МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЧЕРНЯК Тетяна Григорівна

Методика оцінки ризиків кібербезпеки в системах Інтернет- речей / Cybersecurity risks assessment methods for Internet of Things

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБзм -21
Т.Г. Черняк

Науковий керівник
к.т.н., доцент Н.Г. Яцків

Кваліфікаційну роботу
Допущено до захисту:

«____» _____ ___2022 р.

Завідувач кафедри

_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2022

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека
освітньо-професійна програма –Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
____" _____ 2021 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ЧЕРНЯК Тетяна Григорівна
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Методика оцінки ризиків кібербезпеки в системах Інтернет- речей / Cybersecurity risks assessment methods for Internet of Thingsмкерівник роботи к.т.н., доцент Н.Г. Яцків
затверджені наказом по університету від 31 грудня 2021 року № 606

2. Строк подання студентом закінченої випускної кваліфікаційної роботи 16 листопада 2022 року.

3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– провести аналіз основних вимог щодо безпеки IoT;
– дослідити способи виявлення наявних вразливостей IoT-пристроїв;
– дослідити основні теоретичні методи оцінки ризиків;
– проаналізувати якісні підходи до оцінки ризиків IoT;
– проаналізувати кількісні підходи до оцінки ризиків IoT;
– розробити методику оцінки ризиків кібербезпеки в системах інтернет-речей.
5. Перелік графічного матеріалу у роботі.
– вимоги безпеки IoT;
– кроки SWIFT аналізу;
– шестиступінчастий процес вивчення уроків;
– загальний процес аналізу загроз та метод оцінки ризиків.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 11 жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз загроз та ризиків в системах Інтернету речей	12.2021 р. – 03.2022 р.	
2	Теоретичні методи оцінки ризиків	03.2022 р. – 05.2022 р.	
3	Оцінка ризиків безпеки в системах IoT	05.2022 р. – 11.2022 р.	

Студент _____ Черняк Т.Г.
(підпис)

Керівник роботи _____ к.т.н., доцент Н.Г. Яцків
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методика оцінки ризиків кібербезпеки в системах Інтернет- речей» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 73 сторінки і містить 5 ілюстрації, 6 таблиць, 2 додатки та 27 джерел за переліком посилань.

Метою кваліфікаційної роботи є аналіз найбільш ефективних методів оцінки ризиків кібербезпеки, придатної для систем IoT.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи оцінки ризиків, методи аналізу загроз для IoT.

Результати дослідження: підібрано ефективні методи оцінки ризиків кібербезпеки, що притаманні для систем Інтернет- речей.

Досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

Результати роботи можуть успішно застосовуватися при реалізації комунікаційних і інформаційних системах, що отримали у своє розпорядження нові пристрої для Інтернету речей.

Ключові слова: СИСТЕМИ ІНТЕРНЕТ-РЕЧЕЙ, ОЦІНКА РИЗИКІВ, МЕРЕЖІ IOT, IOT-ПРИСТРОЇ.

ABSTRACT

The qualification paper on the topic "Methodology of cyber security risk assessment in Internet of Things systems" for obtaining the Master's degree in the specialty 125 "Cyber Security" of the educational and professional program "Cyber Security" is written in the volume of 73 pages and contains 5 illustrations, 6 tables, 2 appendices and 27 sources according to the list of references.

The purpose of the qualification work is to analyze the most effective methods of cyber security risk assessment suitable for IoT systems.

Research methods. To solve the tasks in this qualification work, the following methods of risk assessment, methods of analyzing threats to IoT were used.

Research results: effective methods of assessing cyber security risks inherent in Internet of Things systems have been selected.

Examples of Internet of Things vectors were studied and their risk indicators were calculated

The results of the work can be successfully applied in the implementation of communication and information systems that have received new devices for the Internet of Things.

Keywords: INTERNET OF THINGS SYSTEMS, RISK ASSESSMENT, IoT NETWORKS, IoT DEVICES.

ЗМІСТ

ВСТУП

Сьогодні IoT знаходить застосування в різних сферах нашого життя – в проектах безпечніших міст і розумних будівель.

Перш за все, слід зазначити, що фізична безпека невіддільна від IoT. Це стає особливо очевидним, якщо врахувати, що галузь безпеки значною мірою покладається на технології IP, які дозволяють інтегрувати пристрої в Інтернет-середовище.

Інтеграція різних пристроїв для роботи в Інтернеті дає багато переваг. Серед них підвищена безпека, кращі інтелектуальні здібності та простота використання.

Необхідно постійно враховувати безпеку мереж, додатків та інфраструктури, інакше втрати дуже високі, але наразі виробники не дуже ретельно захищають свої пристрої. Не забувайте, що у міру впровадження у ваші рішення практик інформаційної безпеки ціна відповідно зростає. Ще однією причиною відмови є висока вартість забезпечення великих обсягів обчислень, що відповідно збільшує енергоспоживання різноманітних автономних пристроїв.

Усе середовище IoT, яке впливає на розробників і користувачів, потребує значного вдосконалення безпеки IoT. Якщо співвідношення буде таким же, зростання галузі може зупинитися в наступні роки. Використання Інтернету речей дійсно допомагає покращити різні сфери життя, але без повної безпеки IoT важко говорити про довіру.

Мета і завдання дослідження. Метою роботи є розробка методики оцінки ризиків кібербезпеки, придатної для систем IoT.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз основних вимог щодо безпеки IoT;

– дослідити способи виявлення наявних вразливостей IoT-пристроїв;

– дослідити основні теоретичні методи оцінки ризиків;

– проаналізувати якісні підходи до оцінки ризиків IoT;

– проаналізувати кількісні підходи до оцінки ризиків IoT;

– розробити методику оцінки ризиків кібербезпеки в системах інтернет-речей.

Об'єкт дослідження – процес оцінки ризиків в системах інтернет-речей;

Предмет дослідження – методи та алгоритми оцінки ризиків Інтернет-речей.

Методи досліджень. Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: методи оцінки ризиків, методи аналізу загроз для IoT.

Наукова новизна одержаних результатів. Удосконалено методику оцінки ризиків кібербезпеки в системах Інтернет-речей з використанням якісних та кількісних підходів до оцінки ризиків.

Практичне значення отриманих результатів. Досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

Публікації та апробація КР.

1. Черняк Т.Г. Оцінка ризиків інформаційної безпеки Інтернет речей. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. – С. 53-55.

2. Яцків Н.Г., Вівчар Д.В., Черняк Т.Г. Аналіз підходів до оцінки ризиків. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 104-106.

1 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Безпека у будь-якій системі, напряму залежить від об’єктів, і підсистем, що до неї безпосередньо входять. Випадки, коли до уже сформованої системи додають деякі інші об’єкти, компоненти, а також пристрої, то рівень безпеки такої системи зазвичай змінюється, але у гірший бік. Таке відбувається у комунікаційних і інформаційних системах, що отримали у своє розпорядження нові пристрої для Інтернету речей. Поряд із новими можливостями і послугами, вони беруть на себе також і роль потенційно вразливої системи [1].

Загрози, які створює Інтернет речей, стають більш поширеними. Таким чином, за останнє десятиліття спостерігалося збільшення випадків порушень кібербезпеки та кіберзлочинів, скоєних з використанням пристроїв IoT. Використовуючи дані про подібні інциденти, можна швидко зробити висновки, що кількість атак на системні дані зростає і прямо пропорційна збільшенню кількості тих же пристроїв IoT. У 2022 році компанія Check Point підготувала звіт Global Threat Index. В якому сформовано рейтинг десяти найбільш часто використовуваних уразливостей в кібератаках. Перші три місця посіли вразливості в Інтернеті речей. Дві з них є критичними, оскільки дозволили віддалено запускати шкідливий код на маршрутизаторі, а одна вразливість успішно обійшла механізми автентифікації маршрутизатора. Ці вразливості IoT дозволили зловмиснику запустити шкідливий програмний код, отримати контроль над пристроями та отримати доступ до певної інформації. Таким чином, певна система була повністю скомпрометована [1].

1.1 Аналіз основних вразливостей в архітектурі Інтернет-речей

Вразливості, що активно використовують кіберзлочинці – їх існує доволі багато, але деякі з яких мають більшу популярність. Згідно із класифікацією OWASP існує 10 основних вразливостей систем безпеки в IoT.

В таблиці 1.1 наведено узагальнені та найбільш важливі проблеми безпеки в IoT [1].

Таблиця 1.1– Найчастіші вразливості в Інтернеті речей на всіх рівнях архітектури

Проблеми безпеки	Рівень інтерфейсів	Рівень служб	Мережевий рівень	Сенсорний рівень
Небезпечний веб-інтерфейс	+	+	+	
Недостатня автентифікація авторизація	+	+	+	+
Небезпечні мережеві послуги		+	+	
Відсутність транспортного шифрування		+	+	
Проблеми конфіденційності		+	+	+
Небезпечний хмарний інтерфейс	+			
Небезпечний мобільний інтерфейс	+		+	+
Небезпечність	+	+	+	

конфігурації				
Небезпечне програмне забезпечення/прошивка	+		+	
Погана фізична безпека			+	+

Недостатній рівень фізичної безпеки. При відсутності засобів фізичного захисту, це дозволяє зловмисникам отримати доступ до конфіденційної інформації, яка може у майбутньому використовуватися для спроби віддаленої атаки або отриманням локального контролю над пристроями. Однією із проблем IoT є те, що її компонента розміщена в просторі та часто встановлюється у публічних а також незахищених місцях. Що дасть деяку можливість зловмиснику отримувати доступ до пристрою а також взяти його під повний контроль або використати його для доступу до усієї мережі. Зловмисники мають можливість [2]:

- отримувати мережеві і фізичні налаштування пристроїв а також встановлювати замість них власні пристрої для прослуховування чи зниження роботи мережі;
- здійснювати злам RFID зчитувачів;
- встановлювати апаратну закладку;
- інфікувати шкідливим ПЗ;
- викрадати дані;
- фізично виводити пристрої з ладу.

Пристрої або системи із небезпечним налаштуванням по замовчуванню або не можуть зробити систему безпечною, при цьому обмежують користувачів у налаштуванні конфігурації. Будь-який виробник хоче заробити більше але витрати менше, у пристроях можливо буде реалізовано більше розумних функцій, при цьому не завжди забезпечена ймовірність конфігурувати безпеку. Це може призвести до відсутності деяких функцій безпеки [2]:

– Відсутність можливості перевірки на надійність паролів. Прості паролі найлегше піддаються зламам шляхом брутфорсу.

– Не можливість створення облікового запису із різними правами доступу. Розмежуванням правил користувача і адміністратора завжди допоможе запобігти випадкових критичних змін у системі користувачем, та відмові у наданні певних функцій у разі зламу облікового запису користувача, тому що, доступ до даних має тільки адміністратор.

– Відсутність логування. Це одна із найважливіших вимог сучасних стандартів у сфері комп'ютерних мереж, а також інформаційної безпеки [2].

– Відсутності сповіщень про безпеку. Найголовнішим завданням системи являється робота у режимі реального часу щоб виявити неправомірної дії у мережі.

Відсутність можливості керувати пристроєм. Відсутності підтримки у безпеці на пристроях, що розгорнуті у виробництві, виключно із керуванням активами, керуванням оновленнями, та безпечний вивід із експлуатації і моніторингу систем та реагуванням. Пристрої IoT являються «чорною скринькою». У них не реалізовано можливість відслідковувати стан роботи, ідентифікація служб та процесів що запущені та із чим вони взаємодіють [3].

Небезпечна передача і збереження даних. При відсутності можливості шифрування або доступом до контролю за конфіденційними даними в будь-якому місці екосистеми, у тому числі і при збереженні, та при передачі або під час обробки. Пристрої IoT збирають і зберігають певні дані про навколишнє середовище, а також різну персональну інформацію. Викрадений пароль, можливо змінити, але ось викрадені дані із біометричного пристрою, такі як сітківка ока, відбиток пальця, біометрія обличчя, уже ні. У той же час, ці пристрої мають можливість не тільки зберігати дані у незашифрованому вигляді, але й передавати їх у мережу. Користувач може використати безпечний канал зв'язку щоб передати дані, але ось шифрування паролів, які

ми зберігаємо, біометричні та інші важливі дані повині забезпечуватися виробником пристроїв. Це призводить до відсутності таких функцій безпеки:

- Відсутність шифрування в каналах. Більше 70% користувачів користуються службами, які не використовують служби шифрування під час передачі своїх даних через мережу. А близько половини мобільних додатків, підключених до Інтернету, хмарних сервісів і локальних мереж, не мають власного безпечного з'єднання. Тому ймовірність прослуховування трафіку, як і ймовірність успішної атаки MITM, дуже висока. Через це зловмисники отримують усі дані, надіслані користувачем, оскільки він діє як вузол між пристроями в кінці шляху [3].
- Відсутності шифрування у каналах з локальною мережею.
- Відсутнє використання SSL/TLS. Протоколи SSL/TLS були розроблені для використання в браузерах, але завдяки певним властивостям вони є одними з найвищих стандартів якості для спілкування в Інтернеті. Теоретично SSL/TLS здатний забезпечити найважливіші фактори безпеки – доступність, цілісність, конфіденційність програмного зв'язку, як з боку клієнта, так і з боку серверів [3].

