УДК 004.738.5 https://doi.org/10.35546/kntu2078-4481.2020.4.7

В.В. ЗАВГОРОДНІЙ
Херсонський національний технічний університет
ORCID: 0000-0003-3282-4402
Є.А. ДРОЗДОВА
Херсонський національний технічний університет
ORCID: 0000-0003-0276-6387
В.М. КОЗЕЛ
Херсонський національний технічний університет
ORCID: 0000-0002-2627-2499

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ IoT ПРИСТРОЇВ

В статті розглянуто проблеми забезпечення захисту доступу до IoT-пристроїв та їхніх мереж. Проаналізовано дослідження фахівців компанії Microsoft, які за результатами опитування встановили, що найбільші проблеми в IoT- мережах стосуються безпеки на рівні мережі. Наявність великої кількості недостатньо захищених пристроїв полегшує проведення DDoS-атак, в яких для нападу на корпоративні системи можуть використовуватися побутові пристрої.

Основна причина відмови виробників компонентів системи IoT впроваджувати елементи безпеки – це великі обчислювальні витрати, що зменшують термін служби елементів живлення пристроїв.

Спеціалісти HPE (Hewlett Packard Enterprise) рекомендують звернути увагу як на проблеми на стороні власників пристроїв, так і на проблеми, які повинні виправити розробники, та надають декілька порад з налаштувань IoT-пристроїв. Фахівцями HPE нараховано близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток і т.д.) та їхніх мобільних і хмарних компонентах, складено перелік найбільших вразливостей та зроблено невтішний висновок: безпечної екосистеми IoT на сьогоднішній день не існує.

Розглянуто статистику зафіксованих впродовж останніх 2х років за допомогою хоніпотів атак на IoT-пристрої, яку зібрали спеціалісти «Лабораторії Касперського». Виявилось, що відбувається зростання кількості атак із збільшенням кількості IP-адрес. Складено список країн, з яких було зафіксовано найбільше спроб виконати атаку. Найбільша кількість атак велась з Китаю та Бразилії.

Розглянуто список загроз, представлений компанією Trend Micro.

Проаналізовано найбільш поширені технології атак, за допомогою яких можуть бути нанесені значні збитки. До таких технологій можна віднести: посилення «Amplification», зміну інформації маршруту, вибіркову розсилку, бездонну воронку «Sinkhole Attack», шаманську атака «Sybil attack», атаку червоточини «Wormhole attack», флуд атаку «HELLO flood attack».

Представлено перелік основних рекомендацій для забезпечення безпеки в IoT системі, а саме: захист паролів, використання окремих мереж, відмова від автоматичного підключення до мережі.

Ключові слова: Інтернет речей (IoT), промислові пристрої інтернету речей (IIoT), міжмашинна взаємодія (M2M), розумний будинок, розумне місто, інформаційна безпека (ІБ), DDoS-атака

В.В. ЗАВГОРОДНИЙ
Херсонский национальный технический университет
ORCID: 0000-0003-3282-4402
Е.А. ДРОЗДОВА
Херсонский национальный технический университет
ORCID: 0000-0003-0276-6387
В.Н. КОЗЕЛ
Херсонский национальный технический университет
ORCID: 0000-0002-2627-2499

АНАЛИЗ ПРОБЛЕМ БЕЗОПАСНОСТИ IoT УСТРОЙСТВ

В статье рассмотрены проблемы обеспечения защиты доступа к IoT-устройствам и их сетям. Проанализированы исследования специалистов компании Microsoft, которые по результатам опроса установили, что наибольшие проблемы в IoT- сетях касаются безопасности на уровне сети. Наличие большого количества недостаточно защищенных устройств облегчает проведение DDoS-атак, в которых для нападения на корпоративные системы могут использоваться, в том числе, и бытовые устройства.

Основная причина отказа производителей компонентов системы IoT внедрять элементы безопасности – это большие вычислительные затраты, уменьшающие срок службы элементов питания устройств.

