УДК 004.49, 004.415.2

ИССЛЕДОВАНИЕ ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ «ИНТЕРНЕТА ВЕЩЕЙ»

Федоров Николай Андреевич[1], Сычёв Пётр Павлович[2]

[1]Студент;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, д. 19;
e-mail: fedorov.nikolay.1110@gmail.com.

[2]Доцент;
Государственный университет «Дубна»;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, д. 19;
e-mail: sychov.p.p@uni-dubna.ru.

Системы «Интернета вещей» имеют негативную репутацию как устройства с большим количеством проблем в безопасности. Несмотря на растущую популярность и применимость в широком наборе сфер, данный аспект «Интернета вещей» ограничивает дальнейшее повсеместное распространение данных решений.

Целью данной работы является рассмотрение основных проблем безопасности систем «Интернета вещей», в результате чего будет разработан прототип программного обеспечения для обнаружения и идентификации проблемных мест в безопасности сканируемой системы «Интернета вещей».

Для формирования основных требований были рассмотрены существующие на рынке средства сканирования устройств на наличие уязвимостей, из которых были выявлены общие преимущества и недостатки. В результате проектирования были созданы общая архитектура системы и графический дизайн приложения.

Результатом работы является программное решение для сканирования систем «Интернета вещей» для выявления уязвимостей с возможностью получения отчета с распределением уязвимостей по уровню угроз, описанием уязвимостей и возможным способом исправления. Данное решение с открытым исходным кодом предоставляет альтернативу уже имеющимся на рынке, где зачастую для обнаружения уязвимостей используются несколько решений для минимизации риска пропуска уязвимости.

Ключевые слова: Интернет вещей, встраиваемые системы, кибербезопасность, сканирование уязвимостей.

Для цитирования:

Федоров Н. А., Сычёв П. П. Исследование вопросов информационной безопасности систем «Интернета вещей» // Системный анализ в науке и образовании: сетевое научное издание. 2023. № 2. С. 27-35. EDN: FGJBSV. URL : https://sanse.ru/index.php/sanse/article/view/576.

A STUDY OF SECURITY ISSUES OF INTERNET OF THINGS (IOT) SYSTEMS

Fedorov Nikolay A.[1], Sychov Petr P.[2]

[1]Student;
Dubna State University;
19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: fedorov.nikolay.1110@gmail.com.

[2]Associate professor;
Dubna State University;
19 Universitetskaya Str., Dubna, Moscow region, 141980, Russia;
e-mail: sychov.p.p@uni-dubna.ru.

Internet of Things (IoT) systems have a negative reputation as devices with a high amount of security vulnerabilities. Despite rapid growth in popularity and adoption in a broad range of industries, this aspect of the IoT restricts continuous adoption of the IoT solutions.

The goal of this works is the research of the main security problems of IoT systems that would result in the development of an application for detection and identification in IoT systems.

In order to form a list of requirements several vulnerability-scanning tools were analyzed from which general advantages and disadvantages were identified. General system architecture and GUI of the developed app were also designed.

The result of this work is an application for vulnerability scanning of IoT systems that provides the ability to receive reports on detected vulnerabilities, their risk level, description and a possible fix. This open-source solution provides an alternative for the existing tools that are usually used in combinations with each other in order to minimize the risk of a vulnerability detection error.

Keywords: Internet of Things, IoT, embedded systems, cybersecurity, vulnerability scanning.

For citation:
Fedorov N. A., Sychov P. P. A study of security issues of internet of things (IoT) systems. *System analysis in science and education*, 2023;(2):27-35 (in Russ). EDN: FGJBSV. Available from: https://sanse.ru/index.php/sanse/article/view/576.

Введение

«Интернет вещей» – концепция, возникшая в 1999 году, и активно развивающаяся по сей день, суть которой заключается во взаимодействии «вещей» (физических и виртуальных устройств) между собой без необходимости непосредственного участия человека в данном процессе [1, 2]. Так прогнозируемый доход от устройств и систем «Интернета вещей» к 2030 составляет более 600 млрд. долларов США [3].

