Оцінювання ризиків кібербезпеки ресурсів інформаційних систем

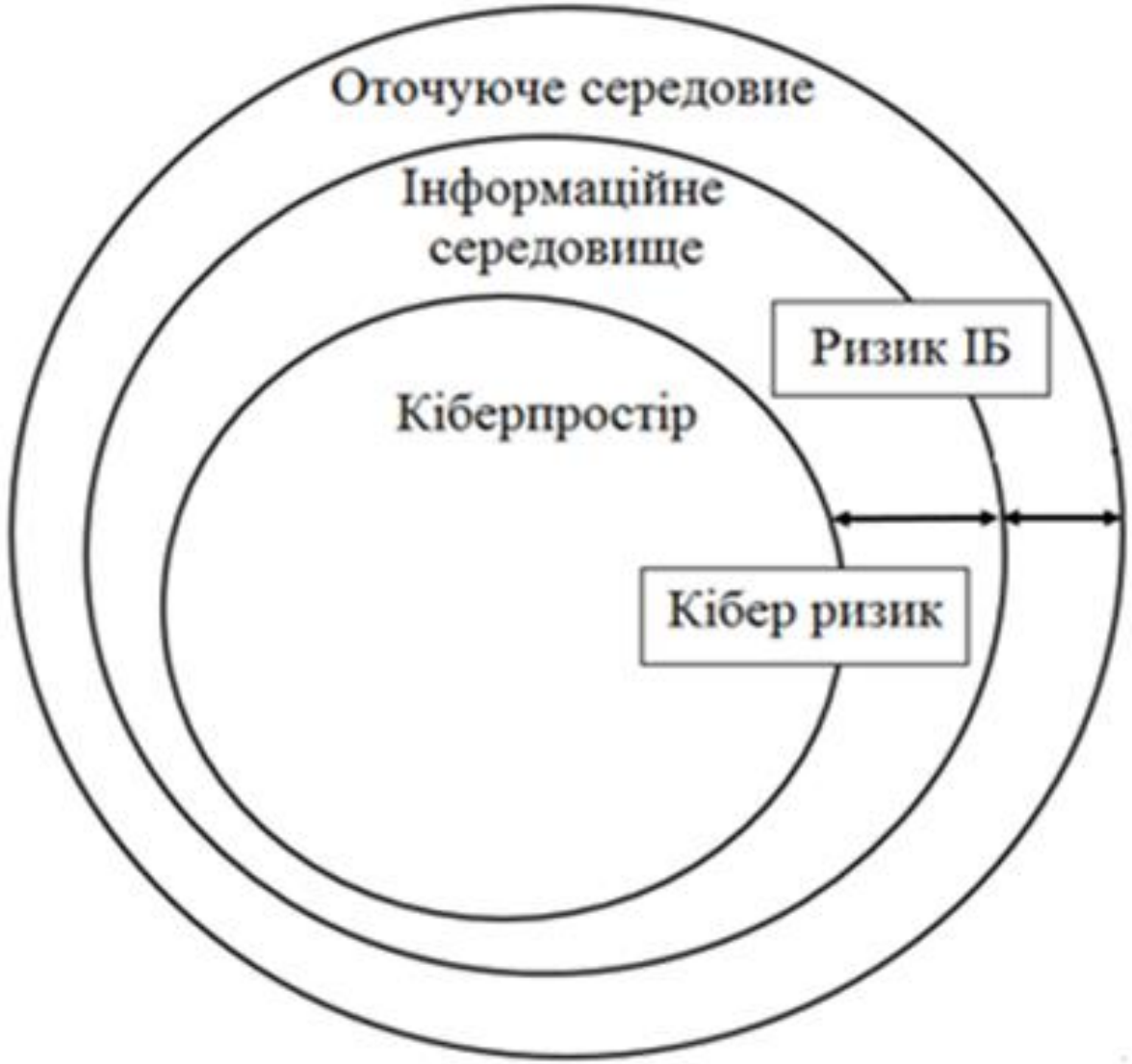
Андрій ДАВИДЮК, аспірант ІПМЕ ім. Г.Є. ПУХОВА

Терміни та визначення

- ***Кібербезпека*** - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.
- ***Кіберзахист*** - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.
- ***Інформаційна безпека*** - стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.
- ***Ризик інформаційної безпеки*** - ризик, пов'язаний з використанням інформаційних систем, які підтримують місію та бізнес-функції організації.
- ***Інформаційні системи*** - організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [
- ***Ресурс інформаційної системи*** - документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах і т.і.). Розрізняють інформаційні ресурси державні та недержавні.

