи щодо обслуговування інформаційної інфраструктури об'єкта.

Апаратні (технічні). Спеціальне обладнання та пристрій, що запобігає витоку, що захищає від проникнення в IT-інфраструктуру.

Програмні. Спеціальне програмне забезпечення, призначене для захисту, контролю, зберігання інформації.

Програмно-апаратні. Спеціальне обладнання із встановленим програмним забезпеченням для захисту даних.

Найширше поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози штучного характеру.

Для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення. Можна виділити такі типи програмних засобів захисту:

Антивірусне ПЗ. Спеціалізований софт для виявлення, нейтралізації та видалення комп'ютерних вірусів. Виявлення може виконуватися під час перевірок за розкладом або запущених адміністратором. Програми виявляють та блокують підозрілу активність програм у «гарячому» режимі. Крім того, сучасні антивіруси можуть відновлювати файли, заражені шкідливими програмами.

Хмарні антивіруси (CloudAV). Поєднання можливостей сучасних антивірусних програм із хмарними технологіями. До таких рішень відносяться сервіси Crowdstrike, Panda Cloud Antivirus, Immunet та багато інших. Весь основний функціонал ПЗ розміщений у хмарі, а на комп'ютері, що захищається, встановлюється клієнт — програма з мінімальними технічними вимогами. Клієнт вивантажує хмарний сервер основну частину аналізу даних. Завдяки цьому забезпечується ефективний антивірусний захист за мінімальних ресурсних вимог до обладнання. Рішення CloudAV оптимально підходять для захисту ПК, які не мають достатньої вільної обчислювальної потужності для стандартного антивірусу.

Рішення DLP (Data Leak Prevention). Спеціальні програмні рішення, що запобігають витоку даних. Це комплекс технологій, які ефективно захищають підприємства від втрати конфіденційної інформації з різних причин. Впровадження та підтримка DLP – вимагає досить великих вкладень та зусиль з боку підприємства. Однак цей захід здатний значно зменшити рівень інформаційних ризиків для IT-інфраструктури компанії.

Системи криптографії. (3DES - 3Data Encryption Standard, AES - Advanced Encryption Standard). Перетворюють дані, після чого розшифровка може бути виконана тільки з використанням відповідних шифрів. Крім цього, криптографія може використовувати інші корисні програми для захисту інформації, у тому числі дайджести повідомлень, методи автентифікації, зашифровані мережеві комунікації, цифрові підписи. Сьогодні нові програми, що використовують зашифровані комунікації, наприклад, Secure Shell (SSH), поступово витісняють застарілі рішення, що не забезпечують в сучасних умовах необхідний рівень безпеки, такі як Telnet та протокол передачі файлів FTP. Для шифрування бездротового зв'язку широко використовуються сучасні протоколи WPA/WPA2. Також використовується досить старий протокол WEP, який поступається з безпеки. ITU-T G.hn та інші провідні комунікації шифруються за допомогою AES, а автентифікацію та обмін ключами в них

забезпечує X.1035. Для шифрування електронної пошти використовують такі програми як PGP та GnuPG.

Міжмережеві екрани. Рішення, які забезпечують фільтрацію та блокування небажаного трафіку, контролюють доступ до мережі. Розрізняють такі види фаєрволів, як мережеві та хост-сервери. Мережеві фаєрволи розміщуються на шлюзових ПК LAN, WAN та в інтрамережах. Міжмережевий екран може бути виконаний у форматі програми, встановленої на звичайний комп'ютер, або мати програмно-апаратне виконання. Програмно-апаратний фаєрвол - це спеціальний пристрій на базі операційної системи з встановленим МСЕ. Крім основних функцій, міжмережеві екрани пропонують низку додаткових рішень для внутрішньої мережі. Наприклад, виступають як сервер VPN або DHCP.

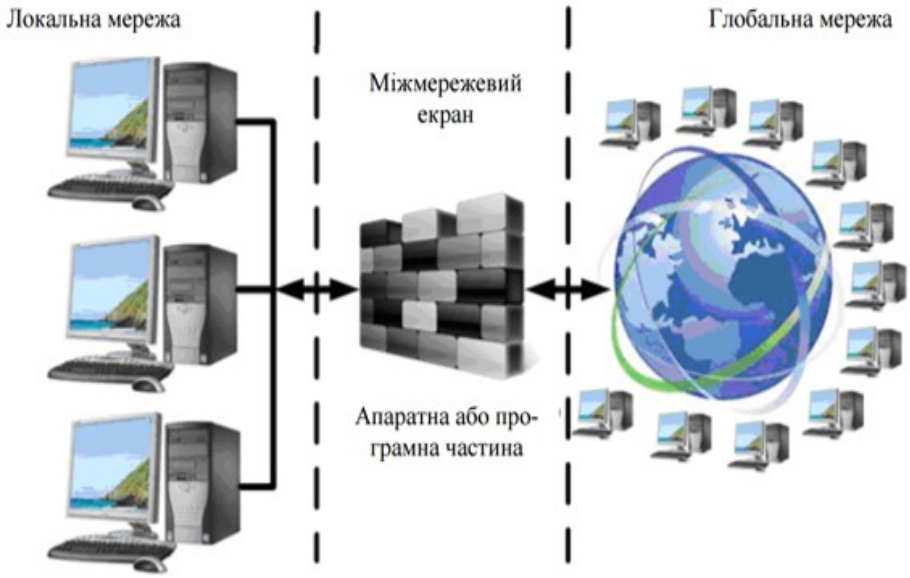

Рисунок 1.2 – Міжмережеві екрани

Віртуальні приватні мережі VPN (Virtual Private Network). Рішення, що використовує у межах загальнодоступної мережі приватну мережу передачі та прийому даних, що дає ефективний захист підключених до мережі додатків. За допомогою VPN забезпечується можливість віддаленого підключення до локальної мережі, створення спільної мережі головного офісу з філією.

Безпосередньо для користувачів VPN дає можливість приховувати розташування та захист дій, що виконуються в мережі.

Проксі-сервер. Виконує функцію шлюзу між комп'ютером та зовнішнім сервером. Запит, який надсилається користувачем на сервер, спочатку надходить на proxy і від його імені надходить на сервер. Повернення відповіді проводиться також із проходженням проміжної ланки - proxy. Перевагою є те, що кеш проксі-сервера доступний для всіх користувачів. Це підвищує зручність у роботі, оскільки найчастіше запитані ресурси перебувають у кеші.

Рішення SIEM - системи моніторингу та управління інформаційною безпекою. Спеціалізоване ПЗ, яке перебирає функцію управління безпекою даних. SIEM забезпечує збір відомостей про події з усіх джерел, що підтримують безпеку, у тому числі від антивірусного ПЗ, IPS, фаєрволів, а також від операційних систем тощо. Також SIEM виконує аналіз зібраних даних та забезпечує їх централізоване зберігання в журналі подій. На підставі аналізу даних система виявляє можливі збої, атаки хакерів, інші відхилення і можливі інформаційні загрози.

Таблиця 1.1 – Головні елементи організації ІБ на підприємстві

N п/п	Елемент інформаційної безпеки	Захисні заходи
1	Виявлення вразливостей	Перелік інформаційних ресурсів, що підлягають захисту
2	Виявлення інформаційних ризиків	Визначення всіх можливих загроз для кожного ресурсу ІКМ
3	Оцінювання рівня загроз	Побудова шкали рівнів інформаційних ризиків для кожного ресурсу ІКМ на випадок кібератаки
4	Контроль управління доступом до інформаційних ресурсів	Сегментування ІКМ підприємства за категоріями доступу до конфіденційної інформації
5	Протидія інформаційним загрозам	Розробка СЗІ, що унеможливлює НСД до інформаційних ресурсів, які обробляють конфіденційну інформацію
6	Впровадження нових СЗІ	Сертифікація та контроль за дотриманням політики безпеки
7	Усунення наслідків кібератак і кіберзагроз	Швидке реагування на НСД до конфіденційної інформації, що обробляється в ІКМ з метою мінімізації завданої шкоди

2 ВИЗНАЧЕННЯ ЦІННОСТІ АКТИВІВ ПІДПРИЄМСТВА

2.1 Цілі та задачі аудиту інформаційної безпеки

До основних цілей проведення аудиту ІБ зазвичай відносять:

− аналіз ризиків, які у свою чергу пов'язані із здійсненням загроз ІБ щодо ресурсів ІС;

− оцінка поточного ступеня безпеки ІС телекомунікаційної компанії;

− локалізація вузьких місць у системі захисту ІС;

− оцінка відповідності ІС чинним стандартам у сфері ІБ;

− формування рекомендацій щодо запровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Зазвичай до основних задач, які розв’язують в межах аудиту ІБ ІС відносять:

− аналіз структури, функцій, використовуваних технологій автоматизованої обробки та передачі інформації в ІС, аналіз бізнес-процесів, нормативно-розпорядчої та технічної документації;

− виявлення значущих загроз ІХ та шляхів їх реалізації, виявлення та ранжування за ступенем небезпеки існуючих вразливостей технологічного та організаційного характеру в ІС;

− складання неформальної моделі порушника, застосування методики активного аудиту для перевірки можливості реалізації порушником виявлених загроз ІБ;

− проведення тесту на проникнення за зовнішнім периметром IP-адрес, перевірка можливості проникнення в ІС за допомогою методів соціальної інженерії;

− аналіз та оцінка ризиків, пов'язаних з загрозами безпеці інформаційних ресурсів, оцінка поточної безпеки функціонування мережі зв'язку та корпоративної ІС;

− оцінка системи управління ІБ на відповідність вимогам міжнародних стандартів та розробка рекомендацій щодо вдосконалення системи управління ІБ;

− розробка пропозицій та рекомендацій щодо запровадження нових та підвищення ефективності існуючих механізмів забезпечення ІХ;

− оптимізація та планування витрат на забезпечення ІБ;

− обґрунтування інвестицій у системи захисту;

− отримання максимальної віддачі від інвестицій, що вкладаються в системи захисту інформації;

− підтвердження того, що використовувані внутрішні засоби контролю відповідають завданням організації та дозволяють забезпечити ефективність та безперервність бізнес-процесів компанії.

