Анатолий П. Дураковский[1], Виталий Н. Цимбал[2]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
[2]Московский университет МВД России имени В.Я. Кикотя
ул. Академика Волгина, 12, Москва, 117997, Россия
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: sedruk@mail.ru, https://orcid.org/0000-0002-0561-148X

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ БЕСПРОВОДНОГО СТАНДАРТА IEEE 802.11

DOI: http://dx.doi.org/10.26583/bit.2022.4.04

Аннотация. Статья посвящена проведению анализа угроз безопасности беспроводных сетей, функционирующих на основе протоколов стандарта IEEE 802.11 (блокирование работы, перехват и/или навязывание ложных данных и т.п.), исследованию уязвимостей и разработке модели угроз безопасности различных систем, использующих указанный стандарт. Киберфизические системы, как средство коммуникации, активно используются в обеспечении информационных процессов. Вследствие низкой унифицированности технических решений, использованию в разработке технологий без учета требований защищенности, такие системы могут быть подвержены со стороны злоумышленника рискам информационной безопасности. Данные риски, как правило, приводят к нарушению работоспособности, конфиденциальности, подконтрольности и иным негативным последствиям для пользователя либо обладателя информации (оборудования). Разработка модели угроз безопасности информации беспроводных сетей, работа которых основывается на протоколах стандарта IEEE 802.11, используемых в функционировании киберфизических систем является актуальной задачей в организации защиты информации. В статье на основе методики оценки угроз безопасности информации ФСТЭК России анализируются негативные последствия, которые могут приводить к реализации различных угроз, их актуальность, обобщаются объекты воздействия. Систематизируются и классифицируются конкретные действия нарушителя, уровни опасности, масштаб потенциального ущерба от реализации угроз за счет использования уязвимостей протоколов стандарта IEEE 802.11.

Ключевые слова: беспроводная сеть, Wi-Fi, модель угроз, угроза безопасности информации, киберфизическая система, нарушитель безопасности информации.
Для цитирования: ДУРАКОВСКИЙ, Анатолий П.; ЦИМБАЛ, Виталий Н. МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ БЕСПРОВОДНОГО СТАНДАРТА IEEE 802.11. Безопасность информационных технологий, [S.l.], т. 29, № 4, с. 42–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1454. DOI: http://dx.doi.org/10.26583/bit.2022.4.04.

Anatoly P. Durakovskiy[2], Vitaly N. Tsymbal[3]
[1,2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Kashirskoe Shosse, 31, Moscow, 115409, Russia
[2]V.Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia,
12 Akademika Volgina str., Moscow, 117997, Russia
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: sedruk@mail.ru, https://orcid.org/0000-0002-0561-148X

Modelling of information security threats for the wireless standard IEEE 802.11

DOI: http://dx.doi.org/10.26583/bit.2022.4.04

Abstract. When building multi-level information protection both in the public and in the private sector, it is necessary to take the measures aimed at preventing threats to information security. Cyberphysical systems, as a means of communication, are actively used for providing information processes. Due to the poor uniformity of such technical solutions, as well as the use of technologies that were developed without taking into account security issues, such systems may be exposed to information security risks from an

attacker. These risks, as a rule, lead to a violation of operability, confidentiality, control and other negative consequences for the user or the owner of the information (equipment). The development of a model of information security threats for the wireless networks, the operation of which is based on the protocols of the IEEE 802.11 standard used in the functioning of cyber-physical systems is an urgent problem in the area of information protection. The negative consequences that can lead to the implementation of various threats, and its relevance are analysed. The objects of influence based on the Methodology of assessing threats to the security of information of the FSTEC Russia are summarised. The specific actions of the violator, the levels of danger, the scale of potential damage from the implementation of threats due to the use of vulnerabilities of protocols of the IEEE 802.11 standard are systematized and classified.
Keywords: wireless network, Wi-Fi, threat model, information security threat, cyberphysical system, information security violator.
For citation: DURAKOVSKIY, Anatoly P.; TSYMBAL, Vitaly N. Modelling of information security threats for the wireless standard IEEE 802.11. IT Security (Russia), [S.l.], v. 29, no. 4, p. 42–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1454. DOI: http://dx.doi.org/10.26583/bit.2022.4.04.

