МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.27.10.000.КРБ

Загорія Єгора Івановича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**
Освітня програма: **«Комп'ютерна інженерія»**
Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:_____

«Аналіз технології "Internet of things" з позиції інформаційної безпеки»

Проектний матеріал складається з пояснювальної записки на 76 сторінках та графічного (презентаційного) матеріалу на 10 аркушах (слайдах)

Виконавець _____ (Загорій Є.І.)
Керівник проекту_____ (Кільдішев В.Й.)

Консультанти:
з охорони праці_____ (Чорновол Н.І.)
з дотримання вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Кривченко Ю.В.)

До захисту допущений
Завідувачка кафедри _____ (Іванова Л.В.)
Завідувач відділення _____ (Скорнякова О.В.)

Захист «26» 06 2023 р. Протокол ДКК № 3
Оцінка ДКК 5 (відмінно)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є аналіз технології "Internet of Things" з позиції інформаційної безпеки.

У бакалаврській проведено дослідження концепції Internet of Things (IoT), в рамках чого представлено ідеї та основні принципи, архітектуру, класифікацію пристроїв. Проведено детальний аналіз загроз та ризиків інформаційної безпеки IoT. Розглянуто причини виникнення загроз, проблематики на різних рівнях сприйняття, найбільш поширені атаки. Проведено формування базової моделі загроз IoT. Представлено базові механізми захисту IoT, методи тестування, рекомендації щодо забезпечення безпеки IoT-пристроїв.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 202____ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Загорій Єгору Івановичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи
Аналіз технології "Internet of things" з позиції інформаційної безпеки

затверджена наказом по коледжу від "17" ЖОВТНЯ 2022 р. № 235-А2-ОД

2. Термін здачі кваліфікаційної роботи 15 ЧЕРВНЯ, 2023 р.

3. Вихідні дані до роботи Архітектура IoT – додатки, управління, шлюз та мережа, датчики. Кількість ділянок в базовій моделі загроз IoT – 4. Області тестування IoT – компоненти, функціональність, під навантаження, безпека. Платформи транзакцій – IOTA, IOTEX, CHAIN.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Вступ. 1. Провести аналіз загроз та ризиків IoT. 2. Оцінити проблематику ІБ IoT на різних рівнях. 3. Оцінити рівень ІБ об'єктів IoT – Apple Pay, ZigBee, Tesla Models. 4. Розглянути механізми захисту технології IoT в аспекті моделі загроз. 5. Охорона праці. Висновки. Перелік використаних джерел. Додаток

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Лист 1 – Технології індустріального Інтернету речей

Лист 2 – Загрози IoT, Класифікація загроз IoT

Лист 3 – Комплексний захист технологій IoT. Рівень апаратної безпеки

Лист 4 – Архітектура програмо-визначеного периметра SDP

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Кільдішев В.Й.*		
Охорона праці	*Чернобол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання Кільдішев В.Й.

Керівник роботи _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1	Вступ. Дослідження концепції Internet of Things	**24.05.2023 р.**	Виконав
2	Аналіз загроз та ризиків інформаційної безпеки Internet of Things	**26.05.2023 р.**	Виконав
3	Механізми захисту IoT в аспекті загроз та ризиків	**03.06.2023 р.**	Виконав
4	Виконання розділу «Охорона праці»	**08.06.2023 р.**	Виконав
5	Виконання графічної частини роботи	**13.06.2023 р.**	Виконав
6	Чистове оформлення пояснювальної записки кваліфікаційної роботи	**15.06.2023 р.**	Виконав
7	Підготовка доповіді та презентації для захисту	**17.06.2023 р.**	Виконав
8	Отримання рецензії, відповіді на зауваження рецензента	**21.06.2023 р.**	Виконав
9	Захист роботи	**23.06.2023 р.**	Виконав

Виконавець _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27.10.000.00 КРБ	*Кваліфікаційна робота*		
А4			БКС 27.10.000.00 КРБ ПЗ	*Пояснювальна*	*1*	
				записка		
			БКС 27.10.000.00 КРБ МП	*Мультимедійна*		
				презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	*БКС 27.10.000.00 КРБ ПЗ*		
Розробив		Загорій Є.І.			Аналіз технології "Internet of things" з позиції інформаційної безпеки	Літ.	Аркуш
Перевірив		Кільдішев В.Й.				*Н Д П*	*3*
						ОТФК ОНТУ гр.БКС-27	
Н. Контр.		Петрашова В.І.					
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

Витік конфіденційної інформації, як правило, призводить до значних фінансових втрат. Крім витоку конфіденційної інформації, існують інші види інформаційних загроз, спрямовані на часткову або повну зупинку робочих процесів організацій і підприємств, блокування оперативного доступу до необхідних зовнішніх і внутрішніх інформаційних ресурсів, зниження продуктивності інформаційно-технологічної інфраструктури або еѐ повну зупинку.

З кожним роком в світі збільшується кількість кіберзлочинів і кібератак. В останні роки в Україні також різко зросла кількість навмисних втручань в роботу інформаційних систем державних і комерційних структур. У переважній більшості випадків, після здійснення кібератак, робота організацій і підприємств блокувалася від декількох годин до декількох днів, що призводило до дуже серйозних наслідків. Тому від ступеня безпеки інформаційних технологій зараз залежать не тільки стабільність і надійність функціонування державних інститутів і комерційних структур, а часто і життя багатьох людей.

IoT швидко змінює наше повсякденне життя. За останні кілька років ми підключили практично всі до Інтернету, але не вклали достатньо коштів у безпеку IoT. Навіть стандартні речі, такі як ідентифікація всіх пристроїв в мережі і знання того, що пристрій було зламано, явно відсутні в більшості систем IoT. Це робить пристрої IoT і дані надзвичайно уразливими для атак. Розуміння загроз і ризиків, формування моделі загроз і вибір профілів захисту на її основі - необхідність сьогодення.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Аналіз безпеки технологій інтернету речей

1.1.1 Проблеми безпеки Інтернету речей

В даний час спостерігається збільшення кількості інцидентів (злочинів) у сфері інформаційної безпеки та інформаційних технологій. Цьому сприяє повсюдне поширення мережевих технологій зберігання даних і широке поширення IoT-речей: у 2018 році кількість підключених пристроїв оцінювалася в 22 млрд з перспективою зростання приблизно до 40 млрд до 2025 (дані дослідницької компанії Strategy Analytics). Ці пристрої можуть містити вразливості, якими можуть скористатися кіберзлочинці і в результаті поставити під загрозу конфіденційність користувача та громадську безпеку [25]. Невипадково кібербезпека IoT викликає занепокоєння у 95% респондентів опитування, проведеного аналітиками IoT Analytics, причому майже 40% «дуже стурбовані» можливими вразливістю Інтернету речей [35]. Таким чином, забезпечення безпеки є однією з основних проблем, пов'язаних з IoT.

Причиною цієї проблеми є той факт, що технології IoT, як і більшість споживчих технологій, розроблені без урахування вимог безпеки, оскільки основним завданням виробників було мінімізувати собівартість та час розробки, здешевити виробництво та збільшити обсяг продукції, що випускається. У результаті подібної політики розумні пристрої відчувають нестачу ресурсів. Через це недоліки більшість інструментів безпеки не можуть бути встановлені в пристроях IoT, що робить пристрої легкою мішенню для кіберзлочинів [38].

Хакери знаходять слабкості вбудованих систем захисту, їх вразливості і можуть використовувати пристрої IoT як інструменти для атак на інші сайти [2] Кіберзлочинці, озброєні технологіями IoT, можуть, перебуваючи у віртуальному просторі, загрожувати безпеці та навіть життю людей, і кількість подібних злочинів зростає. Наприклад, Управління з контролю за якістю харчових продуктів та лікарських препаратів США (FDA) повідомило, що деякі кардіостимулятори (пристрій, який посилає електричні імпульси до серця, щоб встановити серцевий ритм) та супутні медичні пристрої, вразливі до злому [53]. Це означає, що пацієнти з кардіостимулятором можуть потрапити під удар хакерів, здатних захопити контроль над кардіостимулятором.

Цифрові дані IoT є багатим і часто недослідженим джерелом інформації. Більшість виробників IoT-пристроїв демонструють покупцям функціональність їх товару (виконувані функції та можливості), але не згадують про технологію ПЗ, що управляє цими функціями, і не розкривають його вразливості Наприклад, робот-пилосос LG може прибирати кімнату самостійно і повідомляти про виконання завдання , тому що він управляється за допомогою датчиків, що визначають розмір та форму забруднення. Дослідники компанії постачальника рішень з кібербезпеки у всьому світі, 26 жовтня 2017 року виявили в мобільному та хмарному додатках LG у процесі входу на портал LG вразливість, яка дозволила їм віддалено створити підроблений обліковий запис LG , а потім використовувати його, щоб оволодіти обліковим записом та розумними пристроями користувача LG та отримати контроль над пилососом та вбудованою в нього відеокамерою, таким чином оволодівши доступом до відеотрансляції в онлайн-режимі з дому. Це означає, що зловмисник, отримавши контроль над обліковим записом конкретного користувача LG , може контролювати будь-який пристрій LG , пов'язаний з цим обліковим записом, включаючи пилососи, холодильники, плити, посудомийні та пральні машини, фени та кондиціонери [54].

Як користувачі розумних пристроїв можуть захистити себе. Фахівці з безпеки рекомендують змінювати паролі, оновлювати програми та самі пристрої, захищати персональні дані

Інший важливий аспект забезпечення безпеки пов'язаний з адмініструванням пристроїв IoT, а саме з розподілом відповідальності, особливо з урахуванням внутрішньої складності та неоднорідності екосистеми IoT, а також проблем масштабованості.

Якщо узагальнити, то проблеми екосистеми IoT полягають у наступному:

- *Дуже велика площа атаки.*

Загрози та ризики, пов'язані з IoT, різноманітні та швидко розвиваються. Враховуючи їх вплив на здоров'я, безпеку та конфіденційність користувачів, їхню небезпеку не можна ігнорувати. Користувачі можуть не знати, що IoT значною мірою ґрунтується на зборі та обробці великих обсягів даних з різних джерел, включаючи і конфіденційні дані, та обмін ними.

- *Складність екосистеми IoT.*

IoT слід розглядати не як сукупність незалежних пристроїв, а як багату, різноманітну і широку екосистему, що включає пристрої, комунікації, інтерфейси і людей.

- *Відсутність законодавчих актів, норм, стандартів та правил.*

Фрагментоване та повільне прийняття стандартів та правил для впровадження заходів безпеки та передового досвіду у сфері IoT, а також постійна поява нових технологій ще більше ускладнюють відповідні проблеми

- *Широке впровадження у критично важливі системи.*

Проникнення технологій IoT в критично важливу інфраструктуру, що має стратегічне значення для держави, є загрозою безпеці.

- *Складність інтеграції систем безпеки.*

Інтеграція систем безпеки - дуже складне завдання через наявність потенційно суперечливих точок зору та вимог усіх зацікавлених сторін. Наприклад, різні пристрої та системи IoT можуть використовувати різні рішення автентифікації, при цьому їх необхідно інтегрувати та зробити сумісними

- *Економія виробників на безпеці.*

Стрімке впровадження IoT та розширена функціональність розумних пристроїв у кількох критично важливих галузях надають великі можливості для значної економії витрат завдяки використанню таких функцій, як потоки даних, розширений моніторинг, інтеграція та багато інших. І навпаки, низька вартість, якою зазвичай відрізняються пристрої та системи IoT, спричиняє негативні наслідки з погляду безпеки. Виробники можуть обмежувати функції безпеки з метою зниження витрат, і, отже, система безпеки продукту не зможе захистити від певних типів атак хакерів

- *Нестача досвідчених фахівців.*

Це досить нова область, і тому не вистачає людей з відповідним набором навичок та досвідом у сфері безпеки IoT.

Складності із забезпеченням безпеки при оновленні IoT-пристрою. Забезпечити безпеку при встановленні оновлень до IoT надзвичайно складно, оскільки специфіка користувацьких інтерфейсів, доступних користувачам, не дозволяє використовувати традиційні механізми оновлення. Забезпечення безпеки цих механізмів є непростим завданням, особливо з урахуванням використання бездротової мережі.

- *Складності із забезпеченням захисту на всіх етапах створення ПЗ*

Оскільки кількість рішень для IoT, що випускаються, стрімко зростає, виробники приділяють недостатньо часу забезпеченню безпеки та конфіденційності на етапі розробки. З цієї причини, а іноді й через фінансові проблеми, компанії, що

розробляють продукти IoT, зазвичай звертають більше уваги на функціональність та зручність використання пристрою, ніж на його безпеку.

- *Відсутність чітко сформульованої відповідальності.*

Відсутність чіткого розподілу відповідальності може призвести до двозначності та конфліктів у разі інциденту, пов'язаного з безпекою, особливо з урахуванням великого та складного ланцюжка, характерного для виробництва IoT-пристроїв. Більше того, залишається без відповіді питання про те, як забезпечити безпеку, якщо у виробництві одного пристрою брало участь кілька різних сторін (юридичних та/або фізичних осіб). Забезпечення відповідальності є ще однією важливою проблемою.

1.1.2 Класифікація загроз IoT

Екосистема IoT-технологій є комбінацією різних технологічних зон: зона IoT-пристроїв, мережева зона і хмарна зона. Ці зони можуть бути джерелом цифрових даних. Тобто дані можна збирати з розумного пристрою або датчика із внутрішньої мережі, такого як брандмауер або маршрутизатор, або із зовнішніх мереж (хмара або програма). Ці технологічні зони є об'єктом кримінального інтересу кіберзлочинців.

Залежно від місця зберігання даних у системі IoT експерти у сфері IoT-криміналістики виділяють три небезпечні ділянки у ландшафті кіберзагроз: хмара, мережа та пристрій, відповідно виділяються хмарна криміналістика, мережева та криміналістика на рівні пристрою IoT.

Оскільки цінні дані часто зберігаються у хмарі, хмарна інфраструктура є однією з найважливіших цілей зловмисників. Крім того, у хмарі обмежений доступ до інфраструктури та інформації про точне місце зберігання даних [56].

Слід зазначити, що у хмарних сервісів, що використовують віртуальні машини як сервери, дані можуть зберігатися на цих серверах. Реєстри запису або тимчасові інтернет-файли на серверах можуть бути видалені, якщо вони не синхронізовані з пристроями зберігання, наприклад, якщо ці сервери перезапускаються або вимикаються.

Перш ніж з'ясувати, які загрози є характерними для технологій IoT, необхідно визначити, які активи вимагають захисту. Різні загрози несуть різні потенційні небезпеки, які різняться залежно від сценаріїв використання. Нижче наведено класифікацію загроз, характерних для IoT, з описом різних видів (табл. 1.1).

Таблиця 1.1 – Класифікація небезпек [15]

Загроза	**Опис**
1. Умисні дії	
Шкідливе ПЗ	Програмне забезпечення, призначене для виконання небажаних та несанкціонованих дій у системі без згоди користувача. Це може призвести до пошкодження, модифікації або крадіжки інформації. Його небезпека може бути високою
Експлойт	Код, розроблений для використання вразливості для отримання доступу до системи. Цю загрозу важко виявити, і в середовищах I від її небезпека варіюється від високої до критичної, залежно від порушених активів
Цільова атака	Атака, призначена для конкретної мети, яка проводиться протягом тривалого часу в кілька етапів. Основна мета злочинця - залишатися непоміченим і отримати якнайбільше конфіденційних даних, інформації чи контролю. Хоча небезпека цієї загрози є середньою, її виявлення - зазвичай дуже складний і тривалий процес
DDoS -атака	У процесі DDoS-атаки кілька систем атакують одну мету, щоб навантажити її та призвести до збою. Це можна зробити шляхом створення безлічі з'єднань, переповнення каналу зв'язку або багаторазового повторного відтворення тих самих повідомлень
Шкідливе ПЗ	Програмне забезпечення, призначене для виконання небажаних та несанкціонованих дій у системі без згоди користувача. Це може призвести до пошкодження, модифікації або крадіжки інформації. Його небезпека може бути високою

Скомпрометований пристрій	Цю загрозу важко виявити, оскільки скомпрометований пристрій важко відрізнити від оригіналу. Ці пристрої зазвичай мають бекдори і можуть використовуватися для атак на інші системи в навколишньому середовищі.
Втрата конфіденційності	Ця загроза небезпечна як втратою конфіденційності користувача, так і впливом стороннього персоналу на елементи мережі
Модифікація інформації	У цьому випадку мета полягає не в пошкодженні пристрою, а в маніпуляції інформацією, щоб викликати хаос або отримати грошовий прибуток
2. Перехоплення інформації	
Атака «людина посередині»	Активна атака підслуховування, за якої зловмисник передає повідомлення від однієї жертви іншій, щоб змусити їх повірити, що вони розмовляють безпосередньо один з одним
Підключення до активної сесії	Взяти під контроль активного сеансу зв'язку між двома елементами мережі. Зловмисник може отримати важливу інформацію, у тому числі конфіденційну
Перехоплення інформації	Несанкціоноване перехоплення та (іноді) модифікація приватної комунікації, наприклад телефонних дзвінків, миттєвих повідомлень, повідомлень електронної пошти
Мережева розвідка	Пасивне отримання внутрішньої інформації про мережу: підключені пристрої, протокол, відкриті порти, використовувані служби і т.д.
Перехоплення з'єднання	Крадіжка з'єднання для передачі даних, при цьому незаконний хост діє як законний з метою крадіжки, зміни або видалення даних, що передаються
3. Вимкнення	
Вимкнення живлення	Навмисне або випадкове переривання або збій у мережі. Залежно від порушеного сегмента мережі та часу, необхідного для відновлення, небезпека цієї загрози варіюється від високої до критичної.
Збій пристрою	Збій або вихід з ладу апаратного пристрою
Збій системи	Збій програмних служб або програм
IoTеря сервісу підтримки	Недоступність послуг підтримки, необхідні для правильної роботи інформаційної системи
4. Технічний збій	
Уразливості на програмному рівні	Пристрої IoT часто вразливі через слабкі паролі, незмінені паролі, встановлені за умовчанням, програмні помилки та помилки конфігурації.
Сторонні помилки	Помилки в активному елементі мережі, викликані неправильним налаштуванням іншого елемента, що має до нього пряме відношення

5. Катастрофи	
Стихійні лиха	Повені, сильні вітри, сильні снігопади, зсуви ґрунту та інші стихійні лиха, які можуть пошкодити пристрої фізично
Аварії в середовищі IoT	Аварії в середовищі розгортання IoT-обладнання, що призводять до їх непрацездатності
6. Фізична атака	
Модифікація пристрою	Модифікація пристрою, внесення змін до пристрою (наприклад, використання поганої конфігурації портів, використання відкритих портів)
Знищення пристрою	Псування, крадіжка тощо.

1.1.3 Проблеми безпеки технологій індустріального Інтернету речей

Перш ніж з'ясувати актуальні для IoT загрози, необхідно визначити технології, що застосовуються у цій галузі. У табл. 1.2 наведено технології IoT.