2.2 Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства

Вже розроблено багато способів оцінити ризики інформаційної безпеки. Найпопулярніші способи оцінки можна розбити на три групи: методи, управляючі документи та інструменти. На рис. 2.1 представлено їх підгрупи та власне конкретні способи оцінки, що відрізняються як підходом до самої проблеми, так і країною в якій було створено цей спосіб. Для вибору доцільного способу оцінки варто звертати увагу на умовами використання, характеристики та критерії відбору. Для кращого розуміння і вибору найкращого способу оцінки ризику інформаційної безпеки зазвичай використовують порівняння способів за критеріями, які необхідні й найважливіші для підприємства [2].

Одним з ключових документів, що описують вимоги до методу обробки і оцінки ризиків є міжнародний стандарт "ISO 27001: Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки "(далі - стандарт ISO 27001). Процес розрахунку ризиків інформаційної безпеки актуальний на всіх етапах роботи системи захисту інформації (СЗІ) і є цікавим для власника інформації в першу чергу з точки зору можливих економічних втрат.

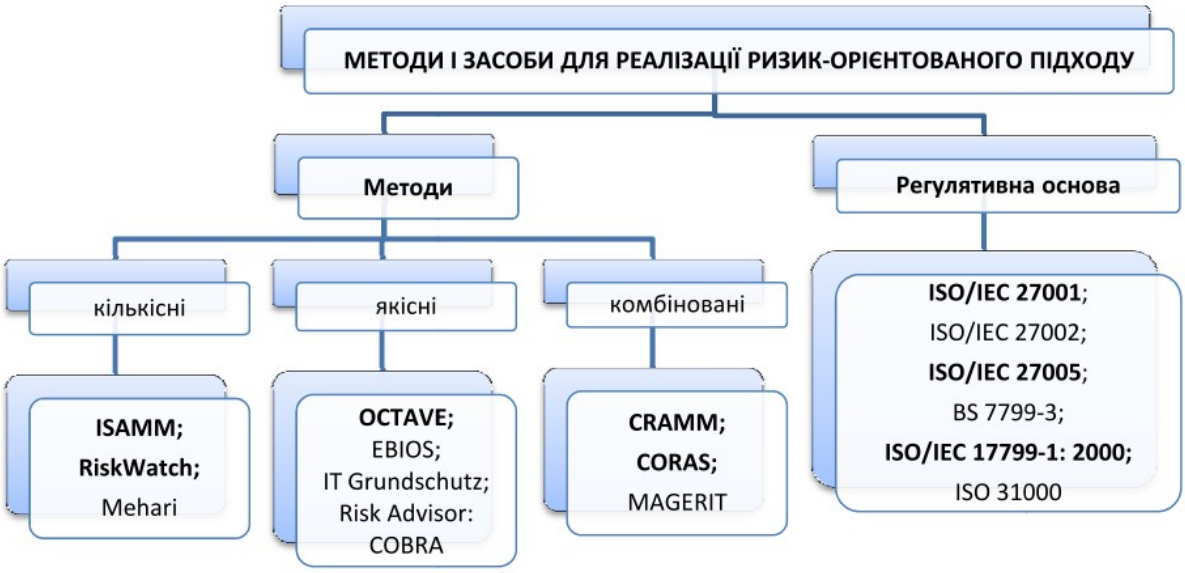

Рисунок 2.1 – Способи оцінювання інформаційних ризиків

Хоча в рамках вимог ISO 27001:2013 не розглядаються явні формули для розрахунку ризиків, виходячи з даних документа можна вибрати наступне:

- в процесі оцінки ризиків повинні бути встановлені критерії прийнятності ризику і критерії для оцінки ризиків ІБ;

- повинні бути дані гарантії того, що оцінка ризиків ІБ дасть обґрунтовані і не суперечливі масиви ризиків ІБ актуальних, для розглянутої системи;

- повинна бути розроблена ідентифікація ризиків ІБ, спрямованих на такі властивості інформаційних ресурсів, як конфіденційність, цілісність і доступність;

- повинна проводитись ідентифікація власника ризику, де під власником цім розуміється фізична, юридична особа, що відповідає за керування ризиком і володіє необхідними для цього повноваженнями. В даному випадку, мова може йти про керівників, фахівців з інформаційного захисту, відділів з ІБ та ін.;

- в процесі аналізу ризиків ІБ повинна бути проведена оцінка потенційних втрат у разі реалізації ризику;

- повинна бути оцінена вірогідність реалізації ризиків і визначена величина ризиків;

- в процесі оцінки ризиків ІБ має бути вироблено

зіставлення ризиків з установленими критеріями, а також визначено вектор пріоритетних напрямків при їхній обробці.

Стандарт ISO 27001:2013 істотно скорочений, на відміну від стандарту ISO 27001:2005, де процес оцінки ризиків був достатньо докладно розглянутий,

і включав в себе такі етапи, як ідентифікація вразливостей та ідентифікація активів і їх власників.

Вибір методу оцінки ризиків ІБ повинен ґрунтуватися на таких факторах:

- тимчасові, фінансові, інформаційні ресурси;

- ступінь невизначеності оцінки ризиків ІБ;

- наявність або відсутність можливості отримання кількості оцінок вихідних даних, де вихідними даними можуть бути думки, рішення, переліки, а також рекомендації, залежно від методу та етапу оцінки ризиків ІБ.

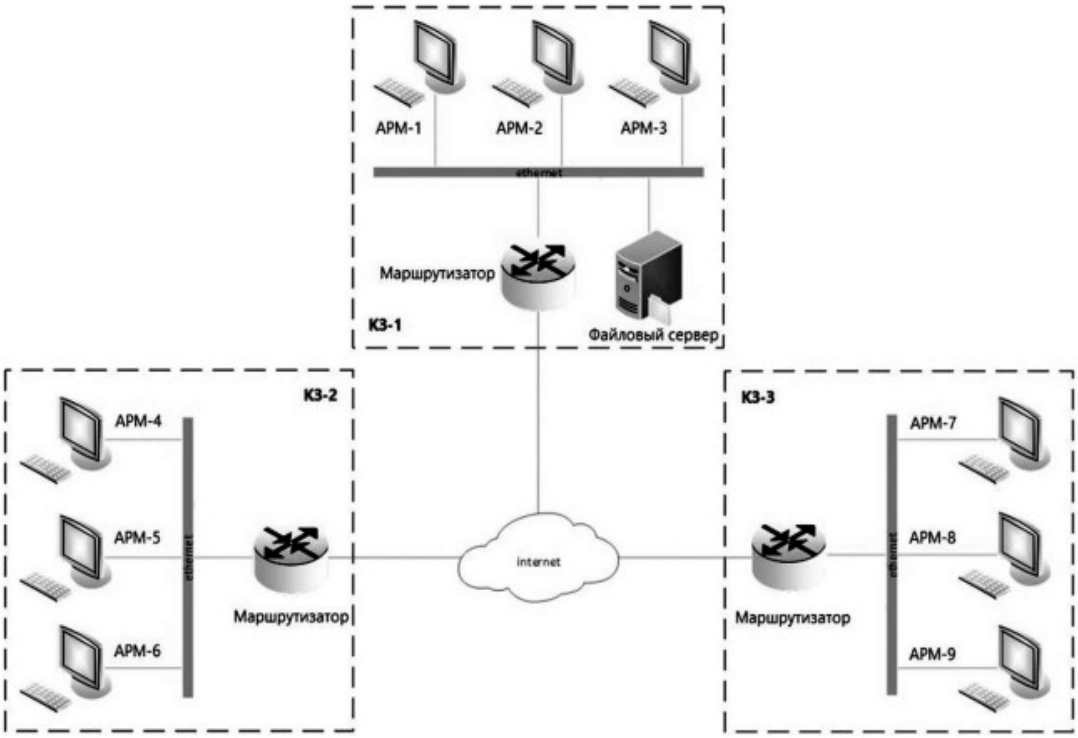

Рисунок 2.2 – Схематичне розположення розподіленої інфокомунікаційної мережі підприємства

На практиці, розрахунок ризиків необхідно починати з документа "Методологія оцінки обробки ризиків ", який розробляється до аналізу і обробки ризиків.

Підсумком заходів, про ведені відповідно до методики має стати звіт з сумарними результатами всіх заходів з оцінки степу ні ризиків та їх обробки.

2.3 Управління інформаційними ризиками

Ризик інформаційної безпеки – це потенційна можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації.

$$Величина\ Ризика = Можливість\ Події * Розмір\ Збитку, \quad (2.1)$$

де

Ймовірність Події = Вірогідність Загрози Величина Вразливості.*

Цілі процесу аналізу ризиків ІБ:

1. Ідентифікувати активи та оцінити їх цінність;

2. Ідентифікувати загрози активам та вразливості у системі захисту;

3. Прорахувати ймовірність реалізації загроз та їх вплив на бізнес;

4. Дотримуватися балансу між вартістю можливих негативних аслідків та вартістю заходів захисту, дати рекомендації керівництву компанії з бробки виявлених ризиків.

Етапи 1-3: оцінка ризику (risk assessment), тобто збирання наявної інформації.

Етап 4: аналіз ризиків (risk analysis), тобто. вивчення зібраних даних, надання вказівок для подальших дій (вибір способу обробки для кожного з оцінених та актуальних кіберризиків, вибір фінансово прийнятного рівня ризиків).

Для кількісного аналізу ризиків пропоную використовувати наступні показники:

ALE - annual loss expectancy, очікувані річні втрати, тобто "вартість" всіх інцидентів за рік;

SLE - single loss expectancy, очікувані разові втрати, тобто "вартість" одного інциденту.

EF – exposure factor, чинник відкритості перед загрозою, тобто який відсоток активу зруйнує загроза за її успішної реалізації.

ARO - annualized rate of occurrence, середня кількість інцидентів на рік відповідно до статистичних даних.

Значення SLE обчислюється як добуток розрахункової вартості активу та значення EF:

$$SLE = AssetValue * EF. \quad (2.2)$$

Значення ALE обчислюється як добуток SLE та ARO:

$$ALE=SLE*ARO. \quad (2.3)$$

2.4 Дослідження методологій ризик-менеджмента

1. Фреймворк "NIST Risk Management Framework" на базі американських урядових документів NIST (National Institute of Standards and Technology, Національний інститут стандартів і технологій США) включає набір взаємопов'язаних т.зв. "спеціальних публікацій" (англ. Special Publication (SP), будемо для простоти сприйняття називати їх стандартами):

Стандарт NIST SP 800-39 "Managing Information Security Risk" ("Управління ризиками інформаційної безпеки") пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Цей стандарт описує методологію процесу управління ризиками: визначення, оцінка, реагування та моніторинг ризиків;

Стандарт NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations" ("Фреймворк управління ризиками для інформаційних систем та організацій") пропонує для забезпечення безпеки та конфіденційності використовувати підхід управління життєвим циклом систем;

Стандарт NIST SP 800-30 "Guide for Conducting Risk Assessments" ("Посібник з проведення оцінки ризиків") сфокусований на IT, ІБ та операційних ризиках, описує підхід до процесів підготовки та проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки;

Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" ("Безперервний моніторинг інформаційної безпеки") описує підхід до процесу моніторингу інформаційних систем та IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ та необхідності їх перегляду.

