УДК 378.147:004.9

АНАЛИЗ УЯЗВИМОСТЕЙ БЕСПРОВОДНЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

Саенко Максим Андреевич[1],
e-mail: xerokan@mail.ru,

Мельников Денис Александрович[1],
e-mail: dmbox2019@gmail.com,

Данилов Михаил Алексеевич[1],
e-mail: mike_m89@mail.ru,
[1]*Российский технологический университет (РТУ МИРЭА), г. Москва, Россия*

В статье исследуется проблема информационной безопасности смарт-систем. Уровень цифровизации смарт-систем непрерывно повышается и соответственно изменяются факторы уязвимостей и угрозы. Исходя из этого обстоятельства, процесс защиты информации необходимо непрерывно совершенствовать. Целью работы является систематизация угроз и уязвимостей современных систем умных вещей, разработка рекомендаций по повышению уровня их информационной безопасности. Приводится систематика угроз для беспроводных технологий Wi-Fi и Bluetooth. Рассматривается пример уязвимостей смарт-системы при использовании технологии Wi-Fi. Приводится типологический ряд технологии Wi-Fi, который выстроен по степени роста защищенности передаваемой информации. Показаны угрозы и уязвимости технологии при использовании конкретных протоколов защиты сети Wi-Fi. На примере показано, что информационные угрозы появляются не только из-за уязвимостей беспроводной технологии передачи информации, но из-за технологических особенностей применения данной технологии в других системах, включая «умные вещи». Проводится сравнение защищенности технологий Bluetooth и Wi-Fi, основанной на применении современного протокола WPA3. Разработаны рекомендации для передачи конфиденциальной информации по каналам Wi-Fi и Bluetooth.

Ключевые слова: беспроводные сети, Bluetooth, Wi-Fi, передача информации, информационная безопасность, уязвимости

THE ANALYSIS OF VULNERABILITY OF WIRELESS INFORMATION TRANSMISSION CHANNELS

Saenko M.A.[1],
e-mail: xerokan@mail.ru,

Melnikov D.A.[1],
e -mail: dmbox2019@gmail.com,

Danilov M.A.[1],
e-mail: mike_m89@mail.ru,
[1]*Russian Technological University (RTU MIREA), Moscow, Russia*

The article examines the problem of information security of smart systems. The level of digitalization of smart systems is continuously increasing and vulnerability factors and threats are changing accordingly. Therefore, the information protection process needs to be continuously improved. The purpose of the work is to systematize the threats and vulnerabilities of modern systems of smart things, to develop recommendations for improving their information security. The systematics of threats to Wi-Fi and Bluetooth wireless technologies is presented. An example of vulnerabilities of a smart system when using Wi-Fi technology is considered. The typological series of Wi-Fi technology is presented, which is created according to the degree of the transmitted information security growth. The threats and vulnerabilities of the technology when using specific Wi-Fi network protection

protocols are shown. The example shows that information threats appear not only because of the vulnerabilities of wireless information transmission technology, but also because of the technological features of the use of this technology in other systems, including "smart things". A comparison is made of the security of Bluetooth and Wi-Fi technologies based on the use of the modern WPA3 protocol. Recommendations have been developed for the transmission of confidential information via Wi-Fi and Bluetooth channels.

Keywords: wireless networks, Bluetooth, Wi-Fi, information transmission, information security, vulnerabilities

DOI 10.21777/2500-2112-2023-1-82-90

Введение

В настоящее время широко применяются системы «умных вещей» (далее – умные вещи), которые могут автоматически выполнять определённый набор заданных программ, имеют выход в интернет и позволяют автоматизировать самые разные процессы [1]. Проблемы безопасности таких интеллектуальных систем (смарт-систем) являются сдерживающим фактором их развития. Угрозы информационной безопасности смарт-систем проявляются через факторы уязвимости. В связи с интенсивным развитием данного направления следует отметить некую терминологическую нестыковку и нарушение терминологических отношений [2]. Однако эта ситуация устраняется по мере накопления опыта и обмена мнениями.

