МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ЛАБОРАТОРНИХ ЗАНЯТЬ
навчальної дисципліни «Моделі ризик-орієнтованого аналізу в кібербезпеки» обов'язкових компонент
освітньої програми другого (магістр) рівня вищої освіти

125 «Кібербезпека» (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від _____ № __

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 17.01.2024 № 1

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від _____ № __

Розглянуто на засіданні кафедри протидії кіберзлочинності.
Протокол від 10.01.2024 № 1

Розробник:
викладач кафедри протидії кіберзлочинності Калякін С.В.

Рецензенти:

1. завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н., професор Петров К.Е.;
2. доцент кафедри кібербезпеки та DATA-технологій факультету №6 ХНУВС, к.т.н., доцент Тулупов В.В.

Розподіл часу навчальної дисципліни за темами
(заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
Тема № 1. Вступ до теорії ризиків ІБ.	**45**	**2**			**2**	**41**	
Тема № 2. Технології аналізу ризиків.	**45**	**2**			**2**	**41**	
Всього по дисципліні	**90**	**4**			**4**	**82**	**Залік**

1. Методичні вказівки до лабораторних занять

Лабораторна робота № 1

Тема: Аналіз ризиків та основні принципи забезпечення інформаційної безпеки (матричний підхід 1).

Мета роботи:

1. Поглиблення та закріплення теоретичних знання з питань:
- поняття ризиків інформаційної безпеки та їх аналіз;
- основні принципи та методи забезпечення інформаційної безпеки.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1.Ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації.

2.Набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення ІБ.

Висновки.

Література:

1. Матеріали лекції 1.
[1, с. 8 – 12, 16 - 19]
2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Стислі теоретичні відомості

1.1. Поняття ризиків інформаційної безпеки

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерному шахрайству, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз інформаційної безпеки та ймовірності реалізації цих загрози.

В зв'язку з цим, також необхідно володіти таким поняття як ризик інформаційної безпеки – потенційна можливість використання загрозою вразливостей інформаційного активу або групи активів для заподіяння шкоди об'єктам або інтересам суб'єктів інформаційних відносин. Виходячи з визначення ризику, для проведення аналізу ризиків потрібні наступні дані про інформаційну систему: перелік цінної інформації із зазначенням її рівня критичності, відомості про уразливість інформаційної системи і загрози, які на неї діють.

При цьому необхідно відзначити, що жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки. Саме тому й проводиться аналіз та оцінка ризиків ІБ.

1.2. Аналіз ризиків інформаційної безпеки – матричний підхід

Розрізняють два методи аналізу та оцінки ризиків: кількісний та якісний.

Для кількісної оцінки ризиків характерне використання об'єктивних чисельних, а саме фінансових характеристик. На відміну від кількісного, якісний аналіз ризиків не ставить своїм завданням отримання чисельних фінансових характеристик. Для оцінки активів і критичність загроз вводиться якісна неформальна або напівформальна шкала, і основною метою такого аналізу стає ранжування загроз відповідно з обраними критеріями.

Оскільки даний курс присвячений основам інформаційній та кібернетичній безпеці, а не менеджменту ІБ, в лабораторній роботі буде розглянуто один із якісних методів аналізу ризиків, а саме матричний підхід аналізу ризиків ІБ, який пов'язує активи, уразливості, загрози та засоби контролю (міри, які організація може прийняти для мінімізації дій загроз на один чи більше активів) і визначає важливість різних засобів контролю, відповідним активам організації.

Матричний підхід використовує три окремих матриці: матрицю уразливостей, матрицю загроз і матрицю засобів контролю, які дозволяють зібрати всі необхідні дані для аналізу ризиків ІБ.

Матриця уразливостей складається із взаємозв'язків між активами і уразливостями в організації, в свою чергу матриця загроз відображає взаємозв'язки між уразливостями і загрозами, а матриця засобів контролю містить взаємозв'язки між загрозами і засобами контролю. Таким чином, кожна клітинка в таблиці відображає значення взаємозв'язку між елементами рядків та стовпців. В даному методі використовується наступна шкала взаємозв'язку (оцінки впливу): немає впливу, слабкий, помірний, сильний вплив.

При первинному аналізі ризиків формуються списки активів, уразливостей, загроз, засобів контролю, які в подальшому додаються до відповідних таблиць. Матриці заповнюються поступово шляхом додавання даних щодо взаємозв'язку елементів стовпця матриці з елементами рядка. Спершу заповнюється матриця уразливостей, дані якої обчислюються за допомогою формули (1.1), для визначення вагомості (значущість) уразливостей, після чого останні переносяться до наступної матриці – матриці загроз. Аналогічно, дані в матриці загроз обчислюються за допомогою формули (1.2), таким чином визначаючи потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці. В результаті чого, формується матриця контролю, яка містить відносну важливість різних засобів контролю. Дана матриця визначає необхідність в застосуванні конкретних мір або засобів захисту для мінімізації впливу загроз на один або більше активів організації зменшуючи рівень ризиків (демонструючи «чистий ризик» – ризик з мінімізованою реалізацією загроз).