2. Стандарти Міжнародної організації зі стандартизації ISO (International Organization for Standardization):

Стандарт ISO/IEC 27005:2018 "Information technology - Security techniques - Information security risk management" («Інформаційна технологія. Методи та засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки») входить до серії стандартів ISO 27000 і є логічно взаємопов'язаним ІБ із цієї серії. Цей стандарт відрізняється фокусом на ІБ під час розгляду процесів управління ризиками;

Стандарт ISO/IEC 27102:2019 "Information security management - Guidelines for cyber-insurance" («Управління інформаційною безпекою. Посібник з кіберстрахування») пропонує підходи до оцінки необхідності придбання кіберстрахування як заходи обробки ризиків, а також до оцінки та взаємодії зі страхом; .

Серія стандартів ISO/IEC 31000:2018 описує підхід до ризик-менеджменту без прив'язки до IT/ІБ.

3. Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки ризиків, з фокусом лише на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем та бізнес-процесів компанії.

5. Методологія FMEA (Failure Modes and Effect Analysis) пропонує проведення оцінки системи з погляду її слабких місць пошуку ненадійних елементів.

6. Методологія CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) пропонує використання автоматизованих засобів управління ризиками.

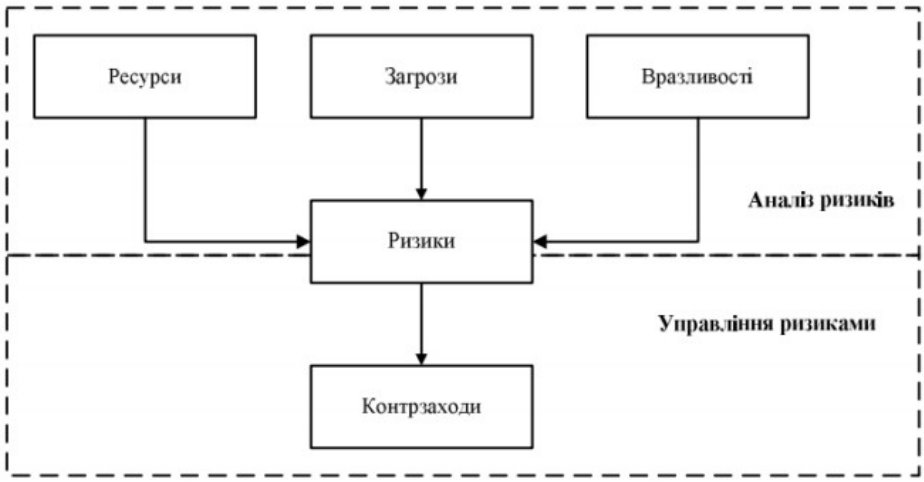

Рисунок 2.3 - Методика CRAMM

7. Методологія FAIR (Factor Analysis of Information Risk) – пропрієтарний фреймворк для проведення кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками на основі економічно ефективного

підходу, прийняття інформованих рішень, порівняння заходів управління ризиками, фінансових показників та точних ризик-моделей.

8. Концепція COSO ERM (Enterprise Risk Management) описує шляхи інтеграції ризик-менеджменту зі стратегією та фінансовою ефективністю діяльності компанії та акцентує увагу на важливості їхнього взаємозв'язку. У документі описані такі компоненти управління ризиками, як стратегія та постановка цілей, економічна ефективність діяльності компанії, аналіз та перегляд ризиків, корпоративне управління та культура, а також інформація, комунікація та звітність.

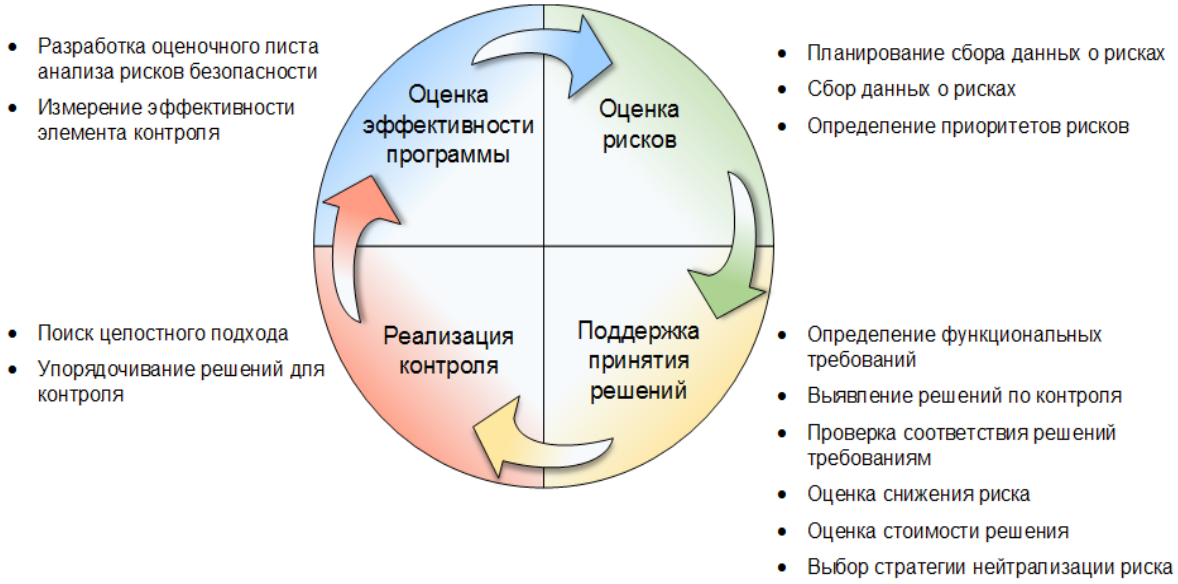

Рисунок 2.4 - Методологія Microcoft

Порівняння методологій оцінювання інформаційних ризиків наведено в таблиці 2.1. Порівняння авторкою здійснювалося за двома напрямками: за загальною характеристикою та вхідними даними, що аналізуються. Знак «+» означає наявність можливості; «-» - відсутність; «?» - не з’ясовано.

Таблиця 2.1 – Порівняння методологій оцінювання інформаційних ризиків

Критерії	CRAMM	CORAS	Risk	OCTAVE	Oracle

			Watch		Crystal Ball
Загальні характеристики					
Розрахованість на організацію різного розміру і сфери діяльності	+	+	+	+	+
Автоматизація «What-if»	-	?	+	-	+
Зручність сприйняття графіків і звітів	-	+	-	+	+
Простота використання	-	+	-	+	+
Безкоштовне використання	-	+	-	+	-
Підтримка	+	+	+	+	+
Кількісна оцінка	+	+	+	-	?
Якісна оцінка	+	+	-	+	?
Українська локалізація	-	?	+	?	-
Підвищення інформативності співробітника	-	-	-	+	?
Придатність до регулярного використання	+	-	?	+	?
Використання незалежної оцінки	+	+	?	-	+
Вхідні дані					
Ресурси	+	+	+	+	+
Тип інформаційної системи	+	?	+	+	-
Цінність ресурсів	+	+	+	+	?
Загрози	+	+	+	+	+
Уразливості системи	+	+	+	+	+
Вибір контрзаходів	+	?	+	-	-
Базові вимоги в сфері безпеки	-	?	+	-	-
Втрати	-	?	+	-	-
Заходи захисту	+	-	+	+	-
Частота виникнення загроз	-	?	+	-	-
Мережеве обладнання	-	?	-	+	-
Види інформації	-	?	-	?	-
Групи користувачів	-	?	-	-	-
Засоби захисту	-	?	-	+	-

2.5 Складання шкали активів

В даному випадку розглядається корпоративна розподільна інформаційна система (ІС), що має підключючи до мереж спільного користування, що обробляє інформацію різного рівня конфіденційності, що не містить відомостей, які складають державну таємницю.

Менеджмент ризику інформаційної безпеки "цінні активи організації умовно можна розділити на основні і додаткові.

Основні активи:

1. Бізнес-процеси - з сукупністю різних видів діяльності, в результаті якої створюється продукт або послуга, що представляють інтерес для споживача.

2. Інформація - відомості, є предметом власності, що підлягають захисту від порушення конфіденційності, цілісності та доступності, відповідно до вимог правових документів і вимогами власника інформації, незалежно від форми подання. Зведення, компрометація яких ніяким чином не вплине на діяльність організації, не розглядаються як ціни на актив.

Додаткові активи:

1. Апаратно-програмний комплекс - сукупність
технічних і програмних коштів, призначених для виконання взаємопов'язаних експлуатаційних функцій по обробці інформації обмеженого розповсюдження, що включає активну апаратуру обробки даних, стаціонарну апаратуру, що периферійні обробляють пристрої, операційні системи і прикладне програмне забезпечення.

2. Носії даних - носій для зберігання даних, включаючи електронний носії та аналоговий.

3. Мережа - сукупність телекомунікаційних пристроїв, для з’єднання декількох фізично віддалених сегментів інформаційної системи.

4. Персонал - всі суб’єкти, які мають правовий доступ у межі контрольованої зони та являються потенційно внутрішніми порушниками.

5. Місце функціонування організації – межі контрольованої зони, в якій функціонує інформаційна система.

Таблиця 2.2 - Шкала цінності активів

Ідентифікатор активаАктив підприємства			Конфіденційність	Цілісність	Доступність	Цінність актива
A	Основні активи інформації	Інформація необхідна для реалізації назначення чи бізнес організації	2	4	4	**4**
B.		Інформація особистого характеру, яка визначена особливим образом, відповідним національним законам про недоторканість приватного життя	3	1	1	**3**
C.		Стратегічна інформація, необхідна для досягнення цілей організації	2	2	1	**2**
D.			3	2	2	**3**
E.	Апаратно-програмний комплекс		-	3	4	**4**
F.	Носії інформації		-	1	2	**2**
G.	Мережа		-	3	4	**4**
H.	Працівники		-	1	1	**1**
I.	Місце функціонування організації		-	1	1	**1**

Інформацію поділяють на: необхідну для реалізації призначення, бізнес організації, інформацію особистого характеру, відповідну національну законам про недоторканність приватного життя, стратегічну інформацію, необхідну для досягнення цілей організації, інформацію обробка якої потребую ют тривалого часу або пов'язані з великими за витратами на її придбання.