Недостатній рівень захисту конфіденційності. IoT-пристрої опрацьовують інформацію про те хто, і що їх оточує. Викрадені таким чином дані про користувача можуть ненавмисно дескредитувати людину, так і можуть бути використовувані при шантажі. Щоб вирішити проблему необхідно точно знати, що за дані збирає пристрій IoT, мобільними додатками і хмарним інтерфейсами. Необхідно переконатися, чи збираються тільки необхідні дані для функціонування пристрою, перевіряти, чи надано дозвіл для зберігання персональної інформації і чи захищена вона, а також чи прописана політика зберігання інформації. При недотриманні умов, у користувача виникають проблеми із законодавством. До наслідків призводить відсутність певних функцій безпеки:

– Збір персональних даних. Чим більше персональних даних збирає пристрій, тим більше ресурсів потрібно для його захисту. Закон про обробку персональних даних прийнятий Європейським Союзом. «Загальний регламент захисту даних» регулює питання обмеження можливості збору інформації про фізичну особу, яка перевищує максимальну величину та обсяг, необхідний для здійснення зазначених дій.

– Перевірка і налаштування дозволів. При відсутності можливості налаштування системи збору інформації це загрожує користувачу [4].

Використання небезпечних або застарілих компонентів. Використовуючи застарілі чи небезпечні програмні компоненти або бібліотеки, що може дозволити скомпрометувати пристрій. Це є небезпечним налаштуванням платформи операційної системи та використанням сторонніх програмних чи апаратних компонентів із небезпечного ланцюга постачання. На початку 2019 року експертом Пол Маррапіз виявлено уразливості у P2P-утилітах iLnkP2P, яка була встановлена на більш ніж 2 мільйонів пристроях, що були підключені до мережі: відеореєстраторах, радіонянях, IP-камерах, розумних дверних дзвінках. При першій вразливості CVE-2019-11219 дозволяється атакувати та ідентифікувати пристрій, другою – вразливість автентифікації у iLnkP2P CVE-2019-11220 – перехопити трафік при відкритому вигляді, при потоковій передачі відео та паролів [4].

Відсутність безпечних механізмів оновлення. Включає у відсутність валідації прошивки на певному пристрої, відсутності безпечної доставки (без шифрування при передачі даних), відсутності механізмів при запобіганні відкату та відсутності повідомлення про заміну безпеки оновлення. Відсутності можливість оновлення пристрою це являється і так слабким місцем безпеки. Неможливості встановювати оновлення, що означає для пристрою протягом певного часу залишатися уразливим. Крім того, і оновлення і прошивка теж являються небезпечними. Тому до таких наслідків призводить відсутність деяких функцій безпеки:

- Шифруванням файлів оновлення.
- Відсутністю налаштуванням параметрів шифрування.
- Підтвердженням оновлення безпосередньо перед завантаженням.
- Конфіденційні дані в оновленні.
- Погіршенням роботи.

Слабкий чи жорстко вказаний пароль. Використовуючи легко зламувані, загальнодоступні або незмінні облікові дані, включаючи бекдори в вбудованому ПЗ або клієнтському ПЗ, що може надавати несанкціонований доступ до розгорнутих систем. До даного часу найбільшим вразливими були слабкі паролі, паролі за замовчуванням чи паролі, злиті в мережу. Очевидністю є необхідність використовувати стійкий пароль, але деякі користувачі й досі не завжди змінюють пароль за замовчуванням. У червні 2019 року цим скористався шкідливий ПЗ Silex, який протягом години перетворив на «цеглу» 2000 пристроїв з Інтернету речей. Раніше відомий ботнет та хробак Mirai устиг заразити 600 тисяч пристроїв з Інтернету речей, використавши базу із 61 стандартних «логін/пароль» [4].

Відсутність багатофакторної автентифікації. Розширення автентифікації, метод з контролю доступом до комп'ютера, у якому користувачу для того щоб отримати доступ до інформації потрібно пред'явити більше ніж один «доказ механізму автентифікації». До доказів відносять:

- Знання – це інформація, яку повідомив суб'єкт. Наприклад: пароль або пін-код.
- Володіння – це річ, володіє якою суб'єкт. Наприклад: електронна чи магнітна карта.
- Властивість, володіє якою суб'єкт. Наприклад: послідовність ДНК, відбитки пальців, райдужна оболонка очей, біометрія [5].

1.2 Основні вимоги щодо безпеки Інтернет-речей

На рисунку 1.2 відображено вимоги до безпеки систем, що складаються із 6 основних критеріїв:

- критерій конфіденційності – дані, що захищені уповноваженими;
- критерій цілісності – надійні дані;
- критерій доступності – дані доступні, де та коли це потрібно;
- критерій безвідмовності – послуга, яка забезпечує надійний аудиторський підхід;
- критерій достовірності – компоненти підтверджують свою ідентичність;
- критерій секретності - служба не бачить автоматично дані про клієнтів [5].

Рисунок 1.2 – Вимоги безпеки IoT

Ризики захисту персональних даних виникають, коли усі об’єкти в IoT збирають і узагальнюють фрагменти, що пов’язані із даними. Тоді особиста інформація перетворюється через підставлення певної кількості точок, через те що місце, та час, і періодичність є контекстом щоб переглядати події. Це являється одним із аспектів виклику певних даних, тому фахівці з безпеки забезпечують, продуманість потенційних ризиків конфіденційності,

пов’язаних із усіма наборами даних. Основними проблемами безпеки в сценарії IoT включено конфіденційність даних, їхня секретність та довіра.

Конфіденційність даних [5]:

- недостатня автентифікація / достовірність;
- небезпечний інтерфейси;
- відсутність шифрування;
- збереження конфіденційності даних;
- управління доступом.

Секретність:

- секретний, захист даних а також управління ризиками;
- секретність за замовчуванням;
- політика конфіденційності інформації;
- відстеження / профілювання / незаконна інформаційна обробка.

Довіра:

- система управлінням особистості ;
- небезпечне ПЗ / прошивка ;
- забезпеченням безперервності а також доступності послуг ;
- виконанням шкідливих атак пристроїв та систем IoT;
- втрата перевірки користувачам / складність у прийнятті рішень.

1.3 Аналіз загроз в системах Інтернету речей

Щоб сформулювати рекомендації щоб посилити безпеку систем Інтернету речей, потрібно проаналізувати всі технології, що використовувалися для атак [5].

Посилення «Amplification» працює за таким принципом: відсилається запит на уразливий сервер, він декілька раз повторюється та спрямовується

до потрібного веб-сайту. В атаці даного типу використовуються протоколи LDAP і TCP [6].

Зміна інформації маршруту. Децентралізовані мережі найбільше підходять під даний тип атаки. Час доставки пакету збільшується тому, що кожен вузол являється маршрутизатором та відповідно змінює маршрутну інформацію.

Вибіркова розсилка. Загроза даного типу проходить наступним чином: скомпрометований вузол мережі здійснює вибіркове видаляння певних пакетів. Більшої ефективності дана атака набуває у комбінації із атаками, що збирають більшу кількість трафіку на певному вузлі мережі. У результаті роботи скомбінованої атаки найбільш страждає цілісність та повна доступність даних, що певним чином знижує рівень сервісу, який був наданий сенсорною мережею [6].

Бездонна воронка «Sinkhole Attack». Дана атака використовує увесь трафік мережі скомпрометованого вузла сенсорної мережі. Зловмисник «прослуховує» широкомовні розсилки, запити за маршрутами та відповідає сенсорним вузлам, що він «знайшовся» найкоротший маршрут до базової станції. Вставши між сенсорним вузлом, який певною мірою транслює, та базовою станцією, скомпрометований вузол виконує деякі дії з пакетами даних.

Шаманська атака «Sybil attack», що діє таким чином: скомпрометований вже вузол, використовує декілька псевдо ідентифікаторів, та видає відразу себе за кілька вузлів одночасно. Такі типи атак використовують для порушення механізму розподіленого зберігання, механізму маршрутизації, механізму агрегації даних, механізму голосування в мережі і т. д. Схильними до даної атаки є мережі з рівноправними вузлами.

Атака червоточини «Wormhole attack». Даний тип атак створює деякий спеціальний шлях щоб передати по ньому перехоплені пакети між двома та більше скомпрометованими вузлами певної сенсорної мережі [6].

Флуд атака «HELLO flood attack». Така атака являється широкомовною, та надсилаючи в сенсорну мережу нескінченну кількість необов'язкових повідомлень, позбавляє дану мережу різноманітних ресурсів – обчислювальної потужності, канальної ємності, енергетичних ресурсів та ін. До всіх сенсорних вузлів мережі зловмисник посилає Hello пакети. Отримавши які, вузли розглядають скомпрометований вузол як свій, і при подальшій роботі з даними, будуть користуватися отриманими з Hello пакетів адресами.

1.4 Способи виявлення наявних вразливостей та методи протидії загрозам Інтернет-речей

Найслабшим місцем для IoT являється безпека. Нажаль майже усі пристрої можуть бути уразливими, що дозволяє хакеру легко їх зламувати. У таблиці 1.2 наведено найбільші загрози IoT та можливі шляхи усунення.

Таблиця 1.2 – Найбільші загрози IoT та шляхи їх усунення

Вразливість	Шлях подолання
Недостатня чи відсутня стандартизація архітектури та протоколів, сертифікація пристрою	Створення єдиного міжнародного стандарту із єдиним переліком вимог до Інтернет речей
Відсутність шифрування бездротового трафіку	Використання протоколів шифрування WPA2/WPA3-PSK з алгоритмом шифрування AES
Робоче використання типових облікових записів, встановлених виробником за замовчуванням	Можливість створення облікових записів для кожної Інтернет речей та створення виробником різних "Нетипових" паролів

	за замовчуванням для кожного пристрою
Слабка аутентифікація і система управління доступом	Створення складного пароля та логіну для кожного облікового запису Інтернет речей
Відсутність підтримки з боку виробника для усунення вразливостей	Використання виробником стандарту безпеки Інтернет речей, створення різних паролів для пристроїв за замовчуванням, наявність технічної підтримки
Складність або неможливість установки оновлень операційної системи	Наявність веб-інтерфейсу домашнього контролера та можливість конфігурування кожної Інтернет речей та наявність можливості встановлення оновлення операційної системи
Використання незахищених мобільних технологій і хмарної інфраструктури	Використання незахищених мобільних технологій і хмарної інфраструктури
Взаємна інтеграція різних пристроїв між собою дозволяє зловмисникові оволодіти всією мережею, зламавши лише одна річ	Шифрування трафіку, що передається від одного пристрою до іншого. Облікові записи для пристроїв
Відсутність брандмауерів і антивірусів	Використання фаерволів з налаштованими списками доступу для захисту вхідного трафіку та антивірусного програмного забезпечення для внутрішнього захисту
Використання небезпечного ПЗ	Використання ліцензійного програмного забезпечення надійного виробника

Можна виділити декілька порад, які могли б мінімізувати ризики зараження пристроїв у IoT [7]:

- закрити доступ до зовнішньої мережі із пристрою без необхідності;
- перезавантаження періодичне допоможе вам позбутися уже встановлених шкідників (але у більшості випадках ризик повторного зараження залишиться);
- регулярно перевіряти наявність нових версій прошивки та оновлювати пристрій;
- використовувати складні паролі довжиною від 8 символів, що включають у себе букви із різного регістра, цифри і спецсимволи;
- заміна заводського паролю після першого завантаження пристрою, а також під час нового налаштування (навіть якщо не просить про це пристрій);
- закрити або заблокувати «зайві» порти, якщо це можливо.

Деякі поради і можуть частково закрити існуючі проблеми а також вразливості пристроїв IoT, але це не може вирішити проблему в цілому, адже принципи розробки інтернету речей залишаються а нові вразливості зловмисники знайдуть [7].

Висновки до першого розділу

У цьому розділі розглянуто основні вразливості систем Інтернету речей і основні типи загроз, а також показано, як загрози Інтернету речей можна практично ідентифікувати, охарактеризувати та змоделювати.

1. Більшу кількість проблем викликали атаки на сервери, робочі станції та смартфони, незашифровані повідомлення, недостатня автентифікація, відсутність контролю над оновленнями програмного забезпечення та політиками безпеки.

2. Крім втрати конфіденційності в постійних мережах зв'язку (прослуховування, фальсифікація отриманої інформації), виникли проблеми з

постійним захистом інформації користувачів. Вони визначаються: − відсутністю простих стандартів не лише захисту, а й взаємодії; – Відсутність інтересу з боку виробників, які є першим етапом реалізації.

3. Найбільшу загрозу ми приписуємо атакам на керування пристроями з DDoS-атаками, між машинною взаємодією, атаками на інфраструктуру передачі даних і кількома іншими типовими атаками типу «людина посередині».

Однак багато пристроїв Інтернету речей вже підпадають під серйозні обмеження щодо експлуатації залежно від природи та умов їх використання. Ці обмеження не дозволяють безпосередньо використовувати базові заходи безпеки, такі як впровадження брандмауерів або використання потужніших криптосистем для створення шифрування зв’язку з іншими пристроями, тоді як низька ціна та вузьке націлювання пристроїв призведе до використання виробник рідко дає надійні системи безпеки.

2 ТЕОРЕТИЧНІ МЕТОДИ ОЦІНКИ РИЗИКІВ

Оцінка ризику є частиною основних елементів управління ризиками, визначених у ISO 31000, якими є:

- спілкування та консультації;
- встановлення контексту;
- оцінка ризику (ідентифікація ризику, аналіз ризику);
- запобігання ризику;
- моніторинг та огляд.

«Оцінка ризику – це загальний процес ідентифікації ризику, аналізу та оцінки ризику» (ISO 31010)

Ризик можна оцінити на будь-якому рівні операцій або цілей компанії. Існує 31 метод оцінки ризику, перерахований у Додатку B ISO/IEC 31010. В другому розділі опишемо найбільш популярні методи оцінки ризиків [8].