Таблиця 1.2 – Технології індустріального Інтернету речей

Технологія	**Опис**
Кінцеві пристрої IoT	Пристрої, оснащені вбудованими технологіями збирання, обробки, зберігання, передачі інформації, інтелектуального прийняття рішень
Міжмашинний зв'язок (M2M)	Технологія, що полегшує прямий зв'язок між пристроями у мережі без участі людини
Аналіз Big Data	Процес вивчення величезної кількості різних типів наборів даних, відео та аудіо, згенерованих у реальному часі інтелектуальними датчиками, пристроями, журналами
Робототехніка	Удосконалені промислові роботи, наділені на вирішення складних завдань інтелектуальними можливостями, такими як здатність вчитися на своїх помилках і підвищувати свою продуктивність.
Штучний інтелект	Алгоритми, які дозволяють комп'ютерам та обчислювальним машинам виконувати завдання, які зазвичай виконують люди.
Машинне навчання	Алгоритми, які дозволяють комп'ютерам діяти та покращувати здатність прогнозувати без явного програмування.
Прогнозне обслуговування	Рішення, які відстежують стан обладнання, прогнозуючи, коли може статися збій, для ефективного обслуговування з

	мінімально можливою частотою.
Моніторинг у режимі реального часу	Технології, що дозволяють збирати та об'єднувати дані про безпеку від компонентів системи, а також відстежувати та аналізувати події, що відбуваються в мережі.
Розширена аналітика збитків	Методи аналізу різних типів втрат, які можуть виникнути серед, з метою їх усунення чи зменшення.
Комп'ютерні обчислення	Рішення, що забезпечують доступ до загальних наборів ресурсів, таких як мережі, сервери та програми, з мінімальними вимогами до управління та взаємодії з постачальником послуг.
Доповнена реальність	Технології, які змінюють сприйняття реального навколишнього середовища, є інструментом для підвищення ефективності завдань (наприклад, ручного складання).

Проблеми IoT та IoT багато в чому повторюють одна одну. Виходячи з перерахованих вище технологій можна виділити ряд **проблем безпеки IoT.**

- *Вразливість пристроїв та систем.*

Щодня кількість нових пристроїв стрімко зростає. Питання безпеки IoT не можна вирішити ізольовано, не забезпечивши інші види безпеки, такі як інформаційна безпека, безпека операційних технологій та фізична безпека. У промислових умовах це може представляти значну проблему, оскільки більшість систем цього типу були розроблені без урахування вимог безпеки [62], і тому вразливості у подібному устаткуванні виявляються дедалі частіше [63].

- *Складність управління процесами.*

Крім великої площі атаки з урахуванням величезної кількості підключених пристроїв слід враховувати безліч складних процесів, пов'язаних з інтелектуальним виробництвом. У системах IoT управління процесами є проблемою з погляду безпеки, тому що функціональність і ефективність роботи пристроїв зазвичай вважаються пріоритетнішими, ніж безпека.

- *Конвергенція інформаційних та операційних технологій* (*IT та OT*). Промислові системи управління перестали бути ізольованими після того, як Використання IT-компонентів у промисловість стало звичайною практикою.

Конвергенція організацій за допомогою IT-мереж спростила управління складними середовищами, а також привнесла нові загрози безпеці. Супутні фактори включають небезпечні мережеві з'єднання (внутрішні та зовнішні), використання технологій з відомими вразливостями, які вносять раніше невідомі ризики.

- *Складність ланцюжка поставок.*

Компанії, які виробляють продукти або рішення, рідко можуть виробляти самостійно весь продукт цілком і зазвичай звертаються за допомогою у виробництві окремих компонентів до третіх осіб. Розробка технологічно складних продуктів призводить до надзвичайно складного ланцюжка поставок за участю великої кількості людей та організацій, що робить його надзвичайно складним з погляду управління. Нездатність відстежити кожен компонент до джерела означає неможливість забезпечити безпеку продукту. Безпека цілого продукту оцінюється за його найслабшою (з точки зору безпеки) ланкою.

- *Застарілі промислові системи управління.*

Застаріле обладнання є суттєвою перешкодою для впровадження систем безпеки. Виробники встановлюють нові системи поверх застарілих, і це може призвести до неефективності колишніх заходів захисту, а також прояву невідомих уразливостей, які були неактивними протягом багатьох років. Додавання нових пристроїв IoT до застарілого обладнання викликає обґрунтовані побоювання, оскільки може дозволити зловмисникам знайти новий спосіб злому систем.

- *Небезпечні протоколи.*

Виробничі компоненти з'єднуються приватними промисловими мережами, використовуючи певні протоколи. У сучасних мережевих середовищах ці протоколи часто не забезпечують належного захисту від загроз.

- *Людський фактор*.

Впровадження нових технологій означає, що робітники та інженери заводу повинні застосовувати нові способи роботи з новими типами даних, мережами та системами. Якщо вони не знатимуть про ризики, пов'язані зі збором, обробкою та аналізом даних, вони можуть стати легкою метою для зловмисників.

- *Невикористовувані функції.*

Промислова техніка призначена для надання великої кількості функцій та послуг, частина яких може бути незатребуваною на окремому виробництві. У промислових середовищах машини або їх окремі компоненти часто використовують не весь доступний функціонал, при цьому функції, що не використовуються, можуть значно розширити область потенційної атаки і стати воротами для зловмисників.

- *Забезпечення безпеки продукту після його реалізації.*

Безпека пристрою повинна бути предметом розгляду протягом усього життєвого циклу продукту, навіть у разі закінчення терміну служби пристрою.

1.1.4 Класифікація загроз індустріального Інтернету речей

Виходячи з певних активів було складено класифікацію загроз IoT, представлену на рис. 1.1 і докладно розкриту на рис. 1.2-1.9.

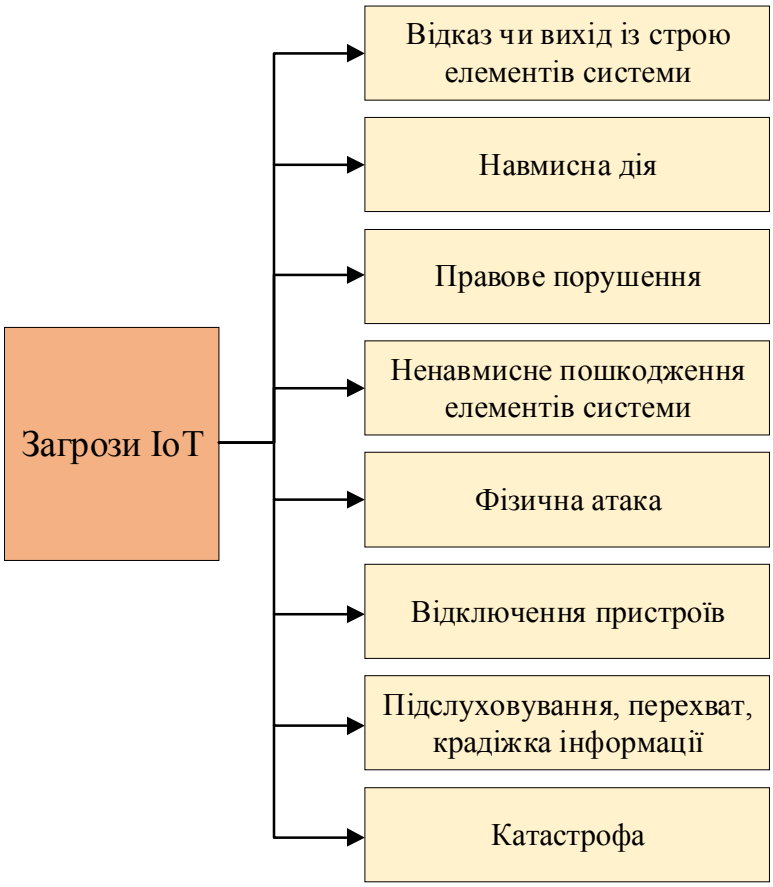


Рисунок 1.1 – Класифікація загроз IoT

Нижче наводиться опис кожної небезпеки.

1. Відмова або вихід із ладу елементів системи:

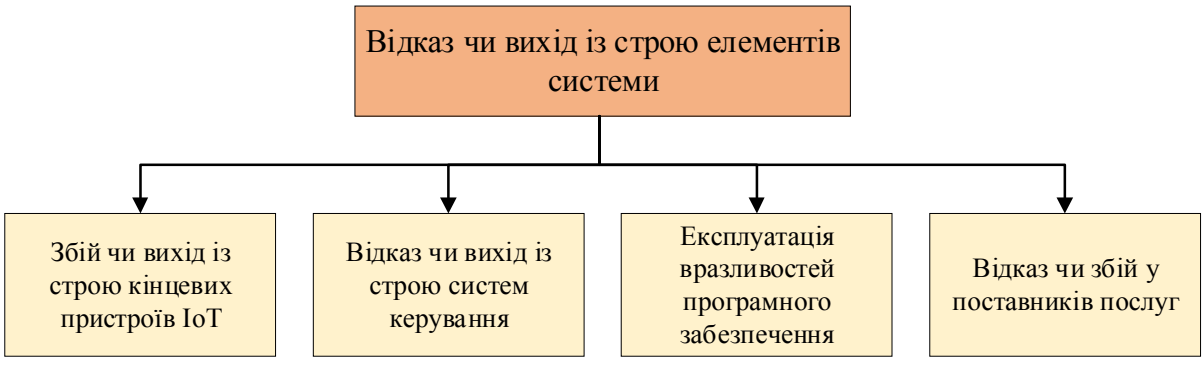


Рисунок 1.2 - Відмова чи вихід із ладу елементів системи

а) *збій чи вихід із ладу кінцевих IoT-пристроїв* виникає за умови неналежного обслуговування та недотримання посібників та інструкцій з експлуатації пристроїв;

б) *відмова або вихід з ладу систем управління* може статися, якщо не забезпечується належне обслуговування та дотримання посібників та інструкцій з експлуатації пристроїв;

в) *експлуатація вразливостей програмного забезпечення* стає можливою через відсутність оновлень, використання слабких паролів або паролів за промовчанням, а також неправильної конфігурації;

г) *відмова або збій у постачальників послуг* тягне за собою порушення процесів, які залежить від сторонніх сервісів.

2. Умисна дія:

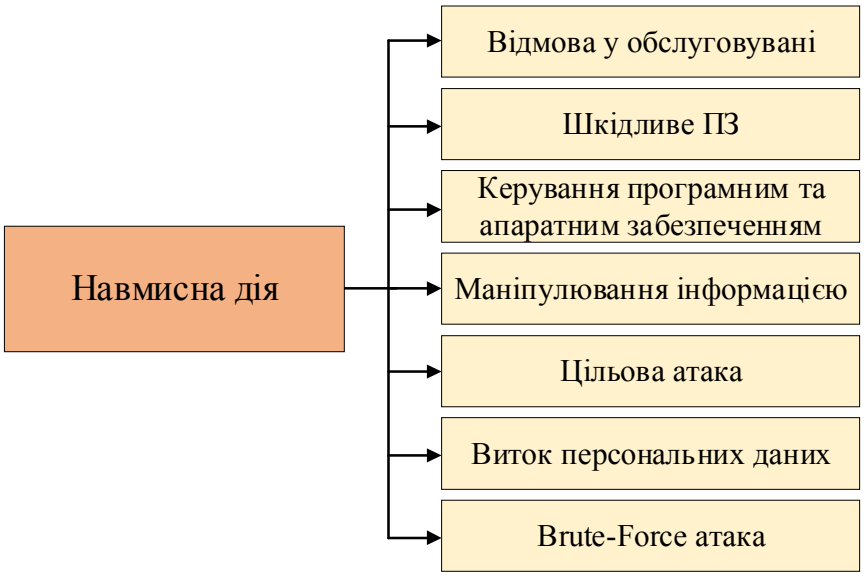


Рисунок 1.3 - Навмисна дія

а) *відмова у обслуговуванні* - атака цього може бути двунаправленной. З однією сторони, вона може бути націлена на систему IoT, при цьому в систему відправляється велика кількість запитів, що призводить до недоступності системи

та збоїв у роботі (DoS-атака – «відмова в обслуговуванні»). З іншого боку, зловмисник може скористатися великою кількістю пристроїв IoT у промисловому середовищі та створити армію бот-мереж IoT як платформу для атаки на будь-яку іншу систему (DDoS -атака – «розподілена атака типу "відмова в обслуговуванні"»);

б) *шкідливе ПЗ* проникає в IoT з метою виконання небажаних та несанкціонованих дій, які можуть завдати шкоди системі, операційним процесів та пов'язаних даних. Віруси, троянські коні та шпигунські програми є типовими прикладами цієї загрози;

в) *керування програмним та апаратним забезпеченням* або додатками пристроїв зловмисником є несанкціонованим і у сфері промислових систем IoT може включати маніпуляції з промисловим роботом, маніпуляції з пристроями і зміна їх конфігурації;

г) маніпулювання інформацією передбачає небажане та несанкціоноване зміна даних зловмисником. Сюди може входити компрометація ВІД або систем підтримки виробництва, таких як SCADA , та маніпулювання даними процесу. Можливі наслідки можуть включати недоречні рішення, що ґрунтуються на фальсифікованих даних;

д) *цільова атака* спрямована на конкретну організацію (або на конкретну людини в цій організації) з метою завдати шкоди організації, наприклад взяти під контроль системи за допомогою різних технічних засобів, таких як злом ключових пристроїв та фальсифікація телеметрії, що вводить в оману непоінформованих операторів. До інших небезпек відносяться заподіяння шкоди репутації або крадіжка секретів компанії. Коли метою є виробнича компанія, зловмисник може, наприклад, спробувати вкрасти формули чи рецепти та продати їх конкурентам. Зловмисник також може використовувати штучний інтелект для виконання

персоналізованої атаки, призначеної для обраної групи або окремих співробітників. Ця атака відрізняється за масштабом від атак, метою яких є зараження пристроїв усієї компанії при підключенні до певного веб-сайту, підготовленого зловмисником, або використання пристрою або програмного забезпечення з певною вразливістю;

е) *витік персональних даних* може призвести до компрометації особистої інформації, що зберігається на пристроях або у хмарі. Мета зловмисника – отримати несанкціонований доступ до даних такого роду та використовувати їх у незаконний спосіб. У виробничих компаніях до подібних даних можуть належати імена та ролі користувачів системи ВІД. Виробничі дані не вважаються конфіденційними, але їх витік також може створювати проблеми, якщо вони пов'язані з роботою окремих співробітників;

ж) Brute - force *атака* («груба сила») означає спробу отримати несанкціонований доступ до ресурсів організації (наприклад, до даних, систем, пристроям і т. д.), вгадавши правильний ключ або пароль за допомогою перебору всіх можливі поєднання символів. Організації, які дозволяють використання нескладних паролів або паролів за промовчанням для промислових пристроїв та систем, особливо вразливі для таких атак.

3. Правове порушення:

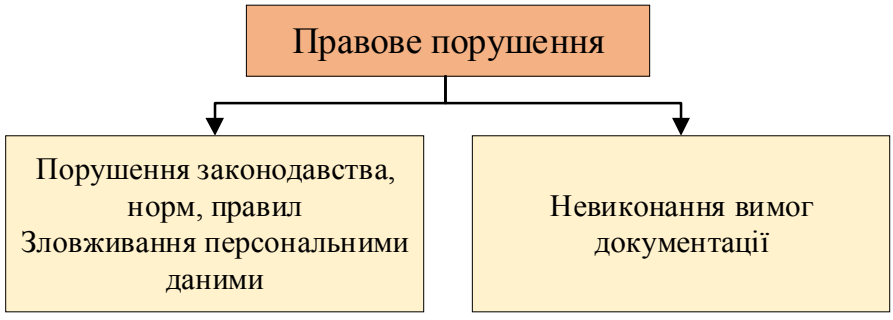


Рисунок 1.4 – Правове порушення

а) *порушення законодавства, норм, правил і зловживання персональними даними може призвести до* юридичних проблем і фінансових потерь . Небезпека пов'язана з обробкою персональних даних, наприклад при використанні кінцевих пристроїв IoT без дотримання місцевих законів чи норм.

б) *невиконання вимог документації* тягне за собою порушення договірних вимог виробниками компонентів та постачальниками програмного забезпечення у разі неможливості забезпечити необхідні заходи безпеки.

4.Ненавмисне пошкодження елементів системи.

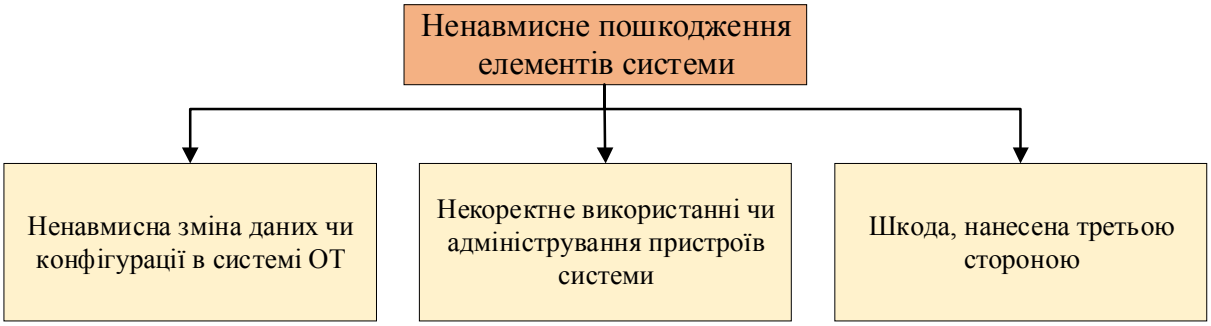


Рисунок 1.5 - Ненавмисне пошкодження елементів системи

а) *ненавмисна зміна даних або конфігурації в системі ОТ,* виконана недостатньо навченим співробітником, може спричинити порушення робочого процесу. Навіть з добрими намірами некваліфікований працівник, не підозрюючи про наслідки, може внести неналежні зміни до системи, особливо якщо він отримує повноваження, перевищують необхідні;

б) *некоректне використання або адміністрування пристроїв та систем* IoT/OT недостатньо навченим співробітником може призвести до порушення робочого процесу або фізичного пошкодження пристрою;

в) *збитки, завдані третьою стороною,* можуть призвести до пошкодження активів ОП . Якщо стороння організація має неконтрольований доступ до системи ОТ, наприклад з метою обслуговування або оновлення

програмного забезпечення, порушення безпеки цією організацією можуть завдати шкоди компанії, яка отримує послугу.

5. Фізична атака.

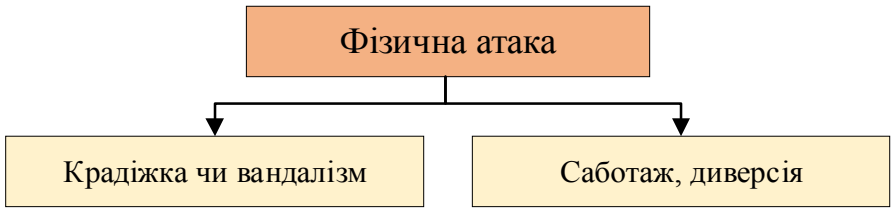


Рисунок 1.6 – Фізична атака

а) *крадіжка та вандалізм* можуть призвести до незапланованих простоїв виробництва, оскільки заміна пошкодженого або вкраденого пристрою потребує часу, іноді значного;

б) *саботаж, диверсія* можуть бути здійснені зловмисником при отриманні фізичного доступу до пристроїв внаслідок неправильної конфігурації портів та їх відкритістю. Зловмисник також може використовувати доступ для виконання несанкціонованих дій оператора.

