УДК 004.771

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ БЕСПРОВОДНОЙ СЕТИ WI-FI

А. И. Кухта
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Беспроводные сетевые технологии приема и передачи информации на основе стандартов IEEE 802.11 занимают важное место в современном мире. Высокий уровень угроз приводит к необходимости искать методы защиты, которые позволяют системно обеспечить информационную безопасность. В работе указаны протоколы, обеспечивающие шифрование данных.Рассмотрены технологии защиты и некоторые способы взлома беспроводных сетей закрытого типа: WEP, WPA, WPA2, WPA3. Указаны недостатки каждой технологии защиты Wi-Fi.В работе осуществлена оценка технологий защиты беспроводной сети Wi-Fi (WEP, WPA, WPA2, WPA3). Исходя из криптостойкости установлена наиболее оптимальная технология защиты. Сформированы рекомендации, позволяющие пользователям беспроводной сети Wi-Fi обеспечить информационную безопасность.
***Ключевые слова*:** технология защиты Wi-Fi, стандарт 802.11, WEP, WPA, WPA2, WPA3, протоколы шифрования, сети Wi-Fi.

ANALYSIS OF PROTECTION METHODS OF A WIRELESS NETWORK WI-FI

A. I. Kuhta
Don State Technical University (Rostov-on-Don, Russian Federation)

Wireless network technologies for receiving and transmitting information based on IEEE 802.11 standards and occupy an important place in the modern world. The high level of threats leads to the need of looking for some protection methods that allow solving systematically the problem of information security. The purpose of the article is to analyze the methods of wireless Wi-Fi networks protection. The article describes the protocols that provide data encryption.Security technologies and some methods of hacking closed-type wireless networks are considered: WEP, WPA, WPA2, WPA3. The disadvantages of every type of Wi-Fi protection technology are indicated.In this article, the evaluation of Wi-Fi wireless network protection technologies (WEP, WPA, WPA2, WPA3) was carried out. Based on the cryptographic stability, the most optimal protection technology has been established. Recommendations are given, compliance which allows users of wireless Wi-Fi network to solve the problem of information security.
Keywords:Wi-Fi security technology, 802.11 standards, WEP, WPA, WPA2, WPA3, encryption protocols, Wi-Fi networks.

Введение.Беспроводные технологии в области приема и передачи информации занимают важное место в современном мире. Сложность прокладки проводных линий связи способствовала распространению беспроводных систем передачи данных. Высокий уровень угроз приводит к необходимости искать собственные методы защиты, позволяющие системно решать задачи по обеспечению информационной безопасности. Любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления объектами информационной инфраструктуры.

Цель работы — провести сравнительный анализ методов защиты беспроводных сетей Wi-Fi. Задачи:

- оценить технологии защиты и некоторые способы взлома беспроводных сетей закрытого типа: WEP, WPA, WPA2, WPA3;
- рассмотреть способы перехвата сетевого трафика и подключения к сети;
- указать недостатки каждой технологии защиты Wi-Fi, а также способы защиты от несанкционированного доступа злоумышленника;
- исходя из криптостойкости установить наиболее оптимальную технологию защиты беспроводной сети Wi-Fi;
- сформировать рекомендации, позволяющие пользователям беспроводной сети Wi-Fi обеспечить информационную безопасность.