2.1 Метод Дельфі

Метод Delphi – це техніка структурованої комунікації або метод, призначений для збору експертних думок шляхом багатораундового опитування з контрольованим зв’язком між окремими раундами. Метою є досягнення зближення думок і певною мірою консенсусу в поглядах на поточні та майбутні події. Концепція методу сягає початку 1950-х років, коли «Проект Delphi» був створений під егідою ВПС США та спонсорований RAND Corporation. За межами сфери державної безпеки цей метод вийшов на перший план лише в 1964 році в дослідженні Гордона і Хелмера, які прагнули зібрати думки про довгострокові тенденції в науці і техніці та їх вплив на суспільство [8].

Метод працює за принципом опитування, коли анкета, складена адміністраторами, надсилається групі від 5 до 20 експертів з даного питання, яким гарантується анонімність. Кожен експерт самостійно та без спілкування з іншими заповнює анкету та повертає її адміністратору. Він оцінює відповіді та повертає анкети разом із відгуком. На основі цього відгуку респонденти можуть змінювати свої відповіді. Метою першого туру є своєрідний огляд загальної дисперсії у відповідях респондентів і переважаючих думок [8].

У другому раунді реєструються переважаючі відповіді, і якщо певного рівня консенсусу не досягнуто, він продовжується до третього раунду. Цю структуру можна змінювати, що призводить до різних модифікацій, як зазначено Граймом і Райтом,.

Метод заснований на ідеї, що думка групи експертів дасть нам краще уявлення про проблему, ніж думка окремої людини. Важливо враховувати, що думка більшості може бути не найвірнішою за думку меншості. Метод придатний для використання в питаннях такого характеру, які отримують вигоду від колективного отримання суб’єктивних думок, а також у сферах, де експертну думку важко встановити за допомогою статистичного аналізу чи інших методів. Іншою причиною для використання можуть бути перешкоди в спілкуванні віч-на-віч, такі як географічна відстань, особисті конфлікти, вартість особистих зустрічей або вплив соціальної бажаності на висловлені думки. До недоліків методу Дельфі відносяться витрати часу, можлива неоднорідність експертних знань між експертами або відповіді експертів можуть бути не зовсім незалежними, оскільки експерти теоретично можуть контактувати один з одним [9].

Метод Delphi подібний до методу ринку прогнозів тим, що обидва вони є методами для агрегування різноманітних думок груп респондентів. Проте в них є відмінності. Грін з командою порівняли їх і зазначили переваги використання того чи іншого методу.

Delphi має такі переваги перед методом прогнозів ринками:

1. Має ширші можливості використання, оскільки з його допомогою можна дізнатися думки про ситуації, які не підлягають перевірці.

2. Багато людей можуть не розуміти, як працюють ринки прогнозів або як інтерпретувати свої очікування в ціні. Через Delphi легше висловити свою думку.

3. Delphi пропонує можливість обґрунтувати свою точку зору, а прозорий обмін інформацією дозволить залученим експертам отримати нові знання в цій галузі.

4. Ринки прогнозів вразливі до атак спекулянтів з метою маніпулювання кінцевим результатом. Адміністратор Delphi контролює, кого він вибере для процесу, і може безпосередньо виключати екстремальні значення з процесу або обчислювати медіану замість середнього [9].

5. Метод Delphi є більш дискретним. У випадку ринків прогнозів отримання прибутку від торгівлі результатами певних серйозних подій можна вважати аморальним. Деякі ринки прогнозів були скасовані наступного дня після відкриття. Це були прогнози терактів або прогнози зміни політичних режимів.

Ринки прогнозів мають такі переваги перед delphi:

1. У Delphi процес найму експертів може бути складним. На ринках прогнозів учасники самі вирішують, чи брати участь, якщо вони вважають, що їхні очікування ще не відображені в прогнозі.

2. Ринки прогнозів можуть мотивувати учасників до довгострокової участі, оскільки будь-яка нова інформація негайно відображається в прогнозі.

3. За допомогою методу Дельфі може не бути справжнього консенсусу думок, оскільки експерти можуть відчувати тиск, змушений відповідати поглядам інших і приховувати свою незгоду. І навпаки, на ринках прогнозів учасники можуть виграти, лише кинувши виклик думці більшості [9].

Загалом ринки прогнозів мають переваги, оскільки вони можуть мотивувати участь. Їх слід використовувати для вирішення більш простих

завдань з можливістю залучення великої кількості учасників. Delphi краще використовувати для складніших проблем, коли потрібні зворотній зв’язок і нові ідеї.

2.2 Попередній аналіз небезпек

Попередній аналіз небезпек (PHA) зазвичай є першою спробою в процесі безпеки системи ідентифікувати та класифікувати небезпеки або потенційні небезпеки в роботі запропонованої асоціації систем, процесів або процедур; Він використовується на ранніх стадіях проектування системи.

Це напівкількісний аналіз, який виконується для визначення всіх потенційних небезпек і аварійних подій, які можуть призвести до аварії, ранжування виявлених аварійних подій відповідно до їх серйозності та визначення необхідних контрольних небезпек і подальших дій [10].

Він також забезпечує обґрунтування контролю за небезпекою та вказує на необхідність більш детального аналізу, наприклад: B. аналіз небезпек підсистеми (SSHA) та аналіз небезпек системи (SHA). PHA, як правило, розроблятиметься з використанням методів безпеки системи, відомих як аналіз режимів і наслідків відмови (FMEA) та/або аналіз слідів енергії та бар’єрів (ETBA).

Попередній аналіз небезпеки, який можна використовувати під різними назвами, наприклад Швидке ранжування ризиків та ідентифікація небезпек (HAZID).

Властивості PHA.

1. Метод спирається на мозковий штурм і експертне судження, щоб оцінити важливість небезпек і призначити рейтинг кожній ситуації.
2. Зазвичай його виконують одна або дві людини, які знайомі з видом діяльності.

3. Він застосовний до будь-якої діяльності чи системи.

4. Його можна використовувати на ранніх етапах життя процесу як високорівневий аналіз [10].

5. Він використовується для створення якісних описів небезпек, пов’язаних із процесом. Забезпечує якісне ранжування небезпечних ситуацій; Це ранжування можна використовувати для визначення пріоритетності рекомендацій щодо зменшення або уточнення небезпек на наступних етапах життєвого циклу.

Якість оцінки залежить від якості та наявності документації, підготовки керівника групи з оцінки щодо використання різних аналітичних методів та досвіду команд з оцінки [10].

Переваги і недоліки PHA.

Переваги:

- допомагає забезпечити безпеку системи;
- модифікації дешевші і простіші в реалізації;
- використовується на ранніх етапах проектування;
- зменшує час розробки за рахунок зменшення кількості непередбачуваних ситуацій.

Недоліки:

- аналітики мають передбачати небезпеки;
- наслідки взаємодії між небезпеками непрості.

Кроки для проведення попереднього аналізу небезпек (PHA):

1. Передумови PHA: Вони включають створення групи PHA, опис системи, що підлягає аналізу, і збір інформації про ризики з вибраних систем.

2. Ідентифікація небезпеки: тут мають бути ідентифіковані всі небезпеки та потенційні інциденти. На цьому етапі слід розглянути всі частини системи. Усі висновки мають бути зафіксовані [11].

Метод PHA можна використовувати під час:

- тестування аналогічних існуючих систем;

- огляду та попередніх аналізів небезпек для подібних систем;
- огляду контрольних списків небезпек і стандартів;
- розгляду потоку енергії через систему;
- розгляду небезпечних за своєю суттю матеріалів;
- розгляду взаємодій між компонентами системи;
- огляду експлуатаційних специфікацій і врахування всіх фактори навколишнього середовища;
- командного мозкового штурму;
- розгляд інтерфейсу людина-машина;
- розгляд змін режиму використання;
- використання дрібномасштабного тестування та теоретичного аналізу;
- використання методу «продуманого аналізу у найгіршому випадку, що якщо»;
- записи пошуку, такі як статистика нещасних випадків, звіти про випадкові випадки/небезпечні випадки, звіти агентств або державних установ.

3. Оцінка наслідків та частоти: щоб визначити рівень ризику, нам потрібно оцінити частоту та тяжкість кожної події нещасного випадку. На цьому етапі розглядаються наслідки та частота кожної небезпеки [11].

4. Оцінка ризику та подальші дії: Ризик визначається як комбінація конкретного/даного наслідку та рівня серйозності тієї самої події/наслідку. Це дозволяє скласти рейтинги події/наслідки в матриці ризиків. Цей ранг визначає подальші дії, необхідні для ризику. Попередній аналіз небезпеки не є статичним документом, його слід переглядати та оновлювати за певних умов. До таких умов відносяться:

- зміна обладнання системи;
- зміни процедур технічного обслуговування або експлуатації;
- після аварії або майже аварії;

- зміни екологічного стану.

2.3 Аналіз небезпеки та працездатності

Аналіз небезпеки та працездатності (HAZOP) – це структурований і систематичний метод тестування системи та управління ризиками. Зокрема, HAZOP широко використовується як техніка для виявлення потенційних небезпек у системі та виявлення операційних проблем, які можуть призвести до дефектних продуктів. HAZOP базується на теорії, яка припускає, що події ризику викликані відхиленнями від проекту або наміру експлуатації. Ідентифікація таких відхилень полегшується за допомогою наборів «керівних слів» як систематичного списку перспектив відхилення. Цей підхід є унікальною особливістю методології HAZOP, яка допомагає стимулювати уяву членів команди під час дослідження потенційних відхилень. Як інструмент оцінки ризику, HAZOP часто описують як [12]:

- техніка мозкового штурму;
- інструмент якісної оцінки ризику;
- індуктивний інструмент оцінки ризику, що означає, що це підхід «знизу вгору» до ідентифікації ризику, де успіх залежить від навичок експертів у відповідній галузі;
- (МСП) для прогнозування відхилень на основі минулого досвіду та загальновідомих знань;
- керівництво з управління ризиками якості ICHQ9 підтримує використання HAZOP (серед інших дозволених інструментів) для управління ризиками якості фармацевтичної продукції;
- на додаток до його корисності в управлінні ризиками якості, HAZOP також широко використовується в оцінці ризиків для промислових і навколишніх застосувань у галузі охорони здоров’я та безпеки.

При описі методології HAZOP важливими є наступні визначення:

Небезпека – потенційне джерело шкоди. Відхилення від конструкції або мети експлуатації можуть становити або спричиняти небезпеку. Небезпеки є центральними для досліджень HAZOP, і слід зазначити, що одна небезпека потенційно може призвести до кількох форм шкоди [12].

Шкода – тілесні ушкодження чи шкода здоров'ю людей або майну чи довкіллю. Шкода є результатом виникнення небезпеки та може приймати різні форми: безпека пацієнтів або користувачів, безпека співробітників, бізнес-ризик, регуляторний ризик, екологічний ризик тощо.

Ризик – поєднання ймовірності виникнення та тяжкості пошкодження. У більш вузькому сенсі «ризик» не завжди чітко визначений у дослідженнях HAZOP, оскільки основна методологія не вимагає ідентифікації ймовірності або серйозності шкоди. Однак групи з оцінки ризиків можуть оцінити ці фактори, якщо це доцільно, для подальшої кількісної оцінки та визначення пріоритетності ризиків [12].

HAZOP найкраще підходить для оцінки небезпек на заводах, обладнанні та процесах, він здатний оцінювати системи з різних точок зору:

Основні завдання HAZOP:

− оцінити здатність конструкції системи відповідати вимогам користувача та стандартам безпеки;

− виявлення вразливостей у фізичному та робочому середовищах систем;

− оцінка навколишнього середовища, щоб переконатися, що система належним чином розгорнута, підтримується, підтримується, локалізується тощо;

− операційний і процедурний контроль;

− оцінка технічних засобів контролю (наприклад, автоматизація), операційних процедур, процедурних засобів контролю (наприклад, взаємодія людей) тощо;

– оцінка різних режимів роботи – запуск, очікування, нормальна робота, сталий і перехідний стани, нормальне відключення, аварійний тощо.

Переваги використання методу HAZOP [13]:

– корисно використовувати під час протистояння небезпеці, яку важко визначити кількісно;

– виникнення небезпеки, пов’язаної з продуктивністю та поведінкою людини;

– виникнення небезпеки, які важко виявити, проаналізувати, виділити, підрахувати, передбачити тощо;

– методологія не змушує вас чітко оцінювати чи вимірювати ймовірність виникнення відхилення, серйозність впливу або здатність виявляти;

– вбудована методологія мозкового штурму;

– систематична та комплексна методологія;

– більш простий і інтуїтивно зрозумілий, ніж інші широко використовувані інструменти управління ризиками.

Недоліки методу HAZOP:

– немає засобів оцінки небезпек, пов’язаних із взаємодією між різними частинами системи чи процесу;

– немає можливості ранжування ризиків або встановлення пріоритетів;

– немає засобів для оцінки ефективності існуючих або запропонованих засобів контролю (запобіжних заходів).

Метод HAZOP складається з наступних етапів [13]:

1. Етап визначення.

Етап визначення зазвичай починається з попередньої ідентифікації членів групи оцінки ризику. HAZOP має бути багатофункціональною командною роботою та покладається на спеціалістів (МСП) з різних дисциплін, що володіють відповідними навичками та досвідом, які

виявляють інтуїцію та розсудливість. МСП слід ретельно вибирати, щоб включати тих, хто має широкі та актуальні знання про системні відхилення.

HAZOP завжди слід проводити в атмосфері позитивного мислення та відвертого обговорення. Під час фази визначення група оцінки ризику повинна ретельно визначити масштаб оцінки, щоб зосередити зусилля. Це включає визначення меж дослідження та ключових інтерфейсів, а також ключових припущень, згідно з якими проводитиметься оцінювання.

2. Підготовчий етап.