6. Відключення пристроїв:

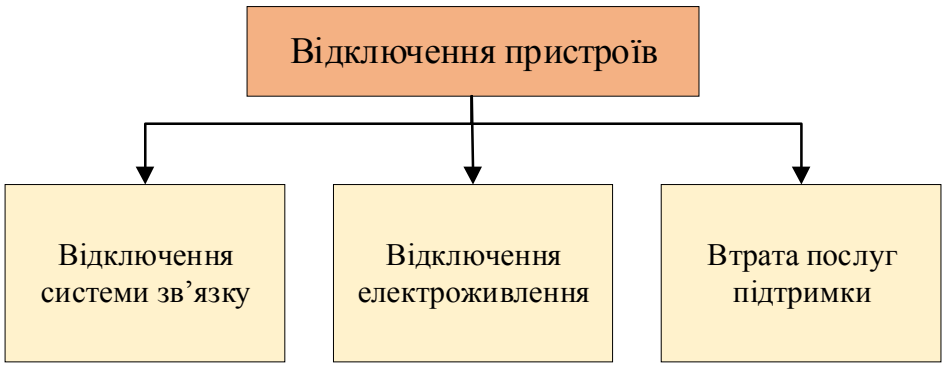


Рисунок 1.7 - Відключення пристроїв

а) *відключення мережі зв'язку може статися* через проблеми з кабельною, бездротовою або мобільною мережею;

б) *відключення електроживлення* може стати результатом збою в роботі або виходу з ладу будь-якого джерела живлення та, у разі відсутності аварійного джерела живлення, призвести до серйозних наслідків через раптове припинення виробничих процесів;

в) *Втрата послуг підтримки* відбувається внаслідок збою або несправності систем, *що підтримують виробництво* або логістику.

7. Підслуховування, перехоплення, крадіжка інформації:

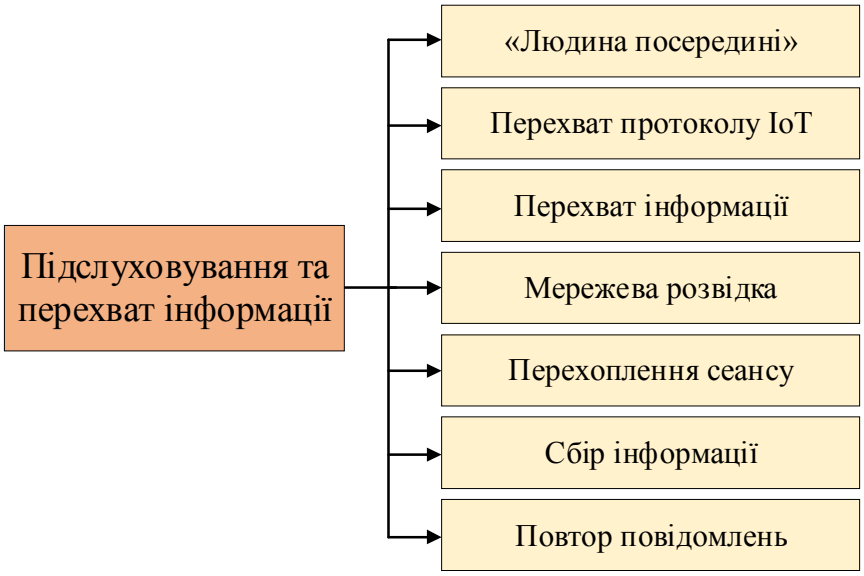


Рисунок 1.8 - Підслуховування, перехоплення та крадіжка інформації

а) *"людина посередині"* (MitM-атака) - активна атака підслуховування, при якій зловмисник передає повідомлення від однієї жертви іншій, щоб змусити їх повірити, що вони розмовляють безпосередньо один з одним;

б) *перехоплення протоколу IoT означає* взяття під контроль існуючого сеансу зв'язку між двома елементами мережі. Зловмисник може прослуховувати цінну інформацію, зокрема паролі. У перехопленні можуть використовуватися агресивні методи, наприклад, примусове відключення або відмова в обслуговуванні;

в) *перехоплення інформації включає* несанкціоноване перехоплення (і іноді модифікацію) особистих повідомлень, таких як телефонні дзвінки, миттєві повідомлення, повідомлення електронної пошти;

г) *мережева розвідка* передбачає пасивний і активний збір внутрішньої інформації про мережу: про підключені пристрої, протокол, відкриті порти, служби, що використовуються, тощо за допомогою загальнодоступних даних і додатків;

д) *перехоплення сеансу* передбачає перехоплення з'єднання для передачі даних і перемикання його на новий хост замість законного для крадіжки, зміни або видалення даних, що передаються;

е) *збір інформації* означає пасивне отримання внутрішньої інформації про мережу: про підключені пристрої, використовуваний протокол і т. д.;

ж) *повтор повідомлень* використовується як атака, щоб маніпулювати цільовим пристроєм або збивати його роботу за допомогою зловмисного використання допустимої передачі даних з багаторазовим відправленням або затримкою.

8. Катастрофа:

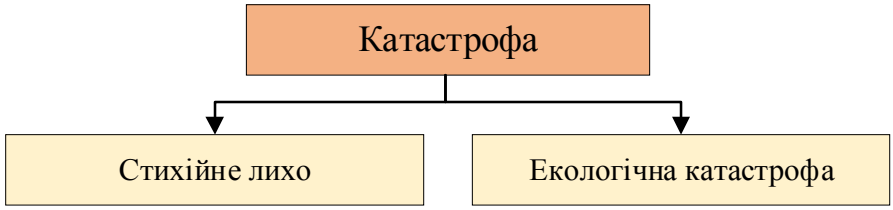


Рисунок 1.9 - Катастрофа

а) *стихійне лихо,* таке як повінь, удар блискавки, сильний вітер, дощ або снігопад, що може завдати фізичної шкоди компонентам довкілля ОТ;

б) *екологічна катастрофа,* наприклад пожежа, забруднення, вибух може призвести до фізичного пошкодження компонентів навколишнього середовища ОТ.

У цьому розділі було проведено аналіз безпеки IoT, виявлено його проблеми, визначено активи IoT та IoT, складено класифікацію загроз відповідно до зазначених активів.

1.2 Безпека Інтернету речей

1.2.1 Фізична та апаратна безпека

Багато IoT-пристроїв знаходяться у віддалених та ізольованих районах, що залишає вразливими датчики та прикордонні маршрутизатори. Апаратне забезпечення також потребує сучасних механізмів захисту, які широко використовуються в процесорах та мікросхемах мобільних та інших споживчих пристроїв.

Корінь довіри.

Перший рівень апаратної безпеки полягає у встановленні кореня довіри (англ. Root of Trust, або RoT). RoT – це процес завантаження з апаратною автентифікацією, який гарантує, що джерело першої виконуваної інструкції не підлягає зміні. Це ключовий етап процесу завантаження, який бере участь у подальшому запуску системи – від BIOS до ОС та додатків. RoT є базовим захистом від руткітів.

Кожен етап процесу завантаження перевіряє справжність наступного етапу, формуючи таким чином ланцюжок довіри. Корінь довіри може використовувати різні методи запуску:

– завантаження образу і кореневого ключа з прошивки або незмінної пам'яті;

– зберігання кореневого ключа в одноразовій програмованій пам'яті за допомогою ф'юз-бітів;

– завантаження коду із захищеної області пам'яті в захищене сховище.

Корінь довіри повинен перевіряти справжність кожного наступного етапу завантаження. Для цього на кожному етапі використовується набір ключів із цифровим підписом (рис. 1.10).

У різних процесорах корінь довіри реалізовано по-різному. Intel та ARM підтримують такі технології:

– ARM TrustZone – ARM продає виробникам чіпів пропрієтарний кремнієвий блок, який надає корінь довіри та інші механізми безпеки. TrustZone ділить апаратні компоненти на безпечні та небезпечні. Таким чином мікропроцесор відокремлюється від небезпечного ядра; він виконує Trusted OS – захищену операційну систему із чітко визначеним інтерфейсом взаємодії з небезпечними компонентами. Захищені ресурси та функції знаходяться в довіреному ядрі і повинні бути якомога легковажнішими. Перехід між компонентами різного типу робиться за допомогою апаратного перемикання контексту, завдяки чому відпадає необхідність безпечного програмного забезпечення для моніторингу. TrustZone також використовується для управління системними ключами, грошовими транзакціями та захистом авторських прав. Постачальникам обладнання є два профілю: A («application») і M («microcontroller»). Поєднання кореня довіри, Trusted OS та цього типу процесорів називається довіреним середовищем виконання (англ. Trusted Execution Environment, або TEE);

– Intel Boot Guard – це апаратний механізм для автентифікації початкового блоку завантаження криптографічними засобами або за допомогою процесу вимірювання. Для перевірки початкового блоку виробник повинен згенерувати 2048-бітний ключ, який складається із двох частин: відкритої та

закритої. Відкритий ключ друкується на платі шляхом детонації ф'юз-бітів на етапі виробництва. Ці біти є одноразовими та не підлягають зміні. Закрита частина ключа генерує цифровий підпис для подальшого автентичності етапу завантаження.

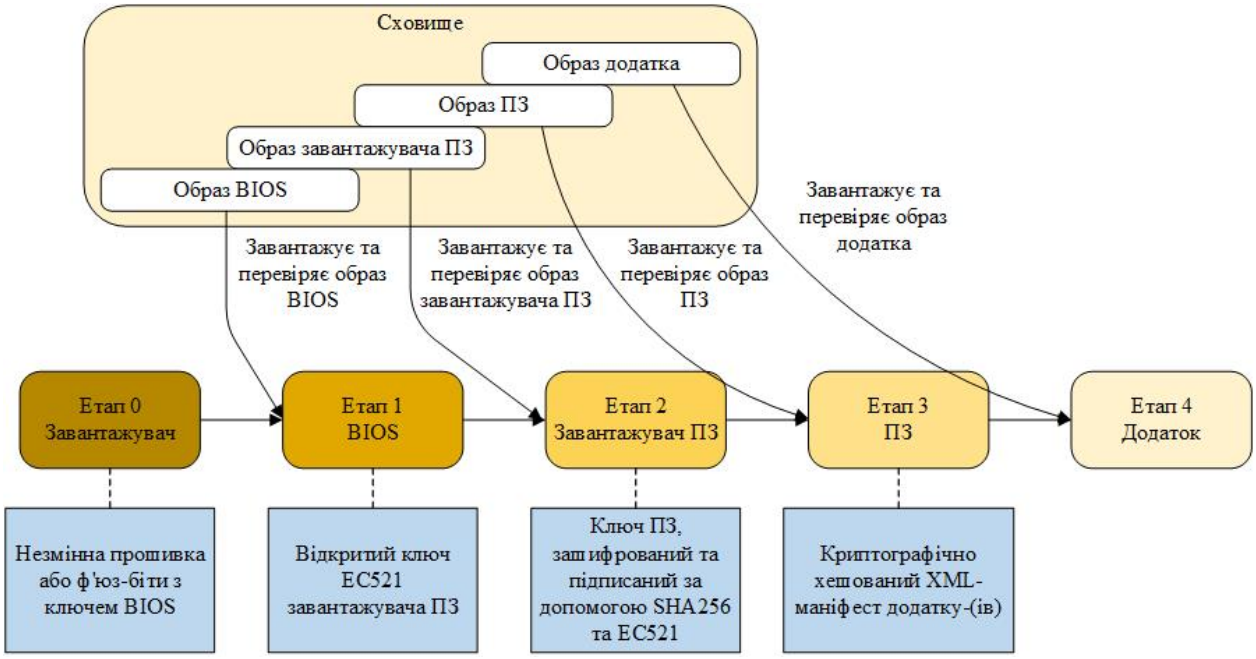


Рисунок 1.10 – Встановлення кореня довіри

Вище представлена п'яти етапне завантаження, яка формує ланцюжок довіри і починається із завантажувача, що знаходиться в незмінній пам'яті. На кожному етапі використовується відкритий ключ, за допомогою якого засвідчується справжність наступного компонента, що завантажується.

Керування ключами та модулі TPM.

Відкриті та закриті ключі є запорукою безпечної системи. Для їхнього захисту потрібен належний механізм управління. Одним з найпопулярніших стандартів апаратного захисту ключів є TPM (Trusted Platform Module – довірений платформний модуль). Його специфікація була створена консорціумом Trusted

Computing Group і є частиною ISO та IEC. Поточну версію TMP 2.0 було випущено у вересні 2016 року.

TPM є окремим апаратним компонентом з RSA-ключом, вшитим на етапі виробництва.

Зазвичай TPM використовується для зберігання, захисту та адміністрування ключів у таких сценаріях, як шифрування диска, завантаження кореня довіри, автентифікація обладнання та програмного забезпечення, а також для керування паролями. TPM може створити хеш перевіреної апаратної або програмної конфігурації, що допоможе виявити стороннє втручання на етапі виконання. Ця технологія також застосовується у створенні хешів типу SHA-1 та SHA-256, шифруванні блоків методом AES, асиметричному шифруванні та генерації випадкових чисел. Виробництвом TPM-пристроїв займаються такі компанії як Broadcom, Nation Semiconductor та Texas Instruments.

Адресний простір у процесорі та пам'яті.

Ми вже обговорили різні експлойти та технології процесора, які їм протистоять. Двома основними механізмами захисту в ЦПУ та ОС, на які слід звернути увагу, є пам'ять, що не виконується, і рандомізація розміщення адресного простору. Обидві вони призначені для ускладнення або запобігання процесу впровадження шкідливого коду на основі переповнення буфера або стека:

– не виконувана пам'ять – це апаратний механізм, за допомогою якого операційна система робить ділянки пам'яті нездійсненними. Кінцева мета полягає в тому, щоб виконуватися могли тільки ті області пам'яті, в яких перевірений і справжній код. При спробі застосування шкодоноса через переповнення стека система помітить відповідну ділянку як невиконуваний, у результаті зсув покажчика поточної інструкції до цієї ділянці призведе до апаратного виключення. Маркування пам'яті виконується за допомогою біта NX (через буфер асоціативної трансляції). На платформах Intel і ARM цей біт називається XD (англ. eXecute

Disable - вимкнення виконання) і, відповідно, XN (англ. eXecute Never - ніколи не виконувати). Ця технологія підтримується у більшості ОС, таких як Linux та Windows, а також у деяких системах реального часу;

– рандомізація розміщення адресного простору – ASLR, швидше, є особливістю роботи з віртуальним адресним простором в операційній системі, ніж апаратною функцією, але її також важливо розглянути. Ця технологія захищає від переповнення буфера та атаки повернення до бібліотеки. Подібні методи злому вимагають від зловмисника розуміння структури пам'яті та полягають у навмисному виконанні певного доброякісного коду чи бібліотек. Це непросте завдання, особливо якщо адресний простір змінюється випадково при кожному завантаженні. У Linux підтримується за допомогою латок PAX та Exec Shield. Microsoft також надає захист для купи, стека та блоків обробки.

Безпека зберігання даних.

Багато пристроїв IoT використовують постійне сховище на прикордонному вузлі або маршрутизаторі/шлюзі. Розумним туманним вузлам (англ. fog nodes) теж потрібно десь зберігати свої дані. Безпека даних є ключовим аспектом запобігання встановлення шкідливого ПЗ та захисту конфіденційної інформації у разі викрадення пристрою. Багато сховищ, таких як flash-накопичувачі та жорсткі диски, підтримують шифрування та захисні технології.

FIPS 140-2 (федеральний стандарт обробки інформації) – це правова норма, яка описує вимоги до шифрування та безпеки для електронних пристроїв, що зберігають конфіденційні дані. Крім технічних вимог вона визначає правила та процедури. FIPS 140-2 передбачає кілька рівнів безпеки:

– рівень 1 – суто програмне шифрування. Обмежена безпека;

– рівень 2 – обов'язкова автентифікація на основі ролей та здатність виявляти фізичне проникнення за допомогою спеціальних пломб;

– рівень 3 – передбачає стійкість до фізичного злому. При спробі проникнення пристрій видаляє важливі параметри безпеки. Включає криптографічний захист, управління ключами та автентифікацію з автентифікацією;

– рівень 4 – просунутий захист від злому для продуктів, призначених для роботи у фізично незахищеному середовищі.

Крім шифрування, також слід подбати про безпеку накопичувачів, що виводяться з експлуатації. Вилучення вмісту із старих систем зберігання даних – відносно просте завдання. Існують додаткові стандарти, що описують безпечний процес видалення даних з накопичувача (чи це диск з магнітними пластинами або пам'ять зі зміною фазового стану). Крім того, лабораторія NIST публікує документи про безпечне знищення вмісту, такі як NIST Special Publication 800-88 for Secure Erase.

Фізична безпека.

Стійкість до проникнення та фізична безпека відіграють важливу роль в інтернеті речей. Багато IoT-пристроїв розміщено віддалено, без будь-якого захисту. Це нагадує історію із проектом «Енігма» під час Другої світової війни. Вилучення робочої шифрувальної машини з німецького підводного човна U-110 допомогло зламати шифр. Зловмисник із безпосереднім доступом до IoT-пристрою може використовувати будь-які інструменти для злому системи, як ми бачили на прикладі експлойту «Ланцюгова реакція».

Раніше вже було надано приклад атаки сторонніми каналами за допомогою аналізу енергоспоживання; злом також може здійснюватися на основі часу, кешу, випромінювання електромагнітного поля та ланцюжка сканування. Головна особливість атак сторонніми каналами полягає в тому, що зламаний пристрій, по суті, перетворюється на тестовий майданчик. Це означає, що воно перебуватиме

під наглядом у контрольованому середовищі та його активність буде всіляко вимірюватися.

Крім того, такі методики, як DPA, використовують статистичний аналіз для виведення закономірності між випадковим уведенням та висновком. Цей підхід застосовується тільки у випадку, якщо система демонструє ідентичну поведінку з тим самим введенням (рис. 1.11).

Методи запобігання цим атакам добре відомі, їх можна ліцензувати і використовувати в різного роду обладнанні. Серед контрзаходів можна виділити такі:

– зміна функції шифрування, щоб мінімізувати використання ключа. Використання ключів, дійсних лише на час поточного сеансу та заснованих на хеші оригінального ключа;

– для атак за часом: випадкова вставка функцій, які не порушують роботу алгоритму; використання випадкових машинних інструкцій для створення великої робочої функції, яку складно зламати;

Рисунок 1.11 – Методики виявлення атак

– видалення умовних відгалужень, які залежать від ключа;

– для атак на основі енергоспоживання: мінімізація витоків та обмеження операцій з ключем. Це зменшить робочий набір показників зловмисника;

– впровадження перешкод у лінії електропередач. Варіювання часу виконання операцій або усунення таймерів;

– зміна порядку проходження незалежних операцій. Це знижує ступінь кореляції навколо обчислень у S-блоці. Зміна функції шифрування, щоб мінімізувати використання ключа. Використання ключів, дійсних лише на час поточного сеансу та заснованих на хеші оригінального ключа;

– для атак за часом: випадкова вставка функцій, які не порушують роботу алгоритму; використання випадкових машинних інструкцій для створення великої робочої функції, яку складно зламати;

– видалення умовних відгалужень, які залежать від ключа;

– для атак на основі енергоспоживання: мінімізація витоків та обмеження операцій з ключем. Це зменшить робочий набір показників зловмисника;

– впровадження перешкод у лінії електропередач. Варіювання часу виконання операцій або усунення таймерів;

– зміна порядку проходження незалежних операцій. Це знижує ступінь кореляції навколо обчислень у S-блоці.