Таблиця 1.1. Матриця уразливостей (взаємозв'язок між активами та вразливостями)

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний C_j	Активи:	Секрети виробництва	Конфіденційна інформація	Репутація (довіра)	Апаратне забезпечення	Програмне забезпечення	Послуги	Комунікації	**Всього**	**Ранжування**
Уразливості:	РП								Σ	
Веб-сервер										
Обчислювальний сервер										
Міжмережевий екран										
Маршрутизатор										
Клієнтський вузол										
База даних										

Припустимо, що є n активів, де відносна вартість активу $a_j \in C_j$ $(j = 1, \cdots, n)$. Також нехай v_{ij} – це відносний вплив уразливості v_i на актив a_j. Тоді потенційний вплив уразливості V_i на активи організації обчислюється за формулою:

$$V_i = \sum_{j=1}^{n} v_{ij} C_j \qquad 1.1$$

Таблиця 1.2. Матриця загроз (взаємозв'язок між уразливостями та загрозами)

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Веб-сервер	Обчислювальний сервер	Міжмережевий екран	Маршрутизатор	Клієнтський вузол	База даних	Передача даних	**Всього**	**Ранжування**
Загрози:	РП								Σ	
Відмова в обслуговуванні (DoS)										
Шкідливе ПЗ										

Помилки користувача										
Спам										
«Фішинг»										
Ворожий агент										

Припустимо, що існує p загроз, які можуть бути реалізовані за допомогою n уразливостей та t_{ki} – відносна можливість використання загрозою t_k уразливості v_i. Тоді потенційна реалізація конкретної загрози T_k обчислюється за формулою:

$$T_k = \sum_{i=1}^{n} t_{ki} V_i \qquad 1.2$$

Таблиця 1.3. Матриця контролю (взаємозв'язок між загрозами та засобами захисту)

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Відмова в обслуговуванні	Шкідливе ПЗ	Помилки користувача	Спам	«Фішинг»	Ворожий агент	Збій електроживлення	**Всього**	**Ранжування**
Засоби контролю:	РП								Σ	
Система виявлення вторгнень (IDS)										
Навчання персоналу										
Міжмережевий екран										
Політика безпеки										
Конфігурація архітектури мережі										
Демілітаризована зона (DMZ)										

Припустимо, що є q засобів контролю (захисту), які можуть пом'якшити (мінімізувати) вплив p загроз, а z_{lk} – відносний вплив засобу контролю z_l на загрозу t_k. Тоді потенційне пом'якшення загроз за допомогою конкретного засобу контролю – Z_l, обчислюється за формулою:

$$Z_l = \sum_{i=1}^{p} z_{lk} T_k \qquad 1.3$$

Таким чином, за допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби

контролю, в результаті чого ми одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

1.2.1. Приклад використання методики аналізу ризиків ІБ

Дослідження аналізу ризиків за допомогою запропонованої методики буде здійснюватися на прикладі компанії «Cyberstec», яка займається розробкою програмного забезпечення. На даний момент компанія займається розробкою проектів в основному зосереджених в таких областях як: безпека робочих станцій і мережева безпека, віртуалізація та віддалений доступ, управління поведінкою системи, обробка даних, робота з мобільними пристроями. Вона має фрагментовану організаційну структуру, працює у декількох містах України (Київ, Львів, Харків, Одеса), а також має бізнес представництво у місті Мюнхен (Німеччина). Це достатньо конкурентний бізнес, де постійно розвиваються ІТ-технології і виробники постійно намагаються обійти один одного, таким чином, інформаційна безпека – є критичним фактором для захисту активів компанії і запобіганню зриву її діяльності.

Саме тому, для правильної організації системи безпеки, вибору конкретних методів захисту, та планування витрат на ІБ, в компанії проводиться аналіз інформаційних ризиків за допомогою запропонованої методики. Три матриці, які пов’язують активи та уразливості, уразливості та загрози, загрози та засоби контролю, представлені в таблицях 1.4, 1.5 та 1.6 відповідно.

Таким чином, у таблиці 1.4 представлено матрицю уразливостей, яка пов’язує уразливості та активи компанії «Cyberstec». Для побудови матриці була визначена відносна цінність активів та проведено їхнє ранжування (з права на ліво). Наприклад, успішність компанії залежить від її здатності розвивати і захищати нові технології; тому вони високо оцінюються. Ґрунтуючись на активах, було визначено ключові уразливості, надано їм ранг пріоритету та встановлено відносний вплив уразливостей на активи компанії. Так як зовнішні порушники (хакери) спершу повинні обійти брандмауер, щоб отримати доступ до конфіденційної інформації, він займає перше місце у матриці уразливостей. Окрім того, як було зазначено раніше, філії компанії територіально розкидані, тому передача та синхронізація даних також оцінюються високо.