Введение

Беспроводные технологии передачи данных функционируют подобно проводным технологиям, однако беспроводные сети используют информационные сигналы в форме радиоволны, передаваемой в воздушной среде [1, 2].

Используются беспроводные сети передачи данных в различных целях: для создания локальных сетей на небольшом пространстве либо удаленных на многие километры друг от друга устройств; для передачи информации большому количеству устройств; для подключения абонентских устройств к провайдеру; для организации связи; для корпоративных и частных целей и т.п., но важным отличием от проводного подключения является высокая мобильность и относительная простота реализации [3].

Несмотря на указанные положительные характеристики беспроводных сетей, существует и негативный аспект их применения [4], к которым можно отнести высокую незащищенность от помех, которые могут быть созданы (возникать) как искусственно, так и в результате естественных причин, небольшая зона покрытия сети, значительный расход оборудования, предназначенного для построения сети, возможность перехвата нарушителем информативного сигнала либо управления, навязывание ложных данных и иное [5, 6].

Анализу существующих угроз безопасности информации (УБИ) беспроводных сетей, построенных на основе протоколов стандарта IEEE 802.11, исследованию существующих уязвимостей, а также разработке модели УБИ посвящена данная работа.

1. Стандарты IEEE 802.11

Группа стандартов IEEE 802.11 относится к беспроводным локальным сетям (WLAN), представляет собой набор спецификаций контроля доступа к среде на канальном и физическом уровнях эталонной модели взаимодействия открытых систем для развертывания беспроводных локальных сетей в диапазоне частот 0,9; 2,4; 3,6; 5 и 60 ГГц. Различные версии стандарта обеспечивают передачу данных со скоростью до 40 Гб/с на расстояниях от 10 до 100 м (в данном случае, эта цифра может изменяться в зависимости от поколения технологии и используемого стандарта Wi-Fi), работает данная сеть в международном нелицензируемом диапазоне частот 2,4 ГГц (2412–2472 МГц) и 5 ГГц (5160–5825 МГц). В данной работе рассматриваются Wi-Fi сети.

Применяются Wi-Fi сети для организации беспроводных локальных подключений на высоких скоростях, с целью передачи мультимедийной информации, доступа к сети Интернет, совершения звонков и иных возможностей. То есть, основной сегмент для чего

разрабатывался стандарт было удовлетворение потребностей пользователей для офисного и домашнего использования и замены проводных соединений.

Версий стандарта IEEE 802.11 более десятка (a, d, i, ac, be и т.д.), различаются они скоростью (от 1 МБ/с до 40 ГБ/с) и подробно рассмотрены в [7].

Строятся такие сети различными способами:

1) с одной точкой доступа (англ. Access Point, сокр. AP) – в качестве средства подключения используется AP, к которой присоединяются абонентские устройства;

2) с несколькими AP – используется несколько AP, которые могут предоставлять связь, как для пользовательского устройства, так и для соединения нескольких AP между собой;

3) без AP – используется сеть Wi-Fi, устройства подключаются друг к другу напрямую, при этом отсутствует необходимость в AP.

Согласно ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ защита информации должна обеспечиваться «…принятием правовых, организационных и технических мер»[1] . Правовые меры в рамках данной работы не рассматриваются, а применению технических и организационных мер, которые реализованы в устройствах беспроводной связи и используемых для ее защиты от неправомерных действий со стороны посторонних лиц уделим внимание подробнее.

Безопасность функционирования и защита информации, передаваемой в беспроводных сетях, является достаточно серьезной задачей и проблемой, решение которых должно обеспечиваться на достаточно высоком уровне. Согласно ГОСТ Р 59162-2020[2] для обеспечения безопасности сети необходимо чтобы обеспечивались:

– конфиденциальность: передаваемая информация не должна разглашаться (злоумышленник не должен прослушивать сеть);

– целостность: передаваемая информация не должна изменяться при передаче (злоумышленник не должен изменять или подменять передаваемые данные);

– доступность: услуги сети должны быть доступны (злоумышленник не должен мешать функционированию сети);

– аутентификация: подлинность пользователей или объектов, запрашивающих доступ к сети, должна быть подтверждена (злоумышленник не должен выдавать себя за санкционированного пользователя);

– контроль доступа: доступ к сетям и AP должен контролироваться (злоумышленник не должен подменять сеть и AP);

– подконтрольность: любое нарушение политики должно быть прослежено до конкретного пользователя или субъекта (злоумышленник не должен иметь возможность скрывать свою активность в сети).