1.2.2 Криптографія

Шифрування та секретність є обов'язковими для IoT-пристроїв. Вони допомагають убезпечити взаємодію, захищаючи прошивку та процес аутентифікації. Шифрування можна поділити на три основні категорії (рис. 1.12):

– симетричне шифрування – для шифрування і дешифрування застосовується один і той же ключ. Симетричними є такі алгоритми як RC5, DES, 3DES та AES;

– шифрування з відкритим ключем – ключ, використаний для шифрування даних, доступний публічно. Але тільки сторона, що приймає, володіє закритим ключем для розшифровки повідомлення. Такий вид шифрування також називають асиметричним. Асиметрична криптографія використовується для забезпечення таємності даних, аутентифікації та невідмовності. Відкриті ключі застосовуються у широко відомих інтернет-протоколах для шифрування та обміну повідомленнями, таких як Elliptic Curve, PGP, RSA, TLS та S/MIME;

– криптографічне хешування – прив'язує дані довільного розміру до бітового рядка (який називають дайджестом). Хеш-функція від початку створюється «односпрямованої». По суті, єдиний спосіб відтворити підсумковий хеш – перепробувати всі можливі комбінації (хеш-функцію не можна виконати у зворотному напрямку). Прикладами однонаправлених хешів є MD5, SHA1, SHA2 та SHA3. Зазвичай вони застосовуються для шифрування цифрових підписів в образах прошивок, імітівставки і при аутентифікації. Під час шифрування невеликих рядків, таких як пароль, введення може бути занадто коротким для створення повноцінного хешу; у цьому випадку до пароля додається сіль або публічний рядок, щоб збільшити ентропію. Сіль – це різновид функції формування ключа (англ. key derivation function, чи KDF).

Тут представлені симетрична, асиметрична та хешируюча функції. Зверніть увагу на використання ключів у перших двох. Симетричний алгоритм вимагає використання ідентичних ключів для шифрування та розшифрування даних. Він виграє за швидкістю у симетричного шифрування, але його ключі повинні зберігатися у безпечному місці.

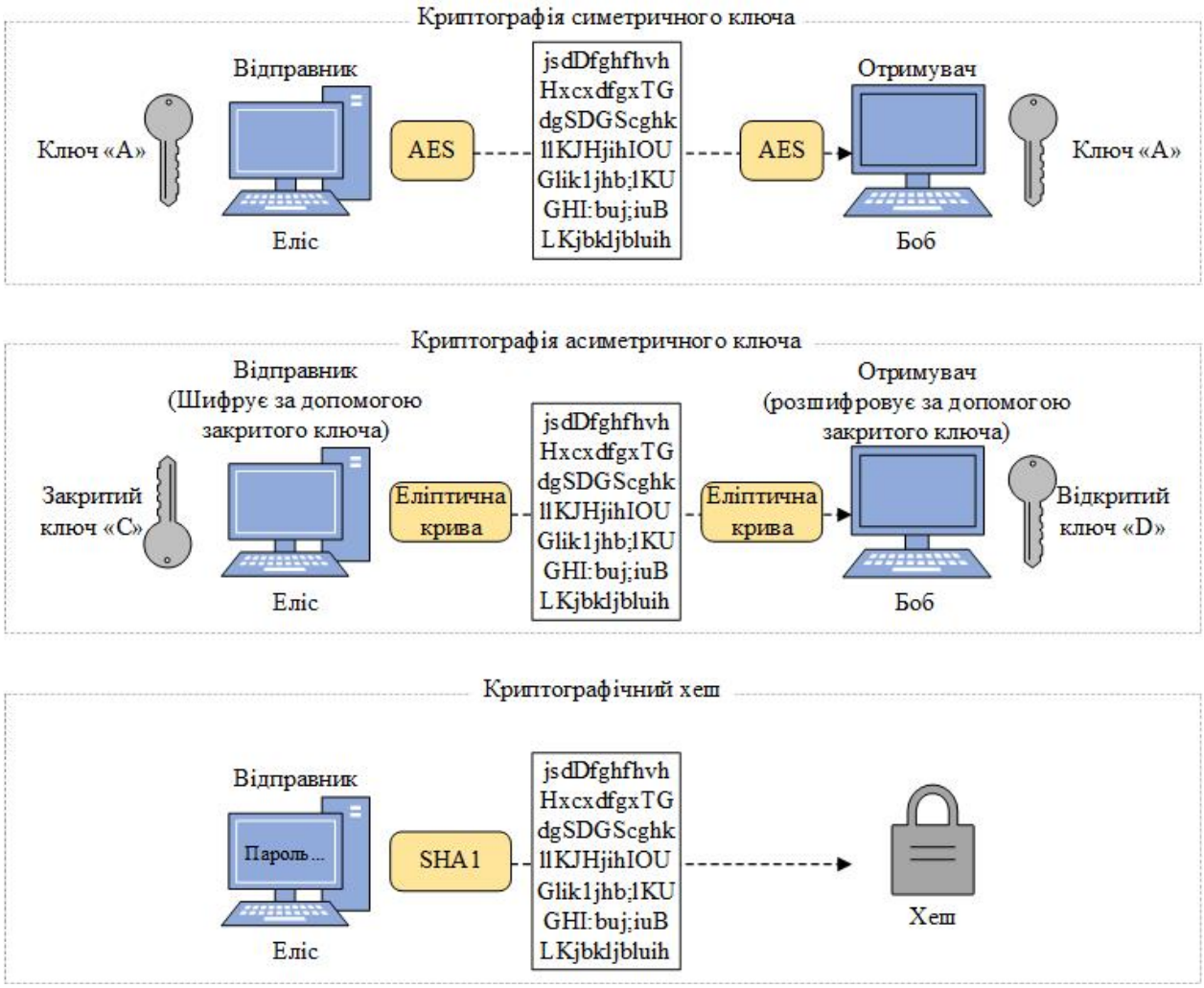


Рисунок 1.12 – Елементи криптографії

Симетрична криптографія.

У криптографії використовуються такі терміни, як простий текст (англ. plaintext) та шифротекст (англ. ciphertext), які позначають незашифроване введення і, відповідно, зашифрований висновок. Поточним стандартом шифрування вважається AES (Advanced Encryption Standard - просунутий стандарт шифрування); він прийшов на зміну старому алгоритму DES, розробленому у 1970-х роках. AES є частиною специфікації FIPS та стандарту ISO/IEC 18033-3, які використовуються у всьому світі. Алгоритми AES засновані на блоках фіксованої

довжини 128, 192 або 256 біт. Повідомлення, що перевищують довжину блоку, розбиваються кілька частин. AES складається із чотирьох основних етапів шифрування.

Довжина ключів AES дорівнює 128, 192 або 256 біт. В цілому, чим довший ключ, тим краще захист. Розмір ключа пропорційний кількості циклів процесора, необхідних для шифрування або розшифрування блоку: 128 біт вимагає 10 циклів, 192 біти – 12 циклів, а 256 бітів – 14 циклів.

Блокові шифри є алгоритмами, які засновані на симетричному ключі і обробляють дані у вигляді послідовних блоків.

Сучасні шифри засновані на статті про промислове шифрування, написаної Клодом Шенноном в 1949 р. Режим шифрування - це алгоритм, який описує багаторазове застосування блокового шифру для перетворення великих обсягів даних, що складаються з безлічі блоків.

Більшість сучасних шифрів використовують вектор ініціалізації (англ. Initialization Vector, або IV), завдяки якому те саме введення щоразу перетворюється на різний шифротекст. Алгоритм AES має кілька режимів роботи:

– режим простої заміни (англ. Electronic Codebook, або ECB) – це найпростіший вид AES-шифрування; він застосовується у поєднанні з іншими режимами для покращення безпеки. Дані поділяються на блоки, кожен із яких шифрується окремо. Ідентичні блоки дають той самий результат, що робить цей підхід щодо ненадійним;

– режим зчеплення блоків (англ. Cipher Block Chaining, або CBC) – перед шифруванням до простого тексту застосовується виключне АБО з попереднім зашифрованим блоком;

– режим зворотного зв'язку по шифротексту (англ. Cipher Block Chaining, або CFB) - схожий на CBC, але формує потік шифрів (виведення попереднього шифру служить введенням для наступного). CFB використовує попередній

зашифрований блок, щоб згенерувати введення для поточного шифру. Через цю залежність CFB не можна виконувати паралельно. Поточні шифри допускають втрату блоку під час передачі; у цьому випадку його буде відновлено на основі наступних блоків;

– режим зворотного зв'язку по виходу (англ. Output Feedback Chaining, або OFB) – цей режим аналогічний CFB, але дозволяє застосовувати коди виправлення помилок ще до шифрування;

– режим лічильника (англ. Counter, або CTR) – перетворює блоковий шифр на потоковий, використовуючи інкрементальний лічильник, який розпаралелює подачу введення кожному блоковому шифру, що прискорює виконання. Як введення використовується поєднання лічильника та випадково згенерованого числа;

– CBC з імітовставкою (CBC-MAC) – імітівставка (англ. Message Authentication Code, або MAC) використовується для автентифікації повідомлення та підтвердження того, що воно надійшло від заявленого відправника. Потім одержувач додає імітівставку до повідомлення для подальшої автентифікації.

Ці режими розроблялися з кінця 1970-х до початку 1980-х. та просувалися Національним інститутом стандартів та технологій у специфікації FIPS 8 у рамках алгоритму DES. Вони забезпечують конфіденційність інформації, але не захищають від її зміни та заміни. У зв'язку з цим почали використовувати цифрові підписи, а співтовариство з безпеки розробило режим CBC-MAC для аутентифікації. Застосування CBC-MAC у поєднанні з вихідними режимами було непростим завданням, доки з'явилися алгоритми на кшталт AES-CCM, які надають як автентифікацію, і секретність. CCM розшифровується як Counter with CBC-MAC Mode (лічильник із режимом CBC-MAC).

CCM – це важливий режим, який використовується для підпису та шифрування даних у цілій низці протоколів, розглянутих у цій книзі, включаючи

Zigbee, Bluetooth Low Energy, TLS 1.2 (після обміну ключами), IPSEC та 802.11 Wi-Fi WPA2.

AES-CCM використовує подвійний шифр: CBC та CTR. AES-CTR (або режим лічильника) застосовується для загального розшифрування вхідного потоку з шифротекстом, який містить зашифровану імітівставку. AES-CTR розшифровує як імітівставку, так і самі дані. На цьому етапі алгоритму формується так звана очікувана імітівставка; оригінальний заголовок кадру та розшифровані блоки, отримані на виході з AES-CTR, позначаються як введення. Дані розшифровані, однак для аутентифікації необхідна імітівставка, що обчислюється AES-CBC; якщо вона відрізняється від тієї, що очікується на етапі AES-CTR, це означає, що дані могли бути змінені у процесі передачі.

На рис. 1.13 показаний зашифрований потік даних, який автентифікується за допомогою AES-CBC та розшифровується в режимі AES-CTR. Таким чином забезпечується автентифікація та секретність оригінального повідомлення.

Важливим аспектом, з точки зору IoT-пристроїв у повнозв'язковій mesh-мережі, є кількість необхідних ключів. Для n вузлів у mesh-мережі з двонаправленою взаємодією цей показник дорівнює n(n-1)/2 або O(n2).

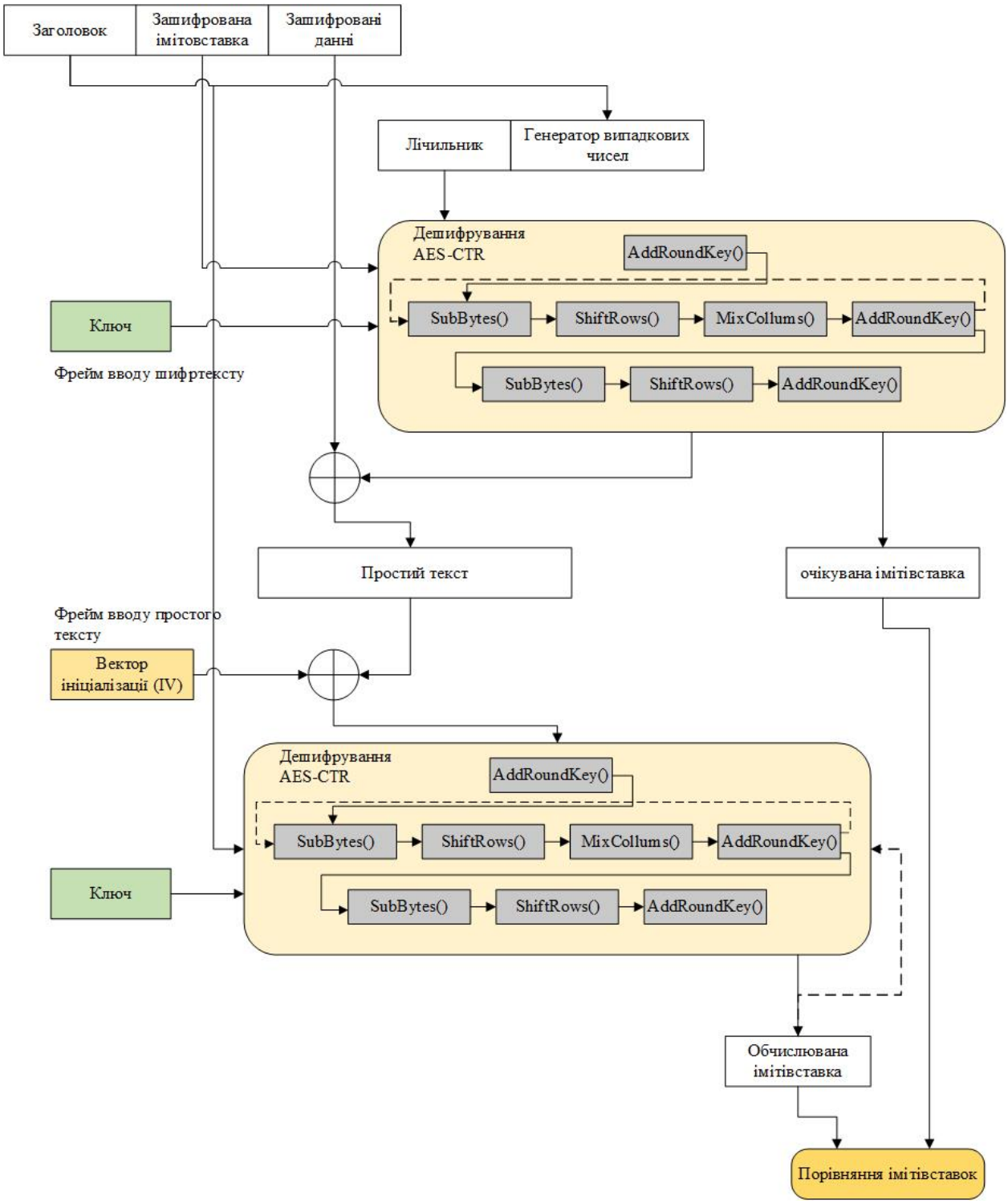


Рисунок 1.13 – Режим AES-CCM

Асиметрична криптографія.

Асиметричну криптографію також називають шифруванням із відкритим ключем. Асиметричні ключі генеруються попарно (для шифрування та дешифрування); вони можуть бути взаємозамінними - тобто один ключ може шифрувати і розшифровувати, хоча це не обов'язкова вимога. Але зазвичай генерується пара ключів один відкритий, а інший закритий. У цьому розділі описано три основні шифри з відкритим ключем: RSA, протокол Діффі-Хеллмана та еліптичні криві.

Варто відзначити, що на відміну від симетричних ключів, кількість яких обчислюється з розрахунку на взаємодію будь-яких двох вузлів у мережі, ассиметричная криптографія вимагає лише 2n або O(n) ключів.

Перший метод асиметричного шифрування з відкритим ключем був описаний в алгоритмі Рівеста-Шаміра-Адлемана (англ. Rivest-Shamir-Adleman, або RSA), розробленому в 1978 р. Він має на увазі, що користувач повинен знайти та опублікувати добуток двох великих простих чисел та допоміжний значення (відкритий ключ). Відкритий ключ дозволяє шифрувати повідомлення і доступний будь-кому, але прості множники залишаються конфіденційними. Алгоритм виглядає так:

1) знаходимо два великі прості числа, p і q;

2) $n = pq$;

3) $\phi(n) = (p1)(q-1)$;

4) відкритий ключ - вибираємо ціле число e, яке є взаємно простим для $\phi(n)$ і знаходиться в діапазоні $1 < e < \phi(n)$; типовим значенням є 216+1=65537;

5) закритий ключ - обчислюємо d для вирішення рівняння конгруенції:

$de \equiv 1 (\mathrm{mod}\ \phi(n))$.

Таким чином, для шифрування повідомлення використовується відкритий ключ (n, e), а для його розшифрування – закритий ключ (n, d):

– шифрування: шифротекст = (простий текст) e mod n;

– розшифровка: простий текст = (шифротекст) dmod n.

Часто до коротких повідомлень перед шифруванням додається зсув, щоб отримати хороший шифротекст.

Напевно, найвідомішим видом обміну асиметричними ключами є протокол Діффі-Хеллмана (названий на честь Вітфілда Діффі та Мартіна Хеллмана) (рис. 1.14). Типовим для асиметричної криптографії вважається поняття односторонньої функції з потайним входом (англ. Trapdoor Function), яка набуває заданого значення A і повертає висновок B; але при цьому B не можна отримати A.

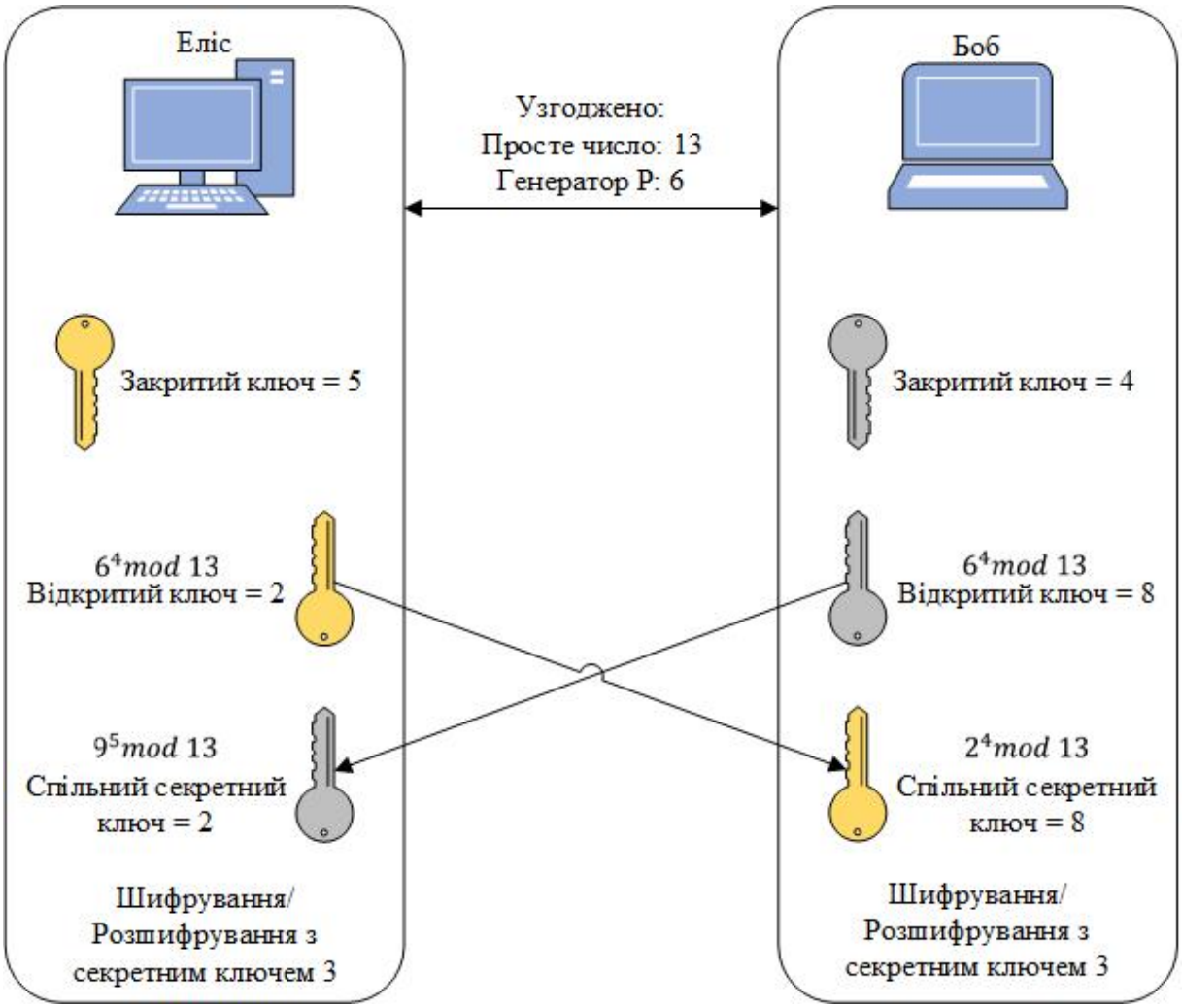


Рисунок 1.14 – Протокол Діффі-Хеллмана

Метод Діффі-Хеллмана дозволяє обом сторонам (Еліс А та Боб В) обмінюватися ключами, не знаючи заздалегідь про загальний ключ s. Алгоритм заснований на відкритому обміні початковим простим числом, p і генераторі простих чисел g, який являє собою первісний корінь p. Нехай закриті ключі Еліс та Боба називаються a та b. Тоді A = ga mod p та B = gb mod p. Свої секретні ключі Еліс та Боб обчислюють як s = Ba mod p та s = Ba mod p.