Виды беспроводных сетей стандарта 802.11.Наиболее быстро развивающимся сегментом телекоммуникаций в настоящее время является беспроводная сеть Wi-Fi, которая обеспечивает прием/передачу информации с помощью радиоволн. Уровень помодели OSI— физический (передача фреймов 802.11). Стандарт 802.11 определяет три типа фреймов: управления (Managementframes), контроля (Controlframes), данных (Dataframes). Каждый фрейм имеет контрольное поле, которое определяет версию протокола 802.11, тип фрейма, индикаторы, например, WPA включен/выключен, управление энергосбережением. Кроме того, все фреймы содержат MAC-адреса клиента и сервера, номер фрейма, тело фрейма и проверочную последовательность фрейма для коррекции ошибок (контрольную сумму). Фреймы 802.11 переносят протоколы и данные более высоких уровней модели OSI внутри тела фрейма.Диапазон частот — СВЧ.Стандарт 802.11n работает на частотах 2,412–2,484 ГГц (14 каналов приема/передачи шириной 20 МГц каждый, канальная скорость — до 600 Мбит\с), а стандарт 802.11ac— начастоте 5 ГГц (23 непересекающихся канала приема/передачи шириной 20 МГц каждый, канальная скорость — до 7000 Мбит\с). С целью увеличения скорости передачи данных ширина каналов может быть увеличена:в диапазоне 2,4 ГГц — с 20 МГц до 40 МГц, ав диапазоне 5 ГГц — с 20 МГц до 160 МГц. Модуляция современного стандарта 802.11 —MU-MIMO (Multi User—Multiple Input Multiple Output) построена на основе множества антенн (создает до 4-х информационных потоков), что обеспечивает высокую скорость передачи данных.Технология Beamforming стандарта 802.11 обеспечивает направленное излучение от роутера к абоненту, что увеличивает скорость приема/передачи и частично защищает абонента от перехвата его трафика злоумышленником.

Беспроводные сети Wi-Fi делятся на два типа — открытые и закрытые. Сети открытого типа не используют защиту для подключения к самому устройствуили используют удалённую защиту доступа к сетив том случае, когда аутентификация пользователя осуществляется не на самом устройстве (при использовании моста или коммутатора), а на удалённом сервере [1]. Программой Nmap (NetworkMapper, пакеты доступны для Linux, Windows и Mac OSX) злоумышленник определит карту сети, состояние портов TCP и UDP жертвы. Изменит MAC-адрес для несанкционированного подключения к сети.

В ОС Linux: #ifconfigeth2 down

#if config eth2 hw ether a3:b4:c5:d7:e6:f8

#ifconfigeth2 up

eth2 — имя интерфейса, для которого осуществляется замена MAC, a3:b4:c5:d7:e6:f8 — назначаемый новый MAC-адрес. Далее утилитой arp проверяем изменения [2].

В ОС Windows: используем редактор реестра. Раздел:

HKEY_LOCAL_MACHINE\SYSTEMCurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318} [2]

Изменяем записи в DriverDesc и NetworkAddress (указываем новый MAC-адрес).

Технология защиты устройств беспроводной связи WEP. Сети закрытого типа Wi-Fi обеспечивают шифрование пакетов данных в канале передачи информации с использованиемследующихтехнологий защиты: WEP (WiredEquivalentPrivacy), WPA и WPA2 (Wi-Fi ProtectedAccess). Шифрование трафика WEP128-битным ключом (схема RC4) обеспечивается за счет сложения 104-битного ключа (пароля), который задается администратором, и 24-битного вектора инициализации (рис. 1).