В настоящее время существуют и применяются различные способы защиты беспроводных сетей стандарта IEEE 802.11, которые можно разделить на защиту:

– техническими способами:

WEP (Wired Equivalent Privacy) – протокол шифрования, основанный на алгоритме шифрования RC4 с 40, 104, 128 и 256-битными ключами, который складывается со сгенерированным вектором инициализации (24 бит) [8, 9];

[1]Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[2] ГОСТ Р 59162-2020 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей. М.: Стандартинформ, 2020. – 32 с.

WPA (Wi-Fi Protected Access) – протокол шифрования, применяющий ключ 256-бит и паролей длиной от 8 до 63 байт, добавлена проверка целостности сообщений и протокол целостности временного ключа – TKIP (Temporal Key Integrity Protocol), позже замененный на AES (Advanced Encryption Standard) [8, 10];

WPA2 – протокол шифрования, использующий криптографический алгоритм AES совместно с режимом счетчика с протоколом кода аутентификации сообщений с алгоритмом блочного шифрования [8, 10];

WPA3 – является новейшим протоколом шифрования, дополняющим и улучшающим перечисленные выше технологии, использует метод аутентификации устройства, применяющий криптографию для предотвращения получения пароля пользователя SEA (Simultaneous Authentication of Equals), и поддерживает PMF (Protected Management Frames) для контроля целостности трафика [11, 12];

фильтрация по MAC-адресу (на маршрутизаторе выключается возможность подключения устройств, которых нет в списке разрешенных адресов либо администратор запрещает сопряжение беспроводного устройства, которое ранее уже имело доступ к сети [13], указанная технология не предусматривается стандартами;

скрытие SSID (Service Set Identifier) – является техническим адресом устройства или идентификатором набора базовых услуг для защиты сети осуществляется отключение передачи в открытый радиоэфир SSID, после этого подключиться к сети возможно, только если знать название данного SSID;

WIDS (Wireless Intrusion Detection Systems) – система беспроводного обнаружения вторжений – путем мониторинга радиоэфира обнаруживают несанкционированные АР, анализируют полученные данные и на основе этой информации осуществляют следующие действия: предупреждение администратора о наличии подозрительной АР, о блокировании ее активности или действий неавторизованного пользователя и т.п.;

WIPS (Wireless Intrusion Prevention System) – система предотвращения вторжений, позволяет определять и реагировать на различные сетевые атаки (DoS, Honeypot, MITM и др.), подмены MAC-адресов, неправильно настроенные или несанкционированные АР и т.п.) и другие;

– организационную: физическое ограничение доступа посторонних лиц к АР, контроль выданных паролей для доступа пользователей к беспроводной сети (в больших организациях), обучение пользователей основам безопасного и защищенного использования АР [14] и т.п.

2. Моделирование УБИ стандарта IEEE 802.11

Согласно ГОСТ Р 50922-2006 [3] под моделью угроз (безопасности информации) понимается физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

ГОСТ Р 56545-2015 [4] определяет *угрозу безопасности информации* как «…совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации».

Целью моделирования УБИ является разработка документа, который позволяет определять совокупность возможных УБИ, реализация которых нарушителем

[3] ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. М.: Стандартинформ, 2008. – 12 с.

[4] ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. М.: Стандартинформ, 2018. – 12 с.

(злоумышленником), в свою очередь, может приводить к нарушению функционирования защищаемого объекта, его сетей и систем, а также выводу его из строя.

Основными угрозами функционирования беспроводного стандарта IEEE 802.11 будем считать нарушение конфиденциальности и аутентичности передаваемой информации, контроля доступа к АР (маршрутизатору), подконтрольности канала связи и используемого оборудования, целостности передаваемых данных, а также нарушение (прекращение) функционирования каналов связи (т.е. доступности).

Документом, регламентирующим оценку угроз безопасности и соответственно виды нарушителей, является методический документ ФСТЭК России[5]. Он определяет порядок и содержание работ по определению УБИ, реализация (возникновение) которых возможна в информационных системах (ИС), автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах. Данный документ определяет обобщенную схему оценки УБИ и разделяет ее на несколько этапов:

1. Определение негативных последствий, которые могут приводить к реализации различных УБИ.
2. Определение объектов воздействия.
3. Оценка возможности реализации угроз и их актуальность.