Підготовчий етап зазвичай включає такі дії:

- ідентифікація та пошук допоміжних даних та інформації;
- визначення аудиторії та користувачів результатів дослідження;
- підготовка до управління проектом (наприклад, планування зустрічей, стенограма тощо);
- консенсус щодо формату шаблону для запису результатів дослідження;
- консенсус щодо довідкових слів HAZOP, які будуть використовуватися під час дослідження. Довідкові слова HAZOP є ключовими допоміжними елементами у виконанні аналізу HAZOP.

Відповідно до стандарту IEC 61882 ідентифікація відхилень від задуму проекту досягається шляхом опитування з використанням заздалегідь визначених «керівних слів». Роль навідного слова полягає в тому, щоб стимулювати образне мислення, зосередити увагу на вивченні та викликати ідеї та обговорення [14].

Групи з оцінки ризиків несуть відповідальність за визначення настановних слів, які найкраще відповідатимуть масштабу та постановці проблеми для їх аналізу.

3. Етап перевірки.

Етап перевірки починається з ідентифікації всіх елементів (частин або кроків) системи або процесу, що підлягають перевірці.

Наприклад:

- за потреби фізичні системи можуть бути розбиті на менші частини;
- процеси можуть бути розбиті на окремі кроки або фази;
- подібні частини або кроки можна згрупувати разом для полегшення оцінювання.

Потім до кожного з елементів застосовуються довідкові слова HAZOP. Таким чином систематично проводиться ретельний пошук відхилень. Слід зазначити, що не всі комбінації настановних слів і елементів, як очікується, дадуть розумні або достовірні можливості відхилення. Як правило, усі умови розумного та неправильного використання, які очікує користувач, мають бути визначені та згодом оскаржені, щоб визначити, чи є вони «достовірними» та чи слід їх додатково оцінювати. Немає необхідності чітко документувати випадки, коли комбінації елементів і керівних слів не дають жодних достовірних відхилень.

4. Етап документування та подальших дій.

Документування аналізів HAZOP часто полегшується за допомогою шаблону форми запису, як описано в стандарті IEC 61882. Групи оцінки ризиків можуть змінювати шаблон за необхідності на основі таких факторів, як [14]:

- нормативні вимоги;
- потреба в більш чіткому рейтингу ризику або пріоритезації (наприклад: ймовірність відхилення рейтингу, серйозність та/або виявлення);
- політика компанії щодо документації;
- потреби в простежуваності або готовності до аудиту;
- інші фактори.

Після завершення аналізу HAZOP результати дослідження та висновки мають бути задокументовані відповідно до характеру ризиків, оцінених у дослідженні, та відповідно до політики документації окремої компанії. У

рамках закриття для аналізу HAZOP слід перевірити, чи існує процес, який гарантує, що призначені дії завершуються задовільним чином.

5. Огляд ризиків.

На довгостроковій основі оперативний зворотний зв’язок має підтверджувати, що етапи оцінки та контролю адекватно вирішують питання ризику. Якщо це не так, можливо, необхідно переглянути всі припущення. Зворотній зв’язок має відповідати забезпеченню того, що зроблені припущення щодо рівня залишкових ризиків залишаються дійсними. Залишкові ризики – це ризики, які, як очікується, залишаться після застосування стратегій контролю ризиків. Важливо також зазначити, що нові ризики можуть виникнути внаслідок практики контролю ризиків. Іноді ризики, які не були спочатку ідентифіковані або могли бути відфільтровані під час первинної оцінки ризику, можуть стати обтяжуючими факторами через впровадження заходів контролю ризиків.

6. Повідомлення про ризики.

HAZOP – потужний інструмент комунікації. Результати інструменту завжди мають бути представлені на рівні деталізації, відповідному для різних зацікавлених сторін. Це важливо не лише для представлення результатів, але й для отримання раннього підходу [15].

У випадках, коли HAZOP використовується як основа для рішення «GxP» або іншого регульованого дозволу, цей підхід слід задокументувати в «Стандартній операційній процедурі». Можливо, немає необхідності включати в процедуру детальні кроки або алгоритми підрахунку балів, але вони повинні бути задокументовані в контрольованому звіті. Слід також контролювати оновлення портфоліо.

2.4 Структурована техніка «що якщо»

Структурована техніка «що-якщо» як інструмент оцінки ризику, є загальною та менш формальною технікою ідентифікації ризиків, яку можна використовувати окремо або як частину поетапного підходу, щоб зробити методи «знизу вгору», такі як FMEA, більш ефективними. SWIFT використовує структурований мозковий штурм під час фасилітованого семінару, поєднуючи заздалегідь визначений набір ключових слів (час, сума тощо) із підказками учасників, які часто починаються з таких фраз, як «Що, якщо?». або "як міг?".

В основі SWIFT лежить перелік ключових слів, які дозволяють всебічний аналіз ризиків або джерел ризиків. На початку семінару обговорюються контекст, сфера застосування та мета SWIFT, а також формулюються критерії успіху. Використовуючи ключові слова та «Що, якщо?», фасилітатор заохочує учасників поставити та обговорити такі питання, як [15]:

- відомі ризики;
- джерела та фактори ризику;
- попередній досвід, успіхи та випадки;
- відомі та існуючі засоби керування;
- нормативні вимоги та обмеження.

Список головних слів використовується модератором для моніторингу обговорення та пропозиції додаткових тем і сценаріїв для обговорення командою. Команда оцінює, чи є контроль адекватним, і, якщо ні, розглядає можливі варіанти покращення. Під час цієї дискусії буде задано більше запитань «Що, якщо?».

Часто створений список ризиків можна використовувати як основу для якісного або напівкількісного методу оцінки ризику, як у випадку з FMEA.

Аналіз SWIFT дозволяє учасникам дивитися на реакцію системи на проблеми, а не просто вивчати наслідки відмови компонентів. Таким чином, він може бути використаний для виявлення можливостей для вдосконалення процесів і систем, і в більш загальному плані може бути використаний для визначення дій, які призводять до та покращують їхні ймовірності успіху.

Аналіз «що-якщо» – це структурована техніка мозкового штурму для виявлення того, що може піти не так, і оцінки ймовірності та наслідків таких ситуацій. Відповіді на ці запитання формують основу для оцінки прийнятності цих ризиків і визначення рекомендованого курсу дій щодо ризиків, оцінених як неприйнятні. Досвідчена команда перевірки може ефективно та продуктивно визначити ключові проблеми, пов'язані з процесом або системою. На чолі з енергійним і цілеспрямованим фасилітатором кожен член команди перевірки бере участь в оцінюванні того, що може піти не так, на основі свого минулого досвіду та знання подібних ситуацій (рис. 2.1) [16].

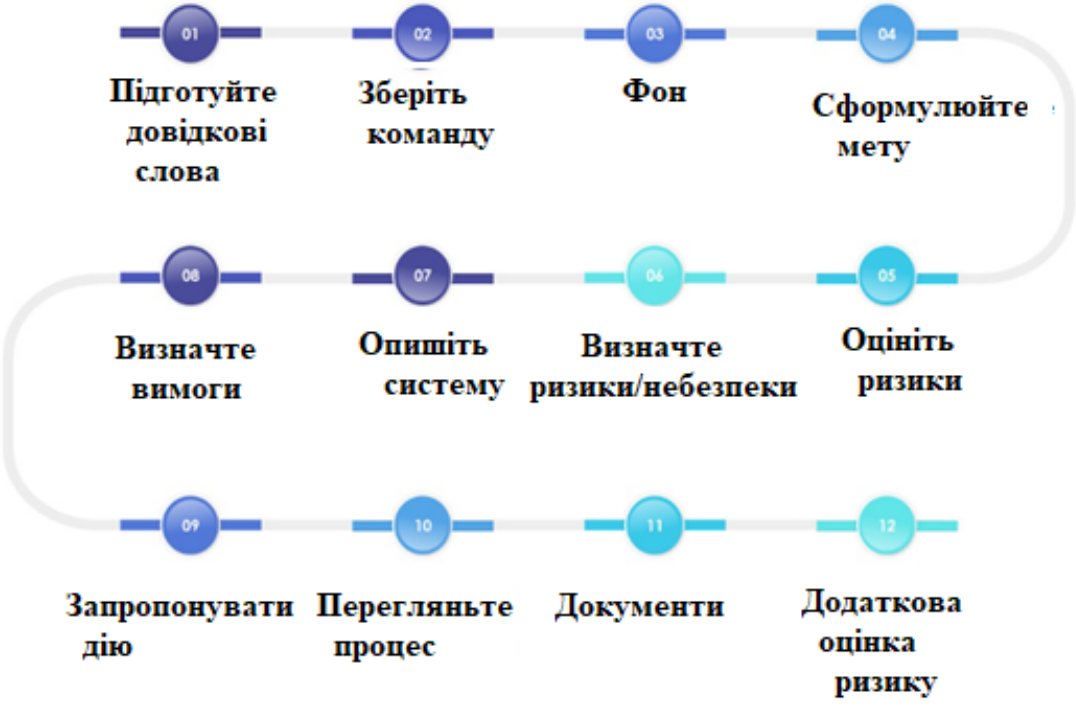

Рисунок 2.1 – Кроки SWIFT аналізу

З рисунку 2.1 можна виділити основні етапи.

1. Підготовка ключових слів: Модератор повинен вибрати набір ключових слів, які будуть використовуватися в SWIFT.

2. Збір команди: виберіть учасників для семінару SWIFT на основі їхніх знань про систему/процес, який потрібно оцінити, і ступеня, в якому вони представляють повний спектр зацікавлених сторін.

3. Формування довідкової інформації: Опишіть тригер для SWIFT (наприклад, нормативні зміни, несприятлива подія тощо).

4. Формування мети: чітко поясніть мету, якій призначено SWIFT (наприклад, покращити ефективність процесу).

5. Визначення вимог: Сформулюйте критерії успішного виконання.

6. Опис системи: надайте текстові та графічні описи на належному рівні системи або процесу, що оцінюється ризиком. Чітке розуміння є необхідним і може бути встановлено шляхом співбесід, збирання багатофункціональної команди та вивчення документів, планів та інших записів [16].

7. Визначення ризиків/небезпек: тут починає діяти структурована техніка «що, якщо». По черзі використовуйте ключові слова/заголовки для кожної системи, підсистеми вищого рівня або кроку процесу. Учасники повинні використовувати підказки, починаючи з таких фраз, як «Що, якщо…» або «Як могло б…», щоб підкреслити потенційні ризики/небезпеки, пов’язані з ключовим словом. Наприклад, якщо процес – «прибуття зразка», а головне слово – «час або швидкість», підказки можуть включати «що, якщо зразок буде доставлено під час зміни» (неправильний час) або «як міг зразок залишити довго чекати за умов навколишнього середовища?» (неправильний час).

8. Оцінка ризиків: оцініть ризик, пов’язаний з ідентифікованими небезпеками, використовуючи загальний підхід або допоміжну техніку аналізу ризиків. У світлі існуючих заходів контролю оцініть ймовірність

того, що вони можуть завдати шкоди, і серйозність шкоди, яку вони можуть завдати. Оцініть прийнятність цих рівнів ризику та визначте будь-які аспекти системи, які можуть вимагати більш детальної ідентифікації та аналізу ризику.

9. Пропозиція дії: запропонуйте плани дій з контролю ризиків, щоб зменшити виявлені ризики до прийнятного рівня.

10. Перегляд процесу: визначте, чи SWIFT досяг своїх цілей, чи деякі частини системи потребують більш детальної оцінки ризиків.

11. Документація: підготуйте оглядовий документ для повідомлення результатів SWIFT.

12. Додаткова оцінка ризику: Проведіть додаткову оцінку ризику з використанням більш детальних або кількісних методів, якщо необхідно. Аналіз SWIFT є дійсно ефективним механізмом фільтрації, щоб зосередити зусилля на найбільш цінних областях.

2.5 Аналіз режимів помилок та наслідків

Аналіз режимів і наслідків відмови (FMEA), започаткований американськими військовими в 1940-х роках, – це простий підхід до виявлення всіх можливих дефектів у проекті, процесі виробництва чи складання, продукті чи послузі. Це звичайний інструмент аналізу процесу.

«Режими відмови» означає способи або режими, за яких щось може вийти з ладу. Збої – це будь-які помилки чи дефекти, особливо ті, що впливають на клієнта, і можуть бути потенційними або фактичними.

«Аналіз ефектів» стосується вивчення наслідків цих помилок.

Помилки впорядковані відповідно до того, наскільки серйозними є їхні наслідки, як часто вони виникають і наскільки легко їх можна виявити.

Метою FMEA є вжиття заходів для усунення або зменшення дефектів, починаючи з дефектів найвищого пріоритету.

Аналіз режиму та наслідків відмов також документує поточні знання та дії щодо ризиків відмов для використання в постійному вдосконаленні. FMEA використовується під час будівництва, щоб уникнути помилок. Пізніше він використовується для контролю, до та під час процесу запуску. В ідеалі FMEA починається на самих ранніх концептуальних стадіях проектування та, як очікується, триватиме протягом усього життя продукту чи послуги [17].

FMEA використовується:

13. коли процес, продукт або послуга розроблені або перепроектовані після розгортання функції якості;

14. коли існуючий процес, продукт або послуга застосовуються по-новому;

15. перед розробкою планів контролю для нового або зміненого процесу;

16. коли плануються цілі вдосконалення для існуючого процесу, продукту чи послуги;

17. при аналізі збоїв існуючого процесу, продукту чи послуги;

18. регулярно протягом усього життєвого циклу процесу, продукту чи послуги.