У результаті, (ga mod p) b mod p = (gb mod p) a mod p.

Сильною стороною такого обміну ключами є генерація по-справжньому випадкового числа для кожного закритого ключа. Найменша передбачуваність у роботі генератора псевдовипадкових чисел може призвести до злому шифру. Однак принциповим недоліком тут є відсутність аутентифікації, що відкриває можливість для MITM-атаки.Процес починається з відкритого обміну заздалегідь узгодженими простим числом та генератором простих чисел. Еліс та Боб генерують незалежні закриті ключі, а відкриті ключі генеруються та відправляються через мережу в незашифрованому вигляді. На основі цього виходить секретний ключ, який використовується для шифрування та розшифровки. Ще один спосіб обміну ключами, протокол Діффі-Хеллмана на еліптичних кривих (англ. Elliptic-Curve Diffie-Hellman, або ECDH), був запропонований Коблитцем і Міллером у 1985 р. заснований на алгебрі еліптичних кривих над кінцевим полем. Алгоритм ECDH отримав підтримку з боку інституту NIST і схвалено NSA для шифрування абсолютно секретних матеріалів з використанням 384-бітних ключів. Криптографія на основі еліптичних кривих (Elliptic Curve Cryptography, або ECC) має наступні відмітні характеристики:

– симетричність по осі x;

– еліптична крива може перетинатися з прямою лінією не більше ніж у трьох точках.

Процес ECC (рис. 1.15) починається з проведення прямої лінії із заданої точки на межі у напрямку MAX. Ця лінія з'єднує A і B. Скалярний добуток точки A використовується для проведення лінії між двома точками, після чого на новому непоміченому перетині креслиться строго вертикальна лінія або вгору або вниз. Цей процес повторюється n разів, де n – розмір ключа.

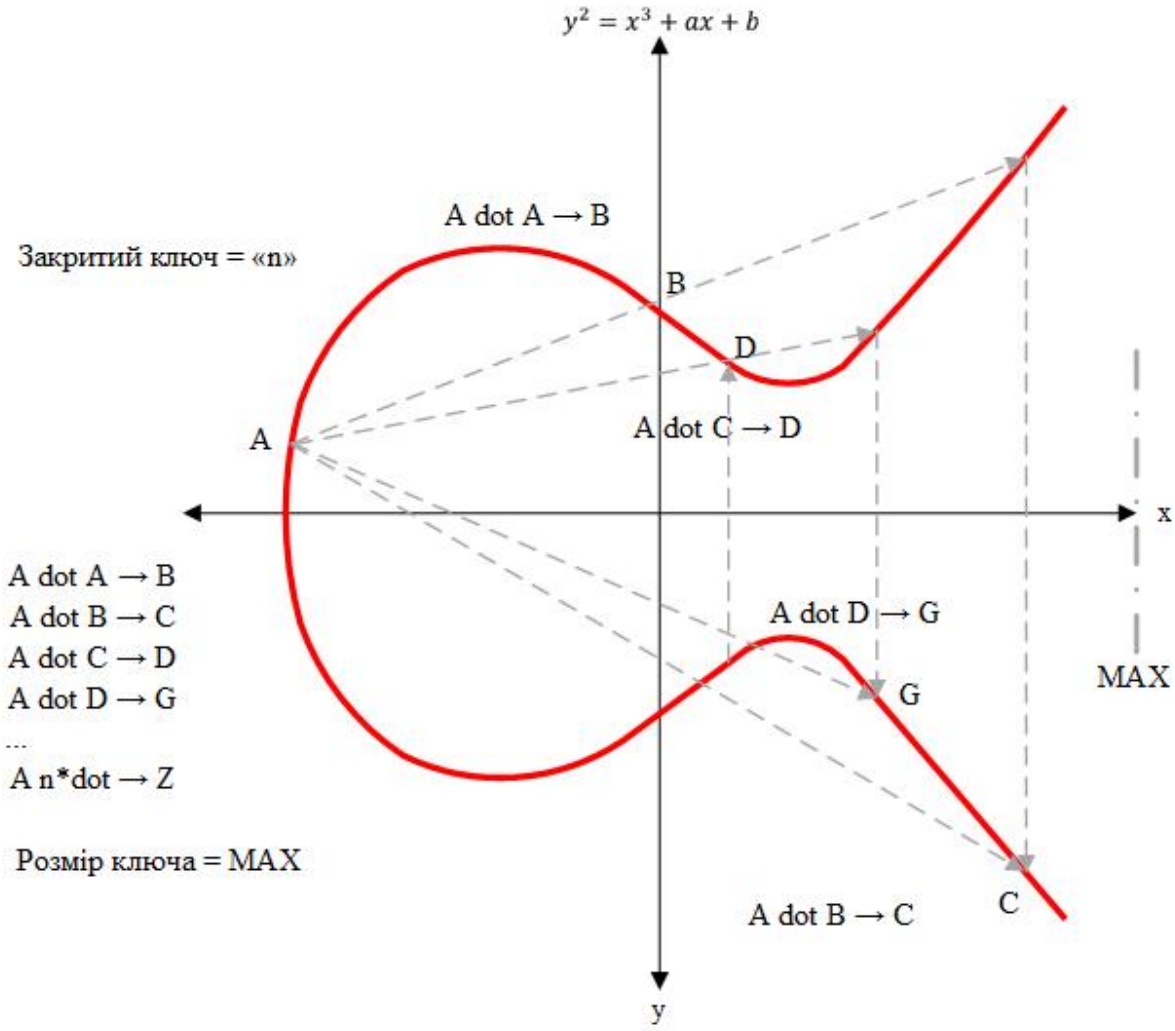


Рисунок 1.15 – Криптографія на основі еліптичних кривих (ECC)

Це схоже на кінцевий результат удару по більярдній кулі після того, як той багато разів ударився об борт столу. Підсумкове розташування кулі не дозволяє спостерігачеві визначити, якою була його вихідна позиція.

MAX – це максимальне значення осі x, яке обмежує віддаленість вершини. Якщо вершина виходить за межі MAX, алгоритм застосовує це значення і встановлює нову точку x-MAX, віддалену від вихідної точки A. Значення MAX еквівалентно розміру ключа, що використовується. Довгий ключ генерує більше вершин та підвищує стійкість до злому. По суті, це функція обгортка.

Тут показано стандартну еліптичну криву на осях x і y. Процес починається з проведення прямої лінії із заданої точки A до другої точки і пошуку третього, непоміченого перетину. Лінія проводиться строго вертикально до протилежного значення осі y, яке в цей момент маркується. Процес продовжується для n точок, що відповідають довжині ключа.

Еліптичні криві починають превалювати над RSA. Сучасні браузери підтримують алгоритм ECDH, який є кращим методом автентифікації SSL/TLS. Як ви пізніше побачите, ECDH можна знайти у Bitcoin та деяких інших протоколах. На сьогоднішній день RSA використовується тільки у випадку, якщо SSL-сертифікат має відповідний RSA-ключ.

Ще одна перевага полягає в тому, що навіть короткі ключі забезпечують таку ж криптографічну стійкість, як застарілі методи. Наприклад, 256-бітний ключ в ECC еквівалентний 3072-бітного ключа в RSA. Цю властивість слід враховувати у контексті обмежених IoT-пристроїв.

Криптографічний хеш (автентифікація та цифровий підпис).

Третім видом технології шифрування є функції, що хешируют.

Зазвичай вони використовуються для створення цифрових підписів і вважаються «односпрямованими» без можливості зворотного виконання. Для відтворення вихідних даних, що пройшли через функцію хешування, довелося б перебирати всі можливі комбінації введення. Ключові характеристики функції хешування:

– завжди генерує один і той же хеш з однакового введення;

– швидка у обчисленні, але не миттєва (див. доказ виконання роботи);

– необоротна; не може згенерувати вихідне повідомлення із хешу;

– найменша зміна введення викликає суттєву ентропію і повністю змінює висновок;

– два різних повідомлення ніколи не будуть мати один і той же хеш.

Алгоритми сімейства SHA активно використовуються в:

– репозиторіях Git;

– цифрових підписах TLS-сертифікатів для веб-браузерів (HTTPS);

– перевірці автентичності вмісту файлу або образу диска.

Більшість хеш-функцій ґрунтуються на структурі Меркла-Дамгарда. У наведеному нижче прикладі введення розбивається на блоки однакового розміру, кожен з яких проходить через функцію стискання із застосуванням результатів стиснення попереднього блоку. Для вибору початкового значення використається вектор ініціалізації. Завдяки функції стиснення хеш виходить стійким до колізій. Алгоритм SHA-1 побудований з урахуванням структури Меркла-Дамгарда (рис. 1.16).

Загалом повідомлення, які подаються на введення алгоритму SHA, повинні бути менше 264 біт. Вони послідовно обробляються у 512-бітових блоках. Стандарт SHA-1 витіснений більш стійкими версіями, такими як SHA-256 та SHA-3. У хешах SHA-1 знайшли можливість колізій; і хоча для цього потрібно приблизно від 251 до 257 операцій, злом хешу на орендованому графічному адаптері коштуватиме лише кілька тисяч доларів. У зв'язку із цим рекомендується перейти на інші різновиди SHA.

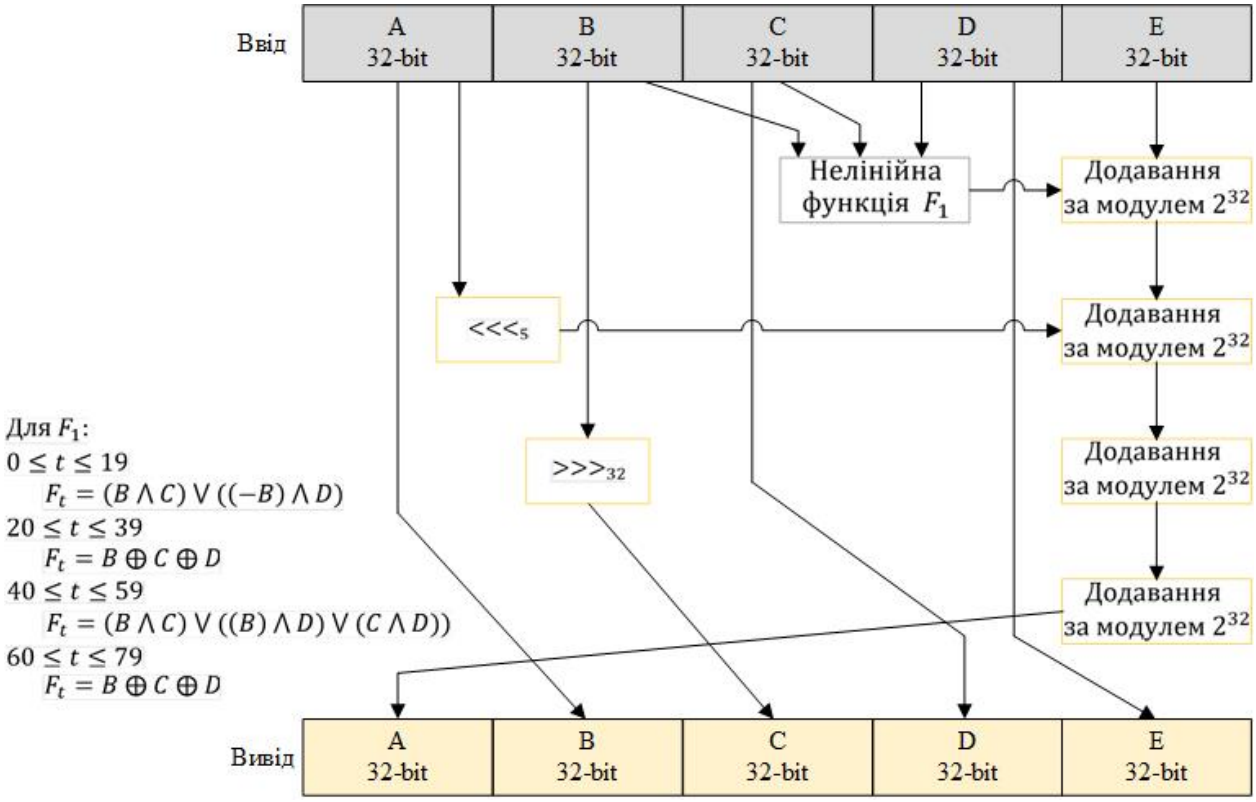


Рисунок 1.16 – Алгоритм SHA-1. Введення розбивається на п'ять 32-бітових блоків

Інфраструктура відкритого ключа.

Асиметрична криптографія (з відкритим ключем) – це основа торгівлі та взаємодії в Інтернеті. Вона повсюдно використовується в SSL та TLS з'єднаннях. Типовим прикладом є ситуація, коли передані дані можуть бути зашифровані за допомогою відкритого ключа (тобто, будь-ким), але розшифрувати їх може той, кому належить закритий ключ. Ще одне застосування пов'язане з цифровими підписами, коли відправник підписує двійкові дані закритим ключем, а одержувач може перевірити їхню справжність, якщо в нього є відкритий ключ.

Щоб налагодити надійну видачу відкритих ключів, використовується процес під назвою інфраструктура відкритого ключа (Public Key Infrastructure, або PKI). Гарантія справжності забезпечується за рахунок центрів, що засвідчують (англ.

Certificate Authorities, або CA), які управляють ролями і правилами, створюючи розподілені цифрові сертифікати. Найбільшими публічними видавцями TLS-сертифікатів є компанії Symantec, Comodo та GoDaddy. Формати сертифікатів на основі відкритих ключів описуються стандартом X.509. Це основа безпечної взаємодії у протоколах TLS/SSL та HTTPS. X.509 визначає такі атрибути як алгоритм шифрування, термін придатності і видавець сертифіката.

До складу PKI входить центр реєстрації (англ. Registration Authority, або RA), який автентифікує відправника, керує окремими ролями/правилами та може відкликати сертифікат. Для передачі списків відкликаних сертифікатів RA взаємодіє з центром автентифікації (англ. Validation Authority, або VA). CA видає сертифікат відправнику. Коли повідомлення отримано, VA може перевірити справжність ключа та переконатися, що він не був анульований.

На рис. 1.17 показано приклад інфраструктури PKI. Тут використовуються системи CA, RA та VA, а шифрування повідомлення передбачає видачу ключа та перевірку його справжності.

Мережевий стек: протокол захисту транспортного рівня.

Протокол захисту транспортного рівня (англ. Transport Layer Security, або TLS) вже не раз згадувався на сторінках цієї книги, починаючи з TLS та DTLS для MQTT та CoAP і закінчуючи мережевою безпекою в WAN та PAN. Кожен із цих протоколів так чи інакше покладається на TLS. Стандарт TLS увібрав у себе всі криптографічні протоколи та технології, які ми вже обговорювали. У цьому розділі ми коротко пройдемося за специфікацією TLS1.2, її структурою та використанням.

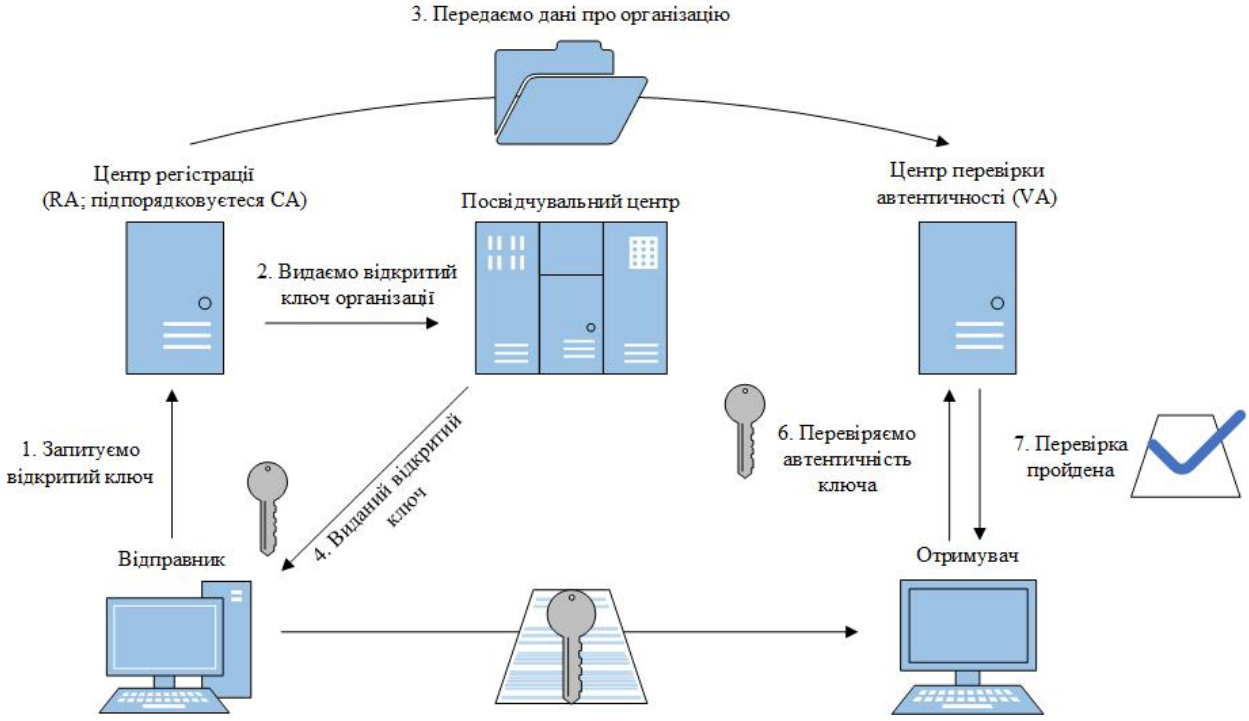


Рисунок 1.17 – Приклад інфраструктури PKI

Спочатку рівень захищених сокетів (англ. Secure Sockets Layer, або SSL) був представлений у 1990 р., але вже за 9 років йому на зміну прийшла технологія TLS. З 2008 р. поточна специфікація TLS1.2 входить до стандарту RFC5246. TLS 1.2 включає генератор хешів SHA-256, який був доданий замість SHA-1 для поліпшення безпеки.