На основе обобщенной схемы регулятора, постараемся обозначить модель УБИ беспроводного стандарта IEEE 802.11 с целью наглядного их представления и акцентирования внимания на основных аспектах уязвимостей.

Первым этапом является *определение негативных последствий*, которые могут приводить к реализации различных УБИ беспроводного стандарта IEEE 802.11, который состоит из следующих составляющих:

1) виды неправомерного доступа: утечка информации, несанкционированный доступ, отказ в обслуживании, модификация данных, несанкционированное использование информации, эксплуатация недостатков протоколов передачи данных; перенаправление, зеркалирование и прослушивание трафика;

2) перечень возможных негативных последствий: отсутствие сигнала, утечка трафика, перехват управления, выход из строя АР, получение аутентификационной информации, получение парольной информации;

3) УБИ: конфиденциальности, целостности, доступности, аутентичности, контроля доступа, подконтрольности и т.п.

Вторым этапом является определение *объектов воздействия*, составляющие его следующие:

1) объекты беспроводной сети: АР и пользовательское оборудование;

2) типы уязвимостей: неправильная настройка устройства, архитектура АР, аутентификация, недостатки в протоколах шифрования.

Объектом воздействия являются линии связи (функционирующие на различных радиочастотах частотах), сетевое оборудование (маршрутизаторы или АР) и абонентское оборудование, которое может находиться в распоряжении отдельно взятого пользователя, групп пользователей, использоваться коммерческими и иными организациями.

Третьим этапом является *оценка возможности реализации угроз и их актуальность*.

Одним из важных направлений, которые необходимо рассмотреть при моделировании УБИ является характеристика нарушителя (злоумышленника), который

[5]Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.).

является одним из ключевых факторов, которые могут воздействовать на безопасность информации, обращаемой в беспроводных сетях и на функционирование самих сетей.

С целью оценки возможностей нарушителя, его потенциала, знаний, подготовленности и иных факторов, влияющих на реализацию УБИ, как правило, разрабатывается модель нарушителя. Приведем расширенную характеристику нарушителя.

Классифицировать потенциал нарушителей можно различными способами: в зависимости от их возможностей (базовые, базовые повышенные, средние и высокие), в зависимости от имеющихся прав и условий доступа к сети (внутренние и внешние), отдельно можно выделить представителей специальных служб иностранных государств, так как их базовые возможности намного выше по сравнению с любыми иными видами нарушителей, а также они могут более эффективно привлекать пользователей для реализации своих намерений.

По типу нарушитель может быть, как внешний (специальные службы иностранных государств, преступные группы (криминальные структуры), конкурирующие организации, если речь идет о коммерческих отношениях, физические лица и т.д.), так и внутренний (обычный пользователь; обслуживающий персонал, имеющий непосредственный доступ к оборудованию и/или защищаемому объекту; сотрудники различных организаций, где развернуты сети Wi-Fi и т.д.).

По виду нарушителем могут выступать как человек, так и животное, либо программное обеспечение (ПО). Человек будет осуществлять либо умышленные, либо неумышленные действия, животное (например, грызуны) выступает в виде угрозы, если повредит оборудование, кабели питания и т.п. ПО (например, вредоносное), может выступать как орудие совершения противоправного действия со стороны нарушителя и конечно же не рассматривается в данном контексте как самостоятельно действующий объект.

Мотивы нарушителя могут быть самые различные: хулиганство, получение информации либо прибыли, месть, и даже совершение преступлений, не всегда связанных с реализацией права на информацию, например, совершение террористических актов.

Выделяя квалификацию нарушителя, предположим, что он может быть начинающим (не иметь опыта в работе с техническими средствами, ПО, не иметь опыта в противоправной деятельности в целом, не иметь либо технического образования, не иметь навыков программирования), специалистом (иметь высшее образование в технических науках и программировании, ранее работать с сетевым оборудованием, участвовать в составлении политик безопасности) и профессионалом (специализироваться на противоправной деятельности в технической и/или программной области и иное).