Несмотря на свою популярность, еще большему распространению решений «Интернета вещей» препятствуют многочисленные проблемы в безопасности данных устройств. Так, среди более 50% компаний, опрошенных в 2022 году лабораторией Касперского, трудности имплементаций устройств «Интернета вещей» связаны непосредственно с опасениями в безопасности данных решений [4].

Данные опасения обоснованы ростом числа обнаруженных уязвимостей устройств «Интернета вещей» - так за 2021 год было обнаружено 797 уязвимостей, из которых 65% были квалифицированы как критические по метрике *CVSS* (*Common Vulnerability Scoring System*) – а также распространением вредоносных программам, нацеленные на заражение устройств «Интернета вещей» [5]. Наиболее популярным типом подобных программ является ботнет – вредоносная программа, объединяющая зараженные устройства в единую сеть, для проведения атак [6].

В данной работе будут рассмотрены основные типы угроз и уязвимостей систем «Интернета вещей». В результате был также разработан прототип монитора безопасности – программного продукта, позволяющего провести сканирование устройств «Интернета вещей» на наличие уязвимостей, а также предоставления информации и общей статистки уязвимостей в системе.

Основные типы угроз и уязвимостей систем «Интернета вещей»

Векторы потенциальных атак на устройства «Интернета вещей» можно разделить на три группы, в зависимости от цели атаки: оборудование, программное обеспечение и передаваемые данные [7]. По причине того, что задача выявления уязвимостей во время передачи данных является отдельной задачей, заключающейся в анализе траффика, в данной работе было уделено внимание первым двум группам.

Технические решения

Специфика оборудования

Для лучшего понимания вредоносных программ для «Интернета вещей» следует рассмотреть основные ограничения систем, имеющие следующие характеристики [8]:

- *Версии Linux для встраиваемых систем (embedded Linux) является наиболее популярной ОС с различными имплементациями/версиями языка С вместе с ядром Linux, работающим с двоичным интерфейсом приложений (Application binary interface – ABI) (версии ядра 2.4-4.3).*
- *низкий объем операционной памяти.*
- *низкий объем постоянной памяти (которая используются в основном для ОС и встроенных программ).*
- *архитектуры, отличные от x86: ARM, MIPS.*
- *поддержка формата ELF (Executable and Linkable Format) исполняемых файлов.*
- *в редких случаях имеется наличие интерфейса пользователя.*
- *устройство встроено в сеть (в большинстве случаев подключено к сети Интернет).*

Маршрутизаторы

Маршрутизатор-шлюз объединяет устройства в одну сеть, по этой причине, данный тип устройства часто является одной из первых целей для атаки. Так порядка 500 тысяч маршрутизаторов и сетевых хранилищ были атакованы ботнетом *VPNFilter* в 2018 году [9].

Маршрутизаторы, как и другие устройства «Интернета вещей», подвержены уязвимостям: так в 2021 году было обнаружено более 500 уязвимостей, 87 из которых были критическими [10].

Для лучшего понимания ситуации на рынке маршрутизаторов институтом Фраунгофера было проведено исследование на основе данных за 31 марта 2022 года, в ходе которого были рассмотрены 122 модели маршрутизаторов [11].

Было получено, что 109 из 122 устройств используют в качестве ОС дистрибутивы *Linux* с устаревшей версией ядра (2.6-4.). Порядка 70% всех устройств имели версию ядра приближающейся или уже находящейся в конце срока службы [11].

Другим проблемным местом было актуальность обновлений системы: из 122 маршрутизаторов только 95 получили обновления за последние 365 дней, тем самым, 27 устройств не получали обновления больше года [11].

Отдельного внимания заслуживает имплементация механизмов защиты в маршрутизаторах: рассмотренные методы включали в себя контроль исполняемых файлов (*Binary Hardening*), неисполняемый бит (*Non-Executable Bit*), метод исполнения, независимо от положения (*Position-Independent Executable*), метод чтения без записи при изменении позиции (*RELocation Read-Only*) и *Stack Canaries*. Было получено, что в среднем относительно малый процент всего программного обеспечения устройств содержит данные методы, однако, результаты сильно разнятся от производителя: некоторые практически не имплементируют данные механизмы обеспечения безопасности, в то время как более 50% всего программного обеспечения других производителей содержит данные методы [11].

