КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2021.11.8599
УДК 351.746.1 : 007-044.64 : 378.6

Лахно Валерій Анатолійович
д.т.н., професор, завідувач кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Блозва Андрій Ігорович
к.пед.н., доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Гусєв Борис Семенович
к.т.н., доцент, доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0003-1658-7822
gusevbs@nubip.edu.ua

Осипова Тетяна Юріївна
к.пед.н., доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Матус Юрій Володимирович
старший викладач кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0003-0974-4789
umatus@nubip.edu.ua

ІНТЕГРУВАННЯ ТА ЗАХИСТ ІОТ ПРИСТРОЇВ У НАЯВНІЙ ІНФРАСТРУКТУРІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗАКЛАДУ ОСВІТИ

Анотація. Розвиток комп'ютерних мереж набирає стрімкого розвитку. Постають нові виклики по забезпеченню безпеки даних та самих кінцевих користувачів. Із появою Інтернет Речей дана проблема встала досить гостро перед мережевими інженерами та кібераналітиками. Все частіше і частіше зустрічаються неправомірні дії щодо втручання у роботу як самої мережі так і використанню у злочинних цілях пристроїв юзерів. Різноманітні розподілені атаки, SQL-ін'єкції та викрадення особистих даних стають все складнішими. Враховуючи розростання інфраструктури як самої мережі так й IoT пристроїв виникає потреба у їх захисті. Особливо, якщо це стосується комп'ютерної мережі закладу вищої освіти. Де, як правило, мало уваги приділяється повноцінному захисту інфраструктури, а з інтеграцією IoT пристроїв, таких можливих прогалин може виникати досить багато.

У даній статті є спроба розкрити теоретичні підходи до проектування та реалізації комп'ютерної мережі закладу вищої освіти, які за останній час все частіше починають потерпати від втручання ззовні. Проаналізовано можливі атаки на інфраструктуру закладу вищої освіти, а також можливість атаки і втручанню у роботу IoT пристроїв на основі підходу вбивчого ланцюжка. Розглянуто можливість використання у таких мережах web application firewall та відповідного програмного забезпечення для здійснення безпеки та реагування на інциденти на рівні L5-L7 OSI. Проведено попереднє тестування мережі на можливість реагувати як на атаки L3-L4 рівня за допомогою стандартних можливостей фаєрволів. Так і з реагуванням на втручання на верхніх рівнях моделі OSI L5-L7, а саме: SQL-ін'єкції, розподілені DDoS, атаки бот-нет мереж. Підведено підсумки та визначено подальші напрямки дослідження, що ґрунтуються на удосконаленні групової політики

безпеки для закладу вищої освіти, розбудови безпекової інфраструктури для IoT пристроїв з можливістю швидкого реагування на нестандартні атаки.

Ключові слова: кібербезпека, комп'ютерна мережа, IoT пристрій, інтеграція систем захисту

ВСТУП

Інтернет дозволяє збирати та передавати дані в режимі реального часу з будь-якого пристрою чи системи, підключеної до нього. Системи інтернету речей (IoT) використовують дані з цих пристроїв, дозволяють автоматизувати рішення та прогнози, а також допомагають підприємствам швидше та ефективніше реагувати на зміни бізнесу та операційні потреби. За своєю сутністю IoT - це спосіб інструментації, зондування та контролю підключених фізичних пристроїв шляхом вбудовування в них IT.

IoT вже сприяє змінам у різних галузях, включаючи вдосконалене обслуговування обладнання та управління активами, пов'язані продукти з новим розумінням поведінки споживачів, автоматизацією процесів поставок та новими формами співробітництва між людьми та машинами [1],[2].

Системи IoT починають проникати навіть у роботу закладів освіти. Моніторинг стану клімату в аудиторіях, навчальних лабораторіях, спеціалізованих приміщеннях, у яких проводяться дослідження. Виникає потреба інтеграції даних пристроїв у комп'ютерну мережу закладу освіти. А враховуючи швидке зростання різноманітних атак та можливих вразливостей на дані пристрої, ще й їх захист.

Фахівці з кібербезпеки знають, що хакери безперервно розробляють нові методи. Постійно з'являються нові загрози, які необхідно виявляти і стримувати з тим, щоб ресурси і зв'язок відновлювалися якомога швидше [3],[4]. Для отримання прибутку багато хакерів не гребують такими методами, як вимагання, шахрайство і крадіжка персональних даних [5]-[7]. Необхідність постійно захищатися від цих атак призвела до створення декількох моделей реагування на атаки та інциденти у мережі, що зокрема, знайшло відображення у багатьох фахових публікаціях [3]-[7].

Ціль дослідження

Огляд та аналіз методів та технологій інтеграції та захисту IoT пристроїв у комп'ютерній мережі на прикладі закладу вищої освіти.

Виклад основного матеріалу

Компонування комп'ютерної мережі закладу вищої освіти (далі ЗВО), як правило, завжди є стандартним. Так, одне підключення до Internet Service Provider, далі ISP, який виділяє декілька білих IP адрес для доступу у мережу. Наявний один маршрутизатор на периметрі мережі, до якого у свою чергу під'єднане комутаційне ядро. Рівень розподілення вже іде на кожен окремий корпус/клас. Враховувати треба різні обставини і розміри ЗВО, але принцип побудови та розгортання завжди залишається схожим. Серверний сегмент мережі, виділявся в окремий VLAN. До якого йшов виділений канал. Така схема побудови є досить простою і не потребує великих, як матеріальних так і фізичних затрат на її розгортання та підтримку.