Процес шифрування в TLS виглядає так:

1) клієнт відкриває з'єднання з сервером, який підтримує TLS (порт 443 для HTTPS);

2) клієнт надає список шифрів, які він підтримує;

3) сервіс вибирає шифр та функцію шифрування та повідомляє клієнт;

4) сервер передає клієнту цифровий сертифікат, виданий посвідчуючим центром і містить відкритий ключ;

5) клієнт підтверджує справжність сертифіката;

6) для генерації ключа сеансу використовується один із двох способів:

1) серверу передається випадкове число, попередньо зашифроване за допомогою його відкритого ключа. Потім сервер та клієнт створюють на його основі ключ сеансу, який використовується протягом взаємодії;

2) ключ сеансу для шифрування та дешифрування генерується за допомогою протоколу Діффі-Хеллмана. Отриманий ключ використовується, доки не закриється з'єднання.

7) взаємодія перетворюється на зашифрований канал.

На рис. 1.18 показаний процес рукостискання двох пристроїв, що взаємодіють через TLS1.2.

Протокол датаграм безпеки транспортного рівня (Datagram Transport Layer Security, або DTLS) – це комунікаційний протокол на основі TLS, який працює поверх UDP (версія DTLS 1.2 заснована на TLS 1.2). Він призначений для забезпечення подібних гарантій безпеки та використовується у легковажному протоколі CoAP.

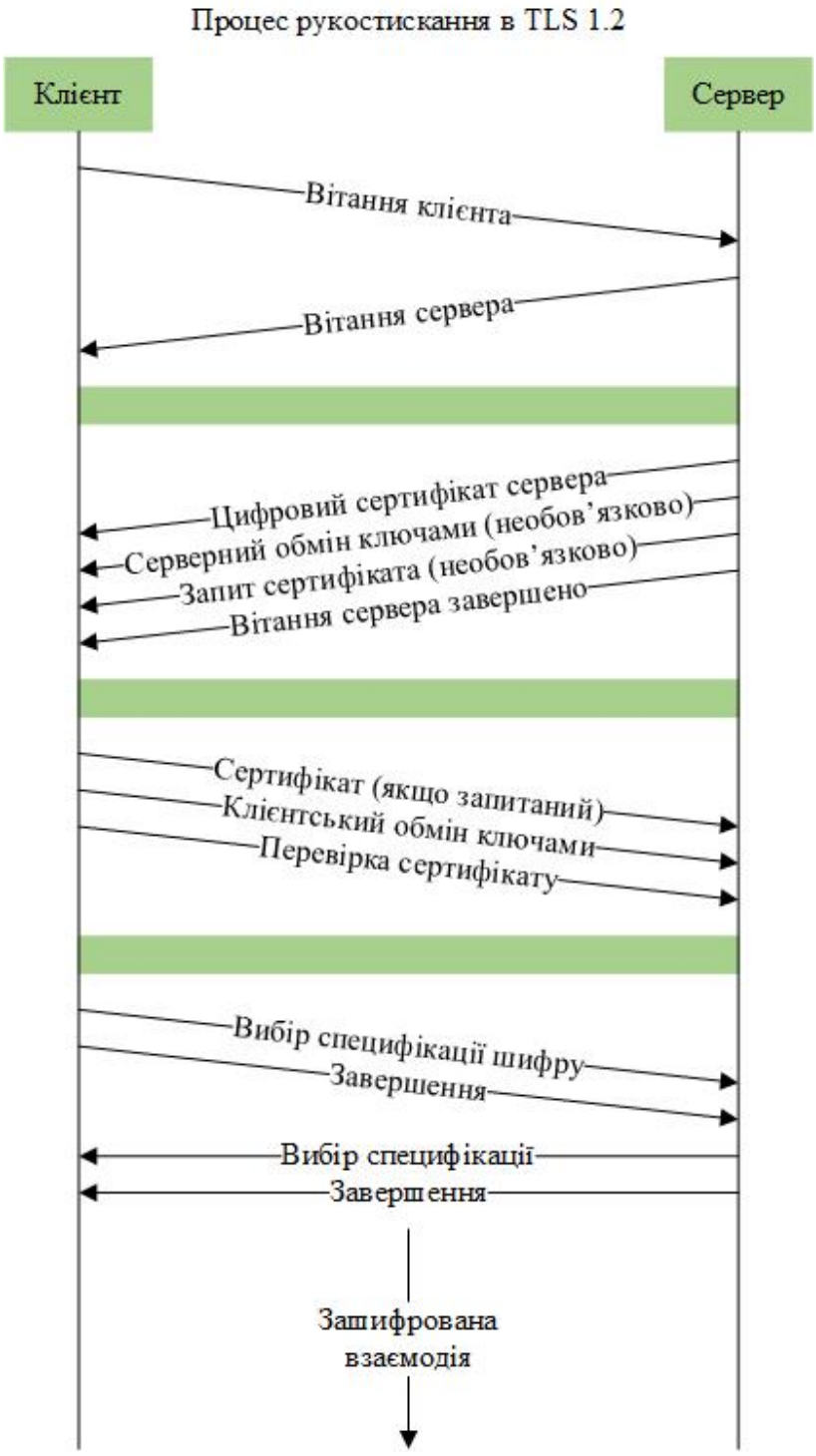


Рисунок 1.18 – Послідовність кроків при рукостисканні в TLS 1.2

1.2.3 Програмно-визначуваний периметр

Раніше ми обговорювали такі поняття, як програмно-визначені оверлейні мережі. Здатність оверлейної мережі створювати мікросегменти є надзвичайно корисною, особливо при масовому масштабуванні IoT-пристроїв та ситуаціях, коли є можливість нівелювати наслідки DDoS-атаки. Програмно-визначені мережі мають додатковий компонент під назвою SDP (Software-Defined Perimeter – програмно-визначуваний периметр), який заслуговує на окрему увагу в контексті безпеки оверлейних мереж.

Архітектура програмно-визначеного периметра.

Програмно-визначуваний периметр (Soft.-Defined Perimeter, або SDP) – це підхід до побудови мережі, який не передбачає жодної моделі довіри. Він заснований на так званій чорній хмарі Департаменту систем захисту інформації (Defense Information Systems Agency, або DISA). У чорній хмарі обмін інформацією відбувається лише за необхідності. SDP може пом'якшити наслідки таких атак, як DDoS, MITM, експлойти нульового дня, сканування серверів і т.д. на запрошення (на основі автентичності).

SDP можна використовувати для створення оверлейної мережі (це мережа, побудована поверх іншої мережі). Наприклад, колись інтернет-сервіси були засновані на телефонних комунікаціях. У такій гібридній моделі розподілений керуючий рівень залишається незмінним. Прикордонні маршрутизатори та віртуальні комутатори направляють дані залежно від правил, описаних на рівні керування. Оскільки стійкість мережі SDN багато в чому подібна до дротових мереж, вона ідеально підходить для додатків реального часу, віддаленого моніторингу та складної обробки подій. Можливість створення декількох оверлейних мереж поверх тих самих прикордонних компонентів дозволяє виконувати мікросегментацію, відкриваючи споживачам прямий доступ до різних

ресурсів. Кожна пара «ресурс-споживач» є незмінною мережею; її доступ межі віртуального оверлея визначається системним адміністратором.

Можливість створення кількох оверлейних мереж поверх тих самих прикордонних компонентів дозволяє виконувати мікросегментацію, коли кожна кінцева точка в глобальній розподіленій мережі IoT може формувати окремі ізольовані сегменти, використовуючи наявну інфраструктуру. Теоретично ми можемо ізолювати кожен датчик. Це потужний інструмент, який дозволяє підключатися до IoT-пристроїв як сервісів, використовуючи з'єднання промислового рівня, а також ізолювати та захищати їх один від одного.

На рис. 1.19 показаний приклад SDN-оверлею.

У якоїсь корпорації є три віддалених магазину з рядом різних IoT-пристроїв та прикордонних компонентів у кожному. Мережа заснована на SDN-оверлеї з мікросегментами, що ізолюють системи POS та VOIP; ті, у свою чергу, корпоративно управляються за допомогою датчиків, призначених для моніторингу безпеки, страхових умов та стану холодильної камери. Сторонні постачальники послуг можуть керувати різними віддаленими датчиками, кожен з яких знаходиться в ізольованій та безпечній віртуальній оверлейній мережі.

Щоб підсилити безпеку SDP, можна розробити систему запрошень, примушуючи парні пристрої аутентифікуватись перед підключенням. У мережу можуть бути додані лише попередньо авторизовані користувачі та клієнти. Керуючий рівень може розширити цей підхід, надаючи запрошення через електронну пошту чи механізм реєстрації. Якщо користувач прийме запрошення, клієнтські сертифікати та повноваження будуть розповсюджуватися лише на систему, з якою він працює. Система запрошень веде список розширених сертифікатів та надає оверлейне з'єднання лише у випадку, якщо обидві сторони прийняли запропоновані ним ролі.

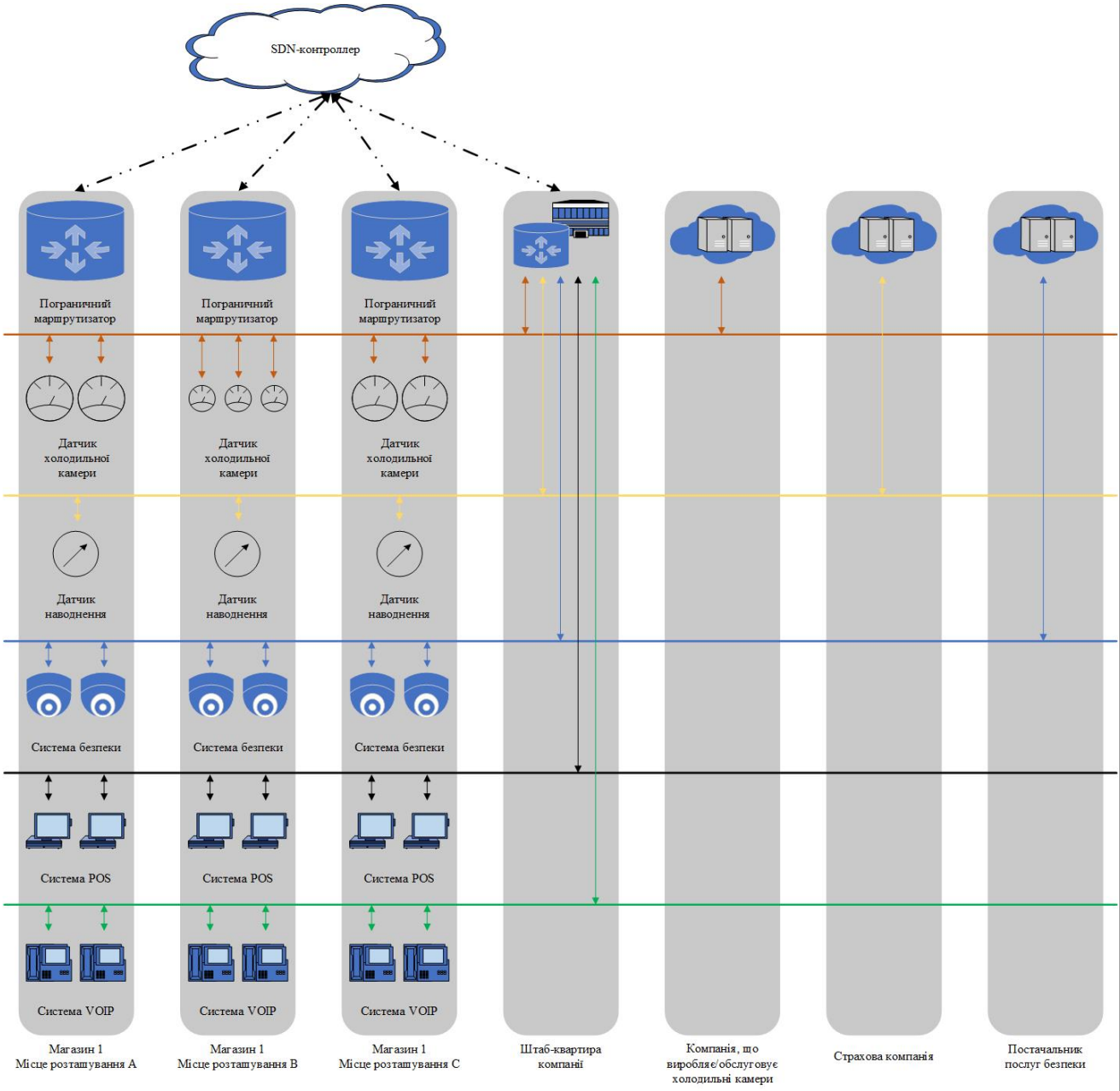


Рисунок 1.19 – Приклад оверлейної SDN-мережі

Як аналогія з реального світу можна навести розсилку запрошень на вечірку. Запрошення надсилаються окремим друзям поштою, із зазначенням дати, часу, адреси та інших подробиць. Кожен із адресатів сам вирішує, чи приймати

запрошення. Як варіант, вечірку можна прорекламувати по інтернету, телевізору чи радіо; у цьому випадку кожен відвідувач перевіряється на вході.

1.2.4 Рекомендації щодо захисту IoT-пристроїв

В інтернеті речей безпека повинна враховуватися від початку, а не заднім числом, після завершення проектування або введення в експлуатацію – на цих етапах буде вже запізно. Крім того, підхід до безпеки повинен бути комплексним та покривати всі аспекти: від апаратного забезпечення до хмари. У цьому розділі розглядається простий проект IoT із захистом, який пронизує всі його рівні, починаючи з датчика та запобіжними заходами, щоб ускладнити завдання потенційним зловмисникам.

Комплексна безпека.

Якщо зосередитися на якомусь одному аспекті інтернету речей, підсумковий ланцюжок безпеки матиме слабкі ланки. Безпека повинна пронизувати всі рівні системи: від датчика до хмари. Це комплексний підхід. Кожен компонент у ланцюжку керування та даних повинен мати контрольний список параметрів безпеки та потенційних загроз. На рис. 1.20 показаний приклад такої багаторівневої системи захисту, яку слід передбачити під час розгортання.

Тут наводиться приклад датчиків з підтримкою Bluetooth, які в основному взаємодіють з хмарним сервісом через прикордонний шлюз. Цілісність та безпека повинні забезпечуватися на кожному рівні. Це стосується як апаратних, так і програмних компонентів. Фізичні пристрої повинні бути захищені від заміни, а радіосигнали – від глушіння та DDoS-атак; обладнання для кореня довіри та ASLR запобігають впровадженню коду, дані шифруються, при поєднанні та зв'язуванні використовується аутентифікація, мережа прокладена через VPN-сервери та брандмауери тощо.

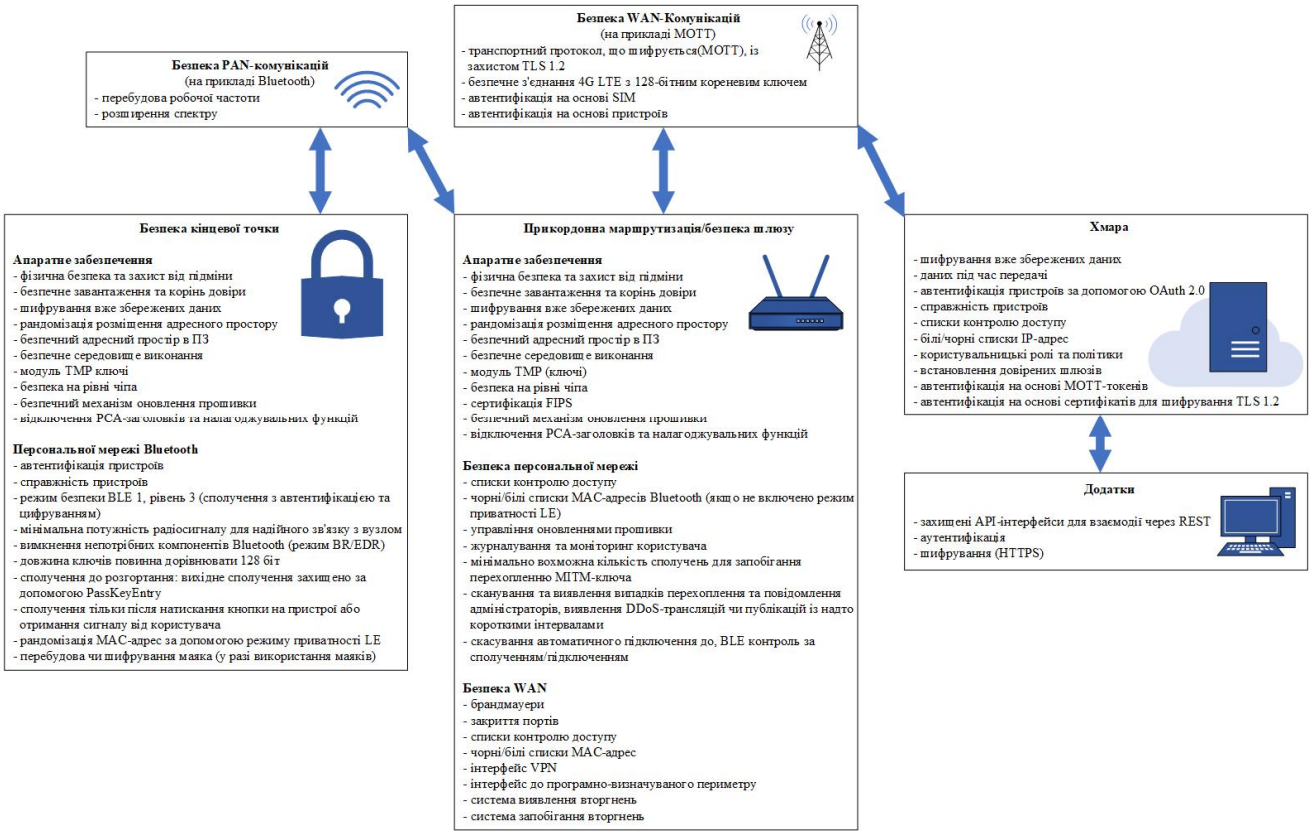


Рисунок 1.20 – Комплексний захист, починаючи з датчика та закінчуючи хмарою

Короткий перелік заходів безпеки.

Нижче наведено список перевірених часом рекомендацій та ідей щодо безпеки. Також важливо мати комплексний захист:

– використовуйте останні версії операційних систем і бібліотек з усіма необхідними латками;

– використовуйте апаратне забезпечення з підтримкою таких функцій захисту, як безпечні середовища виконання, модулі TPM і адресні простори, що не виконуються;

– обфускація коду в надії, що зловмисник не зможе його розплутати, - відносно безнадійна витівка. Підписуйте, шифруйте та захищайте свої прошивки та програмні образи – особливо ті, які доступні на веб-сайті компанії;

– вибирайте вихідний пароль випадковим чином;

– використовуйте корінь довіри та безпечне завантаження, щоб гарантувати, що на пристроях ваших клієнтів працює справжнє програмне забезпечення;

– приберіть паролі з коду прошивок;

– всі IP-порти повинні бути закриті за замовчуванням;

– використовуйте рандомізацію розміщення адресного простору, стікові індикатори та безпечні сегменти пам'яті, які підтримуються в сучасних ОС;

– використовуйте автоматичні оновлення. Надайте виробникам механізм для виправлення помилок та вразливостей у робочих системах. Для цього програмна архітектура має бути модульною;

– плануйте виведення з експлуатації заздалегідь. IoT-пристрої можуть працювати довго та продуктивно, але колись їх доведеться утилізувати. Це включає безпечне видалення і знищення всіх модулів постійної пам'яті (flash) в пристрої;

– пропонуйте своїм клієнтам та користувачам винагороду за знайдені помилки – особливо ті, які можуть призвести до появи вразливостей нульового дня;

– підпишіться на повідомлення про активні загрози, які розсилає US-CERT, щоб завжди бути в курсі про актуальні експлойти та кібератаки;

– побудова проекту на основі таких простих (і небезпечних) протоколів, як MQTT або HTTP, може здатися привабливою, але ви повинні постачати свої пристрої з включеною автентифікацією на основі TLS або DTLS. Шифруйте дані, починаючи з датчика та закінчуючи хмарою;

– використовуйте анти налагоджувальні ф'юз-біти. Детонуйте їх на етапі виробництва для безпечного налагодження, перш ніж випускати продукт.

