МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПРОЦАЙ МИХАЙЛО ОЛЕКСАНДРОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
д.т.н., доцент
_____ Т.В.Нескородєва
«____» _____ 20__ р.

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ОСІБ, ЯКІ ВОЛОДІЮТЬ ІНФОРМАЦІЄЮ ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ ОРГАНІЗАЦІЇ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
Барибін О.І., доцент кафедри
інформаційних технологій,
к.т.н
_____
підпис

Оцінка:___/ ___/ _____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2022

АНОТАЦІЯ

Процай М. О. Рекомендації щодо захисту систем інтернету речей для осіб, які володіють інформацією про критичну інфраструктуру організації. Спеціальність 125 Кібербезпека. Донецький національний університет імені Василя Стуса, Вінниця, 2022.

У кваліфікаційній (бакалаврській) роботі запропоновано рекомендації щодо захисту систем інтернету речей для осіб, що володіють інформацією про критичну інфраструктуру організації відповідно до стандартів IEEE. Результатом роботи є рекомендації щодо захисту систем інтернету речей для осіб, що володіють інформацією про критичну інфраструктуру організації.

Ключові слова: інформаційна безпека, модель порушника, IoT, рекомендації.

29 с., 3 табл., 5 рис., 19 джерел.

Protsai M.O. Recommendations for the protection of the Internet of Things for people who have information about the critical infrastructure owners. Specialty 125 Cybersecurity. Vasyl Stus Donetsk National University. Vinnytsia 2022.

In the bachelor's work on the basis of the analysis of IEEE standards recommendations for the protection of the Internet of Things for people who have information about the critical infrastructure owners is offered.

As a result of the work offered recommendations for the Internet of Things networks for people who have information about the critical infrastructure.

Keywords: information security, threat profile, IoT, recommendations.

29 pages, 3 tables, 5 figures, 19 sources.

ЗМІСТ

ВСТУП

За останнє десятиріччя прилади інтернету речей стали невід'ємною частиною сучасного інформаційного суспільства. Посилаючись на дослідження, що описане в [1], загальна кількість приладів інтернету речей, якими користувалися на момент дослідження в 2019 році становило 7.6 мільярдів приладів. За показником зведеного річного темпу приросту (CAGR) всього в 11%, кількість активно використовуваних девайсів інтернету речей на момент 2030 року становитиме близько 24.1 мільярда приладів. З таким стрімко зростаючим попитом, як правило, у людей, що не користувались такого роду приладами, або не знали, що користуються будуть виникати питання: "Що таке прилади інтернету речей?", а також: "Що я повинен зробити, щоб захистити інформаційну систему інтернету речей?".

Не дивлячись на те, що в точності описати, що ж таке насправді інтернет речей неможливо, тому будемо говорити про IoT як сукупність програмного та апаратного обладнання, що об'єднані між собою та утворюють інформаційні системи, які можуть накопичувати інформацію, ділитися нею з іншими та забезпечити безперешкодне використовування обробленої інформації користувачем [2].

Щодо відповіді на друге питання, то не існує єдиного підходу для забезпечення захисту таких інформаційних систем через їх надзвичайно велику кількість технологічних можливостей, в результаті чого було сформовано низку загальноприйнятих керівництв, що охоплюють специфічні області: Risk and IoT control [3], middleware, IoT in enterprise [4], Sybil attacks in vehicular networks, smart home systems, smart building [5], middleware, IIoT WAN, Smart Factories [6], autonomous vehicle, embedded systems [7], connected vehicles, eHealth, Smart Grid [8, 9], middleware, Smart City platform, embedded devices [10].

Мета бакалаврської роботи: запропонувати рекомендації щодо захисту систем інтернету речей для осіб, які володіють інформацією про критичну інфраструктуру організації (далі особи, що розглядаються). Відповідно до мети роботи можна сформулювати наступні завдання:

1. Проаналізувати існуючі методики, стандарти та рекомендації щодо захисту систем інтернету речей.
2. Побудувати модель порушника.
3. Класифікувати осіб, що розглядаються.
4. Надати рекомендації щодо захисту IoT систем, базуючись на класифікації осіб, що розглядаються.

Об’єктом дослідження бакалаврської роботи є системи інтернету речей.

Предметом дослідження бакалаврської роботи є особи, що володіють критичною інформацією.

РОЗДІЛ 1. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РОЗУМНИХ ДОМАШНІХ СИСТЕМ

1.1. Розумні домашні інформаційні системи

Нам пощастило жити в дивовижний відрізок часу, коли всі галузі нашої планети все стрімкіше стають взаємопов'язаними між собою. Нещодавно повністю функціонуючий автомобіль без водія вважалось сміливою вигадкою науково-фантастичних авторів, над чим сучасні наукові світили зараз розмовляють як над чимось буденним, звичайним.