Таблиця 1.1. Матриця уразливостей «Cyberstec»

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний ҫ	**Активи:**	Новітні розробки (технології)	Конф. інф. (програмний код)	Репутація (довіра)	Доступність сервісів	Комунікації	Програмне забезпечення	Апаратне забезпечення	**Всього**	**Ранжування**
Уразливості:		7	6	5	4	3	2	1	Σ	
Брандмауер	5	9	9	3	9	9	9	9	222	9
Передача даних та лінії зв'язку	5	9	9	3	9	9	3	9	210	8
Фізична безпека	4	9	9	3	1	1	3	9	154	5
Помилки конфігурації серверів екстранет	4	9	9	1	9	3	9	1	186	7
ПК співробітників компанії	3	3	9	1	0	1	9	3	104	2
Бази даних	4	9	9	3	3	1	9	1	166	6
Стійкість паролів	3	9	9	1	1	3	9	1	154	4
Помилки конфігурації серверів інтернет	2	1	1	9	9	3	9	1	122	3
Ненадійне джерело живлення	1	0	0	3	9	9	0	1	79	1

В результаті, як бачимо, в матриці було проведено обчислення потенційного впливу уразливостей на активи «Cyberstec» за формулою (1.1) для того, щоб відранжувати уразливості і таким чином визначити їхню значущість.

Після цього уразливості були перенесені до наступної матриці.

Беручи до уваги наявні уразливості в активах компанії, було визначено ключові загрози, надано їм ранг пріоритету та аналогічним чином, встановлено відносну можливість використання загрозою уразливості.

Таблиця 1.2. Матриця загроз «Cyberstec»

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Брандмауер	Передача даних та	Помилки конфігурації серверів екстранет	Бази даних	Фізична безпека	Стійкість паролів	Помилки конфігурації серверів інтернет	ПК співробітників компанії	Ненадійне джерело живлення	**Всього**	**Ранжування**
Загрози:		9	8	7	6	5	4	3	2	1	Σ	
Відмова в обслуговуванні (DoS/DDos)	5	9	9	9	0	1	1	9	1	1	255	5
Шкідливе ПЗ	4	1	1	9	1	1	1	3	9	1	123	2
Помилки працівника	2	1	1	3	3	3	3	3	9	1	111	1
Збої сервера	5	9	9	9	9	9	1	9	1	9	357	8
Вторгнення (атака на пароль)	3	9	3	9	9	1	9	3	3	1	279	6
Фізичне пошкодження ІТС	3	1	9	3	3	9	0	3	3	3	183	3
«Спуфінг» та «Маскарад»	2	1	9	9	3	1	1	9	9	1	217	4
НСД	5	9	3	9	9	9	9	9	9	1	349	7

В результаті обчислень за допомогою формули (1.2), було визначено потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці.

Останньою формується матриця контролю, до якої, окрім загроз, були внесені запропоновані засоби контролю з відповідним рангом пріоритету. Після чого було встановлено відносний вплив засобу контролю на загрозу з використанням суб'єктивних суджень, і обчислено за формулою (1.3) потенційне пом'якшення загроз. Отримані дані були відранжовані з метою визначення пріоритетних засобів контролю. Ця інформація, в поєднанні з вартістю засобів контролю використовується для планування ІБ.

Таким чином, результати аналізу і узагальнення даних, що містяться в матрицях будуть використовуватися під час процесу інтеграції та вибору програмного забезпечення і апаратного устаткування в компанії «Cyberstec».

Таблиця 1.3. Матриця контролю «Cyberstec»

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Збої сервера	НСД	Вторгнення (атака на пароль)	Відмова в обслуговуванні	«Спуфінг» та «Маскарад»	Фізичне пошкодження ІТС	Шкідливе ПЗ	Помилки працівника	**Всього**	**Ранжування**
Засоби контролю:		8	7	6	5	4	3	2	1	Σ	
Система виявлення вторгнень (IDS)	5	9	9	3	9	9	1	3	3	246	6
Навчання персоналу	2	1	0	9	0	3	3	9	9	110	1
Міжмережеві екрани	5	9	9	9	9	9	1	3	1	280	7
Політика безпеки	4	1	9	9	3	9	1	9	3	200	4
Конфігурація архітектури мережі	5	9	3	1	9	1	0	0	1	149	2
Демілітаризована зона (DMZ)	3	9	9	3	9	3	0	0	3	213	5
Контроль території	4	3	9	9	1	1	9	3	1	184	3

