Лабораторна робота №3

Аналіз ризиків та основні принципи забезпечення безпеки.

Мета лабораторної роботи – ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації; набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення безпеки.

1. Теоретичні відомості

Поняття ризиків

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 безпеки. Її використовують для визначення масштабу загроз 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.

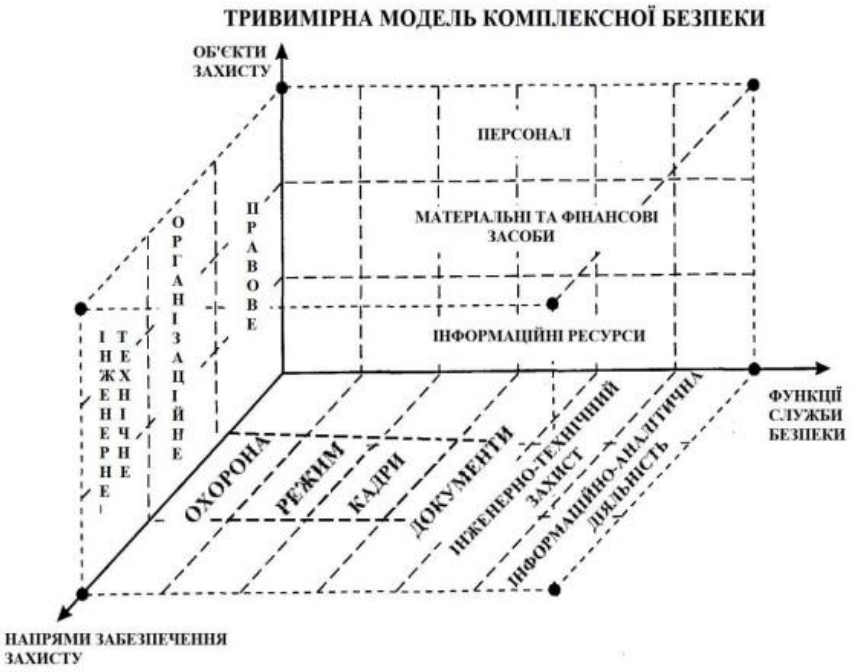
Виходячи з визначення ризику, для проведення аналізу ризиків нам потрібні наступні дані про інформаційну систему: перелік цінної інформації із зазначенням її рівня критичності, відомості про уразливість інформаційної системи і загрози, які на неї діють.

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 безпеки.

Матричний підхід до аналізу ризиків

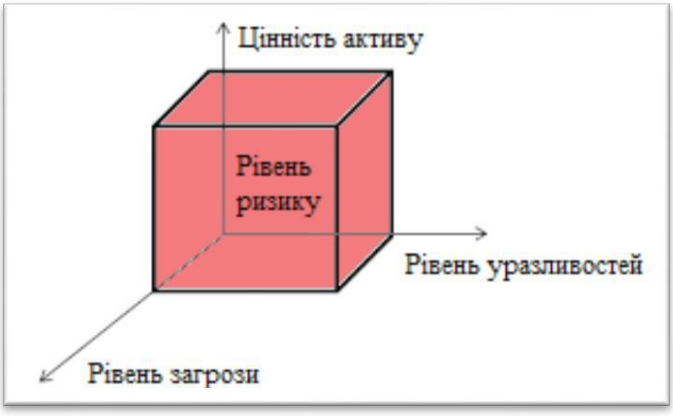
Розрізняють два методи аналізу та оцінки ризиків: *кількісний* та *якісний*. Для кількісної оцінки ризиків характерне використання об'єктивних чисельних, а саме фінансових характеристик. На відміну від кількісного, якісний аналіз ризиків не ставить своїм завданням отримання чисельних фінансових характеристик.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



Запропоновано в лабораторній роботі розглянути один із якісних методів аналізу ризиків, а саме матричний підхід аналізу ризиків безпеки, 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 безпеки.

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*.



Таблиця 3.1.

Матриця уразливостей (активи - уразливості)

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

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 (3.1), для визначення вагомості (значущість) уразливостей, після чого останні переносяться до наступної матриці – матриці загроз. Аналогічно, дані в матриці загроз обчислюються за допомогою формули (3.2), таким чином визначаючи потенційні ризики безпеки, а самі загрози переносяться до останньої таблиці.

Таблиця 3.2.

Матриця загроз (загрози- уразливості)

Матриця загроз Шкала взаємозв'язку *немає* 0 *слабкий* 1 *помірний* 3 *сильний* 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $V_i \leftarrow$	**Активи:**	Секрети виробництва	Конфіденційна інфор-ція	Репутація (довіра)	Апаратне забезпечення	Програмне забезпечення	Послуги	Комунікації	**Всього**	**Ранжування**
Загрози:	РП								$\sum$	
Відмова в обслуговуванні (DoS)										
Шкідливе програмне забезпечення										
Помилки користувача										
Спам										
"Фішинг"										
Ворожий агент										

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).

Припустимо, що є m активів, де відносна вартість активу a_j є $C_j (j = 1, \ldots, m)$. 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:

$$V_i = \sum_{j=1}^{m} v_{ij} \cdot C_j \qquad (3.1)$$

Таблиця 3.3.