Используемое оборудование нарушителем также может быть разнообразно: стандартный компьютер; компьютер с набором специальных утилит (например, операционная система Kali Linux на базе операционной системы Linux); разработанные программные продукты, которые используют уязвимости беспроводного стандарта IEEE 802.11 для реализации атак на них; вредоносное ПО.

Также возможно отметить, что действия нарушителя могут быть как активными (умышленные целенаправленные противоправные действия, которые могут тем или иным образом воздействовать на объект атаки), пассивными (умышленные целенаправленные противоправные действия, которые не воздействуют на объект атаки, но могут получать сведения о нем (из него)) и случайными (неумышленные действия, как правило, связанные со стечением обстоятельств).

В заключительной части модели злоумышленника выделим возможные цели, которые преследует нарушитель, виды нарушителя и его потенциал или уровень возможностей для реализации своих незаконных действий, представлены в табл. 1.

Таблица 1. Виды нарушителя безопасности беспроводного стандарта 802.11 и уровень его потенциальных возможностей

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Категория нарушителя	Потенциал нарушителя
1.	Нанесение ущерба или прекращение функционирования, деятельности органов государственной власти, корпораций, организаций	Специальные службы иностранных государств	Внешний	Высокий
		Террористические организации	Внешний	Средний
2.	Использование сети Интернет или корпоративной сети для распространения вредоносных программ	Преступные группы (криминальные структуры)	Внешний	Базовый повышенный
3.	Нарушение функционирования сети связи организации	Конкурирующие организации	Внешний	Базовый повышенный
4.	Использование беспроводных сетей для реализации преступных намерений	Преступные группы (криминальные структуры)	Внешний	Базовый повышенный
		Физические лица	Внешний	Базовый
5.	Хищение информации ограниченного доступа или распространения	Специальные службы иностранных государств	Внешний	Высокий
		Преступные группы (криминальные структуры)	Внешний	Базовый повышенный
		Физические лица	Внешний	Базовый
		Сотрудники организации	Внутренний	Базовый повышенный
6.	Непреднамеренные, неосторожные или неквалифицированные действия	Преступные группы (криминальные структуры)	Внешний	Базовый повышенный
		Физические лица	Внешний	Базовый
		Сотрудники организации	Внутренний	Базовый повышенный
		Разработчики ПО и программных продуктов	Внутренний	Базовый

Представленный перечень не является исчерпывающим (приведен для примера), существуют и иные вариации, рассматривать полностью все не имеет смысла, как правило, подобные модели разрабатываются для отдельно взятого случая, объекта и конкретной организации.

Кроме этого, возможности различных типов и видов нарушителей, описание конкретных их потенциальных действий описаны в банке данных угроз (БДУ) безопасности информации ФСТЭК России[6].

Выделим некоторые дополнительные этапы, которые не полностью представлены в рассматриваемой методике ФСТЭК России, а именно четвертым этапом, считаем должно быть *определение конкретных действий нарушителя* (сценария), осуществляемые им при реализации УБИ. К ним отнесем следующие: сбор информации о системе и сети, получение доступа к устройству, внедрение вредоносного ПО или кода, закрепление в системе, управление ранее установленной программой или кодом, повышение привилегий, скрытие своих противоправных действий, направленных на необнаружение, получение искомых данных и возможности доступа к иным компонентам системы или сети.

Относительно *источников угроз и факторов*, которые могут влиять на безопасность информации и функционирование беспроводного стандарта IEEE 802.11 выделим основные: техногенные (проявляются в виде различных недостатков в функционировании ПО, средствах связи, программно-аппаратных средств, обеспечивающих систем), антропогенные (как правило, деятельность нарушителей), биологические (грызуны, микробы (плесень) и т.п.) и природные явления (пожары, наводнения, землетрясения, перепады температуры и т.п.) [14, 15].

Пятым этапом, по нашему мнению, должно являться *определение уровня опасности*, измеряться данные уровни могут в виде следующих показателей: низкий, средний или высокий. В данном случае, все зависит от квалификации, подготовленности, опыта и возможностей нарушителя.

Уровень ущерба может быть измеряемым (например, материальный) и неизмеряемым (например, моральный, репутационный). Указанные показатели оценочные, они могут измеряться математически, опытным или экспертным путем.