1.3. Основні принципи та методи забезпечення інформаційної безпеки

З метою протидії основним загрозам ІБ, система забезпечення інформаційної безпеки ІТС повинна вирішувати наступні завдання:

1) розмежування та контроль доступу користувачів до ресурсів ІТС;

2) захист всіх даних, що передаються по каналах зв'язку;

3) реєстрація, збір, зберігання, обробка і видача інформації про всі події, що відбуваються в системі і мають відношення до забезпечення її безпеки;

4) моніторинг роботи користувачів ІТС системою захисту інформації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

5) забезпечення замкнутого середовища функціонування вже перевіреного ПЗ з метою захисту від неконтрольованого впровадження в систему потенційно небезпечних програм (які можуть містити «закладки» або критичні помилки) і засобів подолання системи захисту, а також від впровадження та поширення шкідливого ПЗ;

6) забезпечення доступності інформаційних ресурсів шляхом резервного копіювання даних;

7) забезпечення та контроль цілісності критичних ресурсів системи захисту ІТС.

Також необхідно відмітити, що розрізняють зовнішню та внутрішню безпеку ІТС. Зовнішня безпека полягає в захисті ІТС від загроз природного походження, а також від проникнення в систему зловмисників ззовні. Внутрішня ж безпека повинна створювати надійний і зручний механізм регламентування діяльності усіх законних користувачів та обслуговуючого персоналу ІТС, а також забезпечувати цілісність даних.

Що стосується методів забезпечення інформаційної безпеки то вони достатньо різноманітні, однак їх можна розділити на наступні основні групи: теоретичні, законодавчі (правові), адміністративні (організаційні), інженерно-технічні (програмно-технічні) та криптографічні.

Теоретичні методи забезпечення інформаційної безпеки вирішують два основних завдання. Перше з яких – формалізація різного роду процесів, пов'язаних із забезпеченням інформаційної безпеки. Так, наприклад, формальні моделі управління доступом дозволяють строго описати всі можливі інформаційні потоки в системі – а значить, гарантувати виконання необхідних властивостей безпеки. Звідси безпосередньо випливає друге завдання – суворе обґрунтування коректності і адекватності функціонування систем забезпечення інформаційної безпеки при проведенні аналізу їх захищеності. Така задача виникає, наприклад, при проведенні сертифікації автоматизованих систем за вимогами безпеки інформації.

Законодавчі міри захисту визначаються діючими в країні нормативно-правовими актами, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил. Важливе значення мають стандарти в області захисту інформації (у першу чергу, міжнародні). Серед цих стандартів виділяються «Помаранчева книга», рекомендації X. 800 і «Загальні критерії оцінки безпеки інформаційних технологій».

Адміністративні методи захисту – методи організаційного характеру, які регламентують процеси функціонування ІТС, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою мінімізувати або виключити можливість реалізації загроз безпеки.

Зазвичай вони включають:

- підбір та підготовку персоналу системи;
- організацію охорони та контрольно-пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів та носіїв з інформацією;
- розподіл атрибутів розмежування доступу (паролів, ключів шифрування тощо).

Основою адміністративних методів захисту інформації є формування політика безпеки організації – сукупність вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Криптографічні методи захисту інформації реалізується шляхом перетворення інформації (шифрування, кодування та інші перетворення) з використанням спеціальних (ключових) даних та алгоритму зворотного перетворення з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Можна стверджувати, що на теперішній час, криптографічний метод захисту є одним із найбільш надійніших методів захисту, оскільки захищається безпосередньо сама інформація, а не доступ до неї.

Інженерно-технічні методи захисту інформації засновані на використанні спеціальних інженерно-технічних заходів, апаратних засобів і програмного забезпечення, що входять до складу ІТС і унеможливлюють виток, знищення або блокування інформації, порушення цілісності та режиму доступу до неї.

Однак, необхідно відзначити, що універсальних методів захисту не існує, і тому під час вирішення питання щодо захисту інформації потрібно обов'язково враховувати критичність інформаційних активів, усі наявні ризики, а вже потім використовувати конкретні механізми забезпечення безпеки та планувати витрати на ІБ. Багато в чому успіх при побудові механізмів безпеки для реальної системи буде залежати від її індивідуальних особливостей, облік яких погано піддається формалізації. Тому часто інформаційну безпеку розглядають як певну сукупність неформальних рекомендацій щодо побудови систем захисту інформації того чи іншого типу.

Порядок виконання лабораторної роботи №1:

1. Ознайомитися з короткими теоретичними відомостями.
2. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою матричного підходу
1.
3. На основі отриманих результатів, надати основні рекомендації щодо забезпечення ІБ в даній організації.
4. Оформити звіт згідно до вимог.
5. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.

2. Постановка завдання.

3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.

4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.

5. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.

6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.

7. Висновки та відповіді на контрольні питання.