NIST 8183 Cybersecurity Framework Version 1.1 Manufacturing Profile

- ***Кіберризик*** як ризик фінансових втрат, збоїв у роботі або пошкодження у результаті відмови цифрових технологій, що використовуються для інформаційних та/або операційних функцій, впроваджених до промислової системи за допомогою електронних засобів, із-за несанкціонованого доступу, використання, розкриття, порушення, модифікації або поломки промислової системи.


Оточуюче середовие
Інформаційне середовище
Ризик ІБ
Кіберпростір
Кібер ризик

Процес управління ризиками -

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)

1. Визначитись з методологією оцінювання кіберризиків;
2. Впровадження процедури оцінювання кіберризиків;
3. Впровадження процедури обробки ризиків;
4. Створення звіту про оцінювання кіберризиків в системі менеджменту інформаційної безпеки;
5. Створення заяви про застосовуваність
6. Створення плану обробки кіберризиків.

- Визначити причину втрати конфіденційності, цілісності та доступності;
- Визначити власників ризику;
- Визначитись з критеріями оцінювання наслідків та імовірності;
- Визначитись з тим як буде обчислюватись значення ризику;
- Визначити критерії прийняття ризику.

ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)

- ідентифікувати ризик інформаційної безпеки;
- проаналізувати ризик інформаційної безпеки;
- візуалізувати (наприклад, картою ризиків) та/або проранжувати проаналізований ризик інформаційної безпеки за оцінками (або рівнем).

Для ідентифікування ризику інформаційної безпеки, як приклад, можна скористатися такою таблицею:

№ з/с	Інформаційний актив	Наявні засоби забезпечення безпеки	Уразливості інформаційного активу та/або засобу забезпечення безпеки	Загрози інформаційній безпеці	Наслідки реалізації загрози інформаційній безпеці

- Загрози ІБ можна розділити на три стовпці. Де зазначити: загрози конфіденційності, загрози цілісності, загрози доступності.

Для аналізування ризику інформаційної безпеки, як приклад, можна скористатися такою таблицею:

№ з/с	Інформаційний актив	Наявні засоби забезпечення безпеки	Уразливості інформаційного активу та/або засобу забезпечення безпеки	Загрози інформаційній безпеці	Наслідки реалізації загрози інформаційній безпеці	Оцінка (або рівень) вірогідності реалізації загроз	Оцінка (або рівень) наслідків реалізації загроз	Оцінка (або рівень) ризику інформаційної безпеки

- Оцінюються за шкалою
- Якщо низька, то може обиратися одне зі значень 0, 1, 2.
- Якщо середня, то може обиратися одне зі значень 3, 4, 5.
- Якщо висока, то може обиратися одне зі значень 6, 7, 8.

Оцінка ризику інформаційної безпеки визначається перемноженням оцінок вірогідності та наслідків реалізації загрози. Тож отримаємо, мінімальну оцінку ризику – 1, максимальну – 64.