Неможливо заперечувати, що будь-яка успішна сучасна компанія наразі повністю опирається на інформацію, прилади інтернету речей з якою працюють в режимі реального часу та конвертують ці дані в нові ідеї та можливості. Інтернет речей базується на трьох головних концептах: автоматизм, безпечність прикладаючи менше зусиль [11].

Глобальною ціллю IoT девайсів являється зробити все віртуально розумним за допомогою технологій штучного інтелекту (AI), великих даних і т.п. На сьогоднішній день аналітика даних має деякі обмеження, але маючи в своєму переліку інструментів прилади інтернету речей вони можуть підвищити свої можливості до надзвичайно великих позначок коефіцієнту корисної дії (ККД).

Отже, вся інформація яка циркулює в нашій мережі потребує деякого механізму, що дозволить поєднати наші прилади. Цей механізм призначений для забезпечення внутрішньо-доменних комунікацій та представляє собою такий собі хаб, який можна порівняти з хмарними середовищами. Такі механізми внутрішніх комунікацій зазвичай для виконання своїх завдань використовують такі інструменти як Bluetooth, Wi-Fi, WAN і т.д.

Говорячи про протокольний рівень таких механізмів, більшість із IoT систем мають справу з наступними [12]:

- Рівень сприйняття (perception layer) – відповідальний за сканування та накопичення інформації з різноманітних приладів всередині

інформаційного середовища, таких як розумні датчики, контролери і т.п.;

- Рівень комунікацій (також відомий як network connectivity/edge computing) – включає в себе дротове та бездротове з'єднання, протоколи передачі даних, які в свою чергу відповідальні за з'єднання з приладами, що знаходяться поза мережею. Ще в перелік завдань цього рівня входить обробка та передачі даних з датчиків;
- Рівень обробки інформації (information processing layer);
- Протокол прикладного рівня (application layer) – відповідальний за взаємодію мережі та кінцевого користувача;

Для забезпечення надійних зовнішніх та внутрішніх комунікацій розглянемо сучасну інфраструктуру комунікацій, що називається машинними комунікаціями(машина до машини, далі МдМ). Така інфраструктура дозволяє величезній кількості приладів обмінюватись даними поміж девайсів в мережі та в інтернеті з мінімальною затримкою [13].

Оглядаючись на функціональні можливості, що нам пропонують IoT системи хотілось би поговорити про деякі переваги над звичайними інформаційними системами.

Світ стрімко прямує до автоматизації звичайних для кожного повсякденних процесів, де розумні інформаційні системи абсолютно точно виходять переможцем змагаючись зі всіма відомими корпоративними, домашніми і т.п. системами. Очікуваним наслідком такої автоматизації являється знаходження нових ідей та можливостей для бізнесу тим самим примножуючи їх прибуток. IoT забезпечує нас бездротовим з'єднанням та надає можливість централізовано керувати багатьма процесами, наприклад за допомогою смартфона, що безперечно зводить турбування про повсякденні справи до мінімуму прикладаючи до цього мінімум зусиль.

Взаємодії типу МдМ, в свою чергу, забезпечують нас високою ефективністю та мінімальними затримками при роботі з розумними приладами. Завдяки можливостям, що надає нам така архітектура, людина перебуваючи в

такій системі може більше не турбуватись про переважну більшість своїх обов'язків при користуванні такими системами, так як вони в змозі накопичувати та аналізувати інформацію в реальному часі, відразу пропонуючи вирішення проблем, якщо вони виникають.

Правильно впровадженні в систему та налаштовані розумні прилади здатні автоматизовано накопичувати дані в місцях, які для цього призначені, наприклад хмарне середовище або централізоване сховище даних. Правила та алгоритми збору даних, звичайно, можна завдати на етапі автоматизації цього процесу.

Завдяки взаємопов'язаному середовищу IoT систем, вони забезпечені прозорими комунікаціями [14], які допомагають приладам взаємодіяти більш ефективно.

Навіть не беручи до уваги величезний приріст в сфері приладів розумного будинку вважається, що всесвітній показник споживання енергії за наступні 25 років зросте на 40% [15]. З такого роду проблемою IoT девайси можуть допомогти, адже при відповідному налаштуванню таких приладів вони можуть зберегти багато енергії зменшуючи її гайнування. Посилаючись на описані вище беззаперечні переваги систем розумного будинку, вони, наприклад можуть зафіксувати зміни погоди та базуючись на результатах аналізу відразу ввести відповідні зміни в термостат будинку. В результаті чого користувач не тільки оптимізує свої щомісячні комунальні витрати, а й зробить свій внесок для вирішення глобальної проблеми.

1.2. Особливості захисту IoT систем

Як це зазвичай буває, є і інша сторона монети. Поговоримо про недоліки систем інтернету речей. З одного боку IoT середовище зводить людські зусилля для виконання задач до мінімуму, а з іншого це означає, що людство все більше покладається на інформаційні технології навіть при виконанні самих примітивних задач. Таким чином у людей, що часто покладаються на свої розумні прилади, будуть виникати банальні проблеми в моменті, коли їх помічник вийде з ладу, що в перспективі може відбиватись на моральному стані людини, а внаслідок цього й на здоров'я користувача в цілому. Більш того, прилади розумного будинку занадто сильно залежать від з'єднання до мережі, тому в разі, якщо це з'єднання зникне, то переважна більшість девайсів будинку перестане виконувати поставлені їм задачі.