Все частіше пристрої IoT починають впроваджувати у інфраструктуру закладів освіти. Певні пристрої відслідковують температуру, вологість та тиск, задимленість у аудиторіях. Певні пристрої виконують роль замків та систем доступу до певних приміщень. Досить активно починають використовувати камери відеоспостереження

для розпізнавання обличчя та ідентифікації людини, яка перебуває на даний момент у приміщенні. Весь цей потік даних передається на сервери ЗВО для подальшої обробки.

Однак IoT також представляє підвищену проблему безпеки. Організація безпеки у ЗВО повинна також враховувати і безпеку кінцевих пристроїв. Адже втручання чи можливе вторгнення у їх роботу може завдати значної шкоди всій інфраструктурі. IoT підкреслює необхідність зосередити свою увагу на кібер-стійкості - здатності продовжувати трансформуватись ефективно в умовах посилення загроз з боку інших держав, злочинців, конкурентів та інсайдерів. До таких ризиків належать:

- Дедалі ширше використання технологій IoT як у ЗВО, так і з боку пов'язаних зацікавлених сторін, що призводить до того, що контроль над безпекою даних є майже відсутнім;
- Постійне зменшення розміру пристроїв IoT, що ускладнює їх ідентифікацію та контроль за ними;
- Уразливість взаємопов'язаних пристроїв IoT, які можуть призвести до перехоплення даних або пошкодження цілісності даних;
- Напади, які можуть переривати ключові системи та порушувати діяльність.

Для досягнення кіберстійкості IoT ЗВО повинні почати з ретельної оцінки, виявлення всіх активів, пов'язаних з IoT, які вже існують в рамках операцій, зосередження уваги на інструментах та методах управління доступом, керуванні пристроями IoT протягом усього їх життєвого циклу та наданням активної реакції на інциденти.

Постійний моніторинг пристроїв та трафіку у мережі є ключовим моментом по виявленню вторгнень або вчиненню неправомірних дій. Хакери діють, як правило, за певним алгоритмом – вбивчим ланцюжком. Дану класифікацію запропонувала компанія Lockheed Martin для виявлення і запобігання вторгнень. Ланцюжок кіберзлочину складається з семи кроків, які допомагають аналітикам зрозуміти методи, інструменти та процедури хакерів. Мета при реагуванні на інциденти полягає в тому, щоб виявити і зупинити атаку на якомога більш ранньому етапі ланцюжка кіберзлочину. Чим раніше буде зупинена атака, тим менший збиток буде завдано і тим менше хакер зможе дізнатися про цільову мережу. Ланцюжок кіберзлочину вказує, які дії повинен виконати хакер для досягнення своєї мети.

Якщо хакер буде зупинений на будь-якому етапі, ланцюжок атаки буде розірвано. Розрив ланцюжка означає, що захиснику вдалося успішно відбити вторгнення хакера. Зловмисники досягають успіху, тільки якщо їм вдається дістатися до останнього сьомого етапу.

Розвідувальна атака: зловмисник виконує дослідження, збирає аналітику і вибирає цілі. За цими даними хакер зможе визначити, чи варто братися за атаку. Будь-яка загальнодоступна інформація може допомогти визначити, що, де і як атакувати. Існує великий обсяг загальнодоступної інформації, особливо якщо мова йде про великі організації, включаючи статті новин, веб-сайти, участь в конференціях і загальнодоступні мережеві пристрої. Постійно зростаючі обсяги інформації про співробітників можна отримати в соціальних мережах.

Зловмисник вибирає цільові об'єкти, які були забуті або не були захищені, оскільки ймовірність проникнення або злому цих об'єктів вище. Всі інформація, отримана зловмисником, аналізується з метою визначення її важливості, а також розуміння, чи розкриває вона можливі додаткові джерела доходу від атаки.

Мета наступного етапу полягає в розробці зброї проти певних цільових систем, наявних в організації, з використанням інформації, отриманої за допомогою

розвідувальної атаки. Для розробки цієї зброї конструктор використовує уразливості ресурсів, які були виявлені, і вбудовує їх у засіб, який можна розгорнути. Після застосування цього засобу очікується, що хакер досягне своєї мети щодо отримання доступу до цільової системи або мережі, через що працездатність цієї системи (або всієї мережі) знижується. Зловмисник продовжить вивчати мережу і захист ресурсів з метою виявлення додаткових слабких місць для отримання контролю над іншими ресурсами або розгортання нових атак.

Вибрати зброю для атаки нескладно. Зловмиснику необхідно подивитися, які атаки можна застосувати для виявлених вразливостей. Існує безліч готових атак, які добре протестовані. Одна з проблем полягає в тому, що, оскільки ці атаки так добре відомі, швидше за все, захисники також з ними знайомі. Часто більш ефективним є використання поки ще невідомої атаки, що дозволяє уникнути інструментів виявлення. Зловмисник може прийняти рішення розробити власну зброю, яка буде спеціально призначена для ухилення від інструментів виявлення, використовуючи для цього отриману ним інформацію про мережі і системи.