В сфере информационной безопасности смарт-систем выделяются такие факторы, как «Доступность», «Целостность» и «Конфиденциальность» [3]. Нарушение любого из них приводит к вредоносному воздействию на информационные и другие ресурсы системы. При этом на защиту «Доступности» мобилизуется треть всех усилий по обеспечению информационной безопасности, что необходимо учитывать при реализации защитных действий.

Уровень цифровизации умных вещей непрерывно повышается и соответственно изменяются факторы уязвимостей и угрозы. Исходя из этого обстоятельства, процесс защиты информации необходимо непрерывно совершенствовать на основе систематизации угроз и уязвимостей смарт-систем, чем обусловлена актуальность данной работы.

1. Анализ уязвимостей смарт-системы на примере умного замка

Рассмотрим безопасность умных устройств на примере умного дверного замка [4; 5]. Умный замок – электронный замок, который открывается и закрывается благодаря беспроводному прямому взаимодействию со смартфоном владельца. Это вариант 1. Вторая основная его функция – возможность открывать и закрывать его удаленно также со смартфона. На рисунке 1 показана общая архитектура систем интеллектуальных замков для варианта 1. Умный замок напрямую взаимодействует с пользователем при помощи приложения для смартфона с использованием технологии Bluetooth с низким энергопотреблением (BLE) [6; 7].

Приложение взаимодействует с серверами интеллектуальных замков в облаке через API-интерфейс (Application Programming Interface) по протоколу HTTPS (HyperText Transfer Protocol Secure). В этом случае работа интеллектуального замка зависит от подключения к мобильному устройству пользователя через интернет, которое ему необходимо для получения любых сообщений от сервера в облаке. На рисунке 1 мобильное приложение означает смартфон, который находится у владельца замка. Все три компонента (устройство умного замка, приложение для смартфона и сервер) взаимодействуют и «доверяют» друг другу, создавая систему, которая при этом имеет большое количество уязвимостей.

Технология Bluetooth подразумевает прямое взаимодействие устройств в одном помещении. В помещение может попасть гость, которому владелец дает ключ гостевого пользователя (гостиница). В этом случае гость попадает в список управления доступом смарт-замка. Смарт-замок открывается для тех, кто внесен в список доступа. Владелец помещения и смарт-замка после завершения посещения гостем может отправить сообщение в облачный сервис, которое отменяет ключ гостевого пользователя или меняет срок его действия. После того, как сервер получит сообщение владельца, он отправляет спе-

циальное сообщение смарт-замку для обновления его списка управления доступом. Однако, если человек, использовавший гостевой ключ, просто переводит свой смартфон в режим полета, смарт-замок не сможет использовать его смартфон в качестве ретранслятора для получения обновления состояния с сервера. В этом случае гостевой ключ по-прежнему может быть использован для получения доступа в помещение. Это пример уязвимости при использовании смартфона.

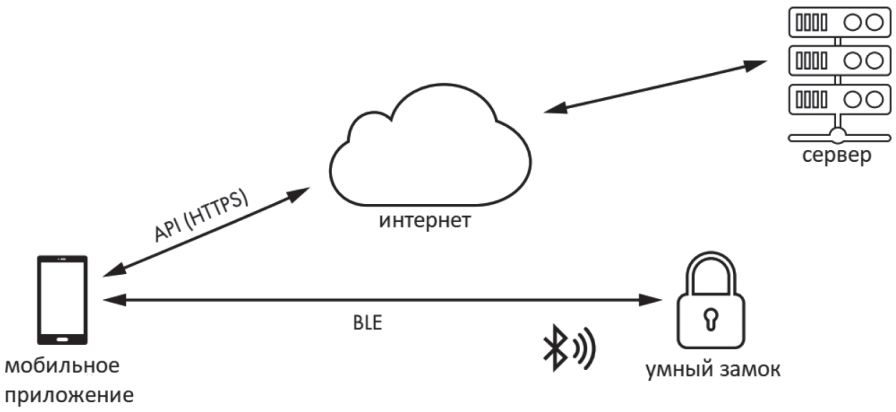

Рисунок 1 – Общая архитектура систем интеллектуальных замков на основе беспроводного прямого взаимодействия со смартфоном владельца

Простая атака сторонним лицом не позволит получить информацию с сервера, но может указать на типы уязвимостей подобных систем. Ограничения, связанные с использованием небольших, маломощных и недорогих встроенных устройств, только повышают уязвимость таких систем. Например, вместо ресурсоемкой криптографии с открытым ключом многие мобильные устройства обычно полагаются только на симметричные ключи для шифрования своих каналов связи. Эти криптографические ключи очень часто не уникальны и жестко запрограммированы в прошивке или оборудовании, что означает возможность для злоумышленника извлекать их, а затем повторно использовать на других таких же устройствах.