Негативним наслідком занадто великого полягання на інформаційні технології також, в разі отримання неправильних результатів можуть призвести до низки негативних сценаріїв.

Ризик того, що персональна інформація, в перспективі, може бути використана в негативному руслі підвищується, так як багато IoT девайсів з'єднані між собою в домашній мережі та мають доступ до глобальної мережі Інтернет в цілому.

Також існує низка соціально-економічних недоліків, що несуть за собою інформаційні системи розумних приладів, тому, посилаючись на викладене вище, можна зробити висновок, що захист таких систем являється критично необхідним для людей будь-якого соціального рівня.

1.3. Вимоги до інформаційних систем

Спільним у всіх методиках, в яких йдеться про забезпечення безпеки в звичайних інформаційних системах є те, що вони націлені на забезпечення виконання трьох головних вимог, а саме:

- Цілісність;
- Доступність;
- Конфіденційність.

На сьогоднішній момент уже існують створені відповідними спеціалістами методики та загальноприйняті керівництва, що охоплюють специфічні області кібербезпеки в IoT середовищах [3-10]. Такого роду системи мають розширений список вимог, до яких відносяться головних три, що згадані вище, та:

- Автентичність;
- Безвідмовність;
- Контроль доступу та авторизації;
- Надійні обчислення;
- Захист від DoS атак;
- Приватність.

Розглянемо кожен із пунктів детальніше. Вимога цілісності інформації вказує на важливість захисту циркулюючої інформації від протиправного спотворення. Дані, якими керується система розумного будинку здебільшого отримується різноманітними сенсорами, тому забезпечення цілісності цієї інформації являється одним із головних викликів.

Забезпечення доступності означає отримання даних по запиту. Забезпечення цієї вимоги є критичним, так як розумні домашні системи являються автоматизованими, тому вся інформація, що накопичується повинна бути доступною керуючим ланкам системи без всіляких обмежень. Отже, в такому середовищі доступність інформації напряму впливає на безпеку такої системи, та, в окремих випадках, на здоров’я користувача.

Вимога конфіденційності досягається захистом інформації від протиправного доступу до читання. Так як розумні прилади постійно накопичують інформацію, завдяки своїм сенсорам, її захист також являється ключовою ланкою в побудові системи, тому що до цих даних відносяться знімки з камер спостереження, домен безпеки та йому подібні.

Під забезпеченням автентичності в IoT системах мають на увазі те, що отримувач може перевірити походження отриманих даних. Виходячи з того, що користувач розумної системи постійно взаємодіє з зібраною всередині інформацією потрібно забезпечитись в тому, що він буде оперувати даними, що надійшли до нього з надійних джерел.

Безвідмовність виконує ту ж задачу що і автентичність, різниця лиш у тому, що в цьому випадку перевірити походження даних може не тільки передбачуваний отримувач, але й будь-яка третя особа. В IoT системах безвідмовність найбільш широко використовується в додатках охорони здоров'я та транспорту.

Контроль доступу та авторизації стає надзвичайно важливим, коли мережею користуються більше ніж одна людина та/або деякі з IoT додатків не передбачені для публічного користування, наприклад через гостьову мережу.

Надійні обчислення відповідають за те, щоб користувач був впевнений в тому, що інформаційна система та послуги, що вона пропонує, при будь-яких обставинах, працюють так, як цього очікує користувач. Дана вимога являється однією із критичних, тому що без неї деякі із описаних вище вимог не можна виконати, або можна, але на недостатньо надійному рівні в сфері безпеки. Якщо розумна домашня система забезпечена надійними обчисленнями, то про неї можна говорити як про таку, що стійка до враження шкідливим програмним забезпеченням пристроїв IoT.

Захист від DoS-атак запобігає прагненню зловмисників вивести систему із ладу або суттєво зменшити її ефективність.

Останньою вимогою є приватність, яка відповідає за те, щоб люди, що користуються IoT мережею могли контролювати як зберігається конфіденційна

інформація про них та як її використовує система. Так як розумні прилади були створені для полегшення повсякденного життя їх власників, то і система, що забезпечена даною вимогою може зберігати, накопичувати та аналізувати інформацію щодо користувача, чим самим може знати як те, яким продуктам власник надає перевагу, так і дізнатись про потенційну хворобу за допомогою додатків для піклування про здоров'я.

1.3.1. IEEE

Інститут інженерів електротехніки і електроніки (IEEE) – міжнародна некомерційна асоціація, завдяки своїм членам являється провідною у різних технічних областях, включаючи комп'ютерну інженерію, біомедичну інженерію, мікроелектроніку, телекомунікації, схеми та системи, твердотілі електронні пристрої і т.п.