Спочатку необхідно визначити цінність активів організації, в даному випадку буде розглянута чотирьох бальна система оцінки цінності активів:

1 бал - реалізація ризику, направленого на конфіденційність, цілісність та доступність активу не буде мати наслідків, як для підприємства в цілому, так і бізнес-процесів, зокрема.

2 бал - реалізація ризику, направленого на конфіденційність, цілісність або доступ активу призведе до незначних втрат в умовах, коли відновлення попереднього стану системи можливо без зупинки бізнес-процесів.

3 бал - реалізція ризику, направленого на конфіденційність, цілісність або доступ активу призведе до значних фінансових втрат і зробить негативний вплив на престиж підприємства, в умовах, коли відновлення попереднього

стану системи можливо, але вимагає великих тимчасових та фінансових ресурсів.

4 бал - реалізація ризику, направленого на конфіденційність, цілісність та доступність активу може призвести до повної зупинки бізнес-процесів, великих фінансових втрат та матиме значний негативний вплив на престиж підприємства.

Оскільки бізнес-процесом є сукупність різноманітних особистих видів діяльності, в результаті якої створюється продукт або послуга, то в переліку актуальних загроз та існуючих вразливостей інших цінних активів будуть міститися загрози і вразливості актуальні і для бізнес-процесів.

Особливістю нашого підприємства є те, що основну шкоду бізнес-процесам підприємству здатні завдати загрози доступності мережевого обладнання та програмно апаратного комплексу, а не загрози, спрямовані на руйнування конфіденційних інформаційних ресурсів підприємства.

2.6 Етапи процесів управління ризиками

2.6.1 Етап визначення ризиків

На першому етапі визначення ризиків організації слід виявити:

припущення про ризики, тобто. ідентифікувати актуальні загрози, уразливості, наслідки, ймовірність виникнення ризиків;

обмеження ризиків, тобто. можливості здійснення оцінки, реагування та моніторингу;

ризик-толерантність, тобто. терпимість до ризиків - прийнятні типи та рівні ризиків, а також допустимий рівень невизначеності у питаннях управління ризиками;

пріоритети та можливі компроміси, тобто необхідно розставити пріоритетні бізнес-процеси, вивчити компроміси, куди може піти організація при обробці ризиків, і навіть тимчасові обмеження та чинники невизначеності, які супроводжують цей процес.

2.6.2 Етап оцінки ризиків організації

На етапі оцінки ризиків організації слід виявити:

небезпеки ІБ, тобто. конкретні дії, осіб або сутності, які можуть бути загрозами для самої організації або можуть бути спрямовані на інші організації;

внутрішні та зовнішні вразливості, включаючи організаційні вразливості у бізнес-процесах управління компанією, архітектурі ІТ-систем тощо;

збитки організації з урахуванням можливостей експлуатації вразливих загроз;

ймовірність виникнення збитків.

Завдяки цьому організація отримує детермінанти ризику, тобто. рівень шкоди та ймовірність виникнення шкоди для кожного ризику.

Для забезпечення процесу оцінки ризиків організація заздалегідь визначає:

інструменти, техніки та методології, що використовуються для оцінки ризику;

припущення щодо оцінки ризиків;

обмеження, які можуть вплинути на оцінки ризиків;

ролі та відповідальність;

способи збору, обробки та передачі інформації про оцінку ризиків у межах організації;

способи проведення оцінки ризиків у організації;

частота проведення оцінки ризиків;

способи отримання інформації про загрози (джерела та методи).

2.6.3 Етап реагування на ризик

На етапі реагування на ризик організація виконує такі роботи:

розробка можливих планів реагування на ризик;

оцінка можливих планів реагування на ризик;

визначення планів реагування на ризик, допустимих з погляду ризик-толерантності організації;

реалізація ухвалених планів реагування на ризик.

Для забезпечення можливості реагування на ризики організація визначає типи можливої обробки ризиків (прийняття, уникнення, мінімізація, поділ або передача ризику), а також інструменти, технології та методології для розробки планів реагування, способи оцінки планів реагування та методи оповіщення про вжиті заходи реагування в рамках організації та/або зовнішніх контрагентів.

2.6.4 Етап моніторингу

На етапі моніторингу ризиків вирішуються такі завдання:

перевірка реалізації прийнятих планів реагування на ризик та виконання нормативних вимог ІБ;

визначення поточної ефективності заходів реагування на ризики;

визначення значущих для ризик-менеджменту змін у ІТ-системах та середовищах, включаючи ландшафт загроз, уразливості, бізнес-функції та процеси, архітектуру ІТ-інфраструктури, взаємини з постачальниками, ризик-толерантність організації та ін.

2.7 Забезпечення управліннями інформаційними ризиками протягом всього життєвого циклу інфокомунікаційної мережі.

Основні парадигми:

забезпечення безпеки та конфіденційності в ІТ-системах протягом усього життєвого циклу;

безперервний моніторинг стану захисту ІТ систем;

надання інформації керівництву для прийняття зважених ризик-орієнтованих рішень.

Типи ризиків: програмний ризик; ризик невідповідності законодавству України; фінансовий ризик; юридичний ризик; бізнес-ризик; політичний ризик; ризик безпеки та конфіденційності (включаючи ризик ланцюжка поставок); проектний ризик; репутаційний ризик; ризик безпеки життєдіяльності; ризик стратегічного планування.

Етапи застосування фреймворку управління ризиками:

підготовка, тобто визначення цілей та їх пріоритетів з точки зору організації та ІТ-систем;

категоризація систем та інформації на основі аналізу можливого негативного впливу від втрати інформації;

вибір базового набору заходів захисту та їх уточнення (адаптація) для зниження ризику до прийнятного рівня на основі оцінки ризику;

впровадження заходів захисту та опис того, як саме застосовуються заходи захисту;

оцінювання впроваджених заходів захисту для визначення коректності їх застосування, працездатності та продукування ними результатів, що задовольняють вимогам безпеки та конфіденційності;

формальне узгодження/затвердження використання систем або заходів захисту на основі висновку про прийнятність ризиків;

безперервний моніторинг систем та застосованих заходів захисту для оцінки ефективності застосованих заходів, документування змін, проведення оцінки ризиків та аналізу негативного впливу, створення звітності щодо стану безпеки та конфіденційності.

2.8 Процедура проведення оцінювання інформаційних ризиків

2.8.1 Підготовка до оцінювання ризиків

Підготовку до оцінювання ризиків включає такі етапи:

Ідентифікація цілі оцінювання ризиків;

Ідентифікація області (англ. scope) оцінювання ризиків;

Ідентифікація специфічних припущень та обмежень;

Ідентифікація джерел попередньої інформації, джерел загроз та вразливостей;

Ідентифікація моделі ризиків, способу оцінки ризиків та підходу до аналізу;

2.8.2 Проведення оцінювання ризиків

Проведення оцінювання ризиків складається з таких етапів:

Ідентифікація та характеризування актуальних джерел загроз;

Ідентифікація потенційних подій загроз, релевантності цих подій, а також джерел загроз;

Ідентифікація вразливостей;

Визначення ймовірності того, що актуальні події загроз призведуть до негативного впливу;

Визначення негативного впливу, породженого джерелами загроз;

Визначення ризику від реалізації актуальних подій загроз.

2.8.3 Комунікування результатів оцінки та передачу інформації всередині організації

Відбувається в два етапи:

Комунікування результатів оцінки ризиків особам, які приймають рішення, для реагування на ризики;

Передача заінтересованим особам інформації щодо ризиків, виявлених в результаті оцінки.

2.8.4. Підтримка досягнутих результатів

Здійснюється в 2 етапи:

Проведення безперервного моніторингу факторів ризику;

Актуалізація оцінки ризиків з використанням результатів безперервного моніторингу факторів ризику.

2.8.5 Способи аналізу факторів ризику

Виділяють 3 способи:

Загрозо-центричний;

Орієнтований на активи;

Орієнтований на вразливості.

2.9 Безперервний моніторинг інформаційних ризиків для інфокомунікаційних установ

2.9.1 Процесний підхід

Рекомендований процесний підхід до вибудовування системи моніторингу ІБ, що складається з:

визначення стратегії безперервного моніторингу ІБ;

розробки програми безперервного моніторингу ІБ;

впровадження програми безперервного моніторингу ІБ;

аналізу знайдених недоліків та звіту про них;

реагування на виявлені недоліки;

перегляду та оновлення стратегії та програми безперервного моніторингу ІБ.

2.9.2 Вибір інструментів моніторингу

Рекомендації щодо вибору інструментів забезпечення безперервного моніторингу ІБ:

підтримка ними великої кількості джерел даних;

використання відкритих та загальнодоступних специфікацій (наприклад, SCAP - Security Content Automation Protocol);

інтеграція з іншим ПЗ, таким як системи Help Desk, системи управління інвентаризацією та конфігураціями, системами реагування на інциденти;

підтримка процесу аналізу відповідності застосовним законодавчим нормам;

гнучкий процес створення звітів, можливість «провалюватися» (англ. drill-down) у глибину даних, що розглядаються;

підтримка систем Security Information and Event Management (SIEM) та систем візуалізації даних.

3 ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Доцільно обробку ризиків ІБ розглядати, як інтерактивний процес, це дозволяє підвищити рівень деталізації оцінки ризиків при кожній наступній ітерації.

Під *ідентифікацією ризику* розуміється процес знаходження і визначення ризиків ІБ, під *оцінкою ризику* розуміється присвоєння числових значень наслідкам реалізації ризику, а також ймовірності його реалізації. Прийняття ризику означає, що збиток від реалізації ризику є прийнятим, а ймовірність його реалізації мала настільки, що дозволяє не проводити процедур обробки ризику ІБ.

Комунікація ризику дозволяє здійснювати обмін інформацією про актуальні ризики між зацікавленими сторонами.

Під *обробкою ризику* розуміється процес мінімізації наслідків від реалізації ризику та процес мінімізації ймовірності реалізації ризику ІБ.