Специалисты HPE (Hewlett Packard Enterprise) рекомендуют обратить внимание как на проблемы на стороне владельцев устройств, так и на проблемы, которые должны исправить разработчики, и предоставляют несколько советов по настройке IoT-устройств. Специалистами HP насчитано около 25 различных уязвимостей в каждом из исследованных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзеток и т.д.) и их мобильных и облачных компонентах, составлен перечень крупнейших уязвимостей и сделан неутешительный вывод: безопасной экосистемы IoT на сегодняшний день не существует.

Рассмотрена статистика зафиксированных в течение последних 2х лет с помощью хонипотов атак на IoT-устройства, которую собрали специалисты «Лаборатории Касперского». Оказалось, что отмечается рост количества атак с увеличением количества IP-адресов. Составлен список стран, из которых было зафиксировано болем всего попыток выполнить атаку. Наибольшее количество атак велось из Китая и Бразилии.

Рассмотрен список угроз, представленный компанией Trend Micro.

Проанализированы наиболее распространенные технологии атак, с помощью которых могут быть нанесены значительный ущерб. К таким технологиям можно отнести: усиление «Amplification», изменение информации маршрута, выборочную рассылку, бездонную воронку «Sinkhole Attack», шаманскую атаку «Sybil attack», атаку червоточины "Wormhole attack», флуд атаку «HELLO flood attack».

Представлен перечень основных рекомендаций для обеспечения безопасности в IoT системе, а именно: защита паролей, использование отдельных сетей, отказ от автоматического подключения к сети.

Ключевые слова: Интернет вещей (IoT), промышленные устройства интернета вещей (IIoT), межмашинное взаимодействие (M2M), умный дом, умный город, информационная безопасность (ИБ), DDoS-атака

V.V. ZAVHORODNII
Kherson National Technical University
ORCID: 0000-0003-3282-4402
Ye.A. DROZDOVA
Kherson National Technical University
ORCID: 0000-0003-0276-6387
V.M. KOZEL
Kherson National Technical University
ORCID: 0000-0002-2627-2499

ANALYSIS OF SECURITY PROBLEMS OF IoT DEVICES

The paper considers the problems securing of protection of access to IoT-devices and their networks. A study by Microsoft experts, who found that the biggest problems in IoT networks are related to network-level security, was analyzed. The presence of a large number of insufficiently protected devices facilitates DDoS-attacks, in which home devices can be used to attack corporate systems.

The main reason for the failure of IoT component manufacturers to implement security features is the high computational costs that reduce the service life of device batteries.

HPE (Hewlett Packard Enterprise) experts recommend paying attention to both device owner issues and developer issues, and provide some tips on setting up IoT devices. HPE experts have identified about 25 different vulnerabilities in each of the studied devices (TVs, door locks, household scales, home security systems, electrical outlets, etc.) and their mobile and cloud components, compiled a list of major vulnerabilities and made a disappointing conclusion: a safe ecosystem IoT does not exist today.

The statistics of attacks on IoT devices recorded during the last 2 years with the help of honeypots, collected by Kaspersky Lab specialists, are considered. It turned out that the number of attacks increases with the number of IP addresses. A list has been compiled of the countries with the highest number of attempted attacks. The largest number of attacks came from China and Brazil.

The list of threats provided by Trend Micro is considered.

The most common attack technologies, which can cause significant damage, are analyzed. Such technologies include: amplification, change of route information, selective mailing, bottomless funnel "Sinkhole

Attack", shamanic attack "Sybil attack", wormhole attack "Wormhole attack", flood attack "HELLO flood attack".

The list of basic recommendations for security in the IoT system is presented, namely: password protection, use of separate networks, refusal of automatic connection to the network.