№ з/с	Інформаційний актив	Наявні засоби забезпечення безпеки	Уразливості інформаційного активу та/або засобу забезпечення безпеки	Загрози інформаційній безпеці	Оцінка (або рівень) вірогідності реалізації загроз	Оцінка (або рівень) наслідків реалізації загроз	Оцінка (або рівень) ризику інформаційної безпеки

№ з/с	Інформаційний актив	Наявні засоби забезпечення безпеки	Уразливості інформаційного активу та/або засобу забезпечення безпеки	Загрози інформаційній безпеці	Оцінка (або рівень) вірогідності реалізації загроз	Оцінка (або рівень) наслідків реалізації загроз	Оцінка (або рівень) ризику інформаційної безпеки	Ранг ризику інформаційної безпеки
					8	8	64	I

- Отримані оцінки візуалізуються, наприклад, картою ризиків. За результатами аналізування, ризик інформаційної безпеки ранжується за його оцінкою. Тож ризик максимальною оцінкою ризику інформаційної безпеки (наприклад, $8 \cdot 8 = 64$) матиме рейтинг I.

Приклади:

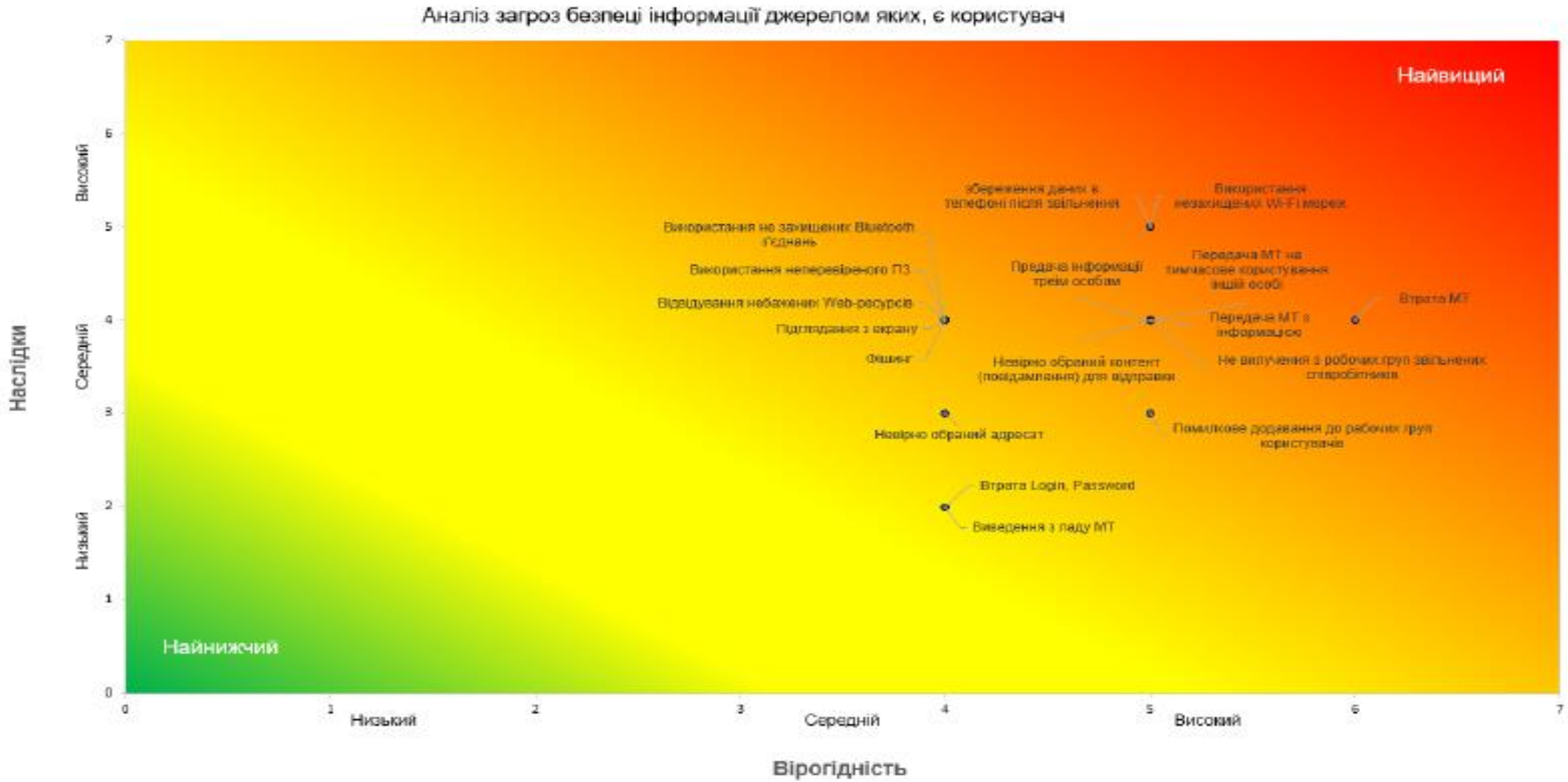

Аналізування загроз ІБ при використання мобільних меседжерів методом Діаграми Ішикави
Використані скорочення:
МТ – мобільний термінал;
ІБ – інформаційна безпека;
ПЗ – програмне забезпечення;
ОС – операційна система;
ММ – мобільний месенджер;
АВПЗ – антивірусне програмне забезпечення.
Порушення властивостей інформації
ISP
Погана якість зв'язку
Відсутність контролю за трафіком
ОС (ПЗ)
Збої ОС
Помилки ОС (ПЗ)
Використання не стабільних оновлень
Вразливості ОС (ПЗ)
Програмні закладки
Невдале оновлення
Отримання вдаваного керування ПЗ МТ
Проблеми підтримки останніх версій застосунків
Отримання інформації про місцезнаходження МТ
ШПЗ
Користувач
Обшант
Втрата МТ
Підглядання з екрану
Виведення з ладу МТ
Втрата Login, Password
Невірно обраний адресат
Передача МТ з інформацією
Передача інформації третім особам
Використання неперевіреного ПЗ
Відвідування небажаних Web-ресурсів
Використання незахищених Wi-Fi мереж
Використання не захищених Bluetooth мереж
Зберігання даних в телефоні після звільнення