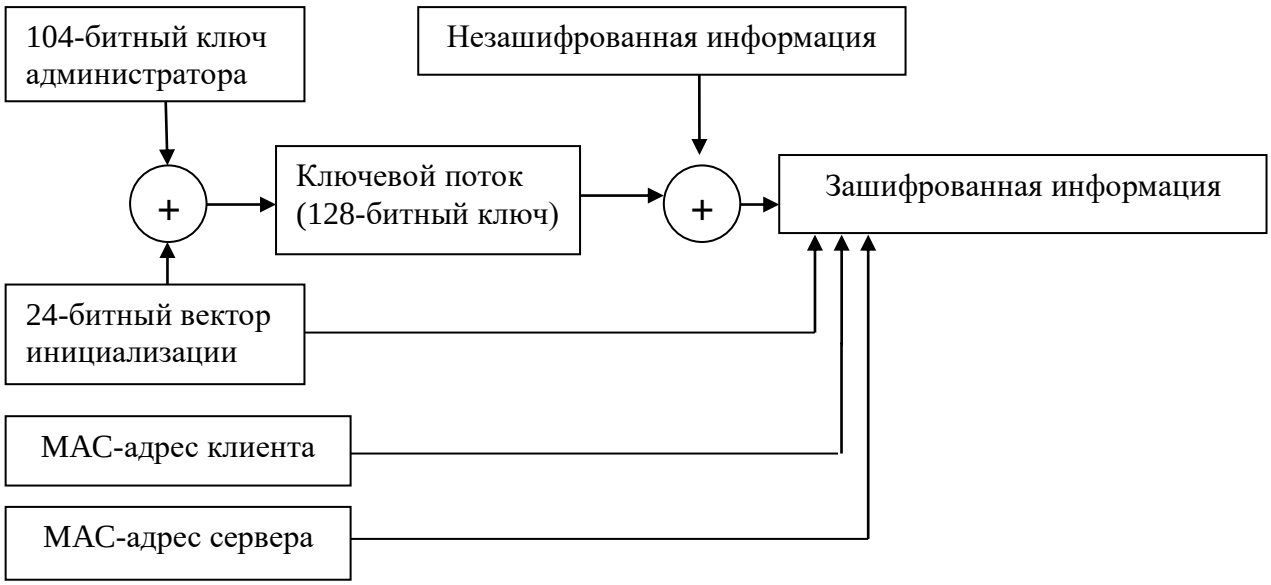

Рис. 1. Шифрование трафика WEP

При перехвате фреймов, возможно вычислить вектор инициализации. 24-битный вектор инициализации находится в фрейме после MAC-адресов (рис. 2).

MAC-адрес	24-битный вектор инициализации (значение увеличивается после каждого фрейма)	Зашифрованная информация

Рис. 2. Фрейм при шифровании трафика WEP

Количество вариантов перебора для вычисления вектора инициализации — 2^{24}. Время расшифровки ключа прямо пропорциональнозависит от объёма перехваченной информации. Вычисление ключаосуществляется методом статистического анализа перехваченных пакетов (несколько десятков тысяч), при этом существует схожесть ключей различных фреймов. В настоящее время на взлом WEP тратятся минуты. Одним из основных инструментов служит сниффер airodump-ng для сбора пакетов и утилита с целью взлома aircrakc-ng (перебор по словарю). Кроме того, возможно применить утилиту wesside-ng (с помощью радужных таблиц).

Технология защиты устройств беспроводной связи WPA.WPA (Wi-FiProtectedAccess) — второе поколение технологии защиты Wi-Fi. Длина пароля — произвольная в диапазоне 8–63 байт, что сильно затрудняет его подбор. Технология WPA является суммой:стандарта 802.1X (генерирует базовый ключ), протокола аутентификации EAP(ExtensibleAuthenticationProtocol),

MIC (проверка целостности пакетов) и TKIP[3]. В основе WPA содержатся: протокол TKIP (TemporalKeyIntegrityProtocol), размер ключа шифрования —128 бит, использование ключа WEP.В протоколе TKIP используется двухуровневая система векторов инициализации (рис. 3). Для каждого нового фрейма растет значение младшего вектора инициализации (как и ранее в стандарте WEP), при этом после прохождения цикла увеличивается значение старшего вектора инициализации и генерируется новый ключ. При смене ключа база статистики для взлома просто не успевает набраться. Кроме того, WPA отличается от WEP тем, что шифрует данные каждого клиента по отдельности[4].