Наступним кроком є визначення ступеня вразливості кожного з цінних активів організації. В рамках даної атестаційної роботи буде розглянуто вибірковий ряд загроз ІБ, найнебезпечніших для нашого підприємства.

I- загроза тривалого утримання обчислювальних ресурсів користувачами;

II - загроза завантаження нештатної операційної системи;

III -загроза приведення системи в стан" відмова в про слугування;

IV - "загроза програмного виведення з ладу коштів зберігання, обробки або введення/виведення/передачі інформації;

V - загроза втрати обчислювальних ресурсів;

VI - загроза втрати носіїв інформації;

VII - загроза фізичного виведення з ладу засобів збереження, обробки або введення/виводу/передачі інформації;

VIII - загроза форматування носіїв інформації;

IX - загроза розкрадання засобів зберігання, обробки;

X - загроза неправомірного шифрування інформації;

XI - загроза поширення «поштових хробаків» ;

XII - загроза фізичного старіння апаратних компонентів;

XIII- загроза надлишкового видалення оперативної пам'яті;

XIV - загроза зміни компонентів системи;

XV - загроза використання інформація про ідентифікацію / автентифікації, визначеної за замовчуванням;

XVI - загроза використання вразливостей протоколів мережево /локального обміну даними;

XVII - загроза дослідження механізмів роботи програми;

XVIII - загроза несанкціонованого видалення конфіденційної інформації;

XIX - загроза перезавантаження апаратних і програмно-апаратних засобів обчислюваної техніки;

XX - загроза пошкодження системного реєстру;

XXI - загроза підвищення привілеїв;

XXII загроза подолання фізичного захисту;

XXIII - загроза впровадження шкідливого коду через рекламу, сервіси і контент;

XXIV - загроза маскування дій шкідливого коду.

3.1 Загроза тривалого утримання обчислювальних ресурсів користувачами

Опис загрози. Загроза полягає в можливості обмеження порушником доступу кінцевих користувачів до обчислювального ресурсу за рахунок примусового утримання його в завантаженому стані шляхом здійснення їм багатократного виконання певних деструктивних дій або експлуатації вразливостей програм, що розподіляють обчислювальні ресурси між завданнями. Ця загроза обумовлена слабкостями механізмів балансування навантаження і розподілу обчислювальних ресурсів. Реалізація загрози можлива коли у порушника є можливість робити запити, які в сукупності вимагають більше часу на виконання, чим запити користувача.

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Інформаційна система, мережевий вузол, носій інформації, системне програмне забезпечення, мережеве програмне забезпечення, мережевий трафік.

Наслідки реалізації загрози. Порушення доступності.

3.2 Загроза завантаження нештатної операційної системи

Опис загрози. Загроза полягає в можливості підміни порушником операційної системи, що завантажується, шляхом несанкціонованої переконфігурації в BIOS/UEFI шляхи доступу до завантажувача операційної системи. Ця загроза обумовлена слабкостями технологій розмежування доступу до управління BIOS/UEFI. Реалізація цієї загрози можлива за умови доступності порушникові наступного параметра налаштування BIOS/UEFI - вказівки джерела завантаження операційної системи.

Джерела загрози. Внутрішній порушник з низьким потенціалом.

Об'єкт дії. Мікропрограмне забезпечення BIOS/UEFI

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, порушення доступності.

3.3 Загроза надлишкового видалення оперативної пам'яті

Опис загрози. Загроза полягає в можливості виділення значних ресурсів оперативній пам'яті для обслуговування запитів шкідливих програм і відповідного зниження об'єму ресурсів оперативної пам'яті, доступних в системі для виділення у відповідь на запити програм легальних користувачів. Ця загроза обумовлена наявністю слабкостей механізму контролю виділення оперативної пам'яті різним програмам. Реалізація цієї загрози можлива за умови знаходження шкідливого програмного забезпечення в системі в активному стані.

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом.

Об'єкт дії: Апаратне забезпечення, системне програмне забезпечення, мережеве програмне забезпечення.

Наслідки реалізації загрози. Порушення доступності

3.4 Загроза зміни компонентів системи

Опис загрози. Загроза полягає в можливості отримання порушником доступу до мережі, файлів, впровадження закладок і тому подібне шляхом несанкціонованої зміни складу програмних або апаратних засобів інформаційної системи, що надалі дозволить здійснювати цьому порушникові(чи іншому - зовнішньому, такому, що виявив несанкціонований канал доступу в систему) несанкціоновані дії в цій системі. Ця загроза

обумовлена слабкостями заходів контролю за цілісністю апаратної конфігурації інформаційної системи. Реалізація цієї загрози можлива за умови успішного отримання порушником необхідних повноважень в системі і можливості підключення додаткового периферійного устаткування.

Джерела загрози. Внутрішній порушник з низьким потенціалом.

Об'єкт дії.: Інформаційна система, сервер, робоча станція, віртуальна машина, системне програмне забезпечення, прикладне програмне забезпечення, апаратне забезпечення.

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, порушення доступності.

3.5 Загроза використання інформація про ідентифікацію/автентифікації, визначеної за замовчуванням

Опис загрози. Загроза полягає в можливості проходження порушником процедури авторизації на основі отриманої з відкритих джерел або від інформаційного сервісу ідентифікаційної і аутентифікаційної інформації, відповідного облікового запису об'єкту захисту, що "за умовчанням" дискредитується. Ця загроза обумовлена тим, що у безлічі програмних і програмно-апаратних засобів виробниками передбачені облікові записи "за умовчанням", призначені для первинного входу в систему або тим, що при проходженні на інформаційному сервісі процедури реєстрації механізм автоматичної генерації паролів видає однакові або схожі паролі користувачам з схожими логінами. Більше того, на багатьох пристроях ідентифікаційна і аутентифікаційна інформація може бути повернена до заданої "за умовчанням" після проведення апаратного скидання параметрів системи(функція Reset).

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з середнім потенціалом.

Об'єкт дії. Засобу захисту інформації, системне програмне забезпечення, мережеве програмне забезпечення, мікропрограмне забезпечення, програмно-апаратні засоби зі вбудованими функціями захисту

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, порушення доступності.

3.6 Загроза використання вразливостей протоколів мережевого /локального обміну даними

Опис загрози. Загроза полягає в можливості здійснення порушником несанкціонованого доступу до інформації, що передається в ІС й підлягає захисту за рахунок деструктивної дії на протоколи мережевого/локального обміну даними в системі шляхом порушення правил використання цих протоколів. Ця загроза обумовлена слабкостями самих протоколів(закладених в них алгоритмів), помилками, допущеними в ході реалізації протоколів, або вразливостями, впроваджуваними автоматизованими засобами проектування/розробки. Реалізація цієї загрози можлива у разі наявності слабкостей в протоколах мережевого/локального обміну даними.

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Системне програмне забезпечення, мережеве програмне забезпечення, мережевий трафік.

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, порушення доступності.

3.7 Загроза дослідження механізмів роботи програми

Опис загрози. Загроза полягає в можливості проведення порушником зворотного інжинірингу коду програми і подальшого дослідження його структури, функціонала і складу в інтересах визначення алгоритму роботи програми і пошуку в ній вразливостей. Ця загроза обумовлена слабкостями механізму захисту коду програми від дослідження. Реалізація цієї загрози можлива у випадках: наявність у порушника доступу до початкових файлів програми; наявність у порушника доступу до дистрибутива програми і відсутності механізму захисту коду програми від дослідження.

Джерела загрози. Внутрішній порушник з середнім потенціалом, зовнішній порушник з середнім потенціалом.

Об'єкт дії. Системне програмне забезпечення, прикладне програмне забезпечення, мережеве програмне забезпечення, мікропрограмне забезпечення.

Наслідки реалізації загрози. Порушення конфіденційності, порушення доступності.

3.8 Загроза несанкціонованого видалення конфіденційної інформації

Опис загрози. Загроза полягає в можливості спричинення порушником економічного, інформаційного, морального і інших видів збитку власникові і операторові інформації, що неправомірно видаляється, шляхом здійснення деструктивної програмної або фізичної дії на машинний носій інформації. Ця загроза обумовлена недостатністю заходів по забезпеченню доступності інформації, що захищається, в системі, а рівно і наявністю вразливостей програмному забезпеченні, що реалізовує ці заходи. Реалізація цієї загрози можлива у разі отримання порушником системних прав на стирання даних або фізичного доступу до машинного носія інформації на відстань, достатню для чинення ефективної деструктивної дії.

Джерела загрози. Внутрішній порушник з низьким потенціалом, зовнішній порушник з низьким потенціалом.

Об'єкт ді. Метадані, об'єкти файлової системи, реєстр.

Наслідки реалізації загрози. Порушення доступності.

3.9 Загроза перезавантаження апаратних і програмно-апаратних засобів обчислюваної техніки

Опис загрози. Загроза полягає в можливості скидання користувачем(порушником) стану оперативної пам'яті(обнулення пам'яті) шляхом випадкового або навмисного здійснення перезавантаження окремих пристроїв, блоків або системи в цілому. Ця загроза обумовлена властивістю оперативної пам'яті обнуляти свій стан при виключенні і перезавантаженні. Реалізація цієї загрози можлива як апаратним способом(натисненням кнопки), так і програмним(локально або видалено) при виконанні наступних умов : наявність в системі відкритих сесій роботи користувачів; наявність у порушника прав в системі(чи фізичній можливості) на здійснення форсованого перезавантаження.

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом. *Об'єкт дії* Системне програмне забезпечення, апаратне забезпечення.

Наслідки реалізації загрози. Порушення цілісності Порушення доступності.

3.10 Загроза пошкодження системного реєстру

Опис загрози. Загроза полягає в можливості порушення доступності частини функціонала або усієї інформаційної системи через пошкодження використовуваного в її роботі реєстру внаслідок некоректного завершення роботи операційної системи(неконтрольоване перезавантаження, виникнення помилок в роботі драйверів пристроїв і тому подібне), порушення цілісності файлів, що містять в собі дані реєстру, виникнення помилок файлової системи носія інформації або внаслідок здійснення порушником деструктивної програмної дії на файлові об'єкти, що містять реєстр. Ця загроза обумовлена слабкостями заходів контролю доступу до файлів, що містять дані реєстру, заходів резервування і контролю цілісності таких файлів, а також заходів відновлення працездатності реєстру із-за збоїв в роботі операційної системи. Реалізація цієї загрози можлива при одній з умов : виникнення помилок в роботі окремих процесів або усієї операційної системи; наявності у порушника прав доступу до реєстру .