Завдання на виконання лабораторної роботи № 1

Таблиця № 1.7. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Організація	Кількість інформаційних активів
1	Державний комерційний банк	8
2	Приватна поліклініка	9
3	Страхова компанія	7
4	Інтернет-магазин	9
5	Адвокатська контора	8
6	Агентство нерухомості	7
7	Рекламне агентство	7
8	Науково-проектне підприємство	9
9	Аудиторська компанія	8
10	Туристичне агентство	7
11	Консалтингова фірма	9
12	Фармакологічна компанія	8
13	Архітектурне агентство	7
14	Інтернет-провайдер	7
15	Будівельна компанія	8
16	Система електронних платежів	9
17	Видавництво	7
18	Благодійний фонд	8
19	Рекрутингове агентство	7

20	Міжнародний комерційний банк	9
21	Військове підприємство	6
22	Компанія-розробник ПЗ	9
23	Дизайнерська фірма	8
24	Організація з розробки електроніки	9
25	Державна поліклініка	8
26	Авіакомпанія	9
27	Редакція газети	7

Контрольні питання

1. Надати визначення наступним поняттям: ризик ІБ.
2. Коротко описати алгоритм аналізу ризиків інформаційної безпеки організації.
3. Які повинна вирішувати завдання система забезпечення інформаційної безпеки ІТС?
4. Коротко охарактеризувати основні групи методів забезпечення ІБ.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. 1. Goel, S., Chen, V. Information security risk assessment – a matrixbased approach. University at Albany. – SUNY. – 2005.

Додаткова література з навчальної дисципліни

5. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // Радіотехніка. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

6. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

7. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

8. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

9. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

10. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

11. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)

Лабораторна робота № 2

Тема: Дослідження якісної оцінки ризиків ІБ з урахування додержання норм, організації та технічного забезпечення підприємства (матричний підхід 2).

Мета роботи: комп'ютерне моделювання ІБ за допомогою засобів Excel.

Придбання та опанування практичних навичок з аналізу та якісної оцінки ризиків ІБ підприємства.

Кількість годин: 2 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Список активів організації.
2. Матриця вразливостей та загроз.
3. Матриця контролю.
4. Шкала ранжування.
5. Оцінка цінностей компанії
6. Аналіз організаційних заходів захисту інформації.
7. Ймовірність реалізації актуальних загроз
8. Аналіз технічних заходів захисту інформації
9. Ризики реалізації загроз інформаційній безпеці для активів.

Висновок.

Література:

1. Матеріали лекції 2.
[2, с. 5 - 9]
2. Нормативні документи [1].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Intertnet.

Заняття проводиться в комп'ютерному класі. Кожний студент забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити питання оцінки ризиків організації та функціонування систем технічного захисту інформації.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

Хід роботи

Порядок виконання лабораторної роботи №2:

6. Ознайомитися з короткими теоретичними відомостями.
7. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 1.7) за допомогою матричного підходу 2.
8. Заповнити даними, згідно свого варіанту та провести розрахунки у табл. 3.1 – 3.12
9. На основі отриманих результатів, надати основні рекомендації щодо оцінки ризиків та забезпечення ІБ в даній організації.
10. Оформити звіт згідно до вимог.
11. Відповісти на контрольні питання та підготуватися до усного опитування.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.
4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені матриці.
6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.
7. Висновки та відповіді на контрольні питання.

Теоретичні відомості

За допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті

чого одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації.

Виконувати комп'ютерне моделювання ІБ за допомогою засобів Excel.

Проведемо оцінку. На першому етапі «Ідентифікація активів» - сформуємо список активів організації. Процес збору адміністратором інформаційної безпеки даних для аналізу ризиків, відбувався шляхом опитування співробітників підприємства. В якість активів: персональні дані, комерційна таємниця, електронні документи, електронна пошта, АРМ, бази даних, сервер.

Таким чином, було сформовано (при зборі даних для аналізу ризиків за матричною методологією) три матриці: матрицю вразливостей (містить зв'язок між активами і слабкими місцями в організації)(табл. .3.1), матрицю загроз (відношення між слабкими місцями та загрозами) (табл. .3.2), матрицю контролю (зв'язки між загрозами та засобами керування) (табл. .3.3).

Значення кожної клітинки матриці показує оцінку відношення між елементом рядка і стовпця. В основному, використовують таку систему оцінок, як «низька», «середня» і «висока».

При формуванні номенклатури активів, слабких місць та загроз, було використано наступну шкалу оцінки взаємо залежностей активів (загроз) і слабких місць (вразливостей):

0 – немає впливу;

1 – слабкий вплив;

3 – помірний вплив;

9 – сильний вплив.

Ранжування пріоритету вразливостей проведено за наступною шкалою:

1 і 2– неважлива;

3– важлива, але не ключова;

4– важлива, але знаходиться під впливом ключової;

5– ключова.