К измеряемому ущербу возможно применить существующие способы (методологии) его оценки, позволяющие сопоставить потенциальный ущерб с конечными количественными значениями, выражающимися в денежном эквиваленте, процентном выражении, времени и т.п.

Однако, не всегда возможно определить размер причиняемого ущерба в количественном выражении, в данном случае целесообразно оценить его в качественном виде. В таком варианте оценивания, применяется проранжированный по различным шкалам показатель, например, трехбалльной (низкий/минимальный, средний, высокий/максимальный), пятибалльной или десятибалльной шкале (от нуля до десяти).

Масштаб ущерба при реализации атаки на беспроводные сети стандарта IEEE 802.11 зависит от того, где они расположены и для каких целей используются. Видами ущерба в данном случае будут индивидуальный (частному пользователю в случае, когда сетевое оборудование используется им для собственных нужд), корпоративный (в случае, когда организация (предприятие) использует АР для обеспечения беспроводных зон покрытия в рабочих помещениях для доступа сотрудников либо для доступа посетителей) или государственный (редкий, при организации доступа в подразделениях (службах) органов власти либо на объектах, имеющих значение для государства, от деятельности иностранных спецслужб).

Уязвимости функционирования беспроводного стандарта IEEE 802.11, которые могут приводить к блокированию работы различных устройств и систем можно разделить на три области:

[6]Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/ (дата обращения: 15.06.2022).

– физическая – связана с нарушением деятельности линий связи, разнообразного коммуникационного оборудования и аппаратуры пользователей;

– технологическая – связана с недоработкой или имеющимися проблемами в протоколах безопасности, пользовательском оборудовании и в среде доставки;

– логическая – связанная с деятельностью пользователя и нарушителя.

В настоящее время специалистами в области информационной безопасности разработано большое количество различных способов определения УБИ и также разнообразных методов моделирования угроз, например, CRAM, MITRE ATT&CK, Attack Trees, CyberKill Chain; БДУ ФСТЭК России, позволяющий получать сведения о выявленных уязвимостях УБИ в ИС и др. В зависимости от осуществляемой деятельности конкретной организации, целесообразно тщательно выбирать способ моделирования угроз, что в свою очередь, позволит превентивно предусматривать способы и средства защиты информации в компьютерных сетях и ИС, организовывать доступ к защищаемым данным, разрабатывать организационно-распорядительную документацию и иное.

Заключение

Моделирование УБИ позволяет устанавливать возможные причины и условия, которые могут привести к нарушению безопасности информации, передаваемой, в частности, посредством беспроводных сетей, функционирующих на основе протоколов стандарта IEEE 802.11.

Предложенная модель УБИ стандарта IEEE 802.11 основана на содержании этапов оценки угроз методического документа регулятора, в которой предложены дополнения касательно расширенного анализа возможностей нарушителя (злоумышленника) и определения уровня опасности от реализации возможных УБИ (уровни ущерба и его возможный масштаб). Классифицированы области уязвимостей оборудования, которое обеспечивает работу сетей Wi-Fi.

Подводя итог рассмотренному, основываясь на знании возможных угроз, существующих уязвимостей и описании потенциального нарушителя безопасности и строя модели перечисленного, специалисту по информационной безопасности, а также рядовому пользователю будет легче продумывать последовательность превентивных мер и действий, направленных на обеспечение бесперебойного функционирования сетевого оборудования, компьютерной системы, а также минимизации ущерба от возможных инцидентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Васильева Н.В. Анализ процессов распространения сигналов в беспроводных сетях. В сборнике: Перспективное развитие науки, техники и технологий. Сборник научных статей материалы 8-й Международной научно-практической конференции. Ответственный редактор А.А. Горохов. 2018, с. 39–42. URL: https://elibrary.ru/item.asp?id=36417485 (дата обращения: 15.06.2022). – EDN VLWADM.
2. Сигов А.В., Сова Ю.С. О методах исследования беспроводных сигналов. В сборнике: Проблемы и перспективы развития россии: молодежный взгляд в будущее. сборник научных статей 4-й Всероссийской научной конференции. Курск, 2021. С. 344–347. URL: https://elibrary.ru/item.asp?id=47172318 (дата обращения: 15.06.2022). – EDN EOHRKZ.
3. Янг С., Ко Х., Ким Е. Способ и устройство для передачи и приема беспроводного сигнала в системе беспроводной связи. Патент на изобретение RU 2705227 C1, 06.11.2019. Заявка № 2019100432 от 15.06.2017. URL: https://elibrary.ru/item.asp?id=41323447 (дата обращения: 15.06.2022). – EDN RHEBAX.
4. Касимов А.О., Жайынбеков А.К. Анализ моделей и методов повышения эффективности сетей беспроводного доступа стандарта IEEE 802.11. Вопросы устойчивого развития общества. 2022, № 6, с. 1133–1136. URL: https://elibrary.ru/item.asp?id=48732883 (дата обращения: 15.09.2022). – EDN OVGEKI.
5. Peng J. Throughput analysis of the IEEE 802.11 DCF in cognitive radio networks. Procedia Computer Science. 2019, vol. 151, p. 264–271. DOI: http://dx.doi.org/10.1016/j.procs.2019.04.038.