Использование жестко закодированных паролей является небезопасной практикой. Однако было обнаружено, что общее число паролей на устройство, где они имеются, ранжируется в пределах от 1 до 4, однако, стоит отметить, что большая часть производителей избегает использования жесткого кодирования паролей. Для производителя, наиболее активно использующего жестко закодированные пароли, около половины оказались скомпрометированы, и находятся в открытом доступе [11].

Таким образом, была получена следующая картина рынка маршрутизаторов: общая статистика мало отличается от статистики по всему рынку «Интернета вещей» и многие устройства имеют те же или схожие проблемы, а именно:

- Использование устаревших версий ОС.
- Долгий период между обновлениями устройств.
- Отсутствие достаточных повсеместных механизмов защиты во время исполнения программ.
- Использование жестко кодированных паролей.

Linux

По причине того, что порядка 80% всех персональных компьютеров используют в качестве ОС *Windows*, долгое время сообщество кибербезопасности не обращало внимания на вредоносные программы для дистрибутивов *Linux* [12, 13].

Рост популярности решений «Интернета вещей», которые зачастую используют в качестве ОС *Linux,* а также их многочисленные проблемы в безопасности, привлекли внимание авторов вредоносных программ. Однако только к концу 2014 года *VirusTotal* признал их как растущую угрозу [12, 14]. Со стороны академических исследований реакция на данную проблему была еще медленнее и до сих пор число исследований на данную тему крайне низкое [12].

Для определения состава угроз, с которыми может столкнуться подключенное к сети Интернет устройство «Интернета вещей» исследователи из *Symantec Research Labs* провели серию экспериментов для изучения аспектов атак на данные системы. Для этого были установлены т.н. ханипоты (*honey pots*), которые имитировали разный функционал «Интернета вещей» (например, маршрутизатор *Netgear*, *IP*-камера *Brickcom* и др.) [6].

После 6 месяцев работы было получено, что наиболее популярным механизмом проникновения является сервис *HTTP*, однако по числу попыток подключений его во много раз превзошел *Telnet*. За данный период на зараженные устройства было загружено 3385 вредоносных файлов, 2401 из которых представляют собой ботнеты, которые будут рассмотрены в следующем разделе. Было также получено, что вредоносные программы зачастую используют порты *Telnet* и *UDP* для заражения устройств [6].

Также стоит отметить, что порядка 1% всех вредоносных программ имплементирует различные методы уклонения от обнаружения, которые включают в себя обнаружение изолированной среды, отмена включения режима отладки и др.

Ботнеты

Ботнет – (образовано от слов *robot* (робот) и *network* (сеть)) – это специальная вредоносная троянские программа, используемая киберпреступниками, чтобы обойти систему защиты компьютеров, получить контроль над ними и объединить их в единую сеть, которой можно управлять удаленно [15, 16].

К особенностям данных вредоносных программ можно отнести то, что большинство из них написано на языке *C* [17]. Исходный код ботов компилируется для разных архитектур, использующих *Linux*. Ботнеты для «Интернета вещей» в большинстве состоят из двух базовых и четырех дополнительных компонентов [8]:

- Боты/зараженные устройства «Интернета вещей», проводящие *DDoS*-атаки.
- Командные серверы (*Command-and-control servers* (*C*2s/*C*&*C*)), которые используются для управления ботами.
- Сканнеры, производящие поиск уязвимых устройств.
- Сервер, принимающий результаты сканирования с ботов или внешнего сканнера.
- Загрузчики получают доступ к уязвимым устройствам и посылают команду загрузки вредоносной программы.
- Сервер, хранящий вредоносную программу, которую загружают зараженные устройства.