Матриця контролю (загрози-засоби контролю)

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

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

$$T_k = \sum_{i=1}^{n} t_{ki} \cdot v_i \qquad (3.2)$$

Припустимо, що є q засобів контролю (захисту), які можуть пом'якшити (мінімізувати) вплив p загроз, а z_{kl} – 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:

$$Z_l = \sum_{l=1}^{p} z_{kl} \cdot T_k \qquad (3.3)$$

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 безпеку організації.

Приклад використання методики аналізу ризиків безпеки

Дослідження аналізу ризиків за допомогою запропонованої методики буде здійснюватися на прикладі компанії "Cyberstec", яка займається розробкою програмного забезпечення. Дана 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 IT-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 безпеку, 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 3.4, 3.5 та 3.6 відповідно.

Таким чином, у таблиці 3.4 представлено матрицю уразливостей, яка пов'язує уразливості та активи компанії "Cyberstec". Для побудови матриці була визначена відносна цінність активів та проведено їхнє ранжування (з правої сторони у ліву). 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 3.4.

Матриця уразливостей "Cyberstec"

Матриця уразливостей Шкала взаємозв'язку *немає* 0 *слабкий* 1 *помірний* 3 *сильний* 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $C_j \leftarrow$	**Активи:**	Новітні розробки (технології)	Конф. інф. (програмний код)	Репутація (довіра)	Доступність серверів	Комунікації	Програмне забезпечення	Апаратне забезпечення	**Всього**	**Ранжування**
Уразливості:	РП	7	6	5	4	3	2	1	∑	
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
База 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 (3.1) 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 3.5.

Матриця загроз “Cyberstec”

Матриця загроз Шкала взаємозв’язку *немає* 0 *слабкий* 1 *помірний* 3 *сильний* 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $V_i \leftarrow$	**Активи:**	Брандмауер	Передача даних та лінії зв’язку	Помилки конфігурації серверів екстранет	Бази даних	Фізична безпека	Стійкість паролів	Помилки конфігурації серверів інтернет	ПК співробітників компанії	Ненадійне джерело живлення	**Всього**	**Ранжування**
Загрози:	РП	9	8	7	6	5	4	3	2	1	∑	
Відмова в обслуговуванні (DoS/DDoS)	5	9	9	9	0	1	1	9	1	1	255	5
Шкідливе програмне забезпечення	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 КМ	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 (3.2), було визначено потенційні ризики безпеки, 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 (3.3) 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 безпеки.

Таблиця 3.6.

Матриця контролю “Cyberstec”

Матриця контролю Шкала взаємозв’язку *немає* 0 *слабкий* 1 *помірний* 3 *сильний* 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний $T_k \leftarrow$	**Загрози:**	Збої сервера	НСД	Вторгнення (атака на пароль)	Відмова в обслуговуванні	“Спуфінг” та “Маскарад”	Фізичне пошкодження КМ	Шкідливе ПЗ	Помилки працівника	**Всього**	**Ранжування**
Уразливості:	РП	8	7	6	5	4	3	2	1	∑	
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
Міжмережевий екран	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

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

Основні принципи та методи забезпечення інформаційної безпеки

З метою протидії основним загрозам безпеки, система забезпечення інформаційної безпеки комп’ютерних мереж повинна вирішувати наступні завдання:

1) розмежування та контроль доступу користувачів до ресурсів системи;

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 комп’ютерних систем зі 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 комп’ютерних систем.

Також необхідно відмітити, що розрізняють зовнішню та внутрішню безпеку комп’ютерних систем. Зовнішня безпека полягає в захисті комп’ютерних систем 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 комп’ютерних систем, а також забезпечувати цілісність даних.

Завдання для виконання

1. Провести аналіз та оцінку ризиків безпеки організації (згідно варіанту в табл. 3.7) за допомогою матричного підходу.

Таблиця 3.7.

Номер варіанта	Організація	Кількість інформаційних активів
1	Інтернет-провайдер	**4**
2	Інтернет-магазин	**3**
3	Туристичне агенство	**4**
4	Охоронна компанія	**5**
5	Агенство нерухомості	**6**
6	Компанія-розробник програмного забезпечення	**4**
7	Приватна поліклініка	**3**
8	Фармакологічна компанія	**5**
9	Державний комерційний банк	**5**
10	Приватна поліклініка	**5**
11	Міжнародний комерційний банк	**5**
12	Будівельна компанія	**6**
13	Компанія-розробник системи платежів	**5**
14	Архітектурне агенство	**5**
15	Інтернет-магазин	**7**
16	Компанія-розробник антивірусних програм	**5**
17	Страхова компанія	**4**
18	Приватна поліклініка	**5**
19	Інтернет-магазин	**6**
20	Інтернет-провайдер	**4**
21	Рекламне агенство	**5**
22	Науково-проектне підприємство	**6**
23	Благодійний фонд	**6**

2. На основі отриманих результатів, надати основні рекомендації щодо забезпечення безпеки в даній організації.

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

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 безпеки в даній організації.

7. Висновки та відповіді на контрольні питання:

- *Як класифікуються загрози за результатами їх впливу на інформацію?*
- *Що таке НСД і які існують способи його реалізації?*
- *Які повинна вирішувати завдання система забезпечення безпеки комп'ютерної системи?*
- *Які існують поширені прийоми НСД?*
- *Які існують основні категорії мережевих атак?*
- *У чому полягають принципи управління доступом?*
- *У чому сенс концепції матриці доступу?*
- *Що є функціями і механізмами захисту?*

8. Оформити звіт до лабораторної роботи.