6. Bosch P., Latré S., Blondia C. An analytical model for IEEE 802.11 with non-IEEE 802.11 interfering source. Computer Networks. 2020, vol. 172, p. 107154. DOI: http://dx.doi.org/10.1016/j.comnet.2020.107154.
7. Дураковский, Анатолий П., Цимбал, Виталий Н. Исследование угроз функционирования киберфизических систем за счет использования уязвимостей беспроводного стандарта IEEE 802.11. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 20–35, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.02. – EDN VQYKGR.
8. Ахметова Б.А., Ахметова Д.А. Атаки на сеть WI-FI вида WEP/WPA/WPA2 и методы борьбы с ними. Вестник современных исследований. 2020, № 8-1(38), с. 4–7. URL: https://elibrary.ru/item.asp?id=44391588 (дата обращения: 15.06.2022). – EDN EWJJJS.
9. Белетова Д.У., Молчанов А.Н. Использование стандарта IEEE 802.1x для защиты от НСД. Электронный журнал: наука, техника и образование. 2017, № 1(10), с. 6–15. URL: https://elibrary.ru/item.asp?id=28807636 (дата обращения: 15.06.2022). – EDN YGKILZ.
10. Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy and Anwar Althubyani «A Survey on Wi-Fi Protocols: WPA and WPA2». International Conference on Security in Computer Networks and Distributed Systems. March 2014. DOI: http://dx.doi.org/10.1007/978-3-642-54525-2_44.
11. Кухта А.И. Анализ методов защиты беспроводной сети Wi-Fi. Молодой исследователь Дона. 2020, № 2(23), с. 41–48. URL: https://elibrary.ru/item.asp?id=42780898 (дата обращения: 15.06.2022). – EDN IKZFGT.
12. Dalal N., Akhtar N., Gupta A., Karamchandani N., Kasbekar G.S., Parekh J. A Wireless Intrusion Detection System for 802.11 WPA3 Networks. URL: https://www.researchgate.net/publication/355225129_A_Wireless_Intrusion_Detection_System_for_80211_WPA3_Networks (дата обращения: 15.06.2022).
13. Гибадуллин Р.Ф., Галимов А.Р., Кормильцев Н.В. и др. Анализ и модернизация защищенности стандарта IEEE 802.11i. Вестник Технологического университета. 2018, т. 21, № 8, с. 100–108. URL: https://www.elibrary.ru/item.asp?id=36351318 (дата обращения: 15.06.2022). – EDN YMJXCX.
14. Muhammad Imran Tariq. Wireless Security and Threats. Conference: 11th Islamic Countries Conference on Statistical Sciences (ICCS-11) At: Lahore, Pakistan. Volume: 21, 2011. URL: https://www.researchgate.net/publication/236585512_Wireless_Security_and_Threats (дата обращения: 15.06.2022).
15. Andysah Putera Utama Siahaan. The Weakness of Wireless Networks. Conference SEMILOKA, 2011. URL: https://www.researchgate.net/publication/304425433_The_Weakness_of_Wireless_Networks (дата обращения: 18.06.2022).
16. Cesar H. Tarazona T. Amenazas informáticas y seguridad de la información. URL: https://core.ac.uk/display/230095193?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1 (дата обращения: 18.06.2022).