Процедура використання FMEA наступна:

1. Зберіть міжфункціональну команду людей з різними знаннями про процес, продукт або послугу та потреби клієнтів. Зазвичай включають такі ролі: проектування, виробництво, якість, тестування, надійність, технічне обслуговування, закупівлі (і постачальники), продажі, маркетинг (і клієнти) і обслуговування клієнтів [17].

2. Визначте сферу застосування FMEA. Це про концепцію, систему, дизайн, процес чи послугу, які межі, наскільки детально ми повинні бути?

Використовуйте блок-схеми, щоб визначити обсяг і переконатися, що кожен член команди розуміє його в деталях.

3. Заповніть ідентифікаційну інформацію у верхній частині форми FMEA (таблиця 2.1 показує типовий формат). Інші кроки вимагають інформації, яка надходить у стовпці форми.

4. Визначте можливості своєї області. Запитайте: «Яка мета цієї системи, дизайну, процесу чи послуги? Чого очікують від нього наші клієнти?» Назвіть це дієсловом, а потім іменником. Зазвичай обсяг буде поділено на окремі підсистеми, елементи, деталі, вузли або етапи процесу та визначено відповідну функцію.

5. Визначте всі можливі джерела помилок для кожної функції. Це можливі режими відмови. Якщо необхідно, поверніться назад і перепишіть функцію з більш детальною інформацією, щоб переконатися, що режими збою вказують на втрату цієї функції.

6. Для кожного режиму відмови визначте будь-який вплив на систему, пов’язані системи, процес, пов’язаний процес, продукт, послугу, клієнта чи регулювання. Це можливі наслідки відключення. Запитайте: «Що відчуває клієнт через цю помилку?» Що відбувається, коли виникає ця помилка?».

Таблиця 2.1 – Типовий формат FMEA

Функція	Режим потенційної несправ	Потенційні наслідки відмови	S	Потенційна(і) причина(и) невдачі	O	Поточний контроль процесу	D	RPN	CRIPT	Рекомендо	Відповідальність і планований термін виконання	Результати дій					
												Дії прийняті	S	O	D	RPN	CRIT

	вності									ваніді ї						
Видайте суму готівки на запит клієнта	Невидає готівку	Клієнт дуже незадоволений Некоректний до депозитної системи до запитання Розбіжність у балансі готівк	8	Без готівки Закликнювання машини Збій живлення під час транзакції	5 3 2	Внутрішня сигналізація про низький рівень золи Внутрішнє сповіщення про застрягання Жодного	5 10 10	200 240 160	45 24 16							

		и														
	Видає забагато готівки	Банк втрачає гроші Розбіжність у балансі готівки	6	Купюри злиплися Номінали в неправильних лотках	2 3	Процедура завантаження (ребристека) Візуальна перевіпер двома людьми	7 4	84 72	12 18							
	Видача готівки займає занадто баг	Клієнт дещо роздратований	3	Інтенсивний трафік комп’ютерної мережі Пере	7 2	Жодного Жодного	10 10	210 60	21 6							

	ато час у			рива ння живл ення під час тран закці ї													

7. Визначте, наскільки серйозним є кожен ефект. Це рейтинг серйозності, або S. Серйозність зазвичай оцінюється за шкалою від 1 до 10, де 1 означає незначне, а 10 – катастрофічне. Якщо режим відмови має більше одного впливу, запишіть лише найвищий рейтинг серйозності для цього режиму відмови в таблиці FMEA.

8. Для кожного виду відмови визначте всі можливі причини. Використовуйте інструменти, класифіковані як інструменти аналізу першопричини, а також найкращі знання та досвід команди. Перелічіть усі можливі причини для кожного типу несправності у формі FMEA.

9. Для кожної причини визначте рейтинг частоти, або O. Цей рейтинг оцінює ймовірність відмови, що виникла через цю причину, протягом усього терміну експлуатації вашої області. Виникнення зазвичай оцінюється за шкалою від 1 до 10, де 1 означає вкрай малоймовірність, а 10 — неминучість. У таблиці FMEA вкажіть рейтинг частоти для кожної причини.

10. Визначте поточні засоби контролю процесу для кожної першопричини. Це тести, процедури або механізми, які ви зараз маєте, щоб запобігти потраплянню помилок до клієнта. Ці засоби контролю можуть запобігти виникненню причини, зменшити ймовірність її виникнення або

виявити помилки після того, як причина вже виникла, але до того, як клієнт постраждає.

11. Для кожного елемента керування визначте оцінку виявлення або D. Ця оцінка оцінює, наскільки добре засоби керування можуть виявити або першопричину, або її режим несправності після її виникнення, але до того, як це вплине на клієнта. Виявлення зазвичай оцінюється за шкалою від 1 до 10, де 1 означає, що контроль абсолютно впевнений у виявленні проблеми, а 10 означає, що контроль точно не виявляє проблему (або відсутній контроль). У таблиці FMEA вкажіть оцінку виявлення для кожної причини.

12. Необов'язковий для більшості галузей промисловості: запитайте: «Чи пов'язаний цей режим відмови з критичною характеристикою?» (Критичні характеристики – це вимірювання чи показники, які відображають безпеку чи державну відповідність і потребують спеціального контролю.) Якщо так, отримує стовпець із позначкою «Класифікація» Y або N, щоб вказати, чи потрібні спеціальні засоби контролю. Як правило, серйозність критичних ознак становить 9 або 10, а частота й показник виявлення перевищують 3.

13. Обчисліть число пріоритету ризику, або RPN, яке дорівнює S × O × D. Крім того, обчисліть критичність, помноживши ступінь серйозності на випадки, S × O. Ці числа є орієнтиром для ранжування потенційних помилок у порядку, у якому їх потрібно виправити.

14. Визначте рекомендовані дії. Ці дії можуть бути змінами конструкції або процесу з меншою серйозністю або випадковістю. Вони можуть бути додатковими елементами керування для покращення виявлення. Також зазначте, хто відповідає за дії та планові дати завершення [18].

Після завершення дій запишіть результати та дату у форму FMEA. Також зверніть увагу на нові рейтинги S, O або D і нові RPN.

Приклад використання FMEA. Банк виконав процес FMEA у своїй системі банкоматів. В таблиці 2.1 показано його частину: функцію видачі

готівки та деякі з режимів несправності цієї функції. Необов'язковий стовпець "класифікація" не використовувався. Для крайніх правих стовпців (дій) відображаються лише заголовки.

Зауважте, що RPN і критичність визначають пріоритети причин по-різному. За даними RPN, «машинні збої» та «інтенсивний трафік комп’ютерної мережі» займають друге та друге місце відповідно.

Високий рівень серйозності або виникнення, помножений на оцінку виявлення 10, дає високий RPN. Критичність не включає оцінку виявлення, тому єдина причина з середніми та високими оцінками як для оцінок серйозності, так і для найвищих показників: «Без грошей». Команда повинна використовувати свій досвід і судження, щоб правильно визначити пріоритети дій [18].

2.6 Метод оцінки ризику «аналіз причин»

Організація може багато чого навчитися зі своїх минулих успіхів і невдач. Уроки можуть допомогти їм покращити якість і ефективність їхніх процесів і систем, а також оптимізувати їх контроль.

Організації виграють від послідовних і систематичних підходів до отримання уроків з успіхів і невдач. Цей підхід називається аналізом причин. Принципи цього підходу наступні:

- організації вчаться на успіхах так само багато, як і на невдачах;
- перш ніж шукати рішення, ми повинні визначити проблему;
- важливо зрозуміти причини, перш ніж підсумовувати уроки, які ми засвоїли;
- заходи повинні вести до поліпшення організації.

Аналіз причин є ключовим інструментом управління ризиками. У той час як оцінку ризику можна розглядати як заглядання вперед і планування на

майбутнє, хороший аналіз причини полягає в застосуванні ретроспективних даних і вивчення минулого. Ми можемо багато чого навчитися з минулих успіхів і невдач, щоб покращити якість і ефективність наших процесів і систем [19].

У процесі управління ризиками аналіз причини є частиною етапу моніторингу та перевірки. Цей крок підтримує реєстр ризиків, ризики, засоби контролю та плани вирішення ризиків в актуальному стані. Частково це досягається шляхом аналізу основних причин критичних успіхів і невдач, а потім застосування цих уроків для подальшого усунення пов’язаних ризиків.

Відповідним методом аналізу причини є процес:

- це відповідає визнаній системі;
- це визначає не лише прямі причини, але й приховані та основні причини;
- це прозоро, залучає відповідних зацікавлених сторін і є кооперативним;
- де фіксуються результати;
- де ідентифікуються та записуються отримані уроки.

Там, де узгоджені дії для усунення причин і призводять до покращення бізнесу.

Broadleaf надає незалежні послуги з проведення аналізу причини. Який би інструмент ми не обрали, ми завжди дотримуємося шести етапного підходу, показаного на рис. 2.2, щоб узгодити цілі, визначити успіхи та невдачі, провести аналіз і застосувати отримані уроки та виконати необхідні дії [19].

Рисунок 2.2 – Шестиступінчастий процес вивчення уроків

Зазвичай ми використовуємо методи «Риб’яча кістка», або методи причинно-наслідкових зв’язків, описані нижче. Однак ми також можемо виконувати аналізи за допомогою інших підходів, таких як MORT або TapRoot, або шляхом розробки дерев несправностей.

Аналіз риб'ячої кістки. Цей підхід дозволяє віднести кілька можливих причин до однієї події. Це допомагає впорядковано класифікувати численні потенційні причини подій і визначити основні причини. Таким чином, для певного успіху чи невдачі можна створити діаграму, щоб визначити й упорядкувати можливі причини [20].

Використовується наступна форма аналізу:

– де, здається, існуючий простий причинно-наслідковий зв’язок;
– де зберігаються дані та факти та подаються на схемі;
– для виконання простого аналізу системи та її продуктивності;
– де безперервна презентація уроку як частина управління ризиками проекту під час реалізації проекту;

– як ефективний комунікаційний засіб для представлення простої причинно-наслідкової інформації іншим.

Щоб аналіз був найбільш ефективним, потрібен навчений фасилітатор, зокрема, щоб допомогти учасникам згрупувати та засвоїти подібні причини та перейти до визначення уроків і завдань щодо покращення.

Ми не використовуємо цей метод:

– для складних систем, процесів і подій з багатьма потенційними та взаємопов’язаними причинами;

– для успіхів і невдач, де виправданий дуже ретельний аналіз величини прибутку чи втрати.

Приклад такої форми аналізу, виконаного для клієнта, показано на рисунку 2.3 [20].

Рисунок 2.3 – Діаграма «Риб’ячої кістки» для успіху

Аналіз причин і наслідків. Ми використовуємо аналіз причин і наслідків, коли потрібне більш ретельне дослідження подій, ніж це можливо за допомогою аналізу риб’ячої кістки. Оскільки він не є нормативним і базується на методології та наборі правил, ми вважаємо його універсальним для всіх проблем, систем і ситуацій.

Даний метод використовується:

– для всіх подій, як успіхів, так і невдач;

- коли задіяний комплекс причин;
- коли справжні причини не ясні, що часто буває.

Ми не використовуємо аналіз причин і наслідків, коли потрібно зіставити лише відомі та непов’язані причини, тоді як аналіз риб’ячої кістки буде більш доцільнішим [21].

Висновки до другого розділу

У цьому розділі розглянуто теоретичні методи оцінки ризиків. Підібрано основні методи оцінки ризиків та розглянуто метод Delphi, призначений для збору експертних думок шляхом багатораундового опитування з контрольованим зв’язком між окремими раундами. Метод попереднього аналізу небезпек (PHA), що зазвичай є першою спробою в процесі безпеки системи ідентифікувати та класифікувати небезпеки або потенційні небезпеки в роботі запропонованої асоціації систем, процесів або процедур. HAZOP, структурований і систематичний метод тестування системи та управління ризиками. Метод SWIFT, який використовує структурований мозковий штурм під час фасилітованого семінару, поєднуючи заздалегідь визначений набір ключових слів із підказками учасників. Метод «Аналіз режимів і наслідків відмови» (FMEA), простий підхід до виявлення всіх можливих дефектів у проекті, процесі виробництва чи складання, продукті чи послузі. Розглянуті методи дозволили визначити основні особливості оцінки ризиків і на основі вибраних методів побудована стратегія оцінки ризиків для IoT.

3 ОЦІНКА РИЗИКІВ БЕЗПЕКИ В СИСТЕМАХ IOT

Процес оцінки ризиків (RAP) передбачає визначення ризиків, пов’язаних з усіма активами в організації, включаючи оцінку ризику та визначення пріоритетів. Оцінка ризику є центральною частиною процесу управління ризиком, оскільки це фундаментальний крок у обробці ризику. Імовірність атаки та вплив атаки є одними з характеристик, які враховуються при оцінці ризику. Існують рекомендації NIST щодо впровадження процесу оцінки ризику. Управління ризиком включає (а) прийняття ризику, коли він нижчий за безпечний рівень (прийняття ризику), (б) пом’якшення ризику шляхом застосування заходів безпеки, (в) передачу ризику або (г) уникнення ризику шляхом усунення сам постраждалий актив [21].

Наразі використовуються деякі популярні рамки RAP, такі як NIST, ISO/IEC і OCTAVE. Кожен метод оцінки ризику має свої унікальні аспекти. Двома критичними аспектами, пов’язаними з вимірюванням ризику, є (а) тип підходу та (б) методологія, що використовується для вимірювання ризику. Тут ми намагаємося вивчити деякі існуючі RAP, конкретну методологію, застосовану кожним RAP, і їх придатність для оцінки ризиків IoT. Існують якісні та кількісні підходи до вимірювання кіберризиків організації.