Keywords: Internet of Things (IoT), industrial devices of the Internet of Things (IIoT), inter-machine interaction (M2M), smart home, smart city, information security (IS), DDoS-attack

Постановка проблеми

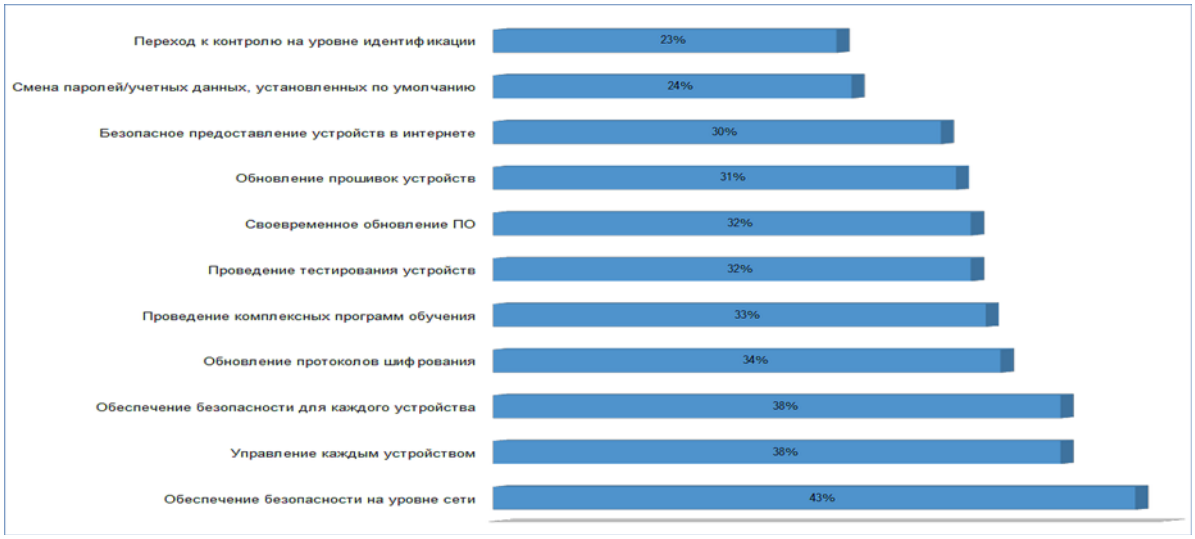
Переваги і можливості, що надають людині нові технології, які стрімко входять в її життя, не викликають сумнівів. До таких новацій безперечно відноситься і концепція «розумного будинку», а в більш широкому сенсі, і «розумного міста», яка реалізується в тому числі на базі Інтернету речей (Internet of Things, IoT). Однак, поряд з усіма очевидними плюсами, слід звертати увагу і на проблеми, викликані поширенням таких технологій. Одна з таких проблем полягає в тому, що виробники компонентів системи Інтернет речей не приділяють належної уваги питанням інформаційної безпеки, які виникають при повсякденному використанні як окремих компонентів системи, так і цілого апаратно-програмного комплексу. З виходом на ринок великої кількості виробників кінцевого, комунікаційного та керуючого обладнання постало питання про інтероперабельність компонентів складної структури, а також про можливість їхньої роботи без загрози виникнення несанкціонованого доступу, витоку або розкриття інформації, що циркулює в системі.

Аналіз останніх досліджень і публікацій

Інтернет речей - це велика кількість пристроїв (яка на порядки перевищує число ПК, ноутбуків і смартфонів), винесених за межі захищеного корпоративного периметра. Крім того, їхньою безпекою довгий час ніхто всерйоз не займався.

Зараз проблема починає усвідомлюватися. В дослідженні Microsoft 2019 року «Найбільш актуальні проблеми Інтернету речей» 19% опитаних респондентів вказали на безпеку як на одну з найважливіших проблем. Чотири найбільш поширені проблеми (складність рішень IP, нестача коштів і кадрів, відсутність необхідних знань і неможливість знайти «правильне» IP-рішення) теж можуть мати своїми наслідками порушення безпеки IP-систем.[1,2]

Що стосується проблем безпеки Інтернету речей, то респонденти опитування Microsoft ранжирували їх наступним чином (рис.1). Найбільше вони стурбовані забезпеченням безпеки на рівні мережі, за кількістю опитаних це складає 43%.[3]