На етапі доставлення, зброю передають в цільову систему за допомогою вектора доставки. Проробити це можливо за допомогою веб-сайту, знімних носіїв USB або вкладень в електронні повідомлення. Якщо зброя не буде доставлена, атака закінчиться невдачею. Для підвищення шансів доставки корисних даних зловмисник буде використовувати кілька різних способів, в тому числі шифрування зв'язку, надання коду виду легітимної програми або маскування коду. Датчики безпеки настільки досконалі, що вони неодмінно визнають код шкідливим, якщо не ввести в нього зміни, що дозволяють уникнути виявлення. Код може бути змінений так, щоб виглядати невинним, при цьому він продовжить виконувати необхідні дії, навіть не дивлячись на те, що на його виконання може витрачатися більше часу.

Після того як зброя буде доставлена, зловмисник зламує систему в уразливому місці і отримує контроль над цільовою системою. Найбільш поширеними цілями експлойтів є додатки, уразливості операційних систем і користувачі. Організатору атаки необхідно використовувати експлойт, який дозволяє досягти потрібного ефекту. Це дуже важливо, оскільки, якщо задіяти неправильний експлойт, вочевидь атака не спрацює, виникнуть небажані побічні ефекти, серед яких відмова в обслуговуванні або численні перезавантаження системи, привернуть непотрібну увагу, в результаті чого аналітики з кібербезпеки зможуть легко отримати інформацію про атаку і наміри хакера.

Саме під час ін’єкції хакер створює прохід у систему, щоб забезпечити постійний доступ до цілі. Для того щоб зберегти цей прохід, важливо, щоб віддалений доступ ніяк не виявлявся аналітиками з кібербезпеки або користувачами. Спосіб доступу повинен залишитися непоміченим після сканування, виконуваного засобами антивірусів і перезавантаження комп'ютера, необхідного, щоб шпарина у системі запрацювала. Цей постійний доступ також може забезпечувати автоматичний зв'язок, що особливо ефективно, коли для управління ботнетом необхідно кілька каналів зв'язку.

Ціль наступного етапу полягає у встановленні управління та контролю над цільовою системою. Зламані хости зазвичай виводяться з мережі і підключаються до контролера в Інтернеті. Це пов'язано з тим, що для здебільшого шкідливого ПО потрібна ручна взаємодія для ексфільтрації даних з мережі. Останній етап ланцюжка кіберзлочину описує досягнення зловмисником поставленої спочатку мети. Це може бути крадіжка даних, проведення DDoS-атаки або використання зламаної мережі для створення і розсилки спаму. На цьому етапі зловмисник вже глибоко укорінився в

системі організації, приховуючи свої дії і замітаючи сліди. Видалити хакера з мережі надзвичайно складно.

Враховуючи дану інформацію, аналітик з інформаційної безпеки надає системному інженеру та інженеру з безпеки рекомендації щодо створення правил безпеки у комп'ютерній мережі та системі моніторингу за різними сегментами мережі.

Спочатку розглянемо підходи у архітектурі комп'ютерної мережі ЗВО, для забезпечення безпеки свої кінцевих пристроїв на рівні L2-L4 . Відомо, що є два основних напрямки атаки зовнішня та внутрішня. Якщо атаки із ззовні можливі і на них намагаються адекватно реагувати. То внутрішні є досить болючими для цілого ЗВО. Чому так виникає. Відповідь криється у загальнодоступності мережі. Будь то студенти чи викладач, кожен генерує трафік, який не відслідковується. Скачана програма із торрент трекерів, перегляд фішингових сайтів, пошта із руткітами та інші види загроз залишають на внутрішніх персональних комп'ютерах розміщених у корпусах. Якщо прослідкувати весь трафік по мережі, то можна побачити, що впливати якимось правилами на L2 трафік можливості немає. Звичайно можна налаштувати безпеку портів, і досить жорстко прив'язати ПК до портів комутатора. Налаштувати ACL для L3/IP. Та все ж відслідковувати трафік, а якщо точніше сказати, проводити інспекцію пакетів неможливо.

Одним із рішень є застосувати на пограничному маршрутизаторі підходу, що називається Zone Base Firewall. Це дає можливість інспектувати трафік на L3-L4 рівнях, зменшує кількість опису правил по трафіку та мережі. Що вивільняє ресурси на обробку пакетів.