3.1 Якісні підходи до оцінки ризиків Інтернет-речей

3.1.1 NIST

Існують якісні та кількісні підходи до вимірювання кіберризиків організації. Рамки Національного інституту стандартів і технологій (NIST) добре задокументовані та містять вказівки щодо оцінки ризиків та впровадження управління, але немає моделі, на яку можна було б посилатися. NIST не включає модель оцінки впливу IoT і оцінює ризики

якісно. Організації цілком можуть вибрати структуру NIST для планування аварій та відновлення. Однак NIST має особливі міркування щодо управління ризиками IoT. NIST IR 8228 документує потенційні проблеми, пов'язані з пристроями Інтернету речей, і міркування щодо ризиків у забезпеченні безпеки пристроїв і даних [22].

25 червня 2019 року NIST опублікував NISTIR 8228, міркування щодо управління ризиками кібербезпеки та конфіденційності Інтернету речей (IoT). У цьому документі розглянуто три загальні міркування, пов'язані з ризиками безпеки та конфіденційності Інтернету речей, і визначено три цілі пом'якшення:

Міркування. Ці міркування ілюструють, чим пристрої IoT відрізняються від традиційних IT-пристроїв.

Примітка 1. Багато пристроїв IoT взаємодіють із фізичним світом так, як традиційні IT-пристрої зазвичай не взаємодіють.

Примітка 2: до багатьох пристроїв IoT неможливо отримати доступ, керувати ними або контролювати їх так само, як до традиційних IT-пристроїв.

Примітка 3. Доступність, ефективність і дієвість функцій кібербезпеки та захисту даних для пристроїв IoT часто відрізняються від традиційних IT-пристроїв.

Цілі зменшення ризику. Ці цілі зменшення ризику є адитивними, при цьому кожна ціль спирається на попередню, не замінюючи її.

- Ціль 1: Захистити безпеку пристрою.
- Ціль 2: Захист безпеки даних.
- Ціль 3: Захист приватного життя особи.

Спираючись на вказівки в NISTIR 8228, 29 травня 2020 року NIST опублікував два міжвідомчі звіти, спрямовані на надання вказівок виробникам пристроїв IoT:

NISTIR 8259, Основні дії з кібербезпеки для виробників Інтернету речей, рекомендує виробникам Інтернету речей виконати чотири дії до виходу на ринок (1-4) і дві дії після виходу на ринок (5-6) для вирішення проблем кібербезпеки в пристроях Інтернету речей.

- Дія 1: Визначте очікуваних клієнтів і визначте очікувані випадки використання.
- Дія 2: Дослідіть цілі клієнтів щодо кібербезпеки.
- Дія 3: Визначте, як досягти цілей клієнтів.
- Дія 4: Плануйте відповідну підтримку для цілей клієнта.
- Дія 5: Визначити підходи до спілкування з клієнтами.
- Дія 6: Вирішіть, що і як спілкуватися з клієнтами.

NISTIR 8259A, Базовий рівень можливостей кібербезпеки пристроїв Інтернету речей, надає шість можливостей, які перехресно посилаються на відповідні галузеві та федеральні стандарти як стандарт для мінімально захищених пристроїв Інтернету речей [22].

Ідентифікація пристрою: пристрій IoT можна однозначно ідентифікувати логічно та фізично.

Конфігурація пристрою: конфігурацію програмного забезпечення пристрою IoT можна змінити, і такі зміни можуть вносити лише авторизовані сторони.

Конфіденційність: пристрій IoT може захистити дані, які він зберігає та передає, від несанкціонованого доступу та модифікації.

Логічний доступ до інтерфейсів: пристрій IoT може обмежити логічний доступ до своїх локальних і мережевих інтерфейсів, а також протоколів і служб, які використовуються цими інтерфейсами, для авторизованих об’єктів.

Оновлення програмного забезпечення: програмне забезпечення пристрою IoT може оновлюватися лише авторизованими сторонами за допомогою безпечного та настроюваного механізму.

Обізнаність про стан кібербезпеки: пристрій IoT може звітувати про свій стан кібербезпеки та надавати цю інформацію лише авторизованим особам [22].

Нові публікації на IoT від NIST.

15 грудня 2020 року NIST випустив проекти спеціальних документів і три додаткові міжвідомчі звіти для розширення свого каталогу вказівок щодо Інтернету речей. Ці проекти випуску відкриті для громадського обговорення до 12 лютого 2020 року.

NIST SP 800-213, Інструкції з кібербезпеки пристроїв Інтернету речей для федерального уряду: встановлення вимог до кібербезпеки пристроїв Інтернету речей, надає проекти вказівок для федеральних агентств, які слід враховувати під час інтеграції пристроїв Інтернету речей у федеральні системи. Він базується на NISTIR 8228, розширює серію NISTIR 8259 і консолідує інструкції з безпеки NIST IoT, які застосовуються до федеральних агентств і будівель. Він також посилається на існуючі вказівки, такі як NIST 800-30 і NIST 800-53.

NISTIR 8259B, IoT Non-Technical Support Capability Core Baseline надає додаткові можливості нетехнічної підтримки, які доповнюють можливості, надані в NISTIR 8259A.

Документація: здатність виробника та/або суб’єкта підтримки створювати, збирати та зберігати інформацію, пов’язану з кібербезпекою пристрою IoT протягом усього процесу розробки пристрою та його подальшого життєвого циклу.

Отримання: можливість виробника та/або суб’єкта підтримки отримувати інформацію та запити від клієнта щодо кібербезпеки пристрою IoT.

Розповсюдження інформації: здатність виробника та/або суб’єкта підтримки поширювати та поширювати інформацію, пов’язану з кібербезпекою пристрою IoT.

Навчання та обізнаність: здатність виробника та/або суб'єкта підтримки підвищувати обізнаність клієнтів і клієнтів про інформацію, пов'язану з кібербезпекою, міркування, можливості тощо пристрою IoT [23].

NISTIR 8259C, Створення профілю з використанням базової лінії IoT Core і Non-Technical Baseline, представляє метод профілювання можливостей NISTIR 8259A та 8259B з використанням трьох ключових концепцій: (1) орієнтація на пристрій, (2) фокус на кібербезпеці та (3) мінімальне резервне копіювання здатність. Він також розглядає застосування інших зовнішніх вихідних документів, таких як вимоги безпеки або рамки, щоб створити більш налаштований і детальний профіль безпеки для пристроїв IoT у певному секторі або випадку використання [23].

NISTIR 8259D, Профіль з використанням основного базового рівня Інтернету речей і нетехнічного базового рівня для федерального уряду. Цей документ містить профіль можливостей пристроїв IoT, необхідних для інтеграції цих пристроїв у федеральну інформаційну систему, яка реалізує низькі базові засоби контролю NIST SP 800-30. Він використовує профільний метод NISTIR 8259C і можливості NISTIR 8259A та 8259B. Результатом є профіль, який зіставляє бажані можливості пристрою IoT з можливими елементами керування NIST 800-53 і надає додаткові відомості про ключові можливості, які пристрої IoT повинні надавати для підтримки цих елементів керування.

3.1.2 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – ще одна структура якісної оцінки ризику, яка пропонує вісім кроків. Ці кроки включають:

- встановлення критеріїв вимірювання ризику;
- розробку профілів активів;
- ідентифікацію контейнерів активів;

- визначення постраждалих територій;
- визначення схем загроз;
- визначення ризиків;
- дослідження ризиків;
- зменшення ризиків.

Операційно критична оцінка загроз, активів і вразливостей (OCTAVE) – це структура, яка використовується для оцінки середовища організації та визначення IT-ризиків. Оскільки OCTAVE є гнучким, його можна налаштувати відповідно до потреб практично будь-якої організації, вимагаючи лише невеликої групи експертів з кібербезпеки, IT та операцій для спільної роботи над цим завданням [24].

Застосовуючи структуру OCTAVE до організації, важливо розуміти, що стандартна модель не завжди підходить організації. Через це було розроблено кілька варіантів, зокрема OCTAVE-S (використовується, коли вся команда вже має глибокі знання про середовище організації), OCTAVE Allegro (який є простішим і краще підходить для невеликих команд) і OCTAVE Forte (найбільш адаптована варіація ще). Ви також можете застосувати гібридний підхід, щоб знайти те, що найкраще підходить для вашого бізнесу.

Незалежно від того, який варіант OCTAVE ви використовуєте, ви можете бути впевнені, що він був розроблений для Міністерства оборони США в Університеті Карнегі-Меллона (CMU) у 2001 році та випробуваний протягом понад двадцяти років.

Переваги моделі загроз OCTAVE.

Використання моделі загроз OCTAVE має низку переваг, але ось основні з них:

Ефективність: OCTAVE зосереджується на найважливіших активах організації, забезпечуючи досягнення найкращих результатів із найменшими зусиллями.

Швидкість: незважаючи на те, що модель OCTAVE складна, вона є однією з найефективніших для виявлення, пріоритезації та пом’якшення ризиків, що робить її одночасно швидкою та ретельною.

Дійсний: негайна реалізація моделі загроз OCTAVE може бути виснажливою, оскільки вона розроблена для реалізації частинами. Через це він розділений на три фази, кожна з яких розбивається на процеси [24].

Комплексність: найбільша перевага моделі загроз OCTAVE полягає в тому, наскільки вона охоплює. З цієї причини він використовується Міністерством оборони та незліченною кількістю інших організацій уже більше двох десятиліть.

Загалом, впровадження моделі загроз OCTAVE вимагає трифазного підходу. Три фази такі:

Створіть профіль усіх своїх активів і відповідних загроз. Для цього потрібна команда, яка сідає та аналізує IT-активи вашої організації та те, що вже робиться для їх захисту. Ви можете знайти прогалини в поточних заходах безпеки та визначити відповідні ризики.

Визначте слабкі місця в інфраструктурі вашої компанії. Після того, як ваша команда виявила вразливі місця, ви повинні рухатися вперед із новими політиками та процедурами для їх усунення та керування ними. На цьому етапі необхідно застосувати кілька тактик, включаючи тестування на проникнення.

Визначте стратегію управління ризиками безпеки. На останньому етапі впровадження ви повинні визначити та визначити пріоритетність ризиків, що залишилися, і приступити до створення довгострокового плану пом’якшення ризиків безпеки та управління ними. Цей план потрібно часто переглядати та коригувати.

На папері це може здатися дуже простим. Однак аналіз, розробка стратегії та реалізація такої комплексної структури займає багато часу. Чи знадобляться на це тижні чи місяці, залежить від розміру вашої команди,

складності вашої організації, чи хтось добре знайомий зі структурою та/або архітектурою вашої організації, щоб очолити ініціативу [24].

Загальні методи використання.

На кожному етапі процесу впровадження ваша команда має бути готова використовувати різноманітні інструменти та методології тестування та аналізу, щоб гарантувати, що жоден камінь на камені не залишиться без уваги та жоден сценарій не залишиться без уваги. Тому ось деякі з поширених прийомів, з якими ви повинні ознайомитися:

Системні аудити розкривають інформацію про структуру мережі та систем вашої компанії. Це показує, де зберігаються активи, як вони підключені та хто до чого має доступ.

Тестування на проникнення допомагає вашій команді виявити вразливі місця в їхній системі та краще зрозуміти точки доступу, які потрібно захистити, закладаючи основу для багатьох знань, які необхідно виявити для успішного впровадження OCTAVE.

Оцінка ризиків виконується майже на кожному етапі процесу реалізації та потребує детального плану, який визначає пріоритетність кожного ризику та окреслює стратегії пом’якшення та запобігання.

Оскільки модель загроз OCTAVE є найбільш широко використовуваною в організаціях, більшість ваших співробітників з IT та кібербезпеки, швидше за все, уже використовують деякі або всі ці методи у своїх звичайних практиках аудиту та моніторингу. Для невеликих організацій, які не знайомі з цими методами, важливо досконало зрозуміти їх і як найкраще їх застосувати, перш ніж їх розгортати [24].

OCTAVE для IoT.

OCTAVE підходить для оцінки ризиків розумного дому, оскільки має контейнер активів для кібер- та фізичної безпеки. OCTAVE допомагає виявити різні прогалини в безпеці розумних будинків на основі IoT,

представляє ризики для мешканців і пропонує підходи для пом’якшення виявлених ризиків. OCTAVE розглядає чотири фази:

1. Встановлення етапу рушійної сили: на цьому етапі розробляються критерії вимірювання ризику, які формують основу для оцінки ризику;
2. Етап профілювання активів: на цьому етапі встановлюються обмеження активів і визначаються вимоги безпеки;
3. Етап визначення загрози: цей етап визначає загрози безпеці з боку активів, де зберігається, транспортується або обробляється інформаційний актив.
4. Етап зменшення ризику: на цьому етапі визначається та виконується стратегія зменшення ризику для ідентифікованих активів.

OCTAVE використовує стандартизовану анкету для класифікації часток ефекту відновлення та не визначає кількісного ризику.

3.1.3 TARA

TARA – це система прогнозування для найбільш важливих ризиків. TARA має три основні переваги. Він розбиває потенційні атаки на керований список ймовірних атак. Він покращує якість оцінювання ризиків і контролю, а також повідомляє про ризики та рекомендації організації. Це може покращити результати, зменшити накладні витрати на аналіз ризиків і допомогти прийняти кращі рішення. Він був розроблений для великого, дуже цінного та різноманітного середовища Intel(R) у відповідь на потребу оцінити ризики безпеці дуже складного середовища загроз, що швидко розвивається. TARA не визначає кількісного впливу ризику та не сприяє захисту від вразливості. У більшості випадків TARA використовується в поєднанні з інфраструктурою NIST, і тут також можна застосувати міркування NIST щодо IoT [25].