REFERENCES:

[1] Vasilyeva N.V. Analysis of signal propagation processes in wireless networks. In the collection: Perspective development of science, engineering and technology. Collection of scientific articles materials of the 8th International Scientific and Practical Conference. Executive editor A.A. Gorokhov. 2018, p. 39–42. URL: https://elibrary.ru/item.asp?id=36417485 (accessed: 15.06.2022) (in Russian). – EDN VLWADM.
[2] Sigov A.V., Sova Yu.S. About methods of studying wireless signals. In the collection: Problems and prospects for the development of russia: youth view into the future. collection of scientific articles of the 4th All-Russian Scientific Conference. Kursk, 2021. P. 344–347. URL: https://elibrary.ru/item.asp?id=47172318 (accessed: 15.06.2022) (in Russian). – EDN EOHRKZ.
[3] Yang Suckchel, KO Hyunsoo, KIM Eunsun. Method and apparatus for transmitting and receiving a wireless signal in a wireless communication system. Patent of invention RU 2705227 C1, 06.11.2019. Request No 2019100432 from 15.06.2017. URL: https://elibrary.ru/item.asp?id=41323447 (accessed: 15.06.2022) (in Russian). – EDN RHEBAX.
[4] Kasimov A.O., Zhayynbekov A.K. Analysis of models and methods for improving the efficiency of IEEE 802.11 wireless access networks. Issues of sustainable development of society. 2022, no. 6, p. 1133–1136. URL: https://elibrary.ru/item.asp?id=48732883 (accessed: 15.06.2022) (in Russian). – EDN OVGEKI.
[5] Peng J. Throughput analysis of the IEEE 802.11 DCF in cognitive radio networks. Procedia Computer Science. 2019, vol. 151, p. 264–271. DOI: http://dx.doi.org/10.1016/j.procs.2019.04.038.
[6] Bosch P., Latré S., Blondia C. An analytical model for IEEE 802.11 with non-IEEE 802.11 interfering source. Computer Networks. 2020, vol. 172, p. 107154. DOI: http://dx.doi.org/10.1016/j.comnet.2020.107154.

[7] Durakovskiy Anatoly P., Tsymbal Vitaly N. Investigation of threats to the functioning of cyber-physical systems due to the use of vulnerabilities of the wireless standard IEEE 802.11. IT Security, [S.l.], v. 29, no. 2, p. 20–35, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.02 (in Russian). – EDN VQYKGR.

[8] Akhmetova B.A., Akhmetova D.A. Ataki na set' WI-FI vida WEP/WPA/WPA2 i metody bor'by s nimi. Vestnik sovremennykh issledovanii. 2020, № 8-1 (38), s. 4–7. URL: https://elibrary.ru/item.asp?id=44391588 (accessed 15.06.2022) (in Russian). – EDN EWJJJS.

[9] Beketova D.U., Molchanov A.N. The use of the IEEE 802.1x standard for protection against NSD. Elektronnyj zhurnal: nauka, tekhnika i obrazovanie. 2017, no. 1(10), p. 6–15. URL: https://elibrary.ru/item.asp?id=28807636 (accessed: 15.06.2022) (in Russian). – EDN YGKILZ.

[10] Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy and Anwar Althubyani «A Survey on Wi-Fi Protocols: WPA and WPA2». International Conference on Security in Computer Networks and Distributed Systems. March 2014. DOI: http://dx.doi.org/10.1007/978-3-642-54525-2_44.

[11] Kukhta A.I. Analiz metodov zashchity besprovodnoi seti Wi-Fi. Molodoi issledovatel' Dona. 2020, № 2(23), s. 41–48. URL: https://elibrary.ru/item.asp?id=42780898 (accessed: 15.06.2022) (in Russian). – EDN IKZFGT.

[12] Dalal N., Akhtar N., Gupta A., Karamchandani N., Kasbekar G.S., Parekh J. A Wireless Intrusion Detection System for 802.11 WPA3 Networks. URL: https://www.researchgate.net/publication/355225129_A_Wireless_Intrusion_Detection_System_for_80211_WPA3_Networks (accessed: 15.06.2022).

[13] Gibadullin R.F., Galimov A.R., Kormil'tsev N.V. i dr. Analiz i modernizatsiya zashchishchennosti standarta IEEE 802.11i. Vestnik Tekhnologicheskogo universiteta. 2018, t. 21, № 8, s. 100–108. URL: https://www.