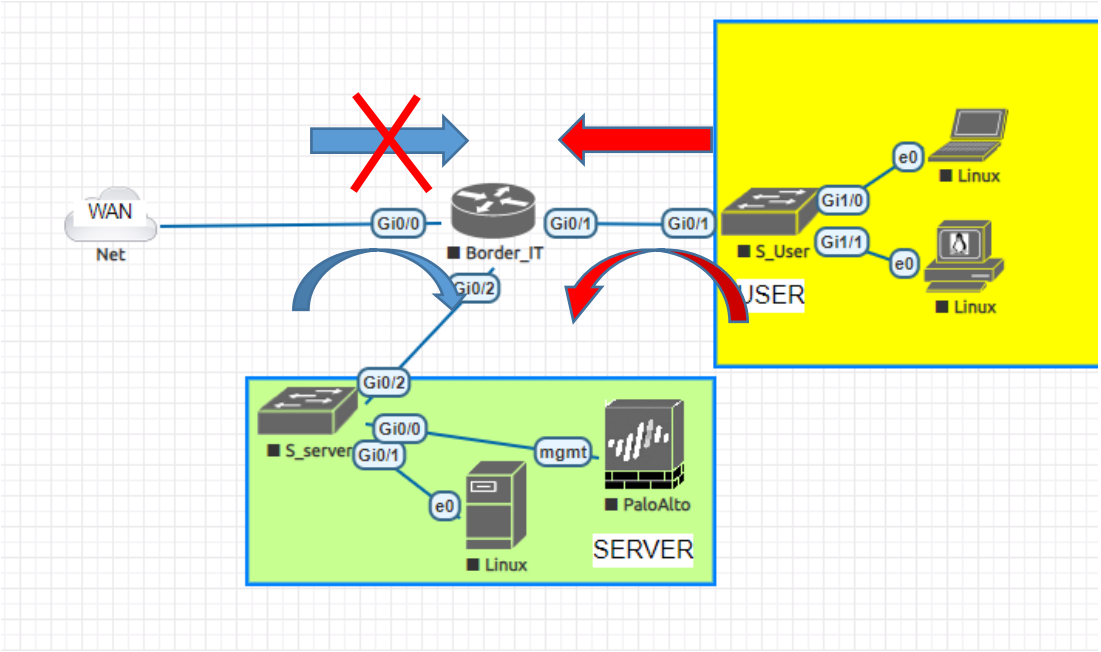

Рис. 1. Приклад застосування ZBF

На рис. 1 показано підхід до використання ZBF. У першу чергу, треба відмітити, що серверний сегмент треба виокремлювати у демілітаризовану зону, що є ще одним правилом у забезпеченні безпеки мережі. Для реалізації ZBF треба визначити зони, до яких відносяться відповідні інтерфейси. Лінки, які направлені сторону ISP відносять до зовнішніх каналів і їх необхідно позначати як зовнішніми (WAN – позначка на

ISSN 2663 - 4023

рисунку). Порти з'єднані із користувачами відносяться до користувацького сегменту – User. Також присутній сегмент серверного забезпечення. Трафік що ініціалізується з користувацького сегменту у мережу Інтернет, буде проходити через маршрутизатор, який у свою чергу запам'ятає сесію і провірить трафік що через нього проходить. Тобто, відповідь на ініціалізований запит буде проходити у середовище до сегменту користувачів. Така ж сама ситуація, коли користувач заходить на серверний сегмент. Відповідь від навчальних порталів буде проходити через маршрутизатор. Перевага застосування саме такого підходу, полягає у тому, що сесія яка створюється пропускає у відповідь тільки відповідний трафік. Дані записуються у лог файл. Також дозволений трафік із зовні до серверного сегменту. Студенти будуть отримувати доступ до навчального порталу з дому. Відповідно такий трафік також буде відслідковуватись і в разі виявлення аномалій буде заблоковано мережу звідки проводяться незаконні дій. Щодо серверного сегменту, він не буде мати можливості виходити у будь яку із раніше описаних зон. Таким чином забезпечується безпека локальних користувачів від можливих загроз з боку серверного сегменту (якщо припустити злом серверів і їх зараження). Так і їх виходу в мережу Інтернет або атак на провайдера.

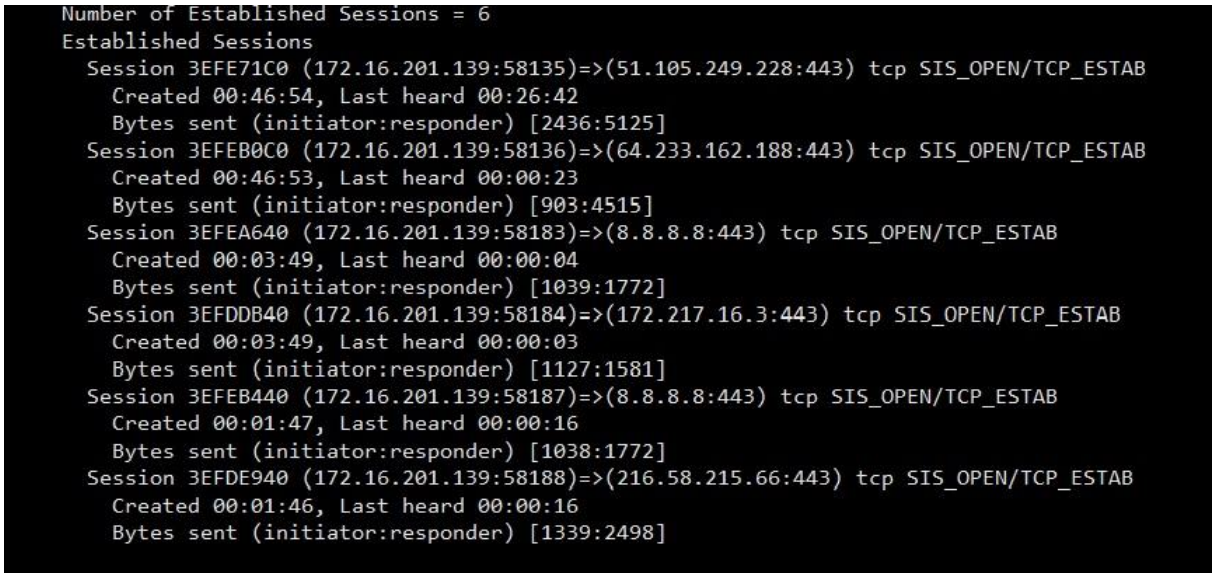

Рис. 2. Приклад інспектування пакетів, що проходять граничний маршрутизатор ЗВО

Розбудова безпеки комп'ютерної інфраструктури не зупиняється тільки на одному підході. Так на границі мережі застосовуються технології переадресації мережевих адрес та форвардування портів на внутрішні адреси. Це також один із елементів захисту. Та все ж такий підхід не дає закрити повністю модель OSI у плані безпеки ЗВО, якщо враховувати модель вбивчого кіберланцюжка.