Общие рекомендации для повышения безопасности

С учетом разносторонности угроз, а также самого состава систем «Интернета вещей», затруднительно составить общий список обязательных процедур, позволяющих полностью защитить систему от атак. Однако, общие рекомендации, позволяющие ограничить некоторые векторы атак, включают в себя [8]:

- Изменение пароля по умолчанию на более надежный.
- Следует всегда обновлять устройство при наличии нового обновления безопасности, предоставленного производителем.

- Неиспользуемые порты и сервисы должны быть отключены.
- Следует изолировать устройства «Интернета вещей» в своей собственной защищенной сети с помощью файрволлов или других способов сегментации сети.
- Следует приобретать устройства «Интернета вещей» у производителей с хорошей репутацией безопасности производимых устройств или с хорошей поддержкой устройств обновлениями безопасности.
- Следует периодически проверять файл журнала файрволла на наличие различного рода аномалий или подозрительного трафика. Особое внимание стоит уделять на трафик на портах 2323 (*Telnet*) и 23/*TCP* (*Telnet*).

В случае атаки на устройство «Интернета вещей», шаги по минимизации последствий включают в себя [8]:

- Отключение устройства от сети Интернет.
- Перезагрузка устройства – большая часть вредоносных программ для «Интернета вещей» располагается в оперативной памяти устройства, и перезагрузка устройства очистит его от вредоносной программы.
- Изменение пароля по умолчанию на более надежный во избежание повторного заражения.
- По возможности обновление ПО устройства. Многие производители выпускают обновления безопасности в случае крупных атак.

Несмотря на то, что обновления безопасности ПО устройства устраняют большинство проблем, большая часть пользователей испытывает трудности с обновлением устройств «Интернета вещей». Больше половины (55%) проблем связана с опасением, что обновление устройства затронет работоспособность всей системы. Также 39% пользователей использует устаревшие устройства, для которых недоступны обновления безопасности [4].

Разработка монитора безопасности

В ходе рассмотрения вопросов безопасности устройств «Интернета вещей» было принято решение по разработке прототипа программного продукта, позволяющего про□вести анализ системы «Интернета вещей» на наличие известных уязвимостей. Среди решений, предоставляющих возможность защиты от атак, направленных на компрометацию сетей, выделяют три обязательных компонента: предотвращение, обнаружение, минимизация последствий [18].

Разрабатываемый программный продукт будет представлять собой монитор безопасности, предоставляя пользователю информацию о системе и о проблемных местах. Таким образом, данный продукт можно отнести к первому компоненту систем защиты, а именно как компонент, нацеленный на предотвращение атак посредством информирования пользователя о возможных векторах атак.

Обзор существующих решений

Для составления списка требований к разрабатываемому монитору безопасности были рассмотрены следующие имеющиеся на рынке решения:

- *Nessus*[1].
- *OpenVAS*[2].
- *Metasploit Project*[3].

Как основные преимущества были выделены возможность проведения сканирования портов, составления отчетов и диаграмм, а также открытость кода (в случае *OpenVAS* и *Metasploit Project*).

[1] https://www.tenable.com/products/nessus
[2] https://www.openvas.org/
[3] https://www.metasploit.com/

Общие недостатки составили ограниченность бесплатных версий, недоступность продуктов в РФ и консольные интерфейсы.

Таким образом, в результате рассмотрения существующих на рынке решений, были выделены следующие требования, которые будут учтены при разработке прототипа монитора безопасности:

- Открытый исходный код.
- Выбор типа сканирования.
- Составление отчетов.
- Визуальное представление информации.
- Предоставление описаний уязвимостей.

Библиотеки уязвимостей и механизмы сканирования

В качестве стандарта наименований уязвимостей в данной работе был выбран единый формат *CVE – Common Vulnerabilities and Exposures*[4]. Для количественных оценок уязвимостей использовался открытый стандарт *CVSS – Common Vulnerability Scoring System*[5].