Общий вывод из рассмотренного примера состоит в том, что использование беспроводных технологий в других технологиях влечет появление новых уязвимостей, обусловленных не только внутренними уязвимостями беспроводной технологии, но технологическими особенностями стыковки беспроводной технологии с другими информационными системами, включая системы «умные вещи». Этот факт необходимо учитывать при комплексировании информационных систем беспроводными технологиями.

2. Анализ угроз в беспроводных сетях Wi-Fi

Беспроводная сеть Wi-Fi [8] имеет открытый доступ во многих местах общественного пользования. Стандарты сети не предусматривают шифрование передаваемых данных в открытых режимах. Поэтому все данные, передаваемые по открытому соединению, могут быть доступны третьим лицам при помощи специальных программ. Отсутствие шифрования – первая угроза таких сетей.

Многие технологии среднего радиуса действия, такие как Thread, Zigbee и Z-Wave, были разработаны для низкоскоростных приложений с максимальной скоростью 250 Кбит/с. Однако режим Wi-Fi был создан для высокоскоростной передачи данных, поэтому Wi-Fi имеет более высокое энергопотребление, чем другие технологии. В России адаптеры Wi-Fi с эквивалентной изотропно-излучаемой мощностью (EIRP – Equivalent Isotropically Radiated Power) превышающей 100 мВт, подлежат регистрации. Соединения Wi-Fi включают точку доступа, сетевое устройство, которое позволяет устройствам Wi-Fi подключаться к сети, и клиента, который может подключаться к точке доступа (рисунок 2).

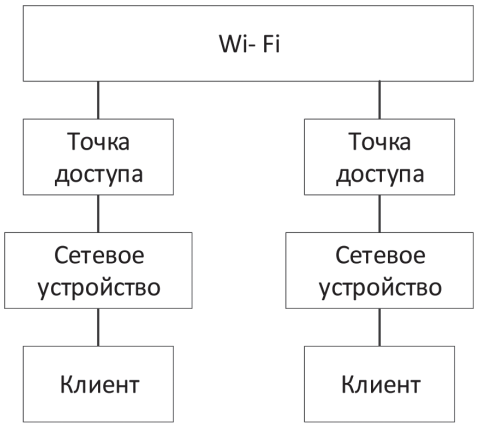

Рисунок 2 – Схема подключения к сети

В практике применяют термин «станция» (STA) для обозначения любого устройства, способного использовать протокол Wi-Fi. Сеть Wi-Fi может работать как в открытом, так и в защищенном режиме. В открытом или опасном режиме точка доступа не будет требовать аутентификации и примет любого клиента, который попытается подключиться.

В защищенном режиме перед подключением клиента к точке доступа необходимо выполнить дополнительную и обязательную процедуру аутентификации. Некоторые сети также могут выбрать режим скрытия сети, в этом случае сеть не будет транслировать свой идентификатор. Соединения Wi-Fi обмениваются данными с использованием набора протоколов, которые поддерживают различные виды модуляции сигналов и работают на разных частотах. Как правило, при оценке безопасности сети Wi-Fi рассматриваются атаки на точки доступа и сетевые устройства (рисунок 2). При тестировании на безопасность сетей Интернета вещей актуальны оба вида атак.

При настройке таргетинга (рекламный механизм, выделяющий целевую аудиторию) на устройства Интернета вещей используется беспроводная карта, поддерживающая режим AP monitor (способность выступать в роли точки доступа) и способная вводить пакеты данных. Режим монитора позволяет устройству отслеживать весь трафик, который оно получает из беспроводной сети. Возможности ввода пакетов позволяют карте подделывать пакеты так, чтобы они выглядели так, как будто они исходят из другого источника.