Велика кількість недостатньо захищених пристроїв полегшує проведення DDoS-атак, в яких для нападу на корпоративні системи можуть використовуватися, в тому числі, і побутові пристрої. Останні часто функціонують з паролем, встановленим «за замовчуванням». Ця уразливість стала причиною виникнення і функціонування ботнету Mirai. Потужність влаштованої за допомогою Mirai атаки на веб-сайт журналіста Brian Krebs, присвячений розслідуванню продажу послуг ботнетів, в піку досягала 665 Гбіт / с, причому здійснювалась вона «розумними відеокамерами».[4,5]

Формулювання мети дослідження

Метою роботи є дослідження проблем існуючих загроз безпеки Інтернету речей, у результаті буде сформульовано перелік основних рекомендацій для забезпечення безпеки в IoT системі.

Викладення основного матеріалу дослідження

Сьогодні ми живемо в світі, де пристроїв, підключених до IoT, більше, ніж людей. Цими пристроями можуть бути як розумний годинник, так і RFID-чіп відстеження запасів. Пристрої, підключені до IoT, обмінюються даними через мережу або хмарні платформи, підключені до Інтернету речей. Можливість отримання інформації з IoT в реальному часі наближає цифрову трансформацію. Інтернет речей спричиняє безліч позитивних змін в галузі охорони праці і здоров'я, в сфері ділових операцій, надає можливість покращення виробничих показників і вирішення глобальних екологічних і гуманітарних проблем.

Мета технології полягає в використанні великого числа невеликих малопотужних з обчислювальної та енергетичної точки зору пристроїв для виконання однотипних простих завдань. Така технологія закладена в основі,наприклад, концепції «розумного будинку» і «розумного міста». Подібні технології використовуються в розподілених геоінформаційних системах. При цьому управління цими пристроями здійснюється за допомогою комп'ютера або смарт-пристрою, а в разі міжмашинної взаємодії (M2M) - і зовсім без участі людини.

Прогнозується, що до кінця 2021р. число пристроїв, інтегрованих в середовище Інтернет речей, перевищить 16 мільярдів. Поряд з інтенсивним поширенням по всьому світу і широким застосуванням цієї технології в багатьох галузях виробництва та життєзабезпечення, гостро постає питання про безпеку не тільки рядових користувачів цієї технології, але й критично важливої інформації, що циркулює при міжмашинній взаємодії. При цьому виробники ігнорують заходи безпеки в своїх системах.

Основна причина відмови виробників впроваджувати компоненти безпеки – це великі обчислювальні витрати, а отже, велика витрата електричної енергії, що має критичну важливість для апаратури, яка працює від автономного джерела живлення, наприклад від акумуляторних батарей. До того ж це призводить до подорожчання системи Інтернету речей.[6]

Виходячи з усього вищевикладеного, розглянемо основні загрози, властиві системам Інтернету речей.

Проблемами безпеки середовища Інтернет-речей в даний час займаються багато дослідників по всьому світу. Це пов'язано перш за все з великим колом проблем, що виникають при експлуатації IoT пристроїв.[7]

Експерти наполегливо заявляють про те, що постачальники послуг і пристроїв ринку IoT порушують принцип наскрізної інформаційної безпеки (ІБ), який рекомендований для всіх пристроїв і послуг Інтернету речей. Згідно з цим принципом, ІБ повинна закладатися на початковій стадії проектування продукту або послуги і підтримуватися аж до завершення їхнього життєвого циклу.

Дослідники HPE (Hewlett Packard Enterprise) звертають увагу як на проблеми на стороні власників пристроїв, так і на проблеми, які повинні виправити розробники. Наприклад, на самому початку експлуатації користувач повинен змінити фабричний пароль, що встановлений за замовчуванням, на свій унікальний, оскільки всі фабричні паролі дублюються на всіх пристроях і не відрізняються стійкістю та надійністю. Частіше за все користувачі не дотримуються цієї поради. Тож, власникам слід подбати про встановлення зовнішнього захисту, оскільки не всі прилади мають вбудовані засоби ІБ-захисту, призначені для домашнього використання, з тим щоб Інтернет-пристрої не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.[8]

В ході проведеного HPE дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротовий трафік. 60% веб-інтрефейсів пристроїв експерти HPE вважають небезпечними через небезпечну організацію доступу і високі ризики міжсайтового скриптингу. У більшості пристроїв передбачені паролі недостатньої стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома.