Для сфери розумних будинків асоціацією був створений стандарт [16], у якому виведено наступні рекомендації для розумних будинків:

1. Внутрішньо-доменні комунікації [17];
2. Безпека розподілу та приватності інформації, що належить до різних доменів;
3. Асоціативність та контроль прийому;
4. Обслуговування системи та пристроїв.

РОЗДІЛ 2. ПРОФІЛЬ ЗАГРОЗ РОЗУМНИХ ДОМАШНІХ СИСТЕМ

Виходячи з всіх рекомендацій, методик та стандартів описаних вище структуруймо процес оцінки загрози потенційного протиправного впливу на інформаційне середовище. Для цього потрібно привести класифікацію осіб, що розглядаються та оцінити цінність інформації, до якої вони мають доступ. Щоб розуміти з якими порушниками нам доведеться мати справу, сформуймо модель порушника для визначення його рівня загрози, базуючись на визначених характеристиках.

Для отримання рівня загрози потенційного впливу сформуймо матрицю відповідностей, де буде співставлення характеристики рівня загрози порушника, що буде виведений із моделі порушника з цінністю інформації, доступ до якої є у особи, що розглядається.

2.1. Модель порушника

Говорячи про профіль безпеки в сфері кібербезпеки спеціалісти відокремлюють три головних типи порушників, до яких відносяться:

- Хактивісти;
- Кіберзлочинці;
- Ліцензовані хакери.

Хактивістами називають кіберзлочинців, які об’єднались в групи та переслідують одну ціль, зазвичай політичну. Своїми цілями хактивісти, як правило, обирають конкретні організації та/або окремі галузі, що, на їх думку, не відповідають їхнім політичним поглядам. Актуальним прикладом такого угрупування, на момент написання цієї роботи, являються хактивісти Anonymous. На сьогоднішній день вони об’явили кібервійну цілій державі, що виступає агресором у війні. Члени цього угрупування мотивуються своїми політичними поглядами та атакують військові та державні об’єкти, внаслідок чого було обнародувано величезна кількість даних про членів уряду держави

агресора та ключові організації, що займаються видобуванням сировини та виводять цю країну на лідируючі місця на ринку по її експорту за кордон. При цьому, в ідеологію групи хактивістів входить пункт про те, що вони ні в якому разі не шкодять звичайним громадянам та не розповсюджують персональну інформацію про них. Зазвичай, хактивісти оголошують про напад заздалегідь, для залучення більшого числа своїх послідовників, завдяки чому привертають увагу засобів масової інформації, які в свою чергу розповсюджують інформацію про політичні події такого роду, що призводить до охоплення ще більшого числа хактивістів. В момент, коли вербування охочих завершується розпочинається етап розвідки, під час якого члени групування шукають слабкі місця, які можуть бути використані для проникнення. Коли угрупування досягає своєї цілі хактивісти розпускають свою команду допоки вербування до нової кіберкампанії не розпочнеться знову.

Розглянемо наступний тип порушників, що називаються кіберзлочинцями. Мотивацією для такого роду злочинців являється власна нажива, тому вони насамперед націлені на викрадення особистої інформації, облікових даних та номерів кредитних карток та номери соціального страхування. Так як темна мережа надає достатній рівень анонімності, тому це означає, що поріг входження достатньо малий, що, в свою чергу, розв'язує їм руки для монетизації своїх дій. До інструментів, якими користуються кіберзлочинці відносять: фішингові атаки, криптомайнери, шкідливе програмне забезпечення – вимагач, троянські програми віддаленого доступу, комплекти експлойтів для соціальних мереж і т.п.

Останнім типом для розгляду залишаються ліцензовані хакери. До них відносяться люди, що "мають дозвіл" на такого роду операції, так як, зазвичай, працюють на уряд, або являються спеціалістами, що наймаються компаніями для перевірки стану захищеності їх організацій. Головною різницею між хакерами цього та всіма іншими є те, що вони працюють в рамках закону та не несуть на собі вагу постійних переживань на рахунок того, що їх рано чи пізно заарештують.

Побудова моделі порушника також потребує ряду визначених характеристик, за якими буде оцінюватись їх потенційна загроза. Посилаючись на метод, описаний в [18], можна виділити наступні характеристики:

- Тип порушника;
- Мотив;
- Спосіб проникнення;
- Наслідки вторгнення.

Для деяких організацій таких характеристик буде достатньо, але не для всіх. Існують специфічні компанії, які потребують розширеного та/або унікального ряду характеристик для оцінки порушників. Зазвичай для цього роблять слідуюче:

- Додають нові характеристики для оцінки;
- Декомпонують існуючі характеристики;
- Видалення із ряду характеристик тих, що не підходять для специфічного випадку.

Виходячи із розглянутого вище, для описання моделі порушника визначимо ряд характеристик, по яким ми будемо проводити його оцінку. Для цього сформулюємо наступні категорії порушників:

- Внутрішній
- Зовнішній

До внутрішніх порушників можна віднести безпосередньо користувачів домашньої мережі, домашніх робітників та сервісних інженерів.