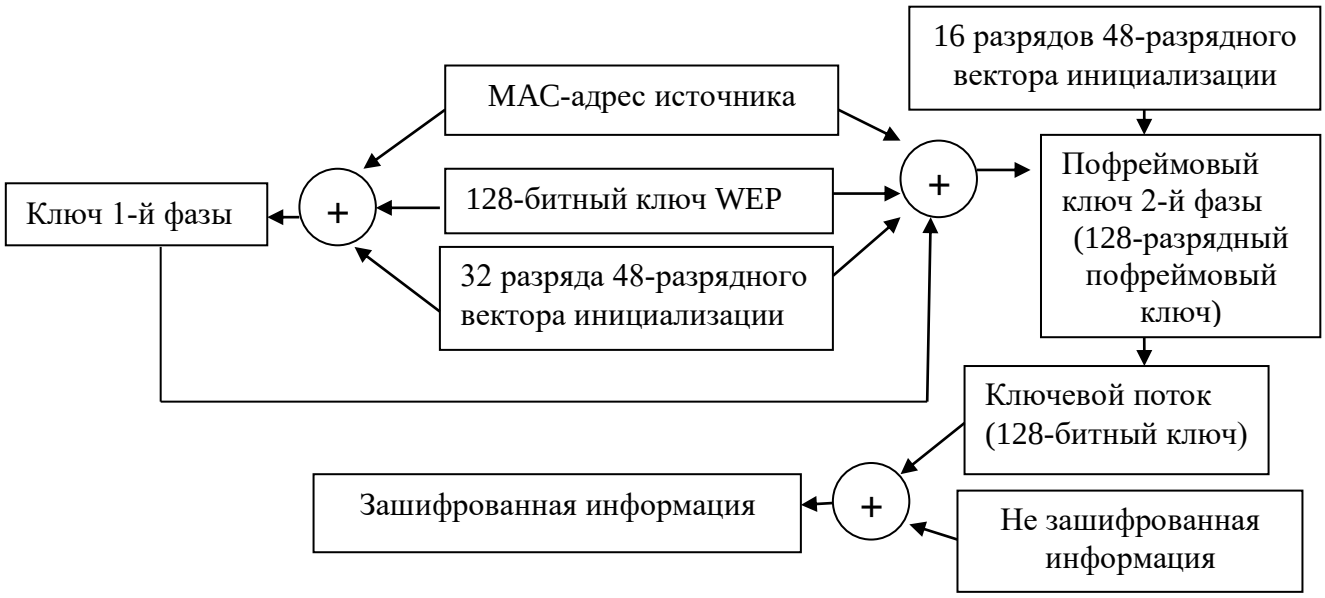

Рис. 3. Шифрование трафика WPA

После аутентификации и авторизации пользователя,так называемого «рукопожатия», генерируется временный ключ (PTK), который используется для кодирования трафика именно одного клиента. Поэтому, даже если злоумышленник проник в сеть, то прочитать пакеты других клиентов сможет только тогда, когда перехватит их «рукопожатия» — каждого по отдельности.

Недостатки WPA:

1. В WPA осуществляется проверка целостности фреймов с помощью системы MIC (MessageIntegrityCheck), рис. 4. В случае получения ложного фрейма, система его отбрасывает. Точка доступа блокирует все коммуникации через себя на 60 с, если обнаруживается атака на подбор ключа. Данную особенность использует злоумышленник, отсылая точке доступа ложные фреймы для блокирования работы сети.

16 разрядов 48-разрядного вектора инициализации	Данные (полезная нагрузка)	64-х разрядный MIC (уникальный ключ)	32 разряда 48-разрядного вектора инициализации

Рис. 4. Фрейм данных с MIC при шифровании трафика WPA

2. В WPA расшифроватьосновной ключ очень сложно.Однакосуществует способ узнать ключ MIC(используется для проверки целостности), а также полезную нагрузку. Для реализации атаки злоумышленник должен знать MAC-адрес клиента, подключённого к Wi-Fi-сети, для

дальнейшей кражи этого адреса и подмены на своём устройстве. В качестве инструмента анализа сети используется утилита с открытым исходным кодом Nmap (пакеты NetworkMapper доступны для Linux, Windows и Mac OSX), апрограмма NetworkManager может переназначать требуемые MAC-адреса. Алгоритм получения фрейма данных с MICизображен на рис. 5.