Всього ж фахівці HPE нарахували близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток і т.д.) та їхніх мобільних і хмарних компонентах.[9]

Висновок експертів HPE невтішний: безпечної екосистеми IoT на сьогоднішній день не існує.

Підсумовуючи наведені дослідження, можна виділити наступні уразливості Інтернету речей:

1. Живлення датчиків;
2. Стандартизація архітектури і протоколів, сертифікація пристроїв;
3. Інформаційна безпека;
4. Стандартні облікові записи від виробника, слабка автентифікація;
5. Відсутність підтримки з боку виробника для усунення вразливостей;
6. Неможливість або складність оновлення програмного забезпечення та операційної системи;
7. Використання текстових протоколів і непотрібних відкритих портів;
8. Можливість для хакера легко потрапити в мережу, використовуючи слабкість одного гаджету;
9. Використання незахищеної хмарної інфраструктури.

В першій половині 2019 року фахівці з «Лабораторії Касперського» за допомогою хоніпотів (ресурсів, які представляють собою приманку для зловмисників) зафіксували 105 млн атак на IoT-

пристрої з 276 тис. унікальних IP-адрес. Ці результати виявилися в сім разів вищими, ніж аналогічні, отримані в першій половині 2018 року, коли було виявлено біля 12 млн атак з 69 тис. IP-адрес. На теперішній час кіберзлочинці, користуючись слабким захистом IoT-продуктів, створюють і монетизують все більше IoT-ботнетів.[10]

Кількість кібератак на IoT-пристрої стрімко збільшується, оскільки все частіше користувачі та організації купують «розумні» пристрої, такі як маршрутизатори або камери відеореєстрації та інші, але не дбають про їхній захист від зловмисників. Кіберзлочинці використовують мережі заражених «розумних» пристроїв для проведення DDoS-атак, або в якості проксі-сервера для інших типів шкідливих дій.

Легко вирахувати, що використовуючи середню швидкість з'єднання 15,85 Мбіт / с (дані операторів зв'язку), для генерування DDOS-атаки шириною 586 Гб/с потрібно близько 37 890 пристроїв (табл.1).

Таблиця 1

Ширина DDoS-атаки з урахуванням мережної активності 24 млрд IoT-пристроїв (Тб/с)

		Доступні пристрої					
		1%	10%	25%	50%	75%	100%
Використання пристроїв	1%	36.28	362.78	906.96	1813.89	2720.83	3.627.78
	10%	362.78	3.627.78	9069.44	18138.89	27208.33	36277.77
	25%	906.96	9069.44	22673.61	45347.21	68020.82	90694.43
	50%	1813.89	18138.89	45347.21	90694.43	136041.64	181888.28
	75%	2720.83	27208.33	68020.82	136041.64	204062.46	272083.28
	100%	3.627.78	36277.77	90694.43	181888.28	272083.28	362777.71

Згідно із зібраними даними, атаки на IoT-пристрої не відрізняються складністю, проте достатньо потайливі, щоб користувачі не помітили їх. Сімейство шкідливих програм Mirai застосовувалося в 39% усіх атак, в рамках яких використовувалися експлойти (програма або код, що використовує недоліки в системі безпеки конкретного додатку для інфікування пристрою), що дозволяють ботнет компрометувати пристрої, експлуатуючи старі уразливості, і контролювати їх. На другому місці опинився Linux-троян Nyadrop (38,57%) із застосуванням техніки брутфорса. Nyadrop також часто служив в якості завантажувача Mirai. Третім найбільш поширеним ботнетом став Gafgyt (2,12% від усіх атак).[11]

Дослідники також визначили країни, які частіше за інші виявлялися джерелами зараження в першій половині 2019 року (табл.2). 30% усіх атак відбувалися в Китаї, 19% – в Бразилії, далі йде Єгипет з показником в 12%. У першій половині 2018 роки ситуація була іншою – Бразилія лідирувала з показником в 28%, Китай посідав друге місце (14%), Японія третє (11%).