Ми детально розглянули ризики безпеки в Інтернеті. Маючи на увазі наявність таких відомих вірусів як Mirai та Stuxnet, спеціально націлених на IoT-

пристрої, архітектори IoT-систем повинні від початку піклуватися про безпеку своїх архітектур. Інтернет речей є ідеальним середовищем для виконання різноманітних атак. Зазвичай системи цього мають менш зрілим захистом проти ПК. IoT-пристрої є найбільш великою поверхнею атаки на планеті, а віддаленість деяких з них дозволяє зловмисникам отримати фізичний доступ до обладнання, немислимий в безпечних офісних умовах. Ці загрози вимагають серйозної уваги, оскільки їхні наслідки можуть торкнутися як окремих пристроїв, так і міст або навіть цілі країни.

2 ОХОРОНА ПРАЦІ

Загальний аналіз умов праці під час роботи з комп'ютерною технікою.

Застосування інформаційних технологій безумовно передбачає вико-ристання комп'ютерної техніки. Головна складова цієї техніки, з якою безпосередньо контактує користувач, – це персональний комп'ютер (ПК). Інтенсивна робота з ПК є причиною виникнення багатьох захворювань. Причина відхилень у здоров'ї користувача – переважно недостатнє дотри-мання принципів ергономіки, неправильна організація робочого місця та санітарно-гігієнічних вимог до умов праці. Все це призводить до виник-нення низки захворювань: порушення зору; кістково-м'язових порушень; захворювань шкіри; порушень, пов'язаних зі стресовими ситуаціями та нервово-емоційним навантаженням. З огляду масовість застосування ПК, ця проблема є дуже важливою та актуальною.

Дія шуму на організм людини та захист від шуму.

Шум – це різноманітні небажані перешкоди сприйняттю мови, музики тощо. Шум як фізичне явище – це сукупність звуків різної частоти й інтенсивності. З фізіологічного погляду шум – шкідливий подразнювальний чинник, який діє на органи слуху і весь організм людини.

Для захисту від шуму вживають такі заходи.

Зменшення шуму в джерелі виникнення. Зменшення шуму в джерелі виникнення досягають шляхом його конструктивних змін: заміна металевих деталей на пластмасові, усунення проміжків у зубчастих передачах, заміна підшипників кочення і зубчатих передач, заміна ударної дії безударною, зменшення частоти обертів валів тощо.

Звукоізоляція. Суть звукоізоляції полягає в тому, що найбільша частина звукової енергії, яка падає на звукоізолювальна засоби, відбивається. До звукоізолювальних заходів належать огородження, стіни, перегородки, перекриття, спеціальні звукоізолювальні кожухи.

Звукопоглинання – це властивість будівельних матеріалів і конструкцій поглинати енергію звукових коливань. Поглинання звуку пов'язане з перетво-ренням енергії звукових коливань у тепло внаслідок втрат на тертя в каналах звукопоглинального матеріалу.

Архітектурно-планувальні заходи. Найшумніші виробництва рекомен-дують компонувати в окремі комплекси із забезпеченням розривів між найближчими сусідами.

Заходи індивідуального захисту. Використання протишумних навуш-ників внутрішніх, що вкладають у вухо, і зовнішніх, які закривають вухо повністю; протишумних касок, спеціального протишумного одягу, які ізолюють тіло і поглинають звук.

Електромагнітне випромінювання і його характеристики.

За сучасних умов виробництва масово застосовують прилади, різно-манітне обладнання та пристрої, робота яких пов'язана з використанням та утворенням електромагнітного випромінювання різних частот – від звукових хвиль до електромагнітних хвиль оптичного діапазону. Робота персоналу з об-слуговування обладнання, а також осіб, які перебувають поряд з обладнанням, пов'язана з впливом цього випромінювання на організм людини, тому потрібен спеціальний захист.

Загальні заходи захисту від дії електромагнітного випромінювання такі.

Захист часом передбачає обмежене перебування людини в електро-магнітному полі (ЕМП). Допустимий час перебування людини в ЕМП залежить від інтенсивності опромінення або напруженості ЕМП.

Захист відстанню застосовують, якщо не можна послабити інтенсивність опромінення в заданій зоні іншими способами. У цьому випадку збільшують відстань між випромінювачем і персоналом.

Зменшення потужності випромінювання безпосередньо в джерелі досягають використанням спеціальних пристроїв – поглиначів потужності (еквівалент антени і навантаження), які повністю поглинають або знижують енергію електромагнітного випромінювального, що передається на шляху від генератора до випромінюючого пристрою.

Екранування джерел випромінювання використовують для зменшення інтенсивності ЕМП на робочому місці. Для цього застосовують заземлені екрани з металевих листів або сіток у вигляді замкнутих камер, кожухів.

Засоби індивідуального захисту. До засобів захисту від ЕМП належать халати і комбінезони з металізованої тканини, з виводом на заземлення. Опір заземлення повинен бути 10 Ом. Для захисту очей від електромагнітного випромінювання використовують захисні окуляри.

Електробезпека.

Широке застосування електроенергії на виробництві потребує правильного поводження з нею, оскільки порушення правил електробезпеки може призвести до важкої і навіть смертельної травми.

Електробезпека – це система організаційних і технічних заходів і засобів, які забезпечують захист людей від шкідливої і небезпечної дії струму, електричної дуги, електромагнітного поля і статичної електрики.

Електричний струм, який проходить через організм людини, спричинює термічну, електролітичну, біологічну і механічну дії.

До головних способів захисту від ураження електричним струмом у разі дотику людини до частин обладнання, що проводять струм, належать: ізоляція, використання малих напруг, електричне розділення мереж, обгороджувальні

пристрої, попереджувальна сигналізація, блокування, засоби захисту, запобіжні пристосування.

Пожежна безпека.

Джерелами запалювання на підприємствах можуть бути: відкрите полум'я, невідповідність або несправність електрообладнання, іскри від удару і тертя деталей машин і обладнання, самозаймання, статична електрика, розряд блискавки та ін.

Пожежна небезпека електрообладнання, електронних приладів, радіо-електронної апаратури, апаратури керування, електроприймачів пов'язана з використанням гуми, пластмас, лаків, олій.

Для організації пожежної безпеки всі приміщення повинні бути забезпечені первинними засобами пожежогасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками. У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і приступити до ліквідації пожежі.

Організація роботи з персональним комп'ютером.

Для створення безпечних умов праці розроблені нормативи, які стосуються обладнання приміщень з комп'ютерною технікою, організації робочих місць з ПК, режиму роботи за ПК.

Вимоги до приміщень та розташування робочих місць з ПК. Згідно з „Державними санітарними правилами і роботи з візуальними дисплейними терміналами електронно-обчислювальних машин", площа приміщення на одне робоче місце користувача повинна становити 6 м^2, а об'єм – не менше 20 м^3.

Не дозволяється розміщувати кабінети обчислювальної техніки у підваль-них та цокольних поверхах.

Покриття підлоги повинно бути матовим з коефіцієнтом відбиття 0,3–0,5. Поверхня підлоги має бути рівною, неслизькою, з антистатичними властивостями. Для внутрішнього оздоблення приміщень з ПК треба використовувати дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7–0,8; для стін 0,5–0,6.

Заборонено застосовувати для оздоблення інтер'єру примі-щень з ПК класів полімерні матеріали (деревинно-стружкові плити, шпалери, які можна мити, рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), які виділяють у повітря шкідливі хімічні речовини, що перевищують гранично-допустимі норми.

Вимоги до обладнання та організації робочих місць користу-вачів ПК. Обладнання та організація робочих місць користувачів ПК ма-ють забез-печувати відповідність конструкцій усіх елементів ро-бочого місця та їхнього взаємного розташування ергономічним вимо-гам з урахуванням характеру і особливостей трудової діяль-ності.

У разі розташування елементів робочого місця користувача ПК треба враховувати: робочу позу користувача, простір для розміщення користувача, можливість огляду елементів робочого місця, мож-ливість ведення записів, розміщення документації і матеріалів, які використовує користувач.

Конструкція робочого місця користувача ПК повинна забезпечити підтри-мання оптимальної робочої пози. Робочі місця з ПК треба так розташовувати щодо ві-кон, щоб природне світло падало збоку переважно ліворуч. Робочі місця з ПК повинні бути розташовані від стіни з вікнами на відстані не менше 1,5 м, від інших стін – на відстані не менше ніж 1 м. У разі розміщенні робочого місця поряд з вікном кут між екраном монітора площиною вікна повинен становити не менше 90° (для уникнення відблисків), частину вікна, що прилягає, потрібно зашторити. Недопустиме розташування ПК, за якого працівник повернений обличчям або спиною до вікон кімнати або до задньої частини ПК, в яку монтують вентилятори. У разі розміщення робочих столів з ПК

треба дотримуватись таких відстаней: між бічними поверхнями ПК – 1,2 м, від задньої поверхні одного ПК до екрана іншого ПК – 2,5 м.

Монітор повинен бути встановлений так щоб верхній край екрана перебував на рівні очей. Екран монітора ПК повинен бути на оптимальній відстані -від очей користувача, що становить 600–700 мм, але не ближче ніж 600 мм з урахуванням розміру літерно-цифрових знаків і символів. Для забезпечення точного та швидкого зчитування інформації в зоні найліпшого бачення площина екрана монітора по-винна бути перпендику-лярною до нормальної лінії зору. Розташування екрана монітора ПК має забезпечувати зручність зорового спостереження у вертикальній площині під кутом 30° до нормальної лінії погляду користувача.

Клавіатура повинна бути розташована так, щоб на ній можна було зручно працювати двома руками. Клавіатуру треба розміщати на поверхні столу на відстані 100–300 мм від краю. Кут нахилу клавіатури до столу повинен бути в межах від 5° до 15°, зап’ястя та долоні рук повинні бути розташовувані горизонтально до площини столу.

Конструкція робочого стола повинна забезпечувати можливість опти-мального розміщення на робочій поверхні обладнання з урахуванням його кількості та конструктивних особливостей (розмір монітора, клавіатури, принтера, ПК тощо) і документів, а також враховувати характер виконуваної роботи.

Висота робочої поверхні столу з ПК повинна бути в межах 680–800 мм, а ширина і глибина – забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600–1400 мм, глибина – 800–1000 мм). Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною – не менше 500 мм, глибиною (на рівні колін) – не менше 450 мм, на рівні простягнутої ноги – не менше 650 мм.

Ноги не повинні бути витягнені під час сидіння далеко вперед, тому що в такому разі м'язи будуть надто напружені; положен-ня „нога на ногу" не рекомендоване, тому що підвищується тиск на сідничний нерв і порушується кровообіг ніг.

Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом нахилу сидіння та спинки, поверхня сидіння має бути плоскою, передній край – заокругленим. Регулювання за кожним із параметрів повинне бути незалежне, а фіксування легким і надійним. Висота поверхні сидіння має бути регульована в межах 400–500 мм, а ширина і глибина становити не менше 400 мм. Кут нахилу сидіння – до 15° вперед і до 5° назад. Висота спинки стільця має становити 300±20 мм, ширина – не менше 380 мм. Кут нахилу спинки має бути регульований у межах 1–30° від вертикального положення, відстань від спинки до переднього краю сидіння – у межах 260–400 мм.

Для зниження статичного напруження м'язів верхніх кінцівок треба використовувати стаціонарні або змінні підлокітники завдовжки не менше 250 мм, завширшки – 50–70 мм, регульовані за висотою над сидін-ням у межах 230–260 мм і відстанню між підлокітниками у межах 350–500 мм.

Поверхня сидіння і спинки стільця має бути напівм'якою з нековзним повітронепроникним покриттям, що легко чистити і яке не електризує.

Робоче місце має бути обладнане підставкою для ніг шириною до 300 мм, глибиною – не менше 400 мм, що регульована за висотою в межах до 150 мм і за кутом нахилу опорної поверхні підставки – до 20°. Підставка повинна мати рифлену поверхню і бортик по передньому краю заввишки 10 мм.

Вимоги до режимів праці і відпочинку під час роботи з ПК. Режими праці й відпочинку у разі роботи з ПК розробляють з урахуванням характеру трудової діяльності, напруженості і важкості праці диференційовано до кожної професії.

За характером трудової діяльності виділено три професійні групи:

1. **розробники програм** (інженери-програмісти) – виконують роботу переважно з ПК та документацією. У цьому разі відбувається інтенсивний обмін інформацією з ПК і висока частота прийняття рішень. Роботу виконують у вільному темпі, вона пов'язана з періодичним пошуком помилок в умовах дефіциту часу, потребує інтенсивної розумової творчої праці з підви-щеним напруженням зору, концентрацією уваги, нервово-емоційним напружен-ням, статичною робочою позою, періодичним навантаженням на кисті рук.

2. **оператори комп'ютерів** – виконують роботу, яка пов'язана з обліком інформації, одержаної з ПК, супроводжується перервами різної тривалості, пов'яза-на з виконанням іншої роботи, її характеризують як роботу з напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня, яку виконують у вільному темпі;

3. **оператор комп'ютерного набору** – виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переведеннями погляду на екран монітора, з уведенням даних з високою швид-кістю, роботу характеризують як фізичну працю з підвищеним навантаженням на кисті верхніх кінцівок, з напруженням зору (фіксація зору переважно на документи), нервово-емоційним напруженням.

Залежно від характеру праці визначають такі внутрішньозмінні режими праці та відпочинку:

- для розробників програм із застосуванням ПК треба призначати регла-ментовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи;
- для операторів із застосуванням ПК треба призначати регламентовані перерви для відпочинку тривалістю 15 хв. через кожні дві години;

- для операторів комп’ютерного набору треба призначати регламентовані перерви для відпочинку тривалістю 10 хв. після кожної години роботи за ПК.

У всіх випадках, коли виробничі обставини не дають змоги застосувати регламентовані перерви, тривалість безперервної роботи з ПК не повинна перевищувати 4 год.

У разі 12-годинної робочої зміни регламентовані перерви повинні бути в перші 8 год. роботи аналогічно до перерв у випадку 8-годиної робочої зміни, а протягом останніх 4 год. роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хв.

Щоб зменшити негативний вплив монотонності на працівника треба чергувати деякі операції, наприклад, уведення тексту за допомогою клавіатури та редагування тексту тощо.

Для зниження нервово-емоційного напруження, втоми зорового аналізато-ра, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіпо-динамії, запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ.

В окремих випадках – у разі постійних скарг працівників з ПК на зорову втому, незважаючи на дотримання санітарно-гігієнічних вимог до режимів праці і відпочинку, а також застосування локального захисту очей – допустимий індивідуальний підхід до обмеження часу робіт з ПК, зміни характеру праці, чергування з іншими видами діяльності, не пов’язаними з ПК.

Активний відпочинок повинен полягати у виконанні комплексу розслаб-лення, відновлення функцій фізіологічних систем, що порушу-ються протягом трудового процесу, зняття втоми очей, поліпшення моз-кового кровообігу і праце-здатності. За умови високого рівня напруже-ності робіт з ПК необхідне психологічне розвантаження у спеціально обладнаних приміщеннях (в

кімнатах психологічного розвантаження) під час регламентованих перерв або в кінці робочого дня.

ВИСНОВОК

Безпека IoT стала одним з найважливіших аспектів нових технологій. Можливо здасться, що не існує ризику для даних, які передаються і зберігаються такими системами, вони не є уразливими, але реальність така, що IoT пристрої, які не мають належного захисту, піддаються атакам, будучи свідомо зараженими шкідливим кодом для створення ботнету. Із зростанням технологічності кількість загроз та ризиків буде тільки зростати, тому будуть потрібні ефективні протидії. В бакалаврській роботі проведено аналіз загроз та ризиків технології IoT. Результати роботи такі:

1. Проведено дослідження концепції Internet of Things, в рамках чого представлено ідеї та основні принципи, архітектуру, класифікацію пристроїв та напрям стандартизації.

2. Проведено детальний аналіз загроз та ризиків інформаційної безпеки IoT.

3. Розглянуто особливості комплексного захисту технології IoT.

4. Проаналізовано методики виявлення атак технології IoT.

5. Запропоновано комплексний захист, починаючи з датчика та закінчуючи хмарою технології IoT.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ивлиев С. Н. Интернет вещей: новые угрозы информационной безопасности // Проблемы и перспективы развития отечественной светотехники, лектротехники и энергетики : мат-лы XII Всерос. науч.-техн. конф. с междунар. участием (г. Саранск, 28–29 мая 2015 г.). Саранск, 2015. С. 435–441.

2. Шиков С. А., Ивлиев С. Н. Интернет вещей: новые угрозы информационной безопасности // Саранск, 2016. С. 278–283.

3. Круз Л. Интернет вещей и информационная безопасность / Л. Круз. // Защита информации. INSIDE. – 2013. – №6. – С. 60–61.

4. Росляков А. В. Интернет вещей / А. В. Росляков. – Самара: ПГУТИ, 2015. – 200 с.

5. Уланов А. В. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия / А. В. Уланов, И. В. Котенко. // Защита информации. INSIDE. – 2007. – №1. – С. 60–67.

6. Алгулиев Р. Интернет вещей / Р. Алгулиев, Р. Махмудов. // Информационное общество. – 2013. – №3. – С. 42–48.

7. Шиков С. А. Проблемы информационном безопасности. Интернет вещей / С. А. Шиков. – 2013.

8. Соколов М. Н. Проблемы безопасности интернет вещей: обзор / М. Н. Соколов, К. А. Смолянинова, Н. А. Якушева. // Вопросы кибербезогласности. – 2015. – №5. – С. 32–35.

9. Щербинина М. Ю. Концепция интернет вещей / М. Ю. Щербинина, Н. А. Стефанова. // «Креативная экономика». – 2016. – №11.

10. Роуз К. Интернет вещей: краткий обзор [Електронний ресурс] / К. Роуз, С. Элдридж. – 2015. – Режим доступу до ресурсу:

https://www.internetsociety.org/wp-content/uploads/2015/10/report-InternetOfThings-20151221-ru.pdf.

11. Сталлингс У. Интернет вещей: сетевая архитектура и архитектура безопасности [Електронний ресурс] / У. Сталлингс. – 2017. – Режим доступу до ресурсу: http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/.

12. Бобылев А. Е. Проблема защиты данных в Интернете вещей [Електронний ресурс] / А. Е. Бобылев, А. В. Трофимова // "NAUKA-RASTUDENT: электронный научно-практический журнал". – 2016. – Режим доступу до ресурсу: http://nauka-rastudent.ru/27/3279/.

13. Мосеев В. Кто обеспечит безопасность Интернету вещей [Електронний ресурс] / В. Мосеев. – 2017. – Режим доступу до ресурсу: https://iot.ru/bezopasnost/kto-obespechit-bezopasnost-internetu-veshchey.