Отже, отримані матриці активів та загроз ТОВ наведені у таблицях 3.1–3.6.

Таблиця 3.1 Матриця активів

Матриця активів	Загрози	Шкідливе програм забезпечення	Хакерські атаки	Втрата інформації (вірус)	Персонал	Пожежа	Всього	Розряд
Уразливості, пріоритет		5	4	3	2	1		
Локальна мережа	5	3	3	3	0	0	36	2
База даних (БД)	4	9	3	9	0	0	84	4
Передача даних через інтернет	5	9	9	9	9	9	129	5
Перерва в подачі енергії	2	1	1	3	1	9	29	1
Апаратно-програмні збої	3	3	3	9	3	9	69	3
Людський фактор (помилки користувача)	5	9	9	9	9	9	135	6

Таблиця 3.2 Матриця загроз

Матриця загроз	Уразливості	Людський фарктор	Передача данних через Інтернет	Бази даних	Апаратно-програмні сбої	Локальна мережа	Перерва з подачі енергії	Всього	Розподіл
Уразливості, пріоритет		6	5	4	3	2	1		
Шкідливе програмне забезпечення	4	9	9	9	9	3	0	168	5
Втрата інформації (вірус)	3	9	9	9	3	1	0	146	3

Хакерські атаки (перехоплення, спотворення, знищення, підміна маршрутів слідування інформації)	4	9	9	9	0	0	0	135	4
Персонал	5	9	3	3	3	3	3	99	2
Пожежа	2	1	0	0	0	1	3	11	1

Сукупні дані про погрози і відповідні засоби управління додаються в матрицю контролю, представлену в таблиці 3.3

Таблиця 3.3 Матриця контролю

Матриця контролю	Загрози	Шкідливе програмне забезпечення	Хакерські атаки	Втрата інформації (вірус)	Персонал	Пожежа	Всього	Розподіл
Управлінські дії, пріоритет		5	4	3	2	1		
Використання ліцензійного ПЗ	5	9	1	1	1	0	54	5
Електронний цифровий підпис	5	0	9	1	9	0	57	6
Антивірусне ПЗ	4	0	0	3	9	0	27	3
Трудовий договір з пунктом про нерозголошення інформації	4	0	0	3	9	0	27	3
Парольний захист на ресурси	5	0	3	0	9	0	30	4
Маршрутизатор (роутер)	3	0	3	3	0	0	21	2
Протипожежна сигналізація	3	0	0	0	0	9	9	1

На другому етапі «Визначення ризиків невідповідності законодавству в області інформаційної безпеки». Присвоюється значення «1», якщо немає,

то – «0». Всі вимоги, яким присвоєно значення «1», підсумовуються, інші значення не враховуються (табл. 3.4).

Отже, рівень ризику невідповідності вимогам до інформаційної безпеки становить $R_n = 0,25$ (табл. 3.5).

Таблиця 3.4 Ризик невідповідності законодавству в області інформаційної безпеки

	Вимоги законодавства	Виконання вимог
1	Реєстрація в якості оператора персональних даних	1
2	Розробка і прийняття документів, що регламентують питання надання доступу і захист персональних даних	1
3	Оформлення допусків співробітників до персональних даних	0
4	Формування переліку оброблюваних персональних даних	1
5	Класифікація інформаційної системи обробки персональних даних	1
6	Підготовка інформаційної системи обробки персональних даних до атестації за вимогами безпеки	1
7	Вживання заходів щодо захисту персональних даних	1
8	Сертифікація системи захисту інформації у складі інформаційної системи обробки персональних даних	0
9	Сертифікація заходів системи захисту інформації у складі інформаційної системи обробки персональних даних	1
10	Встановлення вимог до надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
11	Перевірка на відповідність вимогам надійності і безпеки використовуваних в інформаційних системах апаратних і програмних засобів	1
12	Введення обмежень на придбання і використання окремих видів апаратних і програмних засобів в інформаційній системі	0
13	Технічні (в т.ч. програмні) засоби обмеження доступу в інформаційних системах не створювати загрозу або завдавати шкоди здоров'ю і майну інших осіб	1

14	Обов'язок щодо забезпечення конфіденційності відомостей, що становлять професійну таємницю	1
	Всього	11

Таблиця 3.5 Значення ризику невідповідності вимогам законодавства

Сума виконаних вимог	Ризик невідповідності вимогам законодавств
13–14	0,01
8–12	0,25
Менше або рівне 7	0,5
Не виконуються	0,9

На наступному етапі розробляється модель загроз. Визначається ймовірність виникнення несприятливих подій і актуальність загроз інформаційної безпеки. По завершенню етапу формується список актуальних загроз на кожен актив або групу активів.