Зовнішніми порушниками будемо вважати запрошених гостей, порушників пропускного режиму, конкурентів, технічних спеціалістів (далі хакери), групи хакерів.

Для оцінки рівня потенційної загрози, внаслідок дій категорій порушників, що викладені вище, сформулюємо перелік характеристик, умовні позначення, а також присвоїмо їм рівень загроз від 1 до 10, де 1 – це найнижчий рівень загрози, та 10 – найвищий:

- Тип порушника: внутрішній(ТВ) – 9, зовнішній(ТЗ) – 8;
- Мотивація: експеримент(МЕ) – 4, внесення змін в роботу системи, що не призвели до вагомих наслідків(МВН) – 5, збір даних(МЗ) – 7, внесення змін в роботу системи, що виведе її з ладу(МВЛ) – 8, збір даних з метою їх розповсюдження(МЗР) – 9, завдання репутаційних збитків(МР) – 10;
- Характер дій: випадково(ХВ) – 4, навмисно(ХН) – 8;
- Глибина вторгнення: зупиниться коли зустрінеться з перешкодою(ГП) – 4, зупиниться коли зможе потрапити в систему(ГЗС) – 6, зупиниться коли зустрінеться з вагомою перешкодою(ГВП) – 7, зупиниться коли досягне своєї цілі(ГЦ) – 9, не зупиниться(ГН) – 10;
- Обізнаність в ІТ: початківець(ОП) – 2, любитель(ОЛ) – 4, висока(ОВ) – 8, розробник систем захисту різних призначень(ОР) – 10;

Тип порушника – характеристика, що визначає до якої категорії відноситься порушник, та базуючись на цьому формується оцінка рівня загрози.

Мотивація – характеристика, що визначає рівень загрози порушника, базуючись на цілі, що він переслідує.

Характер дій – характеристика, що визначає рівень загрози, базуючись на тому, чи навмисно було створене вторгнення, чи випадково.

Глибина вторгнення – характеристика, що визначає рівень загрози порушника, базуючись на його намірах.

Обізнаність в ІТ – характеристика, що визначає рівень загрози порушника, базуючись на рівні його обізнаності в інформаційних технологіях.

Для оцінки рівня загрози потенційного порушника будемо використовувати спосіб, в якому сума всіх характеристик буде вказувати на рівень загрози суб’єкту інциденту інформаційної безпеки. Як виглядає ранжування рівнів загрози представлено в таблиці 2.1.

Таблиця 2.1 – Ранжування рівнів загрози порушника

Рівень загрози	Оцінка

Незначна	1-10
Низька	11-25
Середня	26-40
Висока	41-50

Відповідно таблиці 2.1 можна побудувати модель порушника, базуючись на способі, що описаний в [18].

Таблиця 2.2 – Модель порушника

Особа	Тип порушника	Характер дій	Мотивація	Глибина вторгнення	Обізнаність в ІТ	Оцінка
Користувач домашньої мережі	ТВ – 9	ХВ – 4	МВЛ – 8	ГП – 4	ОП – 2	27
Домашній робітник	ТВ – 9	ХВ – 4	МВН – 5	ГП – 4	ОП – 2	24
Сервісний інженер	ТВ – 9	ХН – 8	МЗР – 9	ГВП – 7	ОВ – 8	41
Запрошений гість	ТЗ – 8	ХН – 8	МЗР – 9	ГП – 4	ОЛ – 4	33
Порушник пропускного режиму	ТЗ – 8	ХН – 8	МЗР – 9	ГВП – 7	ОЛ – 4	36
Конкурент	ТЗ – 8	ХН – 8	МР – 10	ГЦ – 9	ОЛ – 4	39
Хакер	ТЗ – 8	ХН – 8	МЗР – 9	ГЦ – 9	ОВ – 8	42
Група хакерів	ТЗ – 8	ХН – 8	МР – 10	ГН – 10	ОР – 10	46

2.2. Класифікація осіб, що розглядаються

Для того, щоб визначити наскільки серйозною є загроза вторгнення для осіб, що розглядаються, проведемо класифікацію цих осіб та присвоїмо їм значення цінності інформації, якою вони оперують. Класифікація приведена на рисунку 2.1, кожна вершина якого являється особою, що розглядається.

Критеріями для оцінювання цінності інформації будуть відповідні словесні значення:

- Незначна – до такої категорії відноситься відкрита інформація про організацію/підприємство;
- Низька – до такої категорії відноситься контрольовано відкрита інформація;
- Середня – до такої категорії відноситься інформація відкрита лише для службового користування, розкриття якої може стати причиною фінансових збитків;
- Висока – до цієї категорії відноситься інформація, розкриття якої може стати причиною репутаційних та/або фінансових збитків.