Список рассмотренных библиотек, использующих стандарт *CVE*, включает в себя:

- *Mend Vulnerability Database*[6] – данная библиотека предоставляет наиболее полную информацию по сравнению с другими библиотеками, однако, долгое время загрузки страницы в виду большого числа элементов на странице, препятствует использование данной библиотеки как основной в виду отправки большого числа запросов при формировании отчета.
- *NIST*[7] – данная библиотека также предоставляет подробную информацию об уязвимостях, в том числе оценку угроз в разных версиях формата *CVSS* со ссылкой на источник.
- *CVE.org*[8] – данная библиотека предоставляет лишь общее описание уязвимости, однако, она также предоставляет загрузку списка известных уязвимостей в файл *CSV*[9], что будет использоваться в работе в дальнейшем.

Таким образом, было принято решение об использовании различных библиотек для различных задач в силу преимуществ и недостатков каждой из библиотек:

- Для быстрого получения оценки угрозы *CVSS* будет использоваться библиотека *NIST*.
- Для получения подробной информации о конкретной уязвимости будет использоваться библиотека *Mend*.
- Файл со списком *CVE* будет использоваться во время сканирования системы.

В качестве сканеров уязвимостей были выбраны *Nmap*[10] и *Shodan*[11]. *Nmap* (*Network mapper*) представляет собой инструмент, предназначенный для настраиваемого сканирования *IP*-сетей. Обнаружение устройств, операционных систем, сервисов/служб в компьютерной сети происходит посредством отправки пакетов и анализа ответов.

Nmap также обладает поддержкой скриптов, предназначенных для обнаружения уязвимостей. Список скриптов, используемых в данной работе, включает в себя: *vuln, Vulscan, Vulners* [19, 20]. Стоит отметить, что *Vulscan* обладает поддержкой внешних БД уязвимостей, повышающее его эффективность, что будет использоваться в данной работе в виде использования файла БД *CVE.org* [21].

По своей сути и функционалу *Shodan* сильно отличается от *Nmap*: *Shodan* иногда описывают как поисковую систему метаданных, которые сервер отправляет клиенту. Это может быть информация о

[4] https://cve.mitre.org/cve/
[5] https://www.first.org/cvss/
[6] https://www.mend.io/vulnerability-database/
[7] https://nvd.nist.gov/
[8] https://www.cve.org/
[9] https://www.cve.org/Downloads
[10] https://nmap.org/
[11] https://www.shodan.io/

программном обеспечении сервера, какие опции поддерживает сервис, сообщение о приветствии или что угодно, что клиент получает при взаимодействии с сервером [22]. Так как *Shodan* периодически проводит сканирование устройств, подключенных к сети Интернет, в случае с системами «Интернета вещей» недавно подключенные устройства могут не оказаться в базе данных *Shodan*. Проведение сканирования конкретного устройства является платной услугой, что затрудняет использования данного инструмента в проекте монитора безопасности.

Несмотря на крайне ограниченную бесплатную версию продукта, *Shodan* представляет собой мощный инструмент для получения информации об устройствах «Интернета вещей», по этой причине интеграция данного механизма сканирования не отбрасывается, а пользователю будет дана возможность ввести (при наличии) свой ключ *API* для использования данного инструмента как альтернативу используемого по умолчанию *Nmap*.

Программная реализация

Используемые инструменты

По причине того, что *Python* 3 является более популярной версией языка и поддерживается как *API Shodan*[12], так и *API Nmap*[13], данный язык был выбран для создания монитора безопасности [23].

В качестве библиотеки для создания графического интерфейса приложения была выбрана мультиплатформенная библиотека *Qt*[14], привязка к *Python* которой осуществлялась через модуль *Pyside* версии 6[15]. Несмотря на то, что мультиплатформенность не является требованием в данном проекте, комбинация *Python+Qt* позволит существенно упростить портирование продукта на другие платформы в будущем. Версия *Qt* 6 поддерживается широким набором платформ, что делает данную библиотеку популярным выбором при создании приложения [24].

Для отправления *HTTP* запросов была использована библиотека *requests*[16].

Для работы с таблицами, которыми являются результаты сканирования сети, была использована библиотека *pandas*[17].