14. Унучек Р. Как я взломал свой фитнес-браслет [Електронний ресурс] / Роман Унучек. – 2015. – Режим доступу до ресурсу: https://securelist.ru/kak-ya-vzlomal-svoj-fitnes-braslet/25324/.

15. AV-Test: тестирование безопасности 7 фитнес-браслетов и смарт часов Apple Watch [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.comss.ru/page.php?id=3238.

16. Clausing E. Internet of Things Security Evaluation of 7 Fitness Trackers on Android and the Apple Watch [Електронний ресурс] / E. Clausing, M. Schiefer. – 2016. – Режим доступу до ресурсу: https://www.av-test.org/fileadmin/pdf/avtest_2016-07_fitness_tracker_english.pdf.

Додаток А. Слайди мультимедійної презентації

Аналіз технології "Internet of things" з позиції інформаційної безпеки

ДИПЛОМНА РОБОТА

Дипломник: Загорій Є.І.

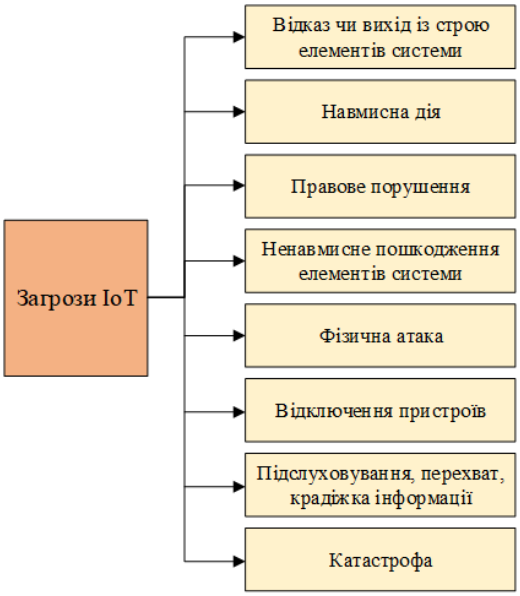
Керівник: Кільдішев В.Й.

2023

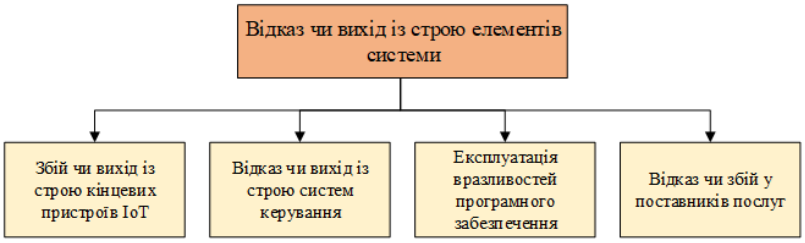
Технології індустріального Інтернету речей

Технологія	Опис
Кінцеві пристрої IoT	Пристрої, оснащені вбудованими технологіями збирання, обробки, зберігання, передачі інформації, інтелектуального прийняття рішень
Міжмашинний зв'язок (M2M)	Технологія, що полегшує прямий зв'язок між пристроями у мережі без участі людини
Аналіз Big Data	Процес вивчення величезної кількості різних типів наборів даних, відео та аудіо, згенерованих у реальному часі інтелектуальними датчиками, пристроями, журналами
Робототехніка	Удосконалені промислові роботи, наділені на вирішення складних завдань інтелектуальними можливостями, такими як здатність вчитися на своїх помилках і підвищувати свою продуктивність.
Штучний інтелект Машинне навчання	Алгоритми, які дозволяють комп'ютерам та обчислювальним машинам виконувати завдання, які зазвичай виконують люди. Алгоритми, які дозволяють комп'ютерам діяти та покращувати здатність прогнозувати без явного програмування.
Прогнозне обслуговування	Рішення, які відстежують стан обладнання, прогнозуючи, коли може статися збій, для ефективного обслуговування з мінімально можливою частотою.
Моніторинг у режимі реального часу	Технології, що дозволяють збирати та об'єднувати дані про безпеку від компонентів системи, а також відстежувати та аналізувати події, що відбуваються в мережі.
Розширена аналітика збитків Комп'ютерні обчислення	Методи аналізу різних типів втрат, які можуть виникнути серед, з метою їх усунення чи зменшення. Рішення, що забезпечують доступ до загальних наборів ресурсів, таких як мережі, сервери та програми, з мінімальними вимогами до управління та взаємодії з постачальником послуг.
Доповнена реальність	Технології, які змінюють сприйняття реального навколишнього середовища, є інструментом для підвищення ефективності завдань (наприклад, ручного складання).

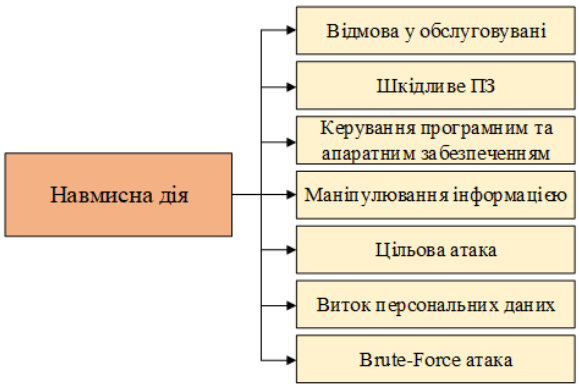
Загрози IoT



Класифікація загроз IoT

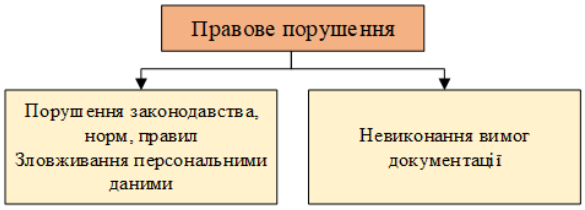


Відмова чи вихід із ладу елементів системи

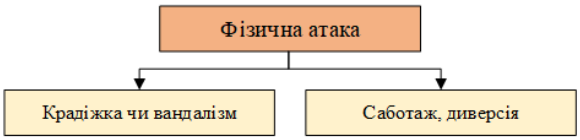


Навмисна дія

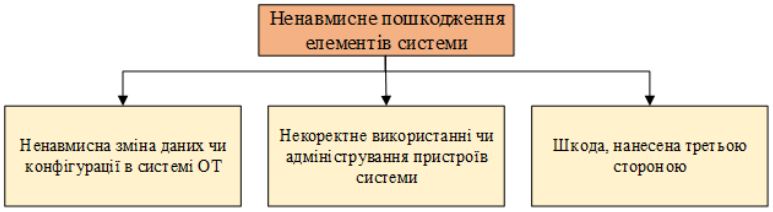
Класифікація загроз IoT



Правове порушення

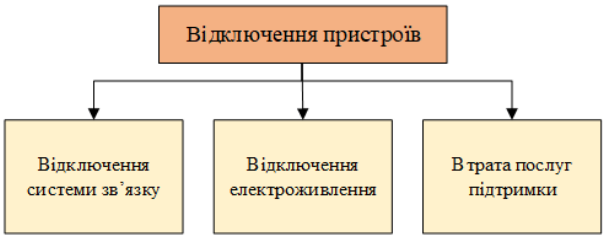


Фізична атака

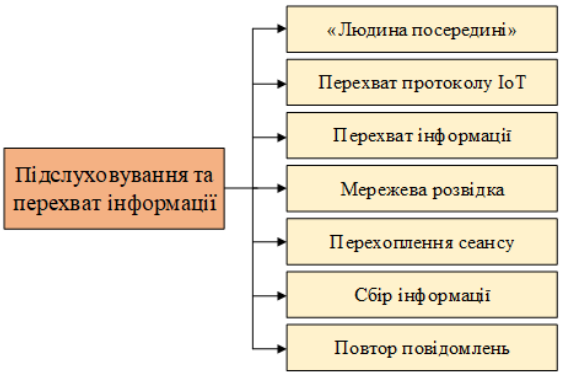


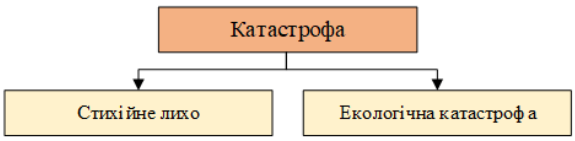
Ненавмисне пошкодження елементів системи

Класифікація загроз IoT



Вимкнення пристроїв



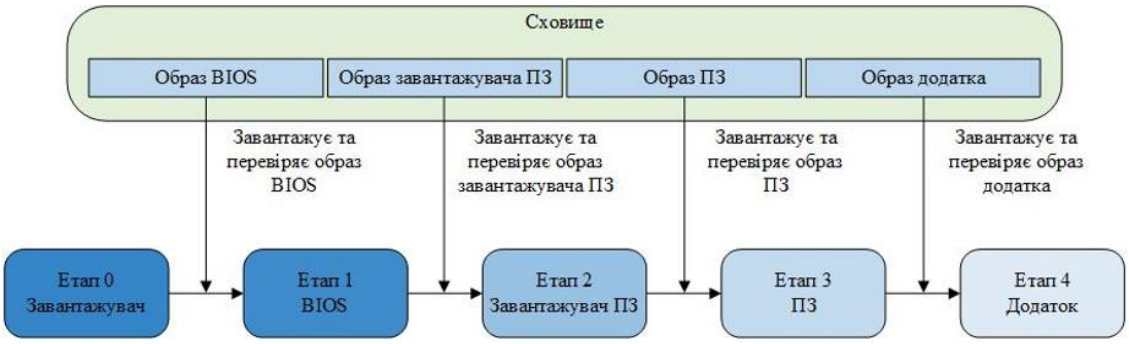


Катастрофа

Підслуховування, перехоплення та крадіжка інформації

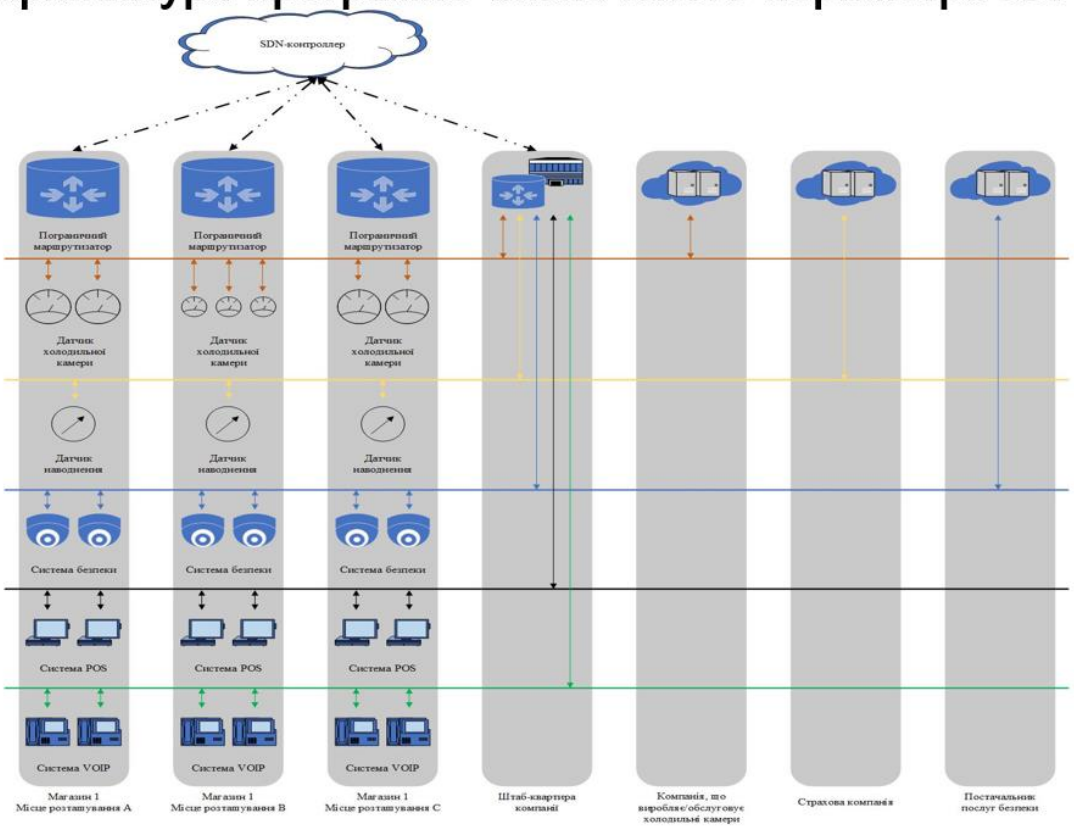
Комплексний захист технології IoT

Рівень апаратної безпеки

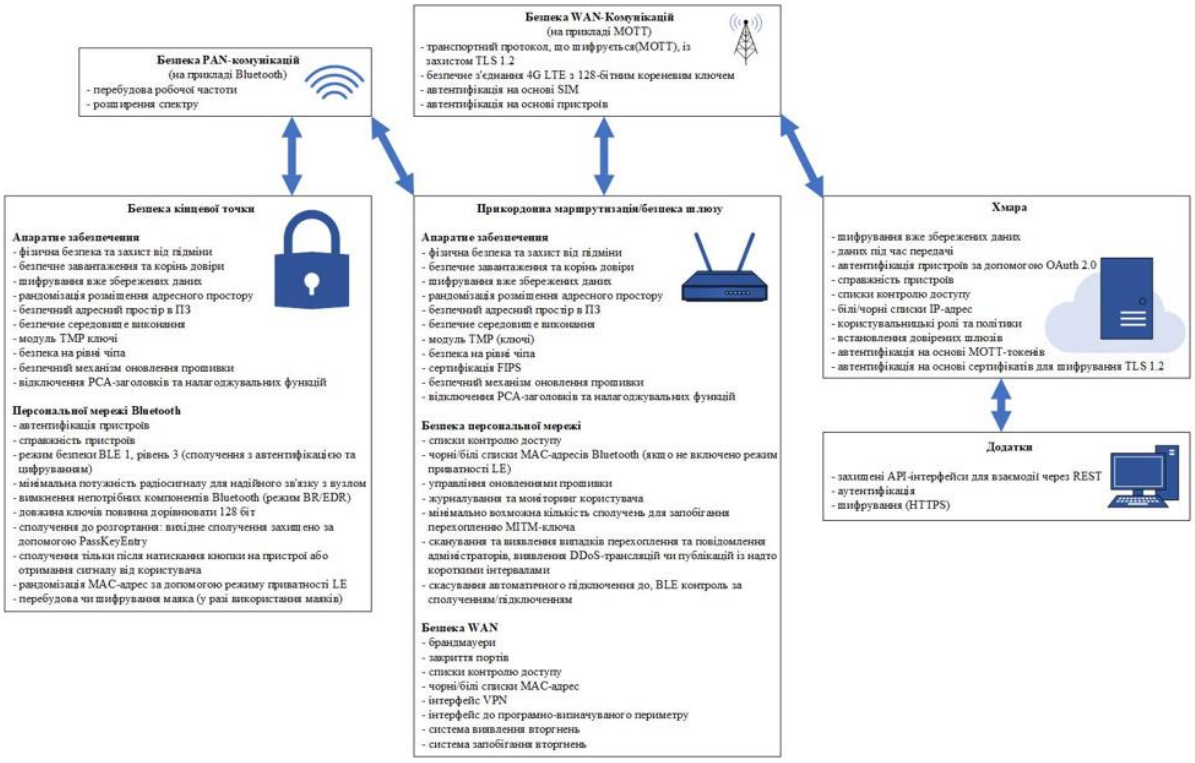


Рівень фізичної безпеки. Методики виявлення атак

Архітектура програмно-визначеного периметра SDP



Комплексний захист, починаючи з датчика та закінчуючи хмарою



ВИСНОВКИ

В бакалаврській роботі проведено аналіз загроз та ризиків технології IoT. Результати роботи такі:

1. Проведено детальний аналіз загроз та ризиків інформаційної безпеки IoT.
2. Розглянуто особливості комплексного захисту технології IoT.
3. Проаналізовано методики виявлення атак технології IoT.
4. Запропоновано комплексний захист, починаючи з датчика та закінчуючи хмарою технології IoT.

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015434926

Дата перевірки:
05.06.2023 15:18:05 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.06.2023 15:24:34 EEST

ID користувача:
100011688

Назва документа: 2БКС-27_Єгор_Загорій

Кількість сторінок: 59 Кількість слів: 11045 Кількість символів: 83733 Розмір файлу: 1.05 MB ID файлу: 1015096080

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

40.7%
Схожість

Найбільша схожість: 25% з Інтернет-джерелом (https://learn.ztu.edu.ua/pluginfile.php/162170/mod_resource/content/1/.

40.7% Джерела з Інтернету	556	..... Сторінка 61

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	5

Підозріле форматування	10 сторінок

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Загорія Єгора Івановича

(прізвище, ім`я та по батькові)

Напрямку підготовки *123 «Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи *«Аналіз технології "Internet of things" з позиції інформаційної безпеки»*

Обсяг пояснювальної записки _____ сторінок

Обсяг графічної (презентаційної) частини проекту _____ аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував технологію "Internet of things" з позиції інформаційної безпеки.

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Розглянуто дослідження концепції Internet of Things, в рамках чого представлено ідеї та основні принципи, архітектуру, класифікацію пристроїв та напрям стандартизації. Проаналізовано методики виявлення атак технології IoT. Розглянуто особливості комплексного захисту технології IoT.

г) перелік позитивних якостей роботи _____

Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.

д) основні недоліки роботи У тексті пояснювальної записки відсутні посилання на використану літературу, для підвищення ефективності захисту було б доцільним провести формування моделі загроз IoT на прикладі приватного підприємства чи будинку.

Оцінка розрахункової частини Відмінно

Оцінка графічної (презентаційної) частини Відмінно

Загальна оцінка Відмінно

Прізвище, ім'я та по батькові рецензента Царьов Роман Юрійович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, старший викладач кафедри комп'ютерної інженерії та інформаційних систем

«16» червня 2023 р. _____ Царьов Р. Ю.

(підпис) (прізвище та ініціали рецензента)

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * 43997335 * ВІДДІЛ КАДРІВ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Загорія Єгора Івановича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Аналіз технології "Internet of things" з позиції інформаційної безпеки»

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) обсяг і якість виконання роботи (розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над кваліфікаційною роботою

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Провів аналіз технології "Internet of things" з позиції інформаційної безпеки. Для підвищення рівня захисту проведено детальний аналіз загроз та ризиків інформаційної безпеки IoT. Розглянуто причини виникнення загроз, проблематики на різних рівнях сприйняття, найбільш поширені атаки.

в) теоретична підготовка бакалавра

відповідає вимогам, що надаються до бакалавра зі спеціальності «Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання _____

У кваліфікаційній роботі розглянуто базові відомості щодо технології "Internet of things" з позиції інформаційної безпеки». Проведено формування базової моделі загроз IoT. Представлено базові механізми захисту IoT, методи тестування, рекомендації щодо забезпечення безпеки IoT-пристроїв.

Оцінка розрахункової частини відмінно

Оцінка графічної (презентаційної) частини відмінно

Загальна оцінка відмінно

Прізвище, ім'я, по батькові керівника роботи Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

«15» 06 2023 р. _____ _____

(підпис) (прізвище та ініціали керівника)

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Загорій Єгор Іванович,
здобувач освіти гр. 2БКС-27, та

Кільдішев Віталій Йосифович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз технології "Internet of things" з позиції інформаційної безпеки» (автор роботи – Загорій Є.І., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Загорій Є.І. /

Керівник _____ / Кільдішев В.Й./

«15» 06 2023 р.