Беспроводные сети Wi-Fi делят на два типа – открытые и закрытые. Сети открытого типа не используют защиту для подключения к самому устройству или используют удалённую защиту доступа к сети в том случае, когда аутентификация пользователя осуществляется не на самом устройстве, а на удалённом сервере. Сети закрытого типа Wi-Fi обеспечивают шифрование пакетов данных в канале передачи информации с использованием следующих технологий защиты: WEP (Wired Equivalent Privacy [9]), WPA (Wi-Fi Protected Access [10]), WPA2, WPA3.

WEP шифрует трафик с использованием 64- или 128-битного ключа в шестнадцатеричном формате. Это статический ключ, весь трафик шифруется с помощью одного ключа. Стандарт шифрования WEP в настоящее время может быть легко взломан из-за слабой криптостойкости алгоритма. На взлом WEP-защиты тратятся минуты, поэтому технология считается устаревшей.

Новые устройства используют более защищенные технологии WPA и WPA2. WPA есть второе поколение ПРО. Протокол WPA использует динамически изменяющий 256-битный ключ, протокол аутентификации EAP (Extensible Authentication Protocol[1]), криптографическую проверку целостности пакетов (Message Integrity Check, MIC) и протокол целостности временного ключа (Temporal Key Integrity Protocol, TKIP [11]). В протоколе TKIP используется двухуровневая система векторов инициализации. Схема шифрования трафика WPA представлена на рисунке 3. При использовании динамического ключа база статистики для взлома не успевает набраться. Кроме того, WPA отличается от WEP тем, что шифрует данные каждого клиента по отдельности.

[1] *Aboba B., Simon D. and Eronen P.* “Extensible Authentication Protocol (EAP) Key Management Framework”, RFC 5247, 2008. – URL: https://www.rfc-editor.org/info/rfc5247 (дата обращения: 10.02.2023). – Текст: электронный.

Рисунок 3 – Схема шифрования трафика WPA

Основной недостаток технологии WPA заключается в том, что в этой технологии осуществляется проверка целостности фреймов с помощью системы MIC (Message Integrity Check). В случае получения ложного фрейма система его отбрасывает. Точка доступа блокирует все коммуникации через себя на 60 секунд, если обнаруживается атака на подбор ключа. Данную особенность используют злоумышленники, отсылая точке доступа ложные фреймы для блокирования работы сети.

WPA2 является в настоящее время относительно надёжной технологией защиты для сетей Wi-Fi. В WPA2 используется протокол CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – протокол блочного шифрования с имитовставкой (MAC) и режимом сцепления блоков и счётчика). Протокол основан на алгоритме расширенного стандарта шифрования AES (Advanced Encryption Standard), обеспечивающего проверку подлинности и целостности сообщения. Протокол CCMP является более надежным, чем используемый в WPA протокол TKIP. В WPA2 устранена уязвимость, связанная с хищением и подменой ключевого потока. Данную технологию можно взломать только с помощью брутфорса (метода угадывания пароля или ключа, используемого для шифрования). В этом случае для повышения уровня защиты рекомендуется частая смена ключа. Но в протоколе WPA2 отсутствуют встроенное шифрование и защита данных в публичных открытых сетях, что делает атаки методом подбора пароля серьезной угрозой.

WPA3 – третья версия протокола защищенного доступа Wi-Fi. В этом протоколе реализованы следующие новые функции:

1. Индивидуальное шифрование данных. Используется протокол DPP (Device Provisioning Protocol), позволяющий пользователям использовать теги NFC или QR-коды для подключения устройств к сети. Для повышения уровня безопасности используется 256-битное шифрование.

2. Применение протокола SAE (Simultaneous Authentication of Equals), который обеспечивает взаимную проверку аутентификации и подключения устройств.

3. Усиленная защита от атак методом подбора пароля. Протокол WPA3 защищает от подбора пароля в автономном режиме. Пользователю позволяется выполнить только одну попытку ввода пароля. Кроме того, устройство пользователя напрямую взаимодействует с устройством Wi-Fi и при каждой попытке ввода пароля требуется физическое присутствие.