Рисунок 2.1 – Класифікація осіб, що розглядаються

На основі викладеного, можемо присвоїти кожному свій рівень загрози потенційного впливу на інформаційне середовище, який буде оцінюватись за допомогою матриці відповідностей, аргументами якої стануть рівень загрози потенційного порушника та цінність інформації, до якої має доступ особа. Матриця приведена на рисунку 2.2.

Таким чином, ми можемо сформулювати деякі типи осіб і привласнити їм рівень цінності інформації, до якої у них є доступ:

- Особа, що працює на державну організацію та має доступ до державної таємниці. Рівень цінності інформації – високий;

- Особа, що працює на державну організацію не маючи доступу до державної таємниці займає керуючу посаду. Рівень цінності інформації – високий;
- Особа, що працює на державну організацію не маючи доступу до державної таємниці і являється штатним працівником. Рівень цінності інформації – середній;
- Особа, що працює в неурядовій установі та являється її власником. Рівень цінності інформації – високий;
- Особа, що працює в неурядовій установі та займає керуючу посаду. Рівень цінності інформації – високий;
- Особа, що працює в неурядовій установі та являється її штатним працівником. Рівень цінності інформації – низький;

		Цінність інформації			
		Незначна	Низька	Середня	Висока
Рівень загрози порушника	Незначний				
	Низький				
	Середній				
	Високий				

Рисунок 2.2 – Матриця визначення рівня загрози потенційного впливу

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ

Базуючись на існуючих рішеннях загальноприйнятого стандарту IEEE, в цьому розділі буде запропонована низка рекомендацій, а також, базуючись на рівнях загроз потенційного впливу на інформаційне середовище осіб, які володіють інформацією про критичну інфраструктуру організації буде сформована таблиця, де будуть запропоновані специфічний набір рекомендацій для кожного з них.

3.1. РК-01 – Налаштування внутрішньо-доменних комунікацій

Налаштування внутрішньо-доменних комунікацій базується на концепті, в якому на протокольному рівні мережі використовується набір із стандартів Time-Sensitive Networking (TSN), домени локальної мережі в яких вважаються чорними ящиками [17]. Внаслідок такого підходу внутрішні комунікації не мають ніякої цінності для навколишнього світу, так як кожен TSN домен відповідальний за створення та знищення потоку даних. Для реалізації цього потрібен звичайний протокол для обміну інформації між доменами, який називається внутрішньо-доменний протокол TSN (TIDP). На рисунку 3.1 представлена схема обміну інформацією, що використовує даний концепт.

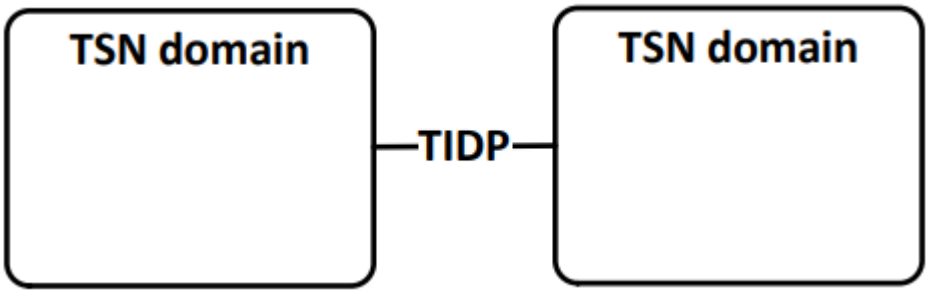

Рисунок 3.1 – Схема обміну інформації [17]

Процес обміну інформацією, що пропонує такий концепт, представлений на рисунку 3.2.

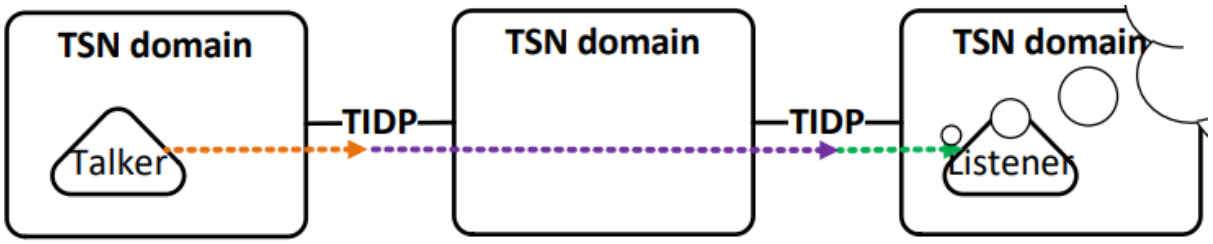

Рисунок 3.2 – Процес обміну інформацією

3.2. РК-02 – Асоціативність та контроль прийому

Досягнення асоціативності та контролю прийому переслідує просту і в той же час важливу ціль, яка полягає в тому, щоб користувач міг під’єднати нові прилади розумного будинку не прикладаючи великих зусиль. Для цього можуть бути створені різноманітні шаблони для різних типів девайсів, приєднуючи до мережі яких, вони проходили процедуру налаштування відповідно завчасно визначеному переліку правил.