Таблиця 2

Країни-джерела Telnet-атак на ханіпоти «Лабораторії Касперського»

1 половина 2018		1 половина 2019	
Бразилія	28%	Китай	30%
Китай	14%	Бразилія	19%
Японія	11%	Єгипет	12%
США	5%	Росія	11%
Греція	5%	США	8%
Туреччина	4%	В’єтнам	4%
Мексика	4%	Індія	4%
Росія	3%	Греція	4%
Південна Корея	3%	Південна Корея	4%
Італія	2%	Японія	4%

10 вересня 2019 року компанія Trend Micro опублікувала дослідження «Uncovering IoT Threats in the Cybercrime Underground», в якому описується, як кібер- кримінальні угруповання використовують пристрої IoT в своїх цілях і які загрози це створює.[12]

Фахівці Trend Micro прогнозують наступні загрози, пов'язані з IoT:

1. Зменшення кількості зламаних маршрутизаторів, оскільки велика частина атак пов'язана зі зміною налаштувань DNS, які легко запобігти. Якщо інтернет-провайдери та виробники роутерів почнуть захищати ці настройки, можлива поява нових векторів атак;
2. Зростання числа атак на промислові пристрої Інтернету речей (IIoT), причому в якості вектора монетизації буде використовуватися вимагання;
3. Поява нових інструментальних засобів для проведення атак на IoT / IIoT і зростання популярності двох основних комерційних наборів шкідливих програм для IoT;
4. Поява більш складних загроз, таких як низькорівневі руткіти або зараження вбудованого ПЗ;
5. Нові оригінальні способи монетизації зараження смарт-пристроїв;
6. Розвиток екосистеми автоматизованих атак.

6 лютого 2020 року компанія Qrator Labs представила нові напрямки в сфері мережевої безпеки, що з'явилися в 2019 році. Зростання ринку IoT пристроїв дозволило зловмисникам використовувати вразливі місця пристроїв та створювати значну смугу атак. Для нанесення значних збитків було можливим використовувати протокол WSDD або протокол Apple ARMS, що було виявлено при атаці на мережу фільтрації Qrator Labs.

Для того, щоб виробити рекомендації щодо посилення безпеки систем Інтернету речей, необхідно проаналізувати технології, що використовуються для атак. Декілька з них описані нижче. [12, 13]

Посилення «Amplification» працює наступним чином: відправляється запит на вразливий сервер, цей запит багаторазово повторюється і спрямовується на веб-сайт. В атаці даного типу можуть використовуватись протоколи LDAP і TCP.

Зміна інформації маршруту. Під даний тип атаки найбільше підходять децентралізовані мережі. При цьому час доставляння пакету збільшується через те, що кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію.

Вибіркова розсилка. Даний тип загрози здійснюється наступним чином: скомпрометований вузол сенсорної мережі здійснює вибіркове видалення деяких пакетів. Більшу ефективність ця атака набуває в комбінації з атаками, які збирають велику кількість трафіку на одному вузлі мережі. В результаті скомбінованої атаки найбільше страждає цілісність і доступність даних, що істотно знижує рівень сервісу, який надається сенсорною мережею.

Бездонна воронка «Sinkhole Attack». Атака використовує весь трафік сенсорної мережі скомпрометованого вузла мережі. Зловмисник «слухає» широкомовні розсилки, запити на маршрути і відповідає сенсорним вузлам, що «знайшовся» короткий маршрут до базової станції. Вдавшись встати між сенсорним вузлом, що транслює, і базовою станцією, скомпрометований вузол може виконувати будь-які дії з пакетами даних.

Шаманська атака «Sybil attack» діє наступним чином: скомпрометований вузол, використовуючи декілька псевдоідентифікаторів, видає себе відразу за кілька вузлів. Такі атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. Схильною до даної атаки є будь-яка мережа з рівноправними вузлами (особливо бездротові і децентралізовані мережі).