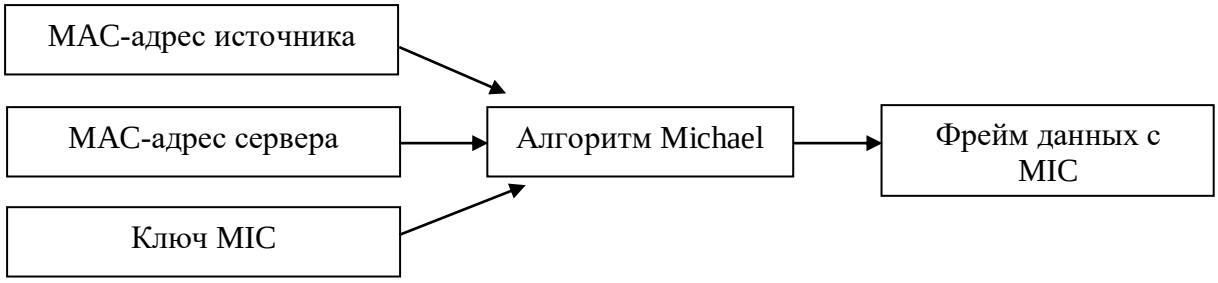

Рис. 5. Алгоритм получения фрейма данных с MIC.

Кроме того, для брутфорса необходимо накапливать пакеты без разрыва соединения, поэтому необходимо, чтобы в сети жертвы была включена WMM и QoS (стандарты регулирующие и обеспечивающие качество передачи трафика). В случае потери пакета, необходимо опять накапливать пакеты для анализа. Всвязи с этим для взлома необходим устойчивый уровень сигнала Wi-Fi.

3. В WPA существует технология WPS (подключение к точке доступа без пароля), которая позволяет беспроводным устройствам упрощенно получить доступ к Wi-Fi-сети при условии физического доступа к маршрутизатору. Она же и стала первой эксплуатируемой уязвимостью WPA[5]. Злоумышленник, используя включенный на роутере WPS, подбирает пин-код WPS с помощью брутфорса. Пин-код состоит из 8-и цифр (количество вариантов перебора паролей — 10^8). Последняя цифра является контрольной суммой, которая высчитывается по семи первым цифрам, следовательно подбор пин-кода составляет 10^7. Однако в самом протоколе существует уязвимость, которая позволяет разделить пин-код на 2, 4 и 3 части, которые подбираются отдельно друг от друга.В таком случае подбор пин-кода —10^4(подбор четырех цифр) и 10^3 (подбор трех цифр) составляет 11000 комбинаций[1]. Злоумышленник используя метод перебора пароля может получить пин-код WPS, который позволит ему в последующем войти в сеть жертвы.

Утилита взлома —wpscrack (работает на ОС Linux). Для реализации поставленной цели злоумышленнику необходимо осуществить мониторинг сети жертвы(программа Nmap), указать имя сетевого интерфейса, изменить свой MAC-адрес адаптера, определить MAC-адрес точки доступа (BSSID) и ее название, а также убедиться, что активирован WPS на взламываемом роутере. Для ускорения процесса можно задать номер канала, уменьшить время ожидания запроса (по умолчанию равен 5-и с). Далее используют брутфорс, т. е. подбор комбинаций пароля способом перебора. При этом в настоящее время злоумышленник стал использовать для брутфорса технологии NVIDIA CUDA и ATI Streamc целью аппаратного ускорения процесса перебора за счет утилита pyrite(GPU), который использует возможности видеокарты. Кроме того, многие производители роутеров на коробке указывают пин-код WPS. Защита от данного метода взлома — это использовать таймер «охлаждения» после неправильного ввода пароля, т. е. блокировать WPS на 1 ч. после пяти неудачных попыток ввода пин-кода (перебор займет 90 дней). Однако утилита Reaver (брутфорс) определяет блокирование WPS со стороны точки доступа и делает паузу в переборе, а также распознает попытки разрыва соединения при неправильном пин-коде. Для предотвращения несанкционированного подключения злоумышленника к беспроводной

сети рекомендуется отключать WPS.

Технология защиты устройств беспроводной связи WPA2.В настоящее время для сетей Wi-Fi технология защиты WPA2 является относительно надёжной. В WPA2используетсянадежный криптографический алгоритм шифрования — AES (AdvancedEncryptionStandard). В WPA2 устранена уязвимость, связанная с хищением и подменой ключевого потока, так же добавлен протокол AES/CCMP с совершенно новым алгоритмом шифрования, который основан на AES256 с дополнительной защитой и проверкой на целостность. Данную технологию, возможно, взломать только с помощью брутфорса, защитой от которого является ежемесячная смена ключа[6]. Структура фрейма представлена на рис. 6.