Таким чином, для ТОВє наступний список актуальних загроз: шкідливе програмне забезпечення, втрата інформації через віруси, пожежа, персонал, хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування інформації).

На останньому етапі – проводиться кількісна оцінка ризиків. Для цього:

1) обираються актуальні загрози – за допомогою моделі загроз складається список актуальних загроз. Ідентифіковані активи зіставляються з спрямованими на них погрозами;
2) визначаються ймовірності виникнення загроз. При цьому, на один актив можуть впливати одночасно декілька загроз. Тому, слід з'ясувати ймовірність того, що хоча б одна загроза реалізується по відношенню до заданого активу.

Ймовірність реалізації хоча б однієї загрози з сукупності ймовірностей загроз $y_1, y_2, \ldots y_n$, де n – кількість загроз, дорівнює різниці між одиницею і добутком ймовірностей протилежних подій.

Отже, маємо наступні ймовірності реалізації актуальних загроз – таблиця 3.6.

Таблиця 3.6 Ймовірність реалізації актуальних загроз

Загроза інформаційній безпеці	Значення ймовірності реалізації загроз
Шкідливе програмне забезпечення	0,3
Втрата інформації через віруси	0,45
Пожежа	0,1
Персонал	0,75
Хакерські атаки (перехоплення, спотворення, підміна, знищення, підміна маршрутів слідування інформації)	0,65

Ймовірність реалізації хоча б однієї загрози зі списку актуальних загроз $R_{угр} = 0,9934$;

3) визначаються цінності активів – ця величина знаходиться в діапазоні від 0 до 1 (показує відношення ціни активів до вартості всього бізнесу). Визначену оцінку представлено у таблиці 3.7;

4) визначаються можливості застосування організаційних і технічних вразливостей. Ймовірність застосування організаційних вразливостей проводиться експертними методом. В процесі виконання аналізу всіх організаційних заходів, виконуваних, присвоюється значення «1», а тим, що не виконуються «0». Аналіз організаційних заходів захисту інформації наведені у таблиці 3.8;

Таблиця 3.7 Оцінка цінностей компанії

Назва активу	Значення оцінки цінностей активу
Персональні данні	0,7
Комерційна таємниця	0,6
Електронні документи	0,55
Електронна пошта	0,5
АРМ	0,35
Бази даних	0,4
Сервер	0,45

Таблиця 3.8 Аналіз організаційних заходів захисту інформації

Організаційні заходи захисту інформації	Оцінка виконання організаційних заходів щодо захисту інформації
Організаційна інфраструктура інформаційної безпеки	1
Координація питань інформаційної безпеки	1
Розподіл обов'язків по забезпеченню інформаційної безпеки	1
Призначення відповідальних за кожен актив або процедуру безпеки	0
Отримання доступу до засобів обробки інформації з боку керівництва та адміністраторів засобів управління	1
Перевірка сумісності з іншим програмним забезпеченням і компонентами системи апаратних засобів	1
Співпраця організацій в області інформаційної безпеки	1
Незалежна перевірка (аудит) інформаційної безпеки	0
Включення вимог безпеки до договорів зі сторонніми особами та організаціями	0
Залучення сторонніх організацій до обробки інформації (Аутсорсинг)	0
Включення вимог безпеки за договором на аутсорсинг	0
Облік активів	1
Інвентаризація активів	1
Класифікація інформації	1
Облік питань безпеки в посадові обов'язки і при прийомі на роботу персоналу	1
Навчання користувачів	1
Контроль доступу до зони контролю	1
Управління передачею даних і операційною діяльністю	1
Безпека електронної пошти	0
Контроль доступу до інформації	1
Управління безперервністю бізнесу	0

Всього	14

Таким чином (табл. 3.9), коефіцієнт уразливості організаційних заходів захисту $К_о = 0,01$.

Таблиця 3.9 Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості організаційних заходів захисту
14–17	0,01
9–13	0,25
Менше або рівне 8	0,5
Не виконуються	0,9

Оцінка технічних вразливостей проведено експертним методом, в ході якого були проаналізовані технічні заходи захисту інформації, які виконуються на ТОВ «Нова Пошта». В процесі виконання аналізу всім технічним заходам, виконуваних, присвоюється значення «1», які не виконуються «0». Аналіз результатів технічних заходів захисту інформації ТОВ наведений у в таблиці 3.10.