В беспроводных сетях Wi-Fi (семейства стандартов IEEE 802.11) проблема безопасности решается путем совершенствования механизмов доступа, аутентификации и шифрования, создания специальных устройств для защиты этих сетей. В таблице 1 приведена систематика угроз Wi-Fi.

Таблица 1 – Систематика угроз Wi-Fi

Протокол	Уязвимость	Виды угроз
WEP открытый	Анализатор трафика, или сниффер	Обычные «прослушивание» сетевого интерфейса с хабами
		Подключение сниффера в разрыв канала
		Ответвление трафика и направление его копии на сниффер
		Анализ побочных электромагнитных излучений
		Атака на канальном или сетевом уровне и перенаправление трафика на сниффер с последующим возвращением трафика в надлежащий адрес
WEP закрытый	Низкая криптостойкость, взлом	Взлом 2 минуты
WPA	Блокировка коммутации при обнаружении ложного фрейма	Умышленная блокировка работы сети с помощью ложных фреймов
		Хищение и подмена ключевого потока
WPA2	Взлом	Взлом с помощью метода угадывания пароля или ключа, используемого для шифрования
WPA3	Атака с понижением рейтинга	Атака по побочному каналу на основе кеша
	Утечка побочного кеша	Атака по побочному каналу на основе синхронизации

В таблице 1 отмечается «сниффер». Это программа-анализатор трафика, которая осуществляет перехват и анализ сетевого трафика.

3. Общий анализ уязвимостей беспроводной сети Bluetooth

Выше был рассмотрен пример применения Bluetooth в «умных» замках. Но данная технология применяется более широко, поэтому целесообразно рассмотреть общие уязвимости. Bluetooth – вторая по значимости технология после Wi-Fi, применяемая в умных устройствах. Первое поколение Bluetooth было основано на стандарте IEEE 802.15.1, который разрабатывался с расчетом на малую мощность. Новое поколение Bluetooth основано на стандарте IEEE 802.15.3. Он также предназначен для небольших сетей и локальной передачи данных, но предусматривает более высокую скорость передачи данных (до 55 Мбит/с) и на большее расстояние (до 100 м).

Главным преимуществом современного Bluetooth является то, что для связи не обязательна прямая видимость устройств – их могут разделять даже такие «радиопрозрачные» препятствия, как человек или стены. Взаимодействующие между собой с помощью технологии Bluetooth приборы могут находиться в движении. Bluetooth применяется во многих видах устройств, от обычных гаджетов до критически важного медицинского оборудования, такого как инсулиновые помпы и кардиостимуляторы и т.д. В промышленных условиях Bluetooth используется в датчиках, узлах, шлюзах и т.д. Он также используется в оружии, где компонентами являются, например, оптические прицелы, управляемые удаленно через Bluetooth. Различные устройства используют Bluetooth в силу преимуществ простоты и надежности этого протокола радиосвязи. По мнению многих специалистов, Bluetooth не имеет равных в своей нише. Более того, стандарт IEEE 802.15.1 стал конкурентом таких технологий, как Wi-Fi, HomeRF и IrDA (Infrared Direct Access – инфракрасный прямой доступ).

Существует версия Bluetooth Low Energy (BLE), которую часто используют устройства Интернета вещей из-за ее низкого энергопотребления и еще потому, что процесс сопряжения устройств проще, чем в предыдущих версиях Bluetooth. BLE потребляет значительно меньше энергии, чем традиционный Bluetooth, но он может очень эффективно передавать только небольшие порции информации. BLE использует 40 каналов, охватывающих диапазон от 2400 до 2483,5 МГц, традиционный Bluetooth использует 79 каналов в том же диапазоне.

Для защиты Bluetooth-соединения предусмотрено шифрование передаваемых данных, а также выполнение процедуры авторизации устройств. Шифрование данных может осуществляться с ключом длиной от 8 до 128 бит, что позволяет устанавливать уровень стойкости шифрования в соответствии

с законодательством разных стран. Bluetooth предусматривает три режима защиты, которые могут использоваться как по отдельности, так и в различных комбинациях:

1. Минимальный (обычно применяется по умолчанию). Данные кодируются общим ключом и могут приниматься любыми устройствами без ограничений.