Атака червоточини «Wormhole attack». Дана атака створює спеціальний шлях для передачі по ньому перехоплених пакетів між двома і більше скомпрометованими вузлами сенсорної мережі. Подібні атаки через відсутність компрометації вузла сенсорної мережі складають серйозну загрозу безпеці сенсорної мережі.

Флуд атака «HELLO flood attack». Атака є широкомовною, і надсилаючи в сенсорну мережу безліч необов'язкових повідомлень, позбавляє мережу різноманітних ресурсів – канальної ємності, обчислювальної потужності, енергетичних ресурсів та ін. До сенсорних вузлів мережі зловмисник розсилає Hello пакети. Отримавши Hello пакети, вузли розглядають скомпрометований вузол як свого сусіда, і при подальшій передачі даних, будуть використовувати отриману з Hello пакетів адресу.

Далі представлено перелік основних рекомендацій для забезпечення безпеки в IoT системі:[12]

Найпростіша, і разом с цим достатньо ефективна дія, яку може виконати користувач - захист паролів. У всіх підключених пристроїв паролі «за замовчуванням» мають бути замінені. У випадку, коли пароль неможливо замінити, даний пристрій краще не впроваджувати в систему Інтернету речей. Для кожного пристрою необхідно надати мінімальні для їх справного функціонування привілеї.

Перед підключенням необхідно перевірити кожен пристрій, та виконати перевірку локальних та хмарних сервісів.

Якщо є можливість, то для IoT пристроїв необхідно створити окрему мережу, захистившись фаєрволом. Створення окремої мережі допоможе виконати ізоляцію небезпечних пристроїв від основних мереж і ресурсів.

Необхідно намагатись не використовувати пристрої з фізичною компрометацією. До таких пристроїв можна віднести пристрої з апаратною кнопкою повернення до фабричних налаштувань, доступними роз'ємами або заданими за замовчуванням паролями.

Краще не використовувати пристрої з функцією автоматичного підключення до відкритих мереж Wi-Fi, або позбавити їх такої можливості.

Не маючи можливості заблокувати весь вхідний трафік IoT пристроїв, необхідно перевірити пристрій на наявність відкритих портів, через які зловмисник може взяти пристрій під контроль.

Перевірити IoT пристрої на наявність обміну даними в зашифрованій формі, і якщо така можливість присутня, то використовувати її.

Не використовувати продукти, які вже не підтримуються виробником, або ті, чий захист вже неможливо забезпечити.

Висновки

Немає сумнівів, що концепція Інтернету речей буде стрімко розвиватися, що викличе швидке поширення новітніх технологій IoT. Парадигма мереж вплине на кожну сферу людського життя – від автоматизованих будинків до розумної охорони здоров'я та моніторингу середовища, інтегруючи інтелект в усі об'єкти навколишнього світу. Впровадження IoT вимагає великих зусиль і сучасних рішень по ліквідації загроз безпеці і приватності.

У статті розглянуті деякі варіанти загроз безпеці IoT-систем. Аналіз досліджень по даній темі показав, що в системах до цього часу не враховувалися питання забезпечення конфіденційності і безпеки користувача. На основі аналізу технологій найбільш поширених атак було складено перелік рекомендацій для забезпечення цілісності мережі з IoT пристроїв.