Оскільки пристрої IoT у більшій своїй сутності працюють із веб-серверами, побудованими на різних технологіях, необхідно продумувати захист, який буде закривати L5-L7 рівень моделі OSI. Одним із підходів є використання Web Application Firewall далі –WAF. Сам WAF, це - сукупність моніторів і фільтрів, призначених для виявлення і блокування мережевих атак на веб-додаток. WAF відносяться до прикладного рівня моделі OSI.

Веб-додаток може бути захищений силами розробників самого додатка без використання WAF. Це вимагає додаткових витрат при розробці. Наприклад, зміст

відділу інформаційної безпеки. WAF увібрав у себе можливість захисту від усіх відомих інформаційних атак, що дозволяє делегувати йому функцію захисту.

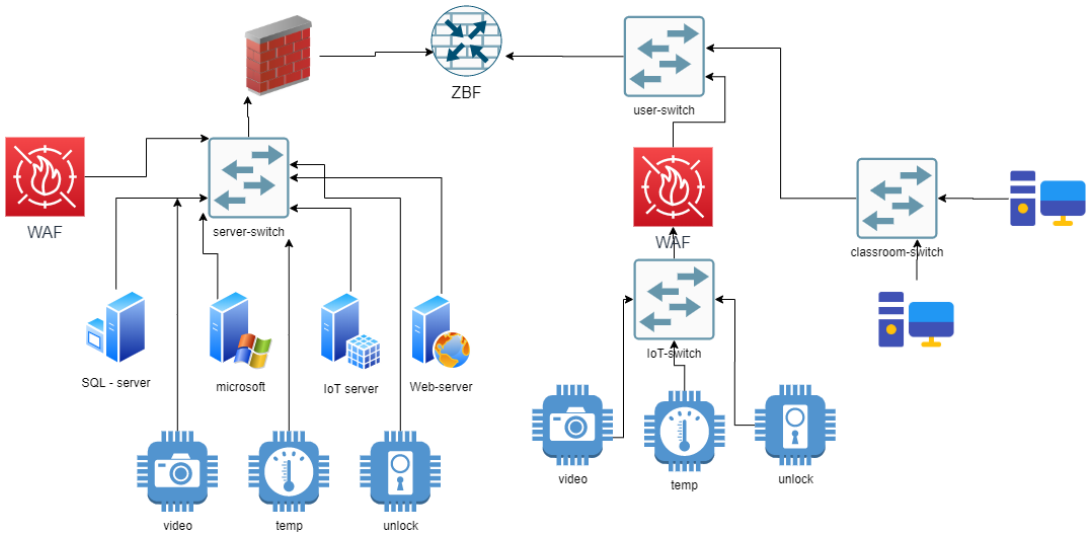

Рис. 3. Схема інтеграції IoT пристроїв у комп'ютерну мережу ЗВО

Робота фаєрвола суттєво затримує швидкість трафіку у мережу. Відбувається перевірка трафіку на наявність шкідливого ПЗ. Необхідно такі точки контролю розставляти із досить високою обережністю. Наприклад, на рис. 3 представлена схема інтеграції IoT пристроїв у комп'ютерну мережу ЗВО. Сама мережа розділена на два сегменти. Одна частина умовно вважається також демілітаризованою зоною, оскільки там знаходиться серверна ферма. Інша частина мережі відноситься до користувачів, аудиторій та лабораторій. Зі схеми видно, що у частині мережі користувачів, всі пристрої підключені до одного комутатора. Даний підхід дає можливість виділити у особливий канал відповідний трафік. У свою чергу це полегшує налаштування WAF, який підключений у режимі мосту між двома комутаторами. Такий підхід дозволяє більш точніше налаштувати фаєрвол під той вид трафіку, що генерують саме IoT девайси. Водночас, він не дозволяє проникнути у мережу IoT простим користувачам. Такий підхід дає можливість елементам штучного інтелекту на WAF більш точніше проводити навчання на виявлення загроз, і розвантажує апаратну частину не навантажуючи її зайвим трафіком.

Серверний сегмент має свою специфіку. По перше, це наявність апаратного фаєрвола, що проводить інспекцію вхідного та вихідного трафіку. Далі іде наявність комутатора серверного сегменту. Тут вже WAF включений як окремий користувач. У цьому випадку WAF працює як пасивний спостерігач за трафіком. У такому випадку канал з'єднання не так уповільнюється швидкістю з'єднання. Порт комутатора працює як дзеркало і весь трафік що генерується передається на WAF. Це дозволяє налаштувати фаєрвол на більш глибше виявлення загроз та сигнатур що несуть небезпеку. При цьому не з'їдаючи канал. IoT пристрої фізично підключені до одного і того ж серверного комутатора, але логічно винесені у віртуальну локальну мережу, що працює за правилами пріоритету доступу до сервера IoT.

Для тестування роботи WAF у запропонованій топології мережі було покладено на програму ModSecurity. Дане програмне забезпечення поширюється під вільною ліцензією і може бути налаштоване під відповідні унікальні потреби. Враховуючи

відкритість коду та застосування під ОС Linux, її також можна удосконалювати і розвивати відповідно до виявлених атак. Існує два варіанти розгортання ModSecurity: розгортання безпосередньо на веб-сервері, інсталяція в якості зворотнього проксі-серверу (Reverse Proxy). В першому випадку ModSecurity перехоплює всі запити до веб-серверу, на якому він встановлений: запит від клієнта спочатку порівнюється з правилами фільтрації, а потім передається на подальшу обробку веб-серверу. ModSecurity також може контролювати відповіді веб-серверу, тобто після формування веб-сторінки відповідь обробляється модулем і у відповідності правилам дозволяє або блокує проходження відповідей від веб-серверу [7]-[10].