Аналіз загроз і оцінка ризиків (часто званий TARA) (рис. 3.1) є ключовими видами діяльності, визначеними ISO/SAE 21434. Багато різних методологій оцінки ризиків було описано як академічним середовищем, так і промисловістю, і більшість (якщо не всі) з них можна реалізувати за допомогою Security Analyst. Робочий процес, описаний нижче, натхненний MoRA (модульна оцінка ризиків). MoRA було розроблено в Fraunhofer AISEC (Інститут прикладної та комплексної безпеки Фраунгофера). Інші популярні підходи часто базуються на деревах атак, які можна використовувати в поєднанні з MoRA або окремо.

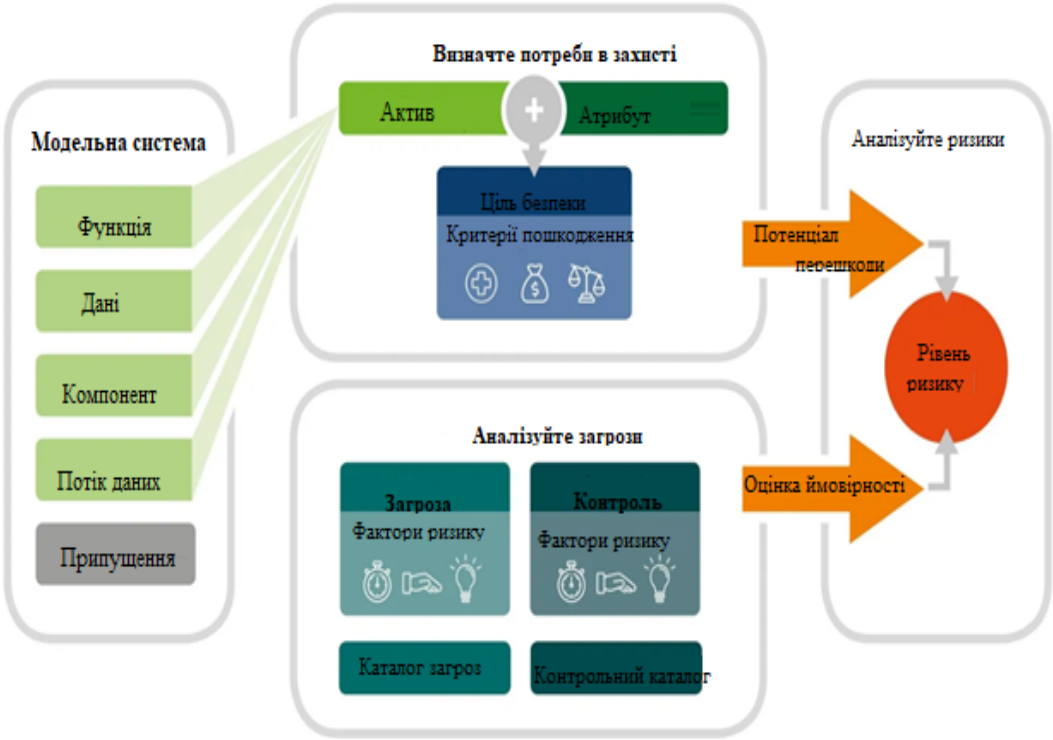

Рисунок 3.1 – Загальний процес аналізу загроз та метод оцінки ризиків (TARA)

Важливо, щоб метод масштабувався залежно від статусу процесу розробки, щоб безпечне проектування системи було можливим із самого початку (безпека за проектом), але також можна було використовувати для існуючих і детальних систем. Це менш складно, якщо досягнуто чіткого

розділення оцінки впливу та оцінки загрози. Модель системи, що оцінюється, є дуже корисною, оскільки вона може служити автономною сутністю, яка пов’язує все разом. Це необхідно для визначення ризику, який визначається як комбінація потенційної шкоди (результат оцінки впливу) та ймовірності виникнення (результат оцінки ризику) [25].

Модель системи. На першому кроці потрібно зібрати або імпортувати дані про систему, що розробляється (SUD) або ціль оцінки (ToE). Основними одиницями моделювання є функції, компоненти, дані та потоки даних. Функції описують функціональні можливості системи. Компоненти представляють обладнання або учасників зв'язку. Дані – це будь-яка інформація, яка зберігається в компонентах або передається між ними. Фактичне спілкування фіксується потоками даних. Крім того, моделюються зв’язки між функціями та іншими сутностями («відображення функцій»).

Зауважте, що ISO21434 називає це визначенням елемента та розглядає це як крок перед виконанням TARA. Однак ми виявили, що це необхідна частина будь-якої TARA, і тому хотіли б бачити це як перший крок у цьому процесі.

Визнати потребу в захисті. Будь-який із системних елементів, описаних вище, може стати активом, якщо пов’язати його з атрибутом безпеки, таким як конфіденційність, цілісність або доступність, напр. «Конфіденційність персональних даних». Це фіксується метою безпеки. Для кожної цілі безпеки необхідно оцінити вплив. Це робиться на основі критеріїв пошкодження. Критеріями можливої шкоди є безпека, фінансові втрати, правові наслідки або втрата репутації. Це призводить до потенційної шкоди. ISO21434 називає це ідентифікацією активів, ідентифікацією сценарію загрози та оцінкою впливу.

Аналіз загрози. Загрози та можливі засоби контролю слід аналізувати за допомогою каталогів відомих загроз або вразливостей і контрзаходів. Виявлені загрози пов’язані з компонентами або потоками даних. Загрози

оцінюються на основі факторів ризику, таких як час, доступ, знання та обладнання. Це призводить до оцінки ймовірності. ISO21434 називає це аналізом шляху атаки та рейтингом здійсненності атаки [25].

Аналіз ризиків. На основі моделі системи можна розрахувати, як можуть бути загрози цілям безпеки. Рівень ризику можна розрахувати, якщо оцінена ймовірність загрози збігається з впливом (потенційним збитком) цілі безпеки. Ми називаємо це відтворенням. Потім ці ризики можна проаналізувати та впоратися з ними належним чином (наприклад, шляхом пом'якшення чи уникнення) або прийняти. ISO21434 назвав ці дії визначенням ризику та рішенням щодо запобігання ризику.

Зменшення ризиків за допомогою засобів контролю. Знання рівнів ризику існуючої системи дає можливість виявити неприйнятні ризики. Неприйнятними є ризики з високим потенціалом шкоди та низьким оціненим зусиллям атаки. Щоб приймати обґрунтовані рішення щодо запобігання ризиків, аналітики безпеки повинні знайти ефективні засоби контролю, які зменшують потенціал збитку (наприклад, страхування, яке зменшує фінансовий збиток) або збільшують зусилля, необхідні для атаки (наприклад, шифрування для посилення конфіденційності).

Однак сам контроль також вводить деякі активи, які потрібно захистити, наприклад в ключ шифрування. Як наслідок, активи, введені разом із контролем, також повинні бути піддані ідентифікації потреб захисту (наприклад, конфіденційність ключа), аналізу загроз і шляхів атак (наприклад, вилучення спільного ключа з іншого пристрою) і аналіз ризиків. Включення елементів керування в аналіз робить TARA ітераційним процесом: аналітики безпеки повертаються до моделювання елементів керування та оцінюють свої результати, доки не знайдуть конфігурацію елементів керування, яка виглядає задовільною [25].

Засоби керування на етапі концепції називаються «вимогами до кібербезпеки», а їх спільні активи (наприклад, конфіденційність ключа) не

розглядаються в TARA ISO21434. Лише на етапі розробки елементи керування виводяться на основі заданих вимог до кібербезпеки, на цьому пізньому етапі вони повинні виконувати той самий цикл, який ми описали тут.

3.2. Кількісні підходи до оцінки ризиків IoT

FAIR. FAIR, скорочення від Factor Analysis of Information Risk, – це методологія кількісного визначення ризику, розроблена для того, щоб допомогти організаціям оцінити інформаційний ризик. FAIR – це єдина міжнародна стандартизована структура кількісної моделі, яка забезпечує операційний ризик та інформаційну безпеку. Ця методологія приносить велику користь зрілим організаціям, які використовують рішення з інтегрованого управління ризиками (IRM).

Основною метою FAIR є підтримка існуючої структури організації та стратегії управління ризиками.

FAIR проти традиційних методів кількісного визначення ризику.

Щоб побачити, чим FAIR відрізняється від інших фреймворків, ми повинні розуміти, що FAIR не є фреймворком кібербезпеки, як NIST CSF. Його не можна використовувати як структуру, але це додаткова методологія, яка працює разом із структурами, такими як NIST, ISO 2700x та іншими структурами галузевого стандарту [25].

З часом в організаціях виникають прогалини у відповідності, і стандартні структури не можуть передбачити ризики, пов’язані з цими прогалинами. Методологія FAIR визначає ризики організації, допомагає організаціям ефективно використовувати свої ресурси для створення прогалин у ризиках, пов’язаних із прийняттям рішень, і масштабує рівні загрози, функції, якої бракує більшості фреймворків.

Оскільки організації переходять від підходу, заснованого на дотриманні вимог, до підходу, що ґрунтується на оцінці ризику, їм потрібна методологія кількісного визначення ризику для підтримки цього переходу. FAIR не тільки підтримує цю зміну на практиці, але й сприяє підвищенню кіберінтересу серед членів правління та нетехнічних керівників. Методологія FAIR унікальна тим, що вона переводить ризики збитків організації у фінансові терміни та дозволяє покращити комунікацію між технічними командами та нетехнічними членами та вищим керівництвом.

На відміну від FAIR, застарілі моделі кількісної оцінки ризиків у тестах на проникнення працюють без внутрішніх знань цільової системи. Тестери не знають про код і конструкції, які не є загальнодоступними.

Ця форма тестування дозволяє тестувальникам визначити ризики та вразливі місця в системі, але тестування чорної скриньки не може визначити фінансовий вплив ризику. Крім того, з обмеженими знаннями тест не може визначити всі загрози та вразливі місця всіх організаційних моделей.

Порівняно із застарілими методами або тестуванням чорної скриньки, FAIR – це метод «скляної скриньки», який надає керівникам уявлення про досягнення показників.

Незважаючи на величезні переваги, широке охоплення безпеки та чудову ідентифікацію рівня загрози, структура FAIR є недосконалою. Деякі загальні недоліки:

− FAIR порівняно складно використовувати, оскільки немає спеціальної чи визначеної документації щодо його методів.

− FAIR не може самостійно оцінювати ризики. Це додаткова методологія, яка покращує оцінку ризиків шляхом координації з іншими структурами.

− FAIR покладається насамперед на ймовірність; Хоча ці ймовірності не є необґрунтованими, вони не зовсім точні через різноманітний характер кібератак та їхньої шкоди.

3.3. Методика оцінки ризиків кібербезпеки в системах Інтернет-речей

Дійсно, очевидно, що неможливо побудувати ідеальну систему оцінки ризиків для пристроїв IoT, якщо вектори ризику або атрибути ризику не визначені. На додаток до вихідних векторів ризику від традиційних систем, спеціальні вектори IoT також повинні бути прийняті до уваги для системи оцінки ризиків IoT.

Резюме оцінки ризиків IoT. Було визначено чотири типи класів векторів ризику IoT: орієнтовані на хмару, орієнтовані на реальний час, автономні та орієнтовані на відновлення. У таблиці 3.1 нижче наведено список векторів ризику IoT для кожного з цих класів, які використовуються для оцінки ризику для кожної системи IoT.

Таблиця 3.1 – Список векторів ризику IoT

С. №	Пов'язані з хмарою	Реальний час	Автономний	Відновлення
1	Платформи хмарних обчислень	Оперативні моделі в реальному часі	Автоматизовані середовища	Економічний ефект
2	Навички хмарних технологій	Індивідуальні продукти	Робототехніка та автономні системи	Оцінка впливу
3	Хмарні центри обробки даних	Платформа для отримання інформації в реальному часі	Робототехніка та штучний інтелект	SWOT-аналіз (сила, слабкість, можливості, загроза).
4	Хмарне	Цифрові записи	Робототехніка в	Фінансово-

С. №	Пов'язані з хмарою	Реальний час	Автономний	Відновлення
	програмне забезпечення	реального часу та сумісні записи	IoT	податковий державний контроль
5	Хмарний моніторинг	Кіберфізичні системи	Штучний інтелект і системи управління	N/A
6	Інтеграція в хмарні обчислення	N/A	N/A	N/A
7	Хмарні мережі безпеки	N/A	N/A	N/A

Шкала та ранжування оцінки ризику.Першим кроком в оцінці ризику є визначення загроз для активу IoT, що розглядається, з наступним визначенням внутрішнього ризику та його впливу. Вплив ризику має такі оцінки, як високий, середній і низький.

Наприклад, «високий» рейтинг впливу означає, що вплив може бути суттєвим. Середній означає, що вплив буде шкідливим, але його можна відновити та/або є незручним. Низький означає, що вплив буде мінімальним або взагалі відсутнім. Наступним кроком є визначення ймовірності даного експлойту з урахуванням середовища контролю, яке має ваша організація. Приклади рейтингів вірогідності:

1. Високий – джерело загрози має високу мотивацію та достатньо спроможність, а засоби контролю для запобігання використанню вразливості неефективні.

2. Середній – джерело загрози вмотивоване та спроможне, але існують засоби контролю, які можуть перешкодити успішному використанню вразливості.

3. Низький – джерело загрози не має мотивації чи можливостей, або існують засоби контролю, щоб запобігти або, принаймні, значно перешкодити використанню вразливості.

Рейтинг ризику можна розрахувати як рейтинг ризику (rr) = вплив (якщо використовується) × ймовірність (експлойту).

Деякі приклади рейтингу ризику:

1. Серйозний – існує значна та термінова загроза для організації, і усунення ризику повинно бути негайним.