Невірно обраний контент (повідомлення) для підправки
Передача МТ на тимчасове користування іншому користувачу
Помилкове додавання до робочих груп користувачів
Не виключення з робочих груп звільнених співробітників
ММ
Можливість одночасного доступу до облікового запису зі стороннього пристрою (Desktop версія)
Можливість одночасного доступу до облікового запису зі стороннього пристрою (Web версія)
Ліцензійною угодою не передбачено корпоративне використання
Використання не захищеного каналу передачі даних
Доступ до файлової системи застосунків
Доступ до акаунту ММ з різних пристроїв
Відсутність контролю за серверами ММ
Клонування застосунку
МТ
Вихід з ладу (частково або повністю)
Вихід з ладу карти пам'яті
Апаратні закладки
Розряд елементів живлення

Ідентифікація ризиків інформаційної безпеки при використанні мобільних месенджерів

Шкала оцінки ризику:		
Н – наслідки; В – вірогідність.	Низькі:	1-2
	Середні:	3-4
	Високі:	5-6

№ з/п	Інформаційний актив	Загрози ІБ	Наслідки реалізації загрози ІБ	Уразливості інформаційного активу та або засобу забезпечення ІБ	Існуючі засоби забезпечення ІБ	Оцінка ризику	
						Н	В
1	2	3	4	5	6	7	
1	Корпоративна інформація	Фішинг	Втрата конфіденційності	Відсутність засобів перевірки репутації ресурсів Необачність користувача	Використання засобів перевірки ресурсів Заборона відвідування сайтів без використання ключів SSL/TLS Організаційні заходи (політики ІБ), навчання співробітників	4	4
2	Корпоративна інформація	Втрата або викрадення МТ	Втрата конфіденційності	Необачність користувача Відсутність встановлених паролів на вхід в ОС Відсутність встановлених паролів на вхід в ММ	Організаційні заходи (політики ІБ) щодо поводження з МТ Встановлення паролів на вхід в ОС встановленої складності Встановлення паролів на вхід в ММ встановленої складності	6	4
			Втрата доступності				
			Відправка повідомлень від імені користувача				

Аналізування ризиків ІБ з використанням карт ризиків



ДЯКУЮ ЗА УВАГУ!