Інсталяція в якості зворотнього проксі-серверу дозволяє перехоплювати запити клієнтів веб-серверу, виконувати перевірку даного трафіку та перенаправляти на інші веб-сервери. Клієнти можуть бачити лише інтерфейс proxy-серверу і не можуть бачити веб-серверів, що розміщуються за ним. Відповідь внутрішнього серверу відправляється через проксі-сервер.

Розгортати ModSecurity можна як на окремо виділеній фізичній так і віртуальній машині. Все залежить від поставлених завдань. У нашій пропонованій схемі буде використано виділений фізичний пристрій. На який у свою чергу попередньо встановлено ОС Linux та веб сервер Apache. Для роботи WAF необхідно мати власний сервер для звернення до бази даних та можливістю віддалених запитів. Приклад розгортання серверу наведений нижче на рисунках 4-6.

```
root@NanoPi-R1:~# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill-dbd-sql
  libaprutill-ldap liblua5.1-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw op
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill
  libaprutill-ldap liblua5.1-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 10 not upgraded.
Need to get 1,412 kB of archives.
After this operation, 4,986 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Рис. 4. Встановлення веб-серверу Apache

Після встановлення веб-серверу Apache необхідно виконати встановлення ModSecurity за допомогою команди apt-get install libapache2-modsecurity.

```
root@NanoPi-R1:~#  apt-get install libapache2-modsecurity
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-security2 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby
The following NEW packages will be installed:
```

Рис. 5. Встановлення ModSecurity

Для перевірки правильності встановлення скористаємося командою apachectl -M grep security. Якщо інсталяція пройшла вдало, команда повинна вивести security2_module (shared).

```
root@NanoPi-R1:~# apachectl -M | grep security
AH00558: apache2: Could not reliably determine the
in name, using 127.0.1.1. Set the 'ServerName' dire
is message
 security2_module (shared)
root@NanoPi-R1:~#
```

Рис. 6. Перевірка правильності встановлення ModSecurity

ModSecurity включає рекомендований файл конфігурації modsecurity.conf-recommended, що розміщений в каталозі /etc/modsecurity. Для того, щоб цей файл працював з ModSecurity необхідно перейменувати його, використовуючи команду mv/etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf.

```
root@NanoPi-R1:~# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
root@NanoPi-R1:~# cd /etc/modsecurity
root@NanoPi-R1:/etc/modsecurity# ls
modsecurity.conf  unicode.mapping
root@NanoPi-R1:/etc/modsecurity#
```

Рис. 7. Перейменування файлу конфігурації

Використовуючи будь-який текстовий редактор, редагуємо вміст файлу modsecurity.conf. Змінюємо «SecRuleEngine Detection Only» на «SecRuleEngine On», зберігаємо зміни та виходимо з текстового редактора.

```
#
SecRuleEngine On


# -- Request body handling ---------------------------------------------------

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On


# Enable XML request body parser.
File Name to Write: /etc/modsecurity/modsecurity.conf
^G Get Help     M-D DOS Format  M-A Append      M-B Backup File
^C Cancel       M-M Mac Format  M-P Prepend     ^T To Files
```

Рис. 8. Редагування файлу modsecurity.conf.

Після редагування файлу перезавантажуємо веб-сервер Apache.

```
root@NanoPi-R1:~# systemctl restart apache2
root@NanoPi-R1:~# systemctl status apache2
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Sat 2021-02-06 18:52:03 UTC; 1min 0s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 23133 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCES
  Process: 23156 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCC
   CGroup: /system.slice/apache2.service
           ├─23171 /usr/sbin/apache2 -k start
           ├─23174 /usr/sbin/apache2 -k start
           └─23175 /usr/sbin/apache2 -k start

Feb 06 18:52:00 NanoPi-R1 systemd[1]: Starting LSB: Apache2 web server...
Feb 06 18:52:00 NanoPi-R1 apache2[23156]:  * Starting Apache httpd web server ap
Feb 06 18:52:01 NanoPi-R1 apache2[23156]: AH00558: apache2: Could not reliably d
Feb 06 18:52:03 NanoPi-R1 apache2[23156]:  *
Feb 06 18:52:03 NanoPi-R1 systemd[1]: Started LSB: Apache2 web server.
lines 1-18/18 (END)
```

Рис. 9. Перезавантаження веб-серверу

ModSecurity постачається з багатьма правилами базового набору (Core Rule Set). CRS направлено на захист веб-додатків від широкого спектру атак (в тому числі від OWASP Top Ten), з мінімальною кількістю хибних спрацювань. Правила CRS зберігаються в каталозі /usr/share/modsecurity-crs.