Последняя версия *PySide6* поддерживает версии *Python* 3.7+, по этой причине для данного проекта была выбрана последняя версия языка на момент выполнения работы – *Python* 3.11.2.

Функционал приложения

Разработанный прототип монитора безопасности представляет собой инструмент для сканирования систем устройств «Интернета вещей» небольших размеров (частная квартира/дом или в пределах небольшого офиса); тестирование работы на крупных сетях не проводилось.

Монитор безопасности состоит из 3 главных окон:

- Главный экран предоставляет основную статистику сканированной системы в виде круговых диаграмм: уязвимости и их оценка уровня угрозы *CVSS*, операционные системы, производители, порты и сервисы.

- Окно списка устройств предоставляет информацию о каждом устройстве: статистика обнаруженных уязвимостей, ОС, производитель, порты и сервисы. Посредством нажатия на область диаграммы уязвимостей пользователь может просмотреть список уязвимостей выбранной группы оценки *CVSS* («низкий», «средний», «высокий» и «критический» уровни

[12] https://pypi.org/project/shodan/
[13] https://pypi.org/project/python-nmap/
[14] https://www.qt.io/
[15] https://pypi.org/project/PySide6/
[16] https://pypi.org/project/requests/
[17] https://pypi.org/project/pandas/

угрозы) с описанием, конкретной численной оценкой, ссылками на источники, а также на возможное исправление при его наличии.

- Страница нового сканирования предоставляет пользователю два главных варианта сканирования: поиск устройств и поиск уязвимостей, а также другие настройки каждого типа сканирования: выбор сканера, скрипта, сканируемые адреса и др.

Разработанное приложение находится в открытом доступе, что позволяет любому пользователю эксплуатировать данный программный продукт, а также свободно просматривать и модифицировать программный код[18].

Заключение

Таким образом, в ходе работы был изучен перечень основных угроз устройствам «Интернета вещей» и общее состояние рынка. Также был разработан программный продукт с открытым исходным кодом для проведения сканирования систем «Интернета вещей», позволяющий получить информацию об устройствах в системе, а также об обнаруженных уязвимостях, как текстовом виде, так и в виде диаграмм. Разработанный прототип монитора безопасности предоставляет указанный функционал.

Возможные перспективы развития продукта включают в себя переход на клиент-серверную архитектуру для снижения нагрузки на сторону пользователя, добавление поддержки *IPv*6, а также имплементацию алгоритмов машинного обучения.

Список источников

1. Gillis A. S. What is the internet of things (IoT)? // TechTarget : [сайт]. – TechTarget, 2005–2023. – Дата публикации: 04.03.2022. – URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.
2. International Telecommunication Union. ITU-T Y.4000/Y.2060 // International Telecommunication Union : [сайт]. – International Telecommunication Union, 2023 – Дата публикации: 15.06.2012. – URL: http://handle.itu.int/11.1002/1000/11559.
3. Vailshery L. S. Internet of Things (IoT) total annual revenue worldwide from 2019 to 2030 // statista : [сайт]. – statista, 2007-2023. – Дата публикации: 23.11.2022. – URL: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/.
4. Kaspersky. Pushing the limits: How to address specific cybersecurity demands and protect IoT // Kaspersky : [сайт]. – AO Kaspersky Lab, 2023. – Дата публикации: 08.02.2022. – URL: https://www.kaspersky.com/blog/iot-report-2022/.
5. Claroty Team82. BIANNUAL ICS RISK & VULNERABILITY REPORT: 2H 2021 // Claroty : [сайт] – Claroty Ltd., 2023. – Дата публикации: 09.12.2022. – URL: https://claroty.com/2h21-biannual-report/.
6. Vervier P.-A., Shen Y. Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape // Research in Attacks, Intrusions, and Defenses – Cham: Springer, 2018. – Pp. 556-576. – DOI: http://dx.doi.org/10.1007/978-3-030-00470-5_26.
7. A survey on security in internet of things with a focus on the impact of emerging technologies / P. Williams, I. K. Dutta, H. Daoud , M. Bayoumi // Internet of Things; Engineering Cyber Physical Human Systems. – 2022. – Vol. 19. – N. 100564. – DOI: https://doi.org/10.1016/j.iot.2022.100564.
8. Angrishi K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets // arXiv.org : [open archive]. – 2017. – 17 p., 15 fig. – arXiv:1702.03681v1 [cs.NI]. – URL: https://arxiv.org/abs/1702.03681. – Submitted on 13 Feb 2017.