2. Підвищений – існує життєздатна загроза для організації, і усунення ризику має бути завершено в розумний період часу.

3. Низький – загрози є нормальними і загалом прийнятними, але все ж можуть мати певний вплив на організацію. Впровадження додаткових удосконалень безпеки може забезпечити додатковий захист від потенційних або непередбачених наразі загроз.

Розрахунок рангу ризику виконується на основі кількісного зважування (це стосується впливу ризику) та оцінки ризику (це стосується ймовірності ризику), як пояснено вище.

Таблиця 3.2 показує, як можна зробити ранжирування для кожного ризику. Якщо ранг ризику дуже високий, то ризик має серйозний вплив. Існує п’ять рівнів ризиків IoT на основі розрахунку рангу. Існують ризики з рангом ≤ 10, і ці ризики належать до дуже низького рівня, оскільки вони не варті розгляду. Необхідно враховувати низькі та помірні ризики. Високі та

дуже високі ризики потребують кращого запобігання, оскільки їхній вплив є сильним.

Таблиця 3.3 показує рейтинг ризику для деяких векторів IoT. Згідно з документом NIST-IoT, ці одиничні вектори належать до категорії «захист пристрою». Як згадувалося, інші дві категорії – це захист даних і особиста конфіденційність. Захист пристрою включає чотири сфери зниження ризиків, включаючи управління активами, керування вразливістю, керування доступом і виявлення інцидентів.

Управління активами: для підтримки точної інвентаризації всіх пристроїв IoT та їхніх відповідних характеристик, що допомагає використовувати цю інформацію для цілей управління ризиками кібербезпеки та конфіденційності.

Управління вразливістю: для виявлення та усунення відомих уразливостей у програмному забезпеченні та мікропрограмі пристроїв Інтернету речей, щоб зменшити ймовірність і полегшити використання та компрометацію.

Таблиця 3.2 – Ранжирування для кожного ризику

Якісний рівень	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг $= W \times S$ (показані приклади)	Діапазон рангів ризику	опис
Дуже високо	96–100	1.0	97×1,0=97	81–100	Ризик викликає дуже велике занепокоєння; сильний вплив
Високий	80–95	0,8	90×0,8=72	51–80	Ризик викликає велике занепокоєння

Якісний рівень	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг = $W \times S$ (показані приклади)	Діапазон рангів ризику	опис
Середній	31–79	0,5	50×0,5=25	21–50	Ризик викликає помірне занепокоєння
Низький	11–30	0,2	25×0,2=5	5–20	Ризик не викликає занепокоєння
Дуже низько	0–10	0,1	10×0,1=1	0–4	Ризик не викликає занепокоєння

Управління вразливістю: для виявлення та усунення відомих уразливостей у програмному забезпеченні та мікропрограмі пристроїв Інтернету речей, щоб зменшити ймовірність і полегшити використання та компрометацію.

Керування доступом: для запобігання несанкціонованому та неправильному фізичному та логічному доступу людей, процесів та інших комп’ютерних пристроїв до пристроїв IoT.

Виявлення інцидентів безпеки пристрою: для моніторингу й аналізу активності пристроїв Інтернету речей на ознаки інцидентів безпеки пристрою.

Виявлення вразливості активів є одним із найважливіших кроків у процесі оцінки ризиків. Пристрої IoT є основними активами, які тут розглядаються. Приклади векторів Інтернету речей і їх обчислення показників ризику наведено в таблиці 3.3 для кожної з вищезазначених

областей зменшення ризику в категорії «Захист пристрою». Ідеальним наступним кроком є визначення загроз, а також впливу та ймовірності ризиків. Мета полягає в тому, щоб захистити пристрій IoT від атак, таких як атаки розподіленої відмови в обслуговуванні (DDoS), прослуховування мережевого трафіку або компрометації інших пристроїв у тому ж сегменті мережі. Як і в цьому прикладі, рейтинг можна розрахувати для ризиків у кожній категорії, включаючи безпеку даних і конфіденційність.

Таблиця 3.3 показує деталі рангу кожного одиничного вектора та наслідки рангу ризику. Наприклад, якщо пристрій IoT не підтримує використання надійних облікових даних, цьому вектору IoT надається вага 95 разом із оцінкою ризику 0,9, що обчислює рейтинг ризику як 85. Цей ранг має високий пріоритет через більшу ймовірність несанкціонованого доступу та підробки через неправильне використання облікових даних.

Таблиця 3.3 – Приклади векторів Інтернету речей і їх обчислення показників ризику

Вектор ризику IoT	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг $=W\times S$	Опис/наслідки
Пристрій IoT не має унікального вбудованого ідентифікатора	75	0,8	60 (середній)	Це впливає на віддалений доступ і керування вразливими місцями
Виробник не розкриває зовнішні залежності пристрою IoT	60	0,7	42 (середній)	Управління ризиком зовнішнього програмного забезпечення та послуг неможливе

Вектор ризику IoT	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг =$W \times S$	Опис/наслідки
Патчі або оновлення для пристрою IoT виробник не випускає	50	0,6	30 (низький)	Відомі вразливості неможливо видалити
Пристрій IoT не може мати виправлення чи оновлення програмного забезпечення	60	0,6	36 (середній)	Відомі вразливості неможливо видалити
Немає сканера вразливостей, який може працювати на пристрої IoT або проти нього	60	0,6	36 (середній)	Неможливо автоматично визначити відомі вразливості
Пристрій IoT не підтримує приховування відображених символів пароля	80	0,7	56 (середній)	Збільшує ймовірність крадіжки облікових даних
Пристрій IoT не підтримує надійні криптографічні маркери облікових даних або багатофакторну автентифікацію)	95	0,9	85 (високий)	Можливе підроблення через неправильне використання облікових даних
Пристрій IoT не підтримує корпоративну систему автентифікації користувачів	90	0,8	72 (середній)	Кожен користувач потребує більше облікових даних
Пристрій IoT не може реєструвати свої робочі події та	70	0,6	42 (середні	Імовірність виявлення зловмисних дій значно

Вектор ризику IoT	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг =$W \times S$	Опис/наслідки
події безпеки			й)	менша

Висновки до третього розділу

В цьому розділі представлено критичний аналіз інфраструктури оцінки ризиків кібербезпеки, придатної для систем IoT. Детально розглянуті якісні системи ризиків, а саме NIST, OCTAVE, TARA та кількісний метод FAIR. Розглядаються ризики IoT цих інфраструктур разом з їхніми сильними та слабкими сторонами, а також напрямками. Наведено короткий виклад оцінки ризиків IoT разом із системою оцінки ризиків, яка підходить для домену IoT, щоб підкреслити кількісний підхід. Ранг ризику для вектора ризику IoT класифікує ризики на низькі, середні та високі категорії. Це дослідження було зосереджено на ширшому домені IoT. Досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

ВИСНОВКИ

Дипломна робота присвячена методам захисту даних і пристроїв Інтернету речей для побудованої системи IoT. Були досягнуті такі результати:

1. Проведено аналіз основних вимог щодо безпеки IoT, що дозволив сформувати особливості побудов систем IoT.

2. Досліджено способи виявлення наявних вразливостей IoT-пристроїв, які дозволили виділити найбільш вразливі місця IoT

3. Досліджено основні теоретичні методи оцінки ризиків, які дозволили підібрати методи найбільш ефективні для виявлення вразливостей IoT.

4. Проаналізовані якісні підходи до оцінки ризиків IoT, що дозволили виділити вразливості для яких вони будуть найбільш ефективні.

5. Проаналізовані кількісні підходи до оцінки ризиків IoT, та виділено ризики до яких такі підходи будуть більш ефективні

6. Розроблено методику оцінки ризиків кібербезпеки в системах інтернет-речей, в якій враховано приклади векторів Інтернету речей і проведено обчислення їх показників ризику, що можуть успішно застосовуватися при реалізації комунікаційних і інформаційних системах, що отримали у своє розпорядження нові пристрої для Інтернету речей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gross G. 9 Key Big Data Security Issues [Electronic resource] / G. Gross // Alien Vault. – 2016. – Access: https://www.alienvault.com/ blogs/securityessentials/9-key-big-data-security-issues.

2. Взлом Tesla [Электронный ресурс] // Kaspersky Lab. – 2017. – Режим доступа: https://www.kaspersky.ru/blog/hacking-tesla-model-x/18169/.

3. Toms L. 5 Common Cyber Attacks in the IoT – Threat Alert on a Grand Scale [Electronic resource] / L.Toms // Global Sign. – 2016. – Access: https://www.globalsign.com/en/ blog/five-common-cyber-attacks-in-the-iot/.

4. Loukas G. Cyber-Physical Attacks: A Growing Invisible Threat / G. Loukas. – MA, USA: Butterworth-Heinemann Newton. – 2015. – 270 p.

5. Тадтаев Г. Холодильник атакует: как киберпреступники используют бытовую технику [Электронный ресурс] / Г. Тадаєв // РБК. – 2016. – Режим доступа:
https://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff971. 107

6. Ализар А. Умный холодильник выдал хакерам пароль от Gmail [Электронний ресурс] / А. Ализар // Хакер. – 2015. – Режим доступа: https://xakep.ru/2015/08/25/ smart-fridge/.

7. Goodin D. Smart TV hack embeds attack code into broadcast signal—no access required [Electronic resource] / D. Gooodin // Arstechnica. – 2017. – Access: https://arstechnica.com/ information-technology/2017/03/smart-tv-hack-embedsattack-code-into-broadcast-signal-no-access-required/.

8. Internet of Things Top Ten [Electronic resource] // OWASP. – 2014. – Access: https://www.owasp.org/images/7/71/ Internet_of_Things_Top_Ten_2014-OWASP.pdf.

9. 2016 Trustwave Global Security Report [Electronic resource] // Trustwave. – 2016. – Access:

https://www.trustwave.com/Resources/Library/Documents/2016- Trustwave-Global-Security-Report/.

10. Атака через Inrternet: учебное пособие / [И.Д. Медведовский, А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков]. – СПб: НПО "Мир и семья-95", 1997. – 296 с.

11. SQL-инъекция [Электронный ресурс] // Национальная библиотека им. Н. Э. Баумана. – Режим доступа: https://ru.bmstu.wiki/SQL-инъекция.

12. Account lockout. Dicttionary [Electronic resource] // Computer Hope. – 2017. – Access: https://www.computerhope.com/jargon/a/accolock.htm.

13. Epp D. Credential Theft and How to Secure Credentials [Electronic resource] / D. Epp // Microsoft. – 2014. – Access: https://technet.microsoft.com/en_us/security/ dn920237.aspx.

14. Geer D. Securing risky network ports [Electronic resource] / D. Geer // CSO. – 2017. – Access: https://www.csoonline.com/article/3191531/networksecurity/securing-risky-network-ports.html.

15. Buffer Overflow [Electronic resource] // OWASP. – Access: https://www.owasp.org/index.php/Buffer_Overflow.

16. UPnP Device Architecture version 1.1 [Electronic resource] // UPnP Forum. – 2008. – Access: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecturev1.0.pdf.

17. Wisniewski C.UPnP flaws turn millions of firewalls into doorstops [Electronic resource] / C. Wisniewski // Naked Security. – 2013. – Access: https://nakedsecurity. sophos.com/ 2013/02/05/upnp-flaws-turn-millions-of-firewallsinto-doorstops/.

18. Hart J. NCSAM: Understanding UDP Amplification Vulnerabilities Through Rapid7 Research [Electronic resource] / J. Hart // RAPID7. – 2016. – Access: https://blog.rapid7.com/2016/10/31/understanding-udp-amplification-vulnerabilitiesthrough-rapid7-research/.

19. Атака “человек посередине” [Электронный ресурс] // Secure List. – Режим доступа: https://securelist.ru/threats/man-in-the-middle-attack-glossary/.

20. Zhao, Jinquan; Huang, Wenying; Fang, Zhaoxiong; Chen, Feng; Li, Kewen; Deng, Yong (2007-06-24). On-Line Voltage Stability Monitoring and Control (VSMC) System in Fujian power grid. 2007 IEEE Power Engineering Society General Meeting. Proceedings, Power Engineering Society General Meeting, 2007. (PDF) (Tampa, FL, USA: IEEE): 1. ISBN 1-4244-1296-X.

21. Карев А. Разбираем уязвимости проверки сертификатов SSL и TLS в небраузерном софте [Электронный ресурс] / А. Карев // Хакер. – 2018. – Режим доступа: https://xakep.ru/2018/03/08/ssl-tls-fuckup/

22. F.R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication Systems for Grid Integration of Renewable Energy Resources," IEEE Network, vol. 25, no. 5, pp. 22-29, Sept. 2011.

23. Energy Future Coalition, "Challenge and Opportunity: Charting a New Energy Future,"Appendix A: Working Group Reports, Report of the Smart Grid Working Group. Режим доступу: https://web.archive.org/web/20080910051559/http://www.energyfuturecoalition.org/pubs/app_smart_grid.pdf

24. IoT maturity in the new digital world URL:https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Get-smart-aboutdata-integration-for-a-truly-smart-city

25. «ETCETERA». Україну підключають до «Інтернету речей»: навіщо це потрібно? [Електронний ресурс]/ «ETCETERA»// Україну підключають до «Інтернету речей»: навіщо це потрібно? URL: https://uk.etcetera.media/ukrayinupidklyuchayut-do-internetu-rechey-navishho-tse-potribno.html

26. Черняк Т.Г. Оцінка ризиків інформаційної безпеки Інтернет речей. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ -

2022), Тернопіль, 2022. – С. 53-55.

27. Яцків Н.Г., Вівчар Д.В., Черняк Т.Г. Аналіз підходів до оцінки ризиків. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 104-106.

ДОДАТОК А

Копії публікацій