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом. *Об'єкт дії* Об'єкти файлової системи, реєстр.

Наслідки реалізації загрози. Порушення цілісності, доступності.

3.11 Загроза підвищення привілеїв

Опис загрози. Загроза полягає в можливості здійснення порушником деструктивної програмної дії на процес(чи систему), що дискредитується, або на інші процеси(чи системи) від його(її) імені шляхом експлуатації неправомірно отриманих порушником додаткових прав на управління дискредитованим об'єктом. Ця загроза обумовлена вразливостями програмного забезпечення, що виконує функції розмежування доступу (у алгоритмі або параметрах конфігурації). Реалізація цієї загрози можлива за наявності у порушника програмного забезпечення(типу "експлойт"), спеціально розробленого для реалізації цієї загрози в системі.

Джерела загрози. Внутрішній порушник з середнім потенціалом, зовнішній порушник з середнім потенціалом.

Об'єкт дії. Системне програмне забезпечення, мережеве програмне забезпечення, інформаційна система

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, доступності.

3.12 Загроза подолання фізичного захисту

Опис загрози. Загроза полягає в можливості здійснення порушником практично будь-яких деструктивних дій відносно інформаційної системи, що дискредитується, при отриманні їм фізичного доступу до апаратних засобів обчислювальної техніки системи шляхом подолання системи контролю фізичного доступу, організованої у будівлі підприємства. Ця загроза обумовлена вразливостями в системі контролю фізичного доступу(відсутністю замків в приміщенні, помилками персоналу і тому подібне). Реалізація цієї загрози можлива за умови успішного застосування порушником будь-якого з методів проникнення на об'єкт(обман персоналу, злом замків та ін.).

Джерела загрози. Зовнішній порушник з середнім потенціалом.

Об'єкт дії. Сервер, робоча станція, носій інформації, апаратне забезпечення.

Наслідки реалізації загрози. Порушення конфіденційності, порушення цілісності, порушення доступності.

3.13 Загроза приведення системи в стан" відмова в обслуговуванні

Опис загрози. Загроза полягає в можливості відмови дискредитованою системою в доступі легальним користувачам при лавиноподібному збільшенні числа мережевих з'єднань з цією системою або при використанні недоліків реалізації мережевих протоколів. Ця загроза обумовлена тим, що для обробки кожного мережевого запиту системою споживається частина її ресурсів, а також слабкостями мережевих технологій, пов'язаними з обмеженістю швидкості обробки потоків мережевих запитів, і недостатністю заходів контролю за управлінням з'єднаннями і помилками реалізації мережевих протоколів. Реалізація цієї загрози можлива за умови перевищення об'єму запитів над об'ємами доступних для їх обробки ресурсів системи, що дискредитується, або наявності помилок реалізації мережевих протоколів(наприклад, формування IP- адреси версії 6 на основі MAC- адреси, визначення доступності IP- адреси, використання функції контролю цілісності PPP- інтерфейсу та ін.)

Джерела загрози. Внутрішній порушник з низьким потенціалом, зовнішній порушник з низьким потенціалом.

Об'єкт дії. Інформаційна система, мережевий вузол, системне програмне забезпечення, мережеве програмне забезпечення, мережевий трафік, телекомунікаційне облаштування.

Наслідки реалізації загрози. Порушення доступності.

3.14 Загроза програмного виведення з ладу засобів зберігання, обробки або введення (виводу) передачі інформації

Опис загрози. Загроза полягає в можливості переривання порушником технології обробки інформації в системі, що дискредитується, шляхом здійснення деструктивної програмної(локально або видалено) дії на засоби зберігання(зовнішніх, знімних і внутрішніх накопичувачів), обробки(процесора, контролера пристроїв і тому подібне) і(чи) введення /виведення /передачі інформації(клавіатури та ін.), в результаті якого об'єкт захисту перейде в стан "відмова в обслуговуванні". При цьому виведення його з цього стану може бути неможливе шляхом перезавантаження системи, а зажадає проведення ремонтно-відновних робіт. Ця загроза обумовлена наявністю вразливостей мікропрограмного забезпечення засобів зберігання, обробки і(чи) введення /виведення /передачі інформації, а також неможливості тривалого знаходження засобів зберігання, обробки і(чи) введення /виведення /передачі інформації в режимі гранично допустимих значень (частота системної шини, центрального процесора, кількості звернень.

Джерела загрози. Внутрішній порушник з середнім потенціалом Зовнішній порушник з середнім потенціалом.

Об'єкт дії. Носій інформації, мікропрограмне забезпечення, апаратне забезпечення, телекомунікаційне облаштування. Наслідки реалізації загрози Порушення цілісності, доступності.

3.15 Загроза втрати обчислювальних ресурсів.

Опис загрози. Загроза полягає в можливості відмови легітимному користувачеві у виділенні ресурсів для обробки його запитів із-за вичерпання порушником вільних ресурсів в системі, здійсненого шляхом їх несанкціонованого виключення із загального пулу ресурсів на основі техніки "витоку ресурсів" або "виділення ресурсів". Ця загроза обумовлена слабкостями механізму контролю за розподілом обчислювальних ресурсів між користувачами, а також заходів міжмережевого екранування інформаційної системи, що дискредитується, і контролю достовірності мережевих запитів на сторонніх серверах. Реалізація цієї загрози можлива за умови наявності у порушника: відомостей про формат і параметри деструктивних дій на систему, вільних ресурсів, що призводять до виключення("витоки" або "виділенню"), із загального пулу ресурсів системи, що дискредитується; привілеїв, достатніх для здійснення деструктивних дій("витоки" або "виділення") в системі, що дискредитується; відсутність у адміністраторів можливості: для техніки "витоку ресурсів" - перезавантаження системи під час відправки порушником великого числа запитів на виділення ресурсів, а для техніки "виділення ресурсів" - форсованого звільнення ресурсів, виділених по запитах шкідливих процесів.

Джерела загрози. Внутрішній порушник з низьким потенціалом, зовнішній порушник з низьким потенціалом.

Об'єкт дії. Інформаційна система, мережевий вузол, носій інформації, системне програмне забезпечення, мережеве програмне забезпечення, мережевий трафік.

Наслідки реалізації загрози. Порушення доступності.

3.16 Загроза втрати носіїв інформації

Опис загрози. Загроза полягає в можливості розкриття інформації, що зберігається на загубленому носії(у разі відсутності шифрування даних), або її втрати(у разі відсутності резервної копій даних). Ця загроза обумовлена слабкостями заходів реєстрації і обліку носіїв інформації, а також заходів резервування даних, що захищаються. Реалізація цієї загрози можлива внаслідок халатності співробітників.

*Джерела загрози***.** Внутрішній порушник з низьким потенціалом.

Об'єкт дії. Носій інформації.

Наслідки реалізації загрози. Порушення конфіденційності, доступності.

3.17 Загроза фізичного виведення з ладу засобів збереження, обробки або введення (виводу) передачі інформації

Опис загрози. Загроза полягає в можливості умисного виведення з ладу зовнішнім порушником засобів зберігання, обробки і(чи) введення /виведення /передачі інформації, що може привести до порушення доступності, а в деяких випадках і цілісності інформації, що захищається. Ця загроза обумовлена слабкостями заходів контролю фізичного доступу до засобів зберігання, обробки і(чи) введення /виведення /передачі інформації. Реалізація цієї загрози можлива за умови отримання порушником фізичного доступу до носіїв інформації(зовнішнім, знімним і внутрішнім накопичувачам), засобів обробки інформації(процесору, контроллерам пристроїв і тому подібне) і засобів введення/виведення інформації(клавіатура і тому подібне).

Джерела загрози. Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Сервер, робоча станція, носій інформації, апаратне забезпечення.

Наслідки реалізації загрози. Порушення цілісності, доступності.

3.18 Загроза форматування носіїв інформації

Опис загрози. Загроза полягає в можливості втрати інформації, що зберігається на носії, що форматується, частенько без можливості її відновлення, із-за умисного або випадкового виконання процедури форматування носія інформації. Ця загроза обумовлена слабкістю заходів обмеження доступу до системної функції форматування носіїв інформації. На реалізацію цієї загрози впливають такі чинники як: час, що пройшов після форматування; тип носія інформації; тип файлової системи носія; інтенсивність взаємодії з носієм після форматування та ін.

Джерела загрози. Внутрішній порушник з низьким потенціалом Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Носій інформації.

Наслідки реалізації загрози. Порушення цілісності, доступності.

3.19 Загроза розкрадання коштів зберігання, обробки

Опис загрози. Загроза полягає в можливості здійснення зовнішнім порушником крадіжки комп'ютера(і підключених до нього пристроїв), USB-накопичувачів, оптичних дисків або інших засобів зберігання, обробки, передачі інформації. Ця загроза обумовлена слабкостями заходів контролю фізичного доступу до засобів зберігання, обробки чи передачі інформації. Реалізація цієї загрози можлива за умови наявності у порушника фізичного доступу до носіїв інформації(зовнішнім, знімним і внутрішнім накопичувачам), засобів обробки інформації(процесору, контролерам пристроїв і тому подібне) і засобів введення/виведення інформації(клавіатура і тому подібне).

Джерела загрози. Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Сервер, робоча станція, носій інформації, апаратне забезпечення.

Наслідки реалізації загрози. Порушення конфіденційності, доступності.

3.20 Загроза неправомірного шифрування інформації

Опис загрози. Загроза полягає в можливості фактичної втрати доступності даних, що захищаються, із-за їх несанкціонованого криптографічного перетворення порушником за допомогою відомого тільки йому секретного ключа. Ця загроза обумовлена наявністю слабкостей в антивірусному захисті, а також в механізмах розмежування доступу. Реалізація цієї загрози можлива за умови успішної установки порушником на комп'ютер засобу криптографічного перетворення інформації, що дискредитується, а також успішного виявлення(ідентифікації) порушником файлів, що захищаються.

Джерела загрози. Зовнішній порушник з низьким потенціалом.

Об'єкт дії. Об'єкт файлової системи.

Наслідки реалізації загрози. Порушення доступності.