Контроль прийому передбачає налаштування ролів користувачів, що експлуатують мережу, наприклад адміністратор, звичайний користувач та гість. При автоматизації процесу асоціативності також можна добавити шаблони для під’єднання користувачів до мережі.

3.3. РК-03 – Використання різних мереж для персонального користування та IoT приладів

Для того, щоб зменшити ризик порушення фундаментальних аспектів захисту інформації, до яких відносяться конфіденційність, цілісність та доступність пропонується використовувати різні мережі для персонального комп’ютера та системи розумного будинку. Дотримання такої рекомендації зменшить ризик витоку, спотворення та виведення з ладу всього інформаційного простору будинку.

3.4. РК-04 – Не купувати розумні товари, що не мають пароля за замовчуванням

Купування розумних девайсів, що не мають пароля за замовчуванням дуже часто призводить до майже безперешкодного вторгнення в інформаційне середовище, де такий прилад використовується, тому категорично не рекомендується купувати девайси розумних будинків, що не мають такого пароля.

3.5. РК-05 – Змінювати стандартний пароль розумних девайсів на унікальний для кожного із них

Зміна паролю, що даний пристрою за замовчуванням, являється першим кроком для забезпечення захисту будь-якої інформаційної системи. Ця процедура обов’язкова для всіх існуючих типів осіб, так як часто при утворенні пароля для девайсу компанії прибігають до утворення певної випадкової унікальної множини, значення якої будуть у випадковому порядку призначенні для кожного IoT приладу, базу даних з якими можна придбати в мережі.

3.6. РК-06 – Вимикання можливостей, що не використовуються

Вимикання функціональних можливостей IoT пристрої, що не використовуються призведе до зменшення ризику протиправного вторгнення в інформаційне середовище, так як кількість точок входу в таку систему зменшиться.

3.7. РК-07 – Встановлення Next-Generation Firewall

Встановлення міжмережевого екрану наступного покоління може бути досягнене тільки при наявності специфічного апаратного забезпечення.

Рекомендовано встановлювати NGFW від компанії CISCO, так як вони забезпечені більшою частиною функціональних можливостей, які зможуть закрити питання більшості вимог описаних в методиках та керівництвах по забезпеченню інформаційної безпеки в IoT середовищах, до яких відносяться: захист від DoS-атак, база даних що містить інформацію про загрози, комплексне запобігання вторгненню в інформаційне середовище мережі, обізнаність і контроль такого апаратного забезпечення для виявлення та блокування потенційно ризикованих додатків та всі можливості, що є у звичайному міжмережевому екрані, наприклад перевірка системи в цілому. Комплект такого апаратного забезпечення показаний на рисунку 3.3.

Рисунок 3.3 – Комплект міжмережевого екрану [19]

1. ASA 5506-X;
2. Консольний кабель;
3. Конверт з ключом активації продукту;
4. Адаптер живлення;
5. Шнур живлення для адаптеру живлення.

3.8. Рекомендації для класифікованих типів осіб

Відповідно до визначеного рівня загрози потенційного впливу на інформаційне середовище осіб, які володіють інформацією про критичну інфраструктуру організації, який визначається в 2-му розділі за допомогою матриці відповідностей, що зображена на рисунку 2.2, в таблиці 3.1 запропоновано дотримання певного переліку рекомендацій для кожного з рівнів.

Таблиця 3.1 – Рекомендації відповідно кожного рівня загрози для осіб, що розглядаються

Рівень загрози потенційного впливу	Рекомендації
Незначний	РК-04, РК-05
Низький	РК-04, РК-05, РК-06
Середній	РК-02, РК-03, РК-04, РК-05, РК-06
Високий	РК-01, РК-02, РК-03, РК-04, РК-05, РК-06, РК-07

ВИСНОВКИ

За результатами дослідження можна сформулювати наступні висновки.

1. На основі розгляду передових методик, стандартів та керівництв по забезпеченню безпеки інформаційних середовищ та їх аналізу виділено основні вимоги по забезпеченню інформаційної безпеки, до яких відносяться: цілісність, доступність, конфіденційність, автентичність, безвідмовність, контроль доступу та авторизації, надійні обчислення, захист від DoS-атак і приватність.

2. Побудовано режим порушника, який відображає його рівень загрози, базуючись на сформованих та оцінених класифікаціях, до яких відносяться: тип порушника, характер дій, мотивація, глибина вторгнення та обізнаність в ІТ.