```
root@NanoPi-R1:~# ls -l /usr/share/modsecurity-crs/
total 44
drwxr-xr-x 2 root root  4096 Feb  6 17:12 activated_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 base_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 experimental_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 lua
-rw-r--r-- 1 root root 13809 Oct 25  2014 modsecurity_crs_10_setup.conf
drwxr-xr-x 2 root root  4096 Feb  6 17:12 optional_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 slr_rules
drwxr-xr-x 8 root root  4096 Feb  6 17:12 util
root@NanoPi-R1:~#
```

Рис. 10. Набір базових правил CRS

Для подальшої роботи буде використовуватися набір правил які складені відповідно під потреби захисту корпоративної мережі ЗВО та захисту IoT пристроїв. Видаляємо набір правил по замовчуванню командою rm -rf /usr/share/modsecurity-crs. Створюємо новий каталог в каталозі Apache, використовуючи команду:

ISSN 2663 - 4023

```
root@NanoPi-R1:~# mkdir /etc/apache2/modsecurity.d
root@NanoPi-R1:~# cd /etc/apache2/
root@NanoPi-R1:/etc/apache2# ls
apache2.conf      conf-available  envvars  mods-available  mods-enabled  sites-available
apache2.conf.in   conf-enabled    magic    modsecurity.d   ports.conf    sites-enabled
root@NanoPi-R1:/etc/apache2#
```

Рис. 11. Створення каталогу modsecurity.d

Завантажуємо основний набір правил Modsecurity. Копіюємо приклад файлу конфігурації із завантаженого набору правил командою cp crs-setup.conf.example crs-setup.conf. Редагуємо файл конфігурації Apache наступним чином:

```
<IfModule security2_module>
        SecDataDir /var/cache/modsecurity
        IncludeOptional /etc/modsecurity/*.conf
        IncludeOptional "/usr/share/modsecurity-crs/*.conf
        IncludeOptional "/usr/share/modsecurity-crs/rules/*.conf
 </IfModule>
File Name to Write: /etc/apache2/apache2.conf
^G Get Help       M-D DOS Format    M-A Append        M-B Backup File
^C Cancel         M-M Mac Format    M-P Prepend       ^T To Files
```

Рис. 12. Редагування файлу конфігурації Apache

Перевіряємо конфігурацію Apache та перезавантажуємо веб-сервер.

Для тестування роботи WAF після попередніх налаштувань, проведемо тестову атаку на ресурси серверного сегменту.

На віддаленому комп'ютері виконуємо наступну команду, для перевірки роботи ModSecurity з XSS-атаками: url http://192.168.1.251/?q="><script>alert(1)</script>'. При цьому отримаємо відповідь від серверу 403 Forbidden.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 192.168.1.251 Port 80</address>
</body></html>
```

Після цього проведемо просту атаку за допомогою SQL-ін'єкції. Вводимо наступний URL в адресний рядок браузера: http://192.168.1.251/?id=3%20or%20%27a%27=%27a%27 та отримуємо, див. рис. 13:

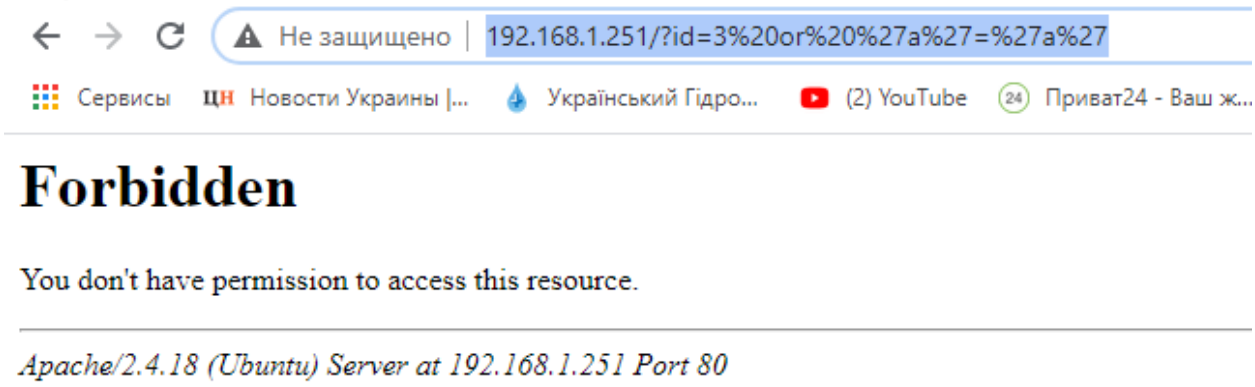

Рис. 13. Вдалий захист від простої SQL-ін'єкції

В журналі аудиту /var/log/apache2/modsec_audit.log можна побачити наступну інформацію, що означає, що ModSecurity заблокував цю атаку за допомогою OWASP v3.3.0, див. рис. 14.

```
--83946356-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/etc/apache2/
Message: Warning. detected SQLi using libinjection with fingerprint 'l&sos' [file "/etc/ap
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score.
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/etc/apache2/m
Action: Intercepted (phase 2)
Stopwatch: 1612810436619109 28052 (- - -)
Stopwatch2: 1612810436619109 28052; combined=20873, p1=6052, p2=13105, p3=0, p4=0, p5=1714
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.0 (http://www.modsecurity.org/); OWASP_CRS/3.3.0.
Server: Apache/2.4.18 (Ubuntu)
Engine-Mode: "ENABLED"
```

Рис. 14. Інформація з журналу аудиту

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Даний підхід інтеграції та захисту у подальшому буде описуватись математичними розрахунками для визначення уразливостей та практичної перевірки на вразливості. Варто відмітити, що IoT будуть досить стрімко розвиватися і все глибше входити у наше життя. Особливо це стосується закладів вищої освіти. Тому у своїх подальших працях ми будемо відпрацьовувати даний підхід.