Заголовок MAC	Заголовок CCMP (8 байт)	Зашифрованные данные (8 байт)	MIC (8 байт)	FSC (8 байт)

Рис. 6. Структура фрейма при использовании WPA2.

Недостатки WPA2:

1.Недостатки соответствуют WPA по протоколу WPS/QSS. Обезопасить себя можно с помощью отключения WPS.

2. Возможен перехват рукопожатия и подбор ключа методом брутфорса. Метод взлома назвали атакой с переустановкой ключа — keyreinstallationattack или сокращенно KRACK. Реализовать атаку можно, воздействуя на четырехстороннее рукопожатие протокола WPA2[5].Злоумышленник подсоединяется к защищенной сети, подтверждая, что он и точка доступа имеют общийBSSID. Атака реализуется следующим образом. Злоумышленник перехватывает третий пакет рукопожатия и ретранслирует клиенту.Это приводит к переустановке ключа и обнулению счетчика пакетов nonce (случайных 32-байтных чисел). Счетчик nonce непосредственно участвует в создании ключевого потока, с помощью которого шифруются пакеты, отправляемые между клиентом и маршрутизатором. В результате атаки следующий после переустановки ключа пакет, отправляемый клиентом, будет зашифрован тем же ключевым потоком, которым был зашифрован первый пакет[6]. Далее осуществляется накопление пакетов и вычисление ключа методом перебора.

Особенностивзлома в случае применения технологий WEP и WPS.В случае технологии WEP для успешного взлома необходимо накопление перехваченных фреймов (накопление векторов инициализации), при этом устойчивость соединения не играет существенной роли, так какне обязательна строгая очередность передачи фреймов между злоумышленником и точкой доступа.

В случае технологии WPS для успешного взлома необходимы строгое следование и очередность передачи пакетов между злоумышленником и точкой доступа с целью проверки при переборе каждого пин-кода. При потере пакета необходимо заново устанавливать WPS-соединение. Всвязи с этим успешность брутфорса зависит от уровня сигнала точки доступа.

Технология защиты устройств беспроводной связи WPA3.Уязвимость четырехстороннего рукопожатия WPA2устранена в WPA3 за счет метода соединения SEA, известного как Dragonfly (технология направлена на защиту сетей Wi-Fi от автономных атак по словарю). Технология SEA (SimultaneousAuthenticationofEquals) описана в стандарте IEEE 802.11s и основана на протоколе обмена ключами Диффи — Хеллмана с использованием конечных циклических групп[7]. В соответствии с SEA две и более стороны устанавливают криптографические ключи, основанные на знании пароля одной или несколькими сторонами.

Результирующий ключ сессии, который получает каждая из сторон для аутентификации соединения, выбирается на основе информации из пароля, ключей и MAC-адресов обеих сторон. Еще одним новшеством WPA3 будет поддержка PMF (ProtectedManagementFrames) для контроля целостности трафика[5]. Как и в WPA2, в WPA3 предусмотрено два режима работы: WPA3-Personal и WPA3-Enterprise. В WPA3-Personal обеспечивается вход по единому паролю, который вводит клиент при подключении к сети. При этом ограничено число попыток аутентификации в рамках одного рукопожатия. Также ограничение не позволит подбирать пароль в режиме офлайн. Вместо ключа PSK в WPA3 реализована технология SEA. BWPA3-Enterprise шифрование осуществляется 192-разрядными ключами. Ключи аутентификации хранятся на отдельном сервере RADIUS.