Список використаної літератури

1. Информационная безопасность интернета вещей (Internet of Things): TADVISER. URL: https://goo.su/2l3u (дата звернення: 18.09.2020).
2. Good Practices for Security of Internet of Things in the context of Smart Manufacturing: enisa. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y--IHVYvLuFhGuvi6o (дата звернення: 11.09.2020).
3. Проблемы и задачи реализации концепции Интернета Вещей: habr. URL: https://habr.com/ru/post/479890/ (дата звернення: 11.09.2020).
4. What is the IoT? Everything you need to know about the Internet of Things right now: zdnet. URL: https://www.zdnet.com/article/how-5g-can-help-unlock-iots-potential/ / (дата звернення: 12.09.2020).
5. internet of things (IoT): IoTAgenda. URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT / (дата звернення: 12.09.2020).
6. What is IoT? The internet of things explained: NETWORKWORLD. URL: https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html (дата звернення: 16.09.2020).
7. Internet of Things (IoT) security: 9 ways you can help protect yourself: Norton. URL: https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html (дата звернення: 20.09.2020).
8. Internet of Things (IOT) security: imperva. URL: https://www.imperva.com/learn/application-security/iot-internet-of-things-security/ (дата звернення: 21.09.2020).
9. Cybersecurity and the Internet of Things: security. URL https://www.securitymagazine.com/articles/90793-cybersecurity-and-the-internet-of-things (дата звернення: 23.09.2020).
10. Cyber risk in an Internet of Things world: deloitte. URL https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html (дата звернення: 25.09.2020).
11. Top 10 Biggest IoT Security Issues: intellectsoft. URL https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (дата звернення: 27.09.2020).
12. What is IoT Security (Internet of Things)? - Tools & Technologies: hackr. URL https://hackr.io/blog/what-is-iot-security-technologies (дата звернення: 28.09.2020).
13. Security in the Internet of Things: mckinsey. URL https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things# (дата звернення: 28.09.2020).
14. Іванчук О.В., Завгородній В.В., Козел В.М., Дроздова Є.А. Аналіз протоколів обміну даними для керування системами інтернету речей. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2020. № 31. С. 99-104.

References

1. Informacionnaya bezopasnost' interneta veshchej (Internet of Things) [Information security of the internet of things]: TADVISER. Available at: https://goo.su/2l3u (accessed: 18.09.2020).

2. Good Practices for Security of Internet of Things in the context of Smart Manufacturing: enisa. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y--IHVYvLuFhGuvi6o (accessed: 11.09.2020).

3. Problemy i zadachi realizacii koncepcii Interneta Veshchej [Problems and tasks of implementing the concept of the Internet of Things]: habr. Available at: https://habr.com/ru/post/479890/ (accessed: 11.09.2020).

4. What is the IoT? Everything you need to know about the Internet of Things right now: zdnet. Available Available at: https://www.zdnet.com/article/how-5g-can-help-unlock-iots-potential/ / (accessed: 12.09.2020).

5. internet of things (IoT): IoTAgenda. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT / (accessed: 12.09.2020).

6. What is IoT? The internet of things explained: NETWORKWORLD. Available at: https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html (accessed: 16.09.2020).

7. Internet of Things (IoT) security: 9 ways you can help protect yourself: Norton. Available at: https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html (accessed: 20.09.2020).

8. Internet of Things (IOT) security: imperva. Available at: https://www.imperva.com/learn/application-security/iot-internet-of-things-security/ (accessed: 21.09.2020).

9. Cybersecurity and the Internet of Things: security. Available at: https://www.securitymagazine.com/articles/90793-cybersecurity-and-the-internet-of-things (accessed: 23.09.2020).

10. Cyber risk in an Internet of Things world: deloitte. Available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html (accessed: 25.09.2020).

11. Top 10 Biggest IoT Security Issues: intellectsoft. Available at: https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (accessed: 27.09.2020).

12. What is IoT Security (Internet of Things)? - Tools & Technologies: hackr. Available at: https://hackr.io/blog/what-is-iot-security-technologies (accessed: 28.09.2020).

13. Security in the Internet of Things: mckinsey. Available at: https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things# (accessed: 28.09.2020).

14. Ivanchuk O.V., Zavgorodii V.V., Kozel V.M., Drozdova Ye.A. Analiz protokoliv obminu danymy dlia keruvannia systemamy internetu rechei [Analysis of data exchange protocols for managing Internet of Things systems]. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Tekhnichni nauky - Scientific notes of TNU named after VI Vernadsky. Series: Technical Sciences, 2020, no.2(31). pp. 99-104. doi: 10.32838/2663-5941/2020.2-1/15 .