2. Защита на уровне устройств. Реализуются процессы аутентификации и авторизации. Для каждой услуги определяется свой уровень доступа. Уровень доступа может указываться непосредственно в чипе.

3. Защита на уровне сеанса связи. Данные шифруются с помощью случайных чисел, которые хранятся в устройствах, участвующих в конкретном сеансе связи. Также выполняется процедура опознания устройств.

Современные Bluetooth-технологии обладают недостаточными средствами для опознания устройств, что делает их уязвимыми к нападениям (радиодезинформации). Кроме того, производители стремятся предоставить пользователям широкие полномочия и контроль над устройствами и их конфигурацией, что приводит к неправильному применению опознавательных Bluetooth-устройств. Крайне слабым местом интерфейса Bluetooth можно считать процесс сопряжения устройств, при котором происходит обмен ключами в незакодированных каналах, что делает их уязвимыми для стороннего прослушивания. В результате перехвата передачи в момент контакта можно получить ключ инициализации. В связи с этим рекомендуется производить процедуру сопряжения устройств в безопасной среде, что значительно уменьшает угрозу подслушивания. Кроме того, риск перехвата можно уменьшить, если пользоваться длинными паролями, которые усложняют их определение из перехваченных сообщений. Однако любое Bluetooth-устройство с личным ключом связи вполне безопасно. Так что меры безопасности по технологии Bluetooth могут защитить соединения только при условии правильной настройки и при правильном пользовании сервисами. В таблице 2 дана систематика угроз технологии Bluetooth. В таблице выделены основные угрозы и не показана их детализация.

Таблица 2 – Систематика угроз Bluetooth

Уязвимости	Угрозы
16 уязвимостей PoC-эксплоит	Вывод из строя
Программное обеспечение	Зависание устройства
	Удаленно выполнять вредоносный код на устройствах
	Сбой в работе
	Захват системы

Общий вывод при сравнении таблиц 1 и 2 заключается в том, что технология Bluetooth существенно уязвимей технологии WPA3.

Заключение

Проведен анализ уязвимостей беспроводных каналов передачи информации. Приведена систематика угроз для беспроводных технологий Wi-Fi и Bluetooth. Проведенный анализ позволяет оценить уязвимости и угрозы беспроводных сетей, использующих стандарты WEP, WPA, WPA2, WPA3. Показано, что стандарт WPA3 является наиболее стойким, но и он имеет уязвимости. Технология Bluetooth является более простым инструментом при настройке и передаче данных. Но эта технология менее быстродействующая и непригодна для передачи конфиденциальной информации. Технология Bluetooth подвержена атакам со стороны нарушителя с низкой квалификацией благодаря ряду инструментов, из которых следует отметить PoC-эксплоит, реализующий 16 угроз. При этом уровень угроз для Bluetooth намного выше, чем для технологий WEP, WPA, WPA2, WPA3. Для передачи конфиденциальной информации наиболее приемлемой является технология WPA3.

На примере показано, что информационные угрозы появляются не только из-за уязвимостей беспроводной технологии передачи информации, но из-за технологических особенностей применения

данной технологии в других системах, включая «умные вещи». Поэтому важным фактором информационной безопасности является планирование ресурсов, в том числе и человеческих ресурсов. Без высококвалифицированных специалистов информационная безопасность любой организации будет находиться под угрозой.