Существенный недостаток WPA3— это использование WPS, QSS. Метод обхода защиты по паролю, так же как в WPA и WPA2,не зависит от сложности пароля доступа к беспроводной сети (до 50-и запросов в секунду для подключения по WPS, при этом для взлома необходимо 10000 попыток подбора WPS-пароля). В настоящее время производители беспроводного оборудования ограничили число попыток входа по паролю WPS.В случаепревышения числа попыток подключения, доступ по WPS автоматически отключаетсяна1 ч. Однако при использовании утилиты Reaver (брутфорс), которая определяет блокирование WPS со стороны точки доступа и делает паузу в переборе, а также распознает попытки разрыва соединения при неправильном вводе пин-кода, взлом составит около семи дней (время прохождения цикла около 10^4запросов).

Существует угроза для всех технологий защиты сетей Wi-Fi— это вид атаки под названием «злой двойник». Суть атаки заключается в копировании имени SSID беспроводной сети (злоумышленник создает копиюбеспроводной точки доступа с более сильным сигналом излучения, чем у настоящей беспроводной сети). Тем самым злоумышленник подменяет оригинальную точку доступа двойником, к которому подключается пользователь, открывая злоумышленнику возможность доступа кконфиденциальной информации[8]. Для защиты от данного вида атаки клиент должен уменьшить время изменения радиоканалов Wi-Fi, а также использовать шифрование при передаче данных (VPN-сервер).

Кроме того, большинство пользователей совсем не думают о безопасности роутеров, забывая менять пароль на роутере Wi-Fi со стандартного admin/admin на что-либо своё. Данная оплошность позволяет злоумышленнику взять под свой контроль работу роутера.

Выводы.Проведен анализ технологии защиты беспроводной сети Wi-Fi. В результате можно сделать вывод, чтона сегодняшний день наиболее оптимальная технология защиты Wi-Fi— это WPA3, внутри которой используется шифрование канала передачи данных на основе 192-разрядных ключей. Однако, клиенту при работе в сети рекомендуется отключить функции WPS/QSS,использовать VPN (виртуальную частную сеть) при подключении к открытым беспроводным сетям. В этом случае весь сетевой трафик от клиента до VPN-сервера будет зашифрован. Кроме того, пользователю необходимо следить за сообщениями браузера о нарушении шифрования или несоответствующихсертификатах безопасности[8]. Соблюдение вышеперечисленных рекомендаций позволит пользователям беспроводной сети Wi-Fi решить задачу обеспечения информационной безопасности.

Библиографический список

1. Варлатая, С. К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником / С. К. Варлатая, О. С. Рогова, Д. Р. Юрьев// Молодой ученый.— 2015. — № 1(81). — С. 36–37.

2. Кенин, А. Самоучитель системного администратора / А. Кенин, Д. Колисниченко // Lyapidov:[сайт]. — URL :https://lyapidov.ru/kenin-kolisnichenko-tutorial-system-administrator-5-edition/ (дата обращения: 12.03.2020).

3. Безопасность WPA3 //SPY-SOFT.NET : [сайт]. — URL : http://www.spy-soft.net/wpa3/ (дата обращения: 01.12.2019).

4. Герасимов, Л. WPA3. Смотрим, что нового в следующем стандарте безопасности Wi-Fi, изучаем прошлые / Л. Герасимов // хакер.ru :[сайт]. — URL : https://xakep.ru/2018/10/26/wpa3/ (дата обращения: 20.11.2019).

5. Wi-Fi сети: проникновение и защита// Хабр :[сайт]. — URL : https://habr.com/ru/post/224955/ (дата обращения: 19.11.2019).

6. Об алгоритме взлома WPA-PSK// Хабр :[сайт]. — URL : https://habr.com/ru/post/122623/ (дата обращения: 01.11.2019).

7. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — Санкт-Петербург : Питер, 2012. — 960 с.

8. Злой двойник // wikipedia:[сайт]. — URL :https://ru.wikipedia.org/wiki/Злой двойник/(дата обращения: 17.11.2019).

Об авторе:

Кухта Алексей Игоревич, магистрант Донского государственного технического университета (344000, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), alexey-semenov82@mail.ru

Authors

Kuhta Aleksei Igorevich, master's degree student, Don State Technical University (344000, Russian Federation, Rostov-on-Don, Gagarina sq. 1), alexey-semenov82@mail.ru