3. Класифіковано типи осіб, які володіють інформацією про критичну інфраструктуру організації, а також присвоєно рівень цінності інформації, до якої вони мають доступ. Серед них:

- Особа, що працює на державну організацію та має доступ до державної таємниці. Рівень цінності інформації – високий;
- Особа, що працює на державну організацію не маючи доступу до державної таємниці займає керуючу посаду. Рівень цінності інформації – високий;
- Особа, що працює на державну організацію не маючи доступу до державної таємниці і являється штатним працівником. Рівень цінності інформації – середній;
- Особа, що працює в неурядовій установі та являється її власником. Рівень цінності інформації – високий;
- Особа, що працює в неурядовій установі та займає керуючу посаду. Рівень цінності інформації – високий;
- Особа, що працює в неурядовій установі та являється її штатним працівником. Рівень цінності інформації – низький;

4. Сформовано перелік рекомендацій, на основі стандартів по забезпеченню інформаційної безпеки в середовищах розумних будинків. Серед них:

- РК-01 – Налаштування внутрішньо-доменних комунікацій;
- РК-02 – Асоціативність та контроль прийому;
- РК-03 – Використання різних мереж для персонального користування та IoT приладів;
- РК-04 – Не купувати розумні товари, що не мають пароля за замовчуванням;
- РК-05 – Змінювати стандартний пароль розумних девайсів на унікальний для кожного із них;
- РК-06 – Вимикання можливостей, що не використовуються;
- РК-07 – Встановлення Next-Generation Firewall.

5. Запропоновано перелік рекомендацій відповідно до рівня загрози потенційного впливу для кожного типу особи. Серед яких:

- Незначному рівню загрози запропоновано: РК-04, РК-05;
- Низькому рівню загрози запропоновано: РК-04, РК-05, РК-06;
- Середньому рівню загрози запропоновано: РК-02, РК-03, РК-04, РК-05, РК-06;
- Високому рівню загрози запропоновано: РК-01, РК-02, РК-03, РК-04, РК-05, РК-06, РК-07.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Foltýnek P, Babiuch M and Šuránek P. Measurement and data processing from Internet of Things modules by dual-core application using ESP32 board. Meas. Control, 2019. Vol. 52, pp. 970-984. DOI: 10.1177/0020294019857748.

2. A. Colakovic and M. Hadžialic "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", Computer Networks, vol. 144, 2018. pp. 17–39. DOI: https://doi.org/10.1016/j.comnet.2018.07.017

3. Macaulay T. RIoT Control. Understanding and Managing Risks and the Internet of Things, Cambridge: Elsevier, 2017. DOI: https://doi.org/10.1016/B978-0-12-419971-2.00001-7

4. Russell B. and Duren D. Practical Internet of Things Security. Birmingham: Packt Pub, 2016.

5. Hu F. Security and Privacy in Internet of Things. Boca Raton: CRC Press, 2016. DOI: https://doi.org/10.1016/B978-0-12-805395-9.00010-1

6. Gilchrist A. Industry 4.0. The Industrial Internet of Things. Apress, 2016. DOI: https://doi.org/10.1007/978-1-4842-2047-4

7. Pathan A.K. Securing Cyber-Physical Systems. Boca Raton: CRC Press, 2015. DOI: https://doi.org/10.1201/b19311

8. Misra S., Maheswaran M. and Hashmi S. Security Challenges and Approaches in Internet of Things. Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-44230-3

9. Sorebo G.N., Echols M.C. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. CRC Press, Taylor & Francis Group, Boca Raton, FL, 2012. ISBN: 1439855870

10. Aziz B., Arenas A., and Crispo B. Engineering Secure Internet of Things Systems. London: CPI Group, 2016. DOI: https://doi.org/10.1049/PBSE002E

11. Lele Chitra. Internet of Things (IoT) A Quick Start Guide: A to Z of IoT Essentials. BPB Publications, 2022. 227 p. ISBN: 9389845866

12. Gianluca Cornetta , Abdellah Touhafi, Gabriel-Miro Muntean. Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies. 2020. 333 p. DOI: https://www.igi-global.com/gateway/book/244250

13. Wang M.M., Zhang J. Machine-Type Communication for Maritime Internet-of-Things: From Concept to Practice. Springer, 2021. 303 p. ISBN: 978-3-030-77907-8

14. Asmiar Reza Agustina, Tutik Rachmawati. The Use of Information Communication and Technology (ICT) to Enable Transparency, Accountability, and Participation in Indonesia. 2020. pp. 589-607. DOI: https://doi.org/10.30589/proceedings.2020.429

15. International Energy Agency. World Energy Outlook 2019. International Energy Agency. 2019. 810 p.

16. IEEE-SA Industry Connections – Convergence of Smart Home and Building Architectures. SmartAmerica Challenge Expo (11 June 2014, Washington Expo Center, Washington DC USA). Washington, 2014. 17 p.

17. Josef Dorr, Stephan Höme, Sven Kerschbaum, Günter Steindl. TSN inter domain communication concept. 2020.

18. Christopher Alberts, Audrey Dorofee. OCTAVE Threat Profiles. Software Engineering Institute Carnegie Mellon University. URL: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/AlbertsDorofee_OCTAVEThreatProfiles.pdf (Last accessed: 09.05.2022).

19. Nazmul Rajib. Cisco Firepower Threat Defense (FTD) Configuration and Troubleshooting Best Practices for the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP). Cisco Press, 2018. 800 p. ISBN: 1-58714-480-8.