3.21 Загроза поширення «поштових хробаків»

Опис загрози. Загроза полягає в можливості порушення безпеки інформації користувача, що захищається, шкідливими програмами, що потайно встановлюються при отриманні користувачами системи електронних листів, що містять шкідливу програму типу "поштовий черв'як", а також мимовільної участі в подальшому протиправному поширенні шкідливого коду. Ця загроза

обумовлена слабкостями механізмів антивірусного контролю. Реалізація цієї загрози можлива за умови наявності у користувача електронної поштової скриньки, що дискредитується, а також наявності в його адресній книзі хоч би однієї адреси іншого користувача.

Джерела загрози Зовнішній порушник з низьким потенціалом.

Об'єкт дії Мережеве програмне забезпечення.

Наслідки реалізації загрози Порушення конфіденційності Порушення цілісності, доступності.

3.22 Загроза фізичного старіння апаратних компонентів

Опис загрози. Загроза полягає в можливості порушення функціональності системи, пов'язаної з безпекою, внаслідок відмов апаратних компонентів цієї системи із-за їх фізичного старіння (іржа, швидке зношення, окислення, забруднення, відшарування, лущення та ін.), обумовленого впливом фізичного довкілля(вологості, пилу, корозійних субстанцій). Можливість реалізації цієї загрози зростає при використанні користувачами технічних засобів в умовах, що не задовольняють вимогам заданих їх виробником.

Джерела загрози. Внутрішній порушник з низьким потенціалом.

Об'єкт дії. Апаратний засіб.

Наслідки реалізації загрози. Порушення доступності.

3.23 Загроза впровадження шкідливого коду через рекламу, сервіси і контент

Опис загрози. Загроза полягає в можливості впровадження порушником в інформаційну систему шкідливого коду за допомогою реклами, сервісів і(чи) контенту(тобто переконання користувача системи активувати посилання, код та ін.) при відвідуванні користувачем системи сайтів в мережі Інтернет або установкою програм з функцією показу реклами. Ця загроза обумовлена слабкостями механізмів фільтрації мережевого трафіку і антивірусного контролю на рівні організації. Реалізація цієї загрози можлива за умови відвідування користувачами системи з робочих місць сайтів в мережі Інтернет.

Джерела загрози. Внутрішній порушник з низьким потенціалом.

Об'єкт дії. Мережеве програмне забезпечення.

Наслідки реалізації загрози. Порушення цілісності, доступності.

3.24 Загроза маскування дії шкідливого коду

Опис загрози. Загроза полягає в можливості приховання в системі дій шкідливого коду за рахунок застосування спеціальних механізмів маскування коду(архівація, зміна формату цих та ін.), які перешкоджають його подальшому аналізу. Ця загроза обумовлена наявністю способів маскування програмного коду, не врахованих сигнатурними базами засобів захисту інформації, а також механізмів операційної системи, що дозволяють здійснити пошук модулів засобів захисту інформації. Реалізація цієї загрози можлива за умови використання в системі застарілих версій засобів захисту інформації.

Джерела загрози. Зовнішній порушник з середнім потенціалом.

Об'єкт дії. Системне програмне забезпечення, мережеве програмне забезпечення.

Наслідки реалізації загрози. Порушення цілісності, доступності.

3.25 Методика оцінювання потенційних вразливостей

У NIST 800-30 «Risk management guide for information technology systems» наводиться наступна класична формула розрахунку ризику:

$$R = P(t) * S, \quad (3.1)$$

де R – значення ризику;

P(t) – ймовірність реалізації загрози інформаційній безпеці (застосовується суміш якісної та кількісної шкали);

S – ступінь впливу загрози на актив (ціна активу в якісній та кількісній шкалі).

У результаті обчислюється значення ризику у відносних одиницях, яке можна ранжувати. за ступенем значущості для процедури управління ризиками інформаційної безпеки.

Також розрахунок ризику відбувається за такою формулою:

$$R = P(t) *P(v)* S, \quad (3.2)$$

де P(t) – можливість реалізації загрози інформаційної безпеки;

P(v) – ймовірність наявності вразливості;

S – цінність активу.

Як приклад значень ймовірностей P(t) і P(v) наведена якісна шкала з трьома рівнями (низьким, середнім та високим). Для оцінки значення цінності активу S перед ставлені числові значення в інтервалі від 0 до 4. Зіставлення їм

якісних значень має зробити організація, в якій проводиться оцінка ризиків інформаційної безпеки.

Відповідно до BS 7799-2:2005 «Специфікація системи управління інформаційною безпекою», рівень ризику обчислюється з урахуванням наступних показників: цінності ресурсу, рівня загрози та ступеня вразливості. Зі збільшенням значень цих параметрів ризик збільшується. Таким чином, формулу можна представити у такому вигляді:

$$R = S * L(t)* L(v), \quad (3.3)$$

де S – цінність активу (ресурсу);

L(t) – рівень небезпеки;

L(v) – рівень (ступінь вразливості).

На практиці обчислення ризиків інформаційної безпеки відбувається за таблицею позиціонування значень рівня загроз, ступеня ймовірності використання вразливості та вартості активу. Значення ризику може змінюватися в діапазоні від 0 до 8, в результаті кожного активу виходить список загроз з різними значеннями ризику. Стандарт пропонує наступну шкалу ранжування ризиків: низький (0-2), середній (3-5) та високий (6-8). Це дозволяє визначити найбільш критичні ризики.

Оцінювання ступеня можливості реалізації загрози інформаційної безпеки проводиться за наступною якісно-кількісною шкалою: нереалізована загроза - 0%, середня - від 21% до 50% і т. д.

Визначення ступеня тяжкості наслідків для різних типів інформаційних активів пропонується оцінювати з використанням якісно-кількісної шкали, тобто мінімальне – 0,5% від величини капіталу підприємства, високе – від 1,5% до 3% від величини капіталу.

У табл. 3.1 представлений результат оцінки уразливості активу для переліку загроз, де

1 - низька вразливість по відношенню конфіденційності, цілісності та/або доступності цін активу організації,

2 -середній ступінь вразливості,

3- висока ступінь вразливості.

Таблиця 3.1 – Ступінь вразливості активу

Загрози ІБ	Цінні активи організації								
	A.	B.	C.	D.	E.	F.	G.	H.	I.
I	-	-	-	-	2	-	-	-	-
II	1	1	1	1	3	-	-	-	-
III	-	-	-	-	2	-	2	-	-
IV	-	-	-	-	3	-	-	-	-
V	2	2	2	2	1	-	-	-	-
VI	-	-	-	-	-	-	1	-	-
VII	1	1	1	1	1	-	1	-	-
VIII	3	3	3	3	-	-	-	-	-
IX	-	-	-	-	2	-	-	-	-
X	2	2	2	2	2	-	-	-	-
XI	-	-	-	-	2	-	-	-	-
XII	1	1	1	1	3	3	-	-	-
XIII	-	-	-	-	3	-	3	-	-
XIV	3	3	3	3	2	2	-	-	-
XV	1	1	1	1	3	3	3	-	-
XVI	3	3	3	3	-	2	-	-	-
XVII	-	-	-	-	1	1	-	-	-
XVIII	1	1	1	1	-	1	-	-	-
XIX	1	1	1	1	2	2	-	-	-
XX	2	2	2	2	-	-	-	-	-
XXI	-	-	-	-	-	-	2	-	-
XXII	-	-	-	-	1	-	1	-	-
XXIII	2	2	2	2	-	-	2	-	-
XXIV	-	-	-	-	1	-	1	-	-

Останнім етапом перед розрахунком ризиків ІБ є ця оцінка ймовірності реалізації загроз ІБ, представлених у табл. 3.1.

Оцінка ймовірності поставлена в табл. 3.2, де

1 – загроза існує, але не зустрічалася у розглянутій сфері, 2-3 рази на рік,

2 загроза виникає в розглядаємій сфері 2-3 рази на рік,

3 - загроза була реалізована в розглянутої системи,

4 - загроза виникає 2-3 рази на рік у цій системі.

Таблиця 3.2 – Ймовірності реалізації загроз

ID загрози	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI	XVII	XVIII	XIX	XX	XX	XXII	XXIII	XXIV
Ймовірність	2	1	2	3	1	2	2	4	2	2	2	3	2	2	2	4	3	3	3	2	2	3	3	2

3.26 Розробка контрзаходів

На сьогодні актуальним завданням у галузі забезпечення ІБ ІС є захист від мережевих атак, заснованих на використанні протоколів транспортного та мережевого рівнів стека TCP/IP. Існуючі засоби захисту не завжди справляються з новими видами таких атак, тому важливим напрямом досліджень та розробок є створення систем захисту, здатних захищати немає від конкретних атак, як від цілих класів атак. Складність процесів виявлення та блокування атак суттєво збільшується внаслідок сучасних тенденцій розвитку інформаційно-телекомунікаційних технологій, у тому числі пов'язаних із зростанням розмірів та продуктивності мереж, ускладненням їхньої топології, зростанням обсягу "швидкого трафіку", обумовленого функціонуванням peer-to-peer-програм, VoIP-трафіком, роботою сканерів безпеки і так далі.

Існуючі мережеві атаки можна розділити на чотири основні класи: збирання інформації, що використовує аналіз результату обробки пакетів; атаки, засновані на помилках у обробці пакетів; сканування хостів та мереж, що базується на використанні помилок у обробці сесій; сканування,заснований на коректному встановленні з'єднань.

Виявлення мережевих атак за допомогою спеціалізованого програмного забезпеченням забезпечення, як правило, полягає в моніторингу мережевого трафіку між клієнтською системою, на яку проводитися атака та системою зловмисника (атакуюча система), а також аналізі підозрілого трафіку мережі, з подальшою оцінкою атаки, ризиків її здійснення, збитків та механізмів протидії атакуючій системі. Найчастіше підозрілий трафік виявляється автоматично, і не вимагає постійного спостереження за трафіком з сторони експерта, що у свою чергу виключає людський фактор у помилковості розпізнавання атаки на ресурси системи До переважаючих методам розпізнавання мережевих атак відносять – сигнатурний аналіз. Величина ризику мережевої атаки не можлива без експертної думки, на основі даної величини має бути прийняте рішення про заходи та способи реагування на мережеву атаку. У випадках з мінімальними ризиками атака може взагалі не заслуговувати на увагу. У протилежних випадках може вимагати швидкої реакцію події.