Таблиця 3.10 Аналіз технічних заходів захисту інформації

Технічні заходи захисту інформації	Оцінка виконання технічних заходів захисту інформації
1	2
Реалізація дозволеної кількості допуску виконавців до інформації та документів у системі	1
Розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів обробки (передачі) і захисту інформації	1
Контроль за діями користувачів	0
Реєстрація дій користувачів інформаційної системи	1

Розв'язка ланцюгів електроживлення об'єктів захисту за допомогою захисних фільтрів, які блокують (пригнічують) інформативний сигнал	0
Використання захищених каналів зв'язку	0
Криптографічне перетворення інформації, що обробляється і передаються засобами обчислювальної техніки і зв'язку	1
Запобігання впровадження в автоматизовані системи програм-вірусів	1
Запобігання впровадження в автоматизовані системи програмних вкладок	0
Всього	5

Таким чином (таблиця 3.11), коефіцієнт уразливості технічним заходам захисту $К_т$ = 0,5;

Таблиця 3.11 Ймовірність реалізації актуальних загроз

Сума заходів захисту, що виконуються	Коефіцієнт уразливості технічних заходів захисту
11–12	0,01
7–10	0,25
Менше або рівне 6	0,5
Не виконуються	0,9

5) визначення чисельного значення ризику (табл. 3.12). Ризик реалізації хоча б однієї загрози з усього переліку актуальних загроз із урахуванням наявності вразливостей по відношенню до конкурентного активу визначається загальній формулі:

$$R = R_{\text{ург}} R_n C \frac{K_0 + K_t}{2} \cdot 100\ \%,$$

де R – чисельна величина ризику реалізації загроз інформаційної безпеки;

Rугр – ймовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз;

R_n – ризик невідповідності вимогам законодавства;

C – цінність активу;

K_0 – ймовірність використання організаційних вразливостей;

K_t – ймовірність використання технічних вразливостей.

На останньому етапі «Визначення допустимого рівня ризику», з таблиці 3.12 маємо значення ризику реалізації загроз інформаційній безпеці близько 5 %, це означає, що ризик реалізації загроз інформаційної безпеки є допустимим для всіх активів. Слід звернути увагу, що високий ризик реалізації загроз інформаційній безпеці, пов'язаний з персональними даними організації.

Таблиця 3.12 Ризики реалізації загроз інформаційній безпеці для активів

Назва активу	Значення ризику реалізації загроз інформаційній безпеці, %
Персональні данні	4,433
Комерційна таємниця	3,799
Електронні документи	3,483
Електронна пошта	3,166
АРМ	2,216
Бази даних	2,533
Сервер	2,849

Таким чином, в результаті оцінки маємо список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози інформаційної безпеки ТОВ.

За допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті чого одержуємо демонстрацію «чистого ризику», тобто ризику з мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

Даний аналіз дозволяє врахувати засоби захисту, які необхідно тримати на постійному контролі для відстеження можливого впливу актуальних загроз на активи організації. Маємо зручні шаблони, які можливо поступово вдосконалюватися з збільшенням кількості доступної інформації; інструмент для проведення прозорого аналізу процесів, адаптуючись до постійно-мінливих загроз, уразливості та активам.

Управління виявленими ризиками інформаційної безпеки дозволяє швидше реагувати на зміни в системі управління та контролювати ситуацію. Використання сучасних інструментів оцінки ризиків інформаційної безпеки допомагає зміцнити «слабкі місця» в системі управління компанією.

Аналіз ризиків інформаційної безпеки підприємства дозволить підтримувати дані про безпеки підприємства в актуальному стані, оперативне розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Висновок

Запропоновано методичні рекомендації щодо оцінювання стану інформаційної безпеки підприємства.

На основі математичної матричної моделі системи захисту проведено якісний аналіз системи захисту інформації ТК.

Виконано комп’ютерне моделювання ІБ за допомогою засобів Excel.

Моделювання показало, що ризик реалізації загроз інформаційної безпеки є допустимим для всіх активів ТК, але є ризик реалізації загроз інформаційній безпеці, пов'язаний з персональними даними організації.

Таким чином, в результаті оцінки маємо список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози інформаційної безпеки ТОВ. Такий підхід до аналізу ризиків ІБ підприємства дозволить підтримувати дані про безпеки підприємства в актуальному стані, оперативне

розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Контрольні запитання

10. Що потрібно визначити на першому етапі?
11. Що таке список активів організації?
12. Як може формуватися список активів організації?
13. Що таке матриця вразливостей?
14. Що таке матриця загроз?
15. Що таке матриця контролю?
16. Що таке шкала ранжування?
17. Об’ясніть, «Ризик невідповідності законодавству в області інформаційної безпеки»?
18. Об’ясніть, як розрахувати ймовірність реалізації актуальних загроз?
19. Як здійсніть оцінка цінностей компанії?
20. Як здійснити аналіз організаційних заходів захисту інформації?
21. Як обчислити ймовірність реалізації актуальних загроз?
22. Як зробити аналіз технічних заходів захисту інформації?
23. Як обчислити ризики реалізації загроз інформаційній безпеці для активів?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП

«Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.

5. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

Додаткова література з навчальної дисципліни

6. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // Радіотехніка. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

7. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

8. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

9. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

10. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

11. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

12. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)