Список литературы

1. *Langley D.J.* et al. The Internet of Everything: Smart things and their impact on business models // Journal of Business Research. – 2021. – Vol. 122. – P. 853–863.
2. *Тихонов А.Н., Иванников А.Д., Цветков В.Я.* Терминологические отношения // Фундаментальные исследования. – 2009. – № 5. – С. 146–148.
3. *Altaf A.* et al. Trust models of internet of smart things: A survey, open issues, and future directions // Journal of Network and Computer Applications. – 2019. – Т. 137. – P. 93–111.
4. *Jeong J.* A study on the IoT based smart door lock system // Information Science and Applications (ICISA) 2016. – Singapore: Springer Singapore, 2016. – P. 1307–1318.
5. *Han D., Kim H., Jang J.* Blockchain based smart door lock system // 2017 International conference on information and communication technology convergence (ICTC). – IEEE, 2017. – P. 1165–1167.
6. *Mackensen E., Lai M., Wendt T.M.* Bluetooth Low Energy (BLE) based wireless sensors // SENSORS, 2012 IEEE. – IEEE, 2012. – P. 1–4.
7. *Barua A.* et al. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey // IEEE Open Journal of the Communications Society. – 2022.
8. *Deng C.* et al. IEEE 802.11 be Wi-Fi 7: New challenges and opportunities // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, No. 4. – P. 2136–2166.
9. *Lashkari A.H., Towhidi F., Hosseini R.S.* Wired equivalent privacy (WEP) // 2009 International Conference on Future Computer and Communication. – IEEE, 2009. – P. 492–495.
10. *Edney J., Arbaugh W.A., Arbaugh W.* Real 802.11 security: Wi-Fi protected access and 802.11i. – Addison-Wesley Professional, 2004. – 480 p. – URL: https://www.amazon.com/Real-802-11-Security-Protected-802-11i/dp/0321136209 (дата обращения: 10.02.2023). – Текст: электронный.
11. *Doomun M.R., Soyjaudah K.M.* Modified Temporal Key Integrity Protocol for Efficient Wireless Network Security//arXivpreprintarXiv:1208.5571.–2012.–URL:https://www.researchgate.net/publication/230750475_Modified_Temporal_Key_Integrity_Protocol_For_Efficient_Wireless_NetworkSecurity (дата обращения: 10.02.2023). – Текст: электронный.

References

1. *Langley D.J.* et al. The Internet of Everything: Smart things and their impact on business models // Journal of Business Research. – 2021. – Vol. 122. – P. 853–863.
2. *Tihonov A.N., Ivannikov A.D., Cvetkov V.Ya.* Terminologicheskie otnosheniya // Fundamental'nye issledovaniya. – 2009. – № 5. – S. 146–148.
3. *Altaf A.* et al. Trust models of internet of smart things: A survey, open issues, and future directions // Journal of Network and Computer Applications. – 2019. – T. 137. – P. 93–111.
4. *Jeong J.* A study on the IoT based smart door lock system // Information Science and Applications (ICISA) 2016. – Singapore: Springer Singapore, 2016. – P. 1307–1318.
5. *Han D., Kim H., Jang J.* Blockchain based smart door lock system // 2017 International conference on information and communication technology convergence (ICTC). – IEEE, 2017. – P. 1165–1167.
6. *Mackensen E., Lai M., Wendt T.M.* Bluetooth Low Energy (BLE) based wireless sensors // SENSORS, 2012 IEEE. – IEEE, 2012. – P. 1–4.
7. *Barua A.* et al. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey // IEEE Open Journal of the Communications Society. – 2022.
8. *Deng C.* et al. IEEE 802.11 be Wi-Fi 7: New challenges and opportunities // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, No. 4. – P. 2136–2166.
9. *Lashkari A.H., Towhidi F., Hosseini R.S.* Wired equivalent privacy (WEP) // 2009 International Conference on Future Computer and Communication. – IEEE, 2009. – P. 492–495.

10. *Edney J., Arbaugh W.A., Arbaugh W.* Real 802.11 security: Wi-Fi protected access and 802.11i. – Addison-Wesley Professional, 2004. – 480 p. – URL: https://www.amazon.com/Real-802-11-Security-Protected-802-11i/dp/0321136209 (data obrashcheniya: 10.02.2023). – Tekst: elektronnyj.
11. *Doomun M.R., Soyjaudah K.M.* Modified Temporal Key Integrity Protocol for Efficient Wireless Network Security // arXiv preprint arXiv:1208.5571. – 2012. – URL: https://www.researchgate.net/publication/230750475_Modified_Temporal_Key_Integrity_Protocol_For_Efficient_Wireless_NetworkSecurity (data obrashcheniya: 10.02.2023). – Tekst: elektronnyj.