Залежно від ступеня критичності атаки, існують різні рівні реагування ними. Зауважимо, що за рівнем критичності атаки зазвичай визначається ступінь реакцію неї. Загалом, критичність атаки пов'язана з величиною ризику та можливої шкоди від даної атаки. Для вирішення задачі захисту від мережевих атак необхідна концепція, визначальна об'єкти захисту, цілі, завдання та основні принципи захисту, а також склад і послідовність робіт із попередження, виявлення та реагування на атаки. Таким чином, можна сказати, що аналіз ризиків ІБ є одним з методів реагування на мережеві атаки.

У зв'язку з вищесказаним у цьому розділі пропонується наступний алгоритм реагування на атаку.

На першому етапі за допомогою відомих програм для запису трафіку (наприклад, ПЗ Zabbix і т.п.) в режимі онлайн проводиться протоколювання телекомунікаційного трафіку (навантаження мережі) залежно від часу.

По суті, вихідні дані є дискретний цифровий ряд, зручний для подальшого аналізу. На другому етапі з використанням методів фрактального аналізу даним значенням обчислюються показник Херста та спектр потужності. За зниження

значення показника Херста до рівня 0,5-0,55 можна судити про те, що трафік перетворюється на аномальний стан. Однак судити про те, що в цей момент починається мережева атака, тільки по зниженню даного значення недоцільно. Як показано, наприклад, [14], невелике зниження показника Херста може відбуватися і у разі постійно збільшеної навантаження мережі протягом певного інтервалу часу.

Таблиця 3.3 Рекомендовані контрзаходи

Цінний актив організації	Загрози	Ризик	Допустимий ризик	Планові заходи	Остаточний ризик
Інформація необхідна для реалізації назначення чи бізнес організації	VIII	48	Від 1 до 19	Система резервного копіювання, система захисту від НСД	12
	XIV	24		Система антивірусного захисту, міжмережеве екранування	12
	XVI	48		Облік носіїв інформації	12
	XXIII	24		Система антивірусного захисту, міжмережеве екранування; Організаційні заходи	8
Апаратно-програмний комплекс	IV	36	Від 1 до 19	Міжмережеве екранування, система довіреної загрузки, система антивірусного захисту; Організаційні заходи	12
	XII	36		Система відеонагляду, адекватні засоби фізичного захисту; Організаційі заходи	12
	XIII	24		Система міжмережевого екранування	12
	XV	24		Система міжмережевого екранування	12
	XIX	24		Система відеонагляду, адекватні засоби фізичного захисту; Організаційні заходи	8
Мережа	XIII	24	Від 1 до 19	Система міжмережевого екранування	12
	XV	24		Система міжмережевого екранування	12
	XXIII	24		Система антивірусного захисту, міжмережеве екранування; Організаційні заходи	8

Припустимо, що керівник підприємства приймає рішення, що ризики з числовим значенням вище 20 підлягають обробці з метою їхньої мінімізації. Можливі контрзаходи представлені у табл. 3.3. Після обробки ризиків ІБ, залишковий ризик став прийнятним для кожної з актуальних загроз інформаційній безпеці.

ВИСНОВКИ

В кваліфікаційній роботі були розглянуті міжнародні та національні стандарти у сфері захисту інформації, регламентуючі питання менеджменту ризиків інформаційної безпеки. Зокрема, було встановлено основні вимоги до оцінки та обробки ризиків інформаційної безпеки, виходячи з міжнародного стандарту ISO 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки», а також проведено порівняння цього стандарту з його версією від 2005 року. Як провідний метод оцінки та обробки ризиків був обраний якісний метод, як найбільш економічний, в умовах відсутності готових даних про кількість реалізованих атак у розглянутій інформаційній системі за окремий проміжок часу.

У ході виконання кваліфікаційної роботи було розглянуто цінні активи організації, та, ґрунтуючись на бізнес-процесах телекомунікаційного підприємства були виділені основні та другорядні активи, а також відповідні їм загрози інформаційній безпеки.

Результатом виконаної роботи став розрахунок ризиків інформаціїційної безпеки, заснований на виділенні цінних активів організації, ступеня потенційної шкоди при реалізації загроз на такі активи та ймовірності реалізації загроз для аналізованої інформаційної системи телекомунікаційного підприємства. Крім цього, були виділені прийнятні ризики, обробка яких не потрібна у зв'язку з тим, що фактична вартість їх мінімізації вища за збитки від реалізації відповідних їм загроз. У 3-му розділі були запропоновані можливі заходи щодо мінімізації ризиків інформаційної безпеки, що включають систему резервного копіювання, систему захисту від несанкціонованого доступу, систему антивірусного захисту, міжмережеве екранування, а також організаційні заходи та заходи фізичного захисту.

Запропонований метод дозволяє однозначно й обґрунтовано оцінити, нитка ризики інформаційної безпеки організації в умовах недостатності вихідних даних, а також відсутність додаткових програмно-апаратних засобів для оцінки ризиків інформаційної безпеки, що дозволяє застосовувати його для типових організацій, ґрунтуючись лише на масштабуванні аналізованої системи, за умови відсутності в обробці даних, що складають державну інформацію таємницю.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
2. Закон України "Про інформацію" [Електронний ресурс]. – 1992. – Режим доступу до ресурсу: https://www.tax.gov.ua/diyalnist-/dpa-i-gromadskist/normativno-pravova-baza-u-sferi/arhiv-normativno-pravova-baza/53366.html.
3. Закон України “Про електронні документи та електронний документообіг” [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/851-15#Text.
4. Закон України “Про основні засади забезпечення кібербезпеки України”" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
5. Закон України "Про електронні довірчі послуги" [Електронний ресурс] // 2017 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
6. Указ Президента України від 15 березня 2016 року № 96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/96/2016#Text.
7. Золотарьов В. Безпека інфокомунікаційних мереж // Інформаційні мережі зв’язку. Ч.4 Технології надання інформаційних послуг: навч. Посібник / Безрук В.М., Корольов В.М., Золотарьов В.А., Боцман П.Д., Костромицький А.І., Астраханцев А.А.,Капуста С.О. . – Харків:ХНУРЕ,2011. – с.324-391.
8. SIEM-система в защите компании от кибератак [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://gsminfo.com.ua/24276-siem-systema-v-zashhyte-kompanyy-ot-kyberatak.html.
9. Шевцов Л. Н. Анализ стандартов, топологий и технологий мультисервисных сетей доступа // Наука, техника и инновации:

гипотезы, проблемы, результаты / Л. Н. Шевцов, Л. Н. Щитов. // Наука, техника и инновации: гипотезы, проблемы, результаты: сборник научных трудов по материалам XI Международного междисциплинарного форума молодых ученых, 10 октября 2017 г. – 2017. – С. 181 – 189.

10. Мареева Е. В. Как бороться с кибератаками на центры обработки данных [Електронний ресурс] / Е. В. Мареева, Е. Н. Шкоркина // Защита информации. Инсайд. – 2019. – Сентябрь-октябрь – Режим доступу до ресурсу: https://systempb.ru/company/our-articles/kak-borotsya-s-kiberatakami-na-tsentry-obrabotki-dannykh/.
11. Топ угроз ИБ в корпоративных сетях, 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/.
12. Топ угроз ИБ в корпоративных сетях, 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/.
13. Сеть хранения данных (SAN — Storage Area Network) [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.itc.by/storage-area-network/
14. Безопасность в сетях хранения данных [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: http://www.ishodniki.ru/art/net/storing/1026.html.
15. Организация надежных каналов связи [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://rascom.ru/information/blog/organizaciya-nadezhnykh-kanalov-svyazi/.
16. Что такое VLAN: логика, технология и настройка. Реализация VLAN в устройствах CISCO [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://e-server.com.ua/sovety/chto-takoe-vlan-logika-tehnologija-i-nastrojka-realizacija-vlan-v-ustrojstvah-cisco.
17. Решение Cisco по контролю доступа в сеть для беспроводных LAN [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.cisco.com/web/RU/netsol/ns466/netbr0900aecd80355b2f.html.
18. Олещенко Л. М. Організація комп'ютерних мереж. Конспект лекцій / Л. М. Олещенко. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.

19. Смирнов А. Маршрутизатор — определяем типы атак [Електронний ресурс] / Андрей Смирнов. – 2021. – Режим доступу до ресурсу: https://14bytes.ru/marshrutizator-opredelyaem-tipy-atak/

20. Стецюк В. І. Методи контролю інформаційних потоків в телекомунікаційних системах / В. І. Стецюк, В. В. Мішан, О. В. Боженок. // Вісник Хмельницького національного університету. – 2018. – С. 209–216.

21. Юдін О. К. Аналіз та класифікація систем контролю та управління доступом на підприємстві / О. К. Юдін, О. М. Веселовська. // Науково-ємні технології. – 2018. – №2. – С. 220–225.

22. Дегтярьова Л.М. Аналіз структури системи захисту інформації / Л.М.Дегтярьова, М.В.Мірошникова, С.В.Волошко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 2 (54). – С. 78-82.

23. Захарченко С.М. Основи побудови захищених мереж на базі обладнання компанії Cisco : навчальний посібник // С. М. Захарченко, Т. І. Трояновська, О. В. Бойко – Вінниця : ВНТУ, 2017. – 136 с

24. Захарченко С. М. Метод багаторівневого захисту даних в корпоративних мережах [Електронний ресурс] / С. М. Захарченко, О. В. Войцеховська, Ю. В. Куцак – Режим доступу до ресурсу: https://conferences.vntu.edu.ua/index.php/mn/mn2020/paper/viewFile/8483/7089.

25. Концепция построения многоуровневой системы защиты на основе ОС Solaris [Електронний ресурс] – Режим доступу до ресурсу: https://www.opennet.ru/docs/RUS/solaris_sec/solsec_1.html.

26. Рагозин Ю. Н. Инженерно-техническая защита информации: учебное пособие / Ю. Н. Рагозин. – Санкт-Петербург: ИЦ "Интермедия", 2018. – 168 с.

27. Корченко О. Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах / О. Корченко, Ю. Дрейс, І. Лозова. // Захист інформації. – 2016. Т.18, № 1– С. 39–47.

28. Дрейс Ю. О. Підхід до аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / Ю. О. Дрейс, А. О. Дейсан, Д. Ю. Бєляк. // «68-ма науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів»: Матеріали конференції, 4-6 грудня 2013 р., Част. 3. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С. 117–120.

29. Полтавцева М. А. Безопасность данных: проблемы и перспективы / М. А. Полтавцева, А. Р. Хабаров. // Программные продукты и системы. – 2016. – С. 36 – 41.