[18] https://github.com/Borpa/iot_monitor_prototype

9. Unwala I., Taqvi Z., Lu J. IoT Security : ZWave and Thread // 2018 IEEE Green Technologies Conference. – 2018. – Pp.176-182. – DOI: https://doi.org/10.1109/GreenTech.2018.00040.

10. Kaspersky. 87 critical vulnerabilities discovered in routers in 2021 // Kaspersky : [сайт]. – AO Kaspersky Lab, 2023. – Дата публикации: 08.06.2022. – URL: https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

11. Dorp J. v. , R. Helmke Home Router Security Report 2022 / FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE. – 2022. – Date of publication: 11.2022. – URL: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/2022-11-28_HRSR_2022.pdf.

12. Understanding Linux Malware / E. Cozzi, M. Graziano, Y. Fratantonio, D. Balzarotti // 2018 IEEE Symposium on Security and Privacy. – 2018. – Pp. 161-175. – DOI: https://doi.org/10.1109/SP.2018.00054

13. StatCounter, Desktop Operating System Market Share Worldwide. // StatCounter : [сайт]. – StatCounter, 2023. – Дата публикации: 24.04.2023. – URL: http://gs.statcounter.com/os-market-share/desktop/worldwide.

14. Tung L. Google's VirusTotal puts Linux malware under the spotlight. // Zdnet : [сайт]. – Zdnet, 2023. – Дата публикации: 12.11.2014. – URL: http://www.zdnet.com/article/googles-virustotal-puts-linux-malware-under-the-spotlight/.

15. Kaspersky. Что такое ботнет? // Kaspersky : [сайт] – AO Kaspersky Lab, 2023. – Дата публикации: 17.10.2017. – URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks.

16. Trend Micro Incorporated. Botnet // Trend Micro Incorporated : [сайт] – Trend Micro Incorporated, 2023. – Дата публикации: 10.09.2020. – URL: https://www.trendmicro.com/vinfo/us/security/definition/botnet.

17. Nguyen H.-T., Ngo Q.-D., Le V.-H. A novel graph-based approach for IoT botnet detection // International Journal of Information Security 19 – 2020. – Vol. 19. – Pp. 567-577. – DOI: https://doi.org/10.1007/s10207-019-00475-6.

18. Butun, I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, Attacks and Counter measures // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22. – N. 1. – Pp.616-644. – DOI: https://doi.org/10.1109/COMST.2019.2953364.

19. Lyon G. Chapter 9. Nmap Scripting Engine // Nmap : [сайт]. – Nmap, 2023. –URL: https://nmap.org/book/nse.html#nse-intro.

20. Lyon G. Scripts // Nmap : [сайт]. – Nmap, 2023. – URL: https://nmap.org/nsedoc/categories/vuln.html.

21. Vulscan : [project storage] // GitHub : [web platform]. – GitHub, Inc., 2023. – URL: https://github.com/scipag/vulscan (accessed date: 12.04.2023).

22. Shodan. HTTP Strict-Transport-Security // Shodan : [сайт]. – Shodan, 2023 – URL: https://www.shodan.io/search?query=HTTP+Strict-Transport-Security.

23. Vailshery L. S. Python version ranking from 2017 to 2021, by usage // statista : [сайт] – statista, 2007-2023. – Дата публикации: 20.10.2022. – URL: https://www.statista.com/statistics/1338383/most-used-python-version/.

24. The Qt Company. Supported Platforms // The Qt Company : [сайт]. – The Qt Company, 2023 – URL: https://doc.qt.io/qt-6/supported-platforms.html.