У подальших дослідженнях планується проводити роботу над удосконаленням методики забезпечення захисту та моніторингу інфраструктури ЗВО. Удосконалення програмної частини щодо виявлення можливих загроз, їх ідентифікацію та впровадження у роботу WAF-фаєрволів елементів штучного інтелекту. Для виявлення загроз направлених на пристрої Інтернет Речей.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, швидкий розвиток IoT приніс можливості закладам вищої освіти розвиватися у напрямку Смарт Сіті та бути інтегрованими у таку структуру.

Враховуючи і той факт, що самі ЗВО і є генераторами ідей та віянь у сфері ІТ використання таких пристроїв, дасть змогу науковцям підходити більш практично до таких речей. Різноманітні системи моніторингу якості повітря, стану аудиторій та лабораторій, перевірки присутності та системи електронних карток дають можливість більш якісніше автоматизувати різноманітні процеси.

Роблячи висновок по вище викладеному матеріалу, можна сказати, що: необхідність із найменшими затратами інтегрувати IoT пристрої у ІТ структуру ЗВО та захист таких девайсів стає дуже важливим, оскільки вони можуть надати зловмисникам інформацію про персональні дані, що можуть зберігатися на цифрових носіях ЗВО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
2 Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, *32*(5), 715-728.
3 Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4(*5), 666-674.
4 Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, (93), 849-859.
5 Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.
6 Завгородній, В. В., Дроздова, Є. А., & Козел, В. М. (2020). Аналіз проблем безпеки Iot пристроїв. *Вісник Херсонського національного технічного університету*, *4* (75), 59-66.
7 Трохименко, Д. В., & Курдеча, В. В. (2019). Захист даних в інтернеті речей. *Міжнародна науково-технічна конференція 228 «Радіотехнічні поля, сигнали, апарати та системи»*, 228-230.
8 Altiparmak, F., Dengiz, B., & Smith, A. E. (2003). Optimal design of reliable computer networks: A comparison of metaheuristics. *Journal of heuristics*, *9*(6), 471-487.
9 Cononelos, T., & Oliva, M. (1993). Using computer networks to enhance foreign language/culture education. *Foreign Language Annals*, *26*(4), 527-534.
10 Lee, H. C., & Ke, K. H. (2018). Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation. *IEEE Transactions on Instrumentation and Measurement*, *67*(9), 2177-2187.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Valerii A. Lakhno
Dr. Tech. Sc., Professor,
Head of the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Andrii I. Blozva
Cand. Pedag. Sc. (Ph.D.),
Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Borys S. Husiev
Cand. Tech. Sc. (Ph.D), Docent,
Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-1658-7822
gusevbs@nubip.edu.ua

Tetiana Y. Osypova
Cand. Pedag. Sc. (Ph.D),
Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Yurii V. Matus
Senior Lecturer at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-0974-4789
umatus@nubip.edu.ua

INTEGRATION AND PROTECTION OF IOT DEVICES IN THE AVAILABLE INFRASTRUCTURE OF THE COMPUTER NETWORK OF THE EDUCATIONAL INSTITUTIONS

Abstract. The development of computer networks is gaining momentum. There are new challenges to data security and the end users themselves. With the advent of the Internet of Things, this problem has become quite acute for network engineers and cyber analysts. Increasingly, there are illegal actions to interfere with the work of the network itself and the use of users' devices for criminal purposes. Various distributed attacks, SQL injections and identity theft are becoming more complex. Given the growing infrastructure of both the network and IoT devices, there is a need to protect them. Especially when it comes to the computer network of a higher education institution. Where little attention is usually paid to full infrastructure protection, and with the integration of IoT devices, such possible gaps can occur quite a lot.

This article attempts to reveal theoretical approaches to the design and implementation of a computer network of higher education institutions, which in recent years are increasingly beginning to suffer from outside interference. Possible attacks on the infrastructure of higher education institutions are analyzed, as well as the possibility of attack and interference in the work of IoT devices based on the killer chain approach. Internet The possibility of using a web application firewall and appropriate software for security and incident management at the L5-L7 OSI level is considered in such networks. Preliminary testing of the network for the ability to respond to L3-L4 level attacks using standard firewall capabilities. And with the response to interventions at the upper levels of the OSI L5-L7 model, namely: SQL injections, distributed DDoS, bot-net attacks. The results are summarized and further directions of research are determined, which are based on the improvement of the group security policy for the higher

education institution. Development of security infrastructure for IoT devices and the ability to respond quickly to non-standard attacks.

Keywords: cybersecurity, computer network, IoT device, integration of security systems

REFERENCES

1 Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
2 Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, *32*(5), 715-728.
3 Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666-674.
4 Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, (93), 849-859.
5 Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.
6 Zavgorodniy, VV, Drozdova, EA, & Kozel, VM (2020). Analysis of Iot device security issues. *Bulletin of Kherson National Technical University*, *4* (75), 59-66.
7 Trokhimenko, DV, & Kurdecha, VV (2019). Data protection on the Internet of Things. *International scientific and technical conference 228 "Radio fields, signals, devices and systems"*, 228-230.
8 Altiparmak, F., Dengiz, B., & Smith, A. E. (2003). Optimal design of reliable computer networks: A comparison of metaheuristics. *Journal of heuristics*, *9*(6), 471-487.
9 Cononelos, T., & Oliva, M. (1993). Using computer networks to enhance foreign language/culture education. *Foreign Language Annals*, *26*(4), 527-534.
10 Lee, H. C., & Ke, K. H. (2018). Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation. *IEEE Transactions on Instrumentation and Measurement*, *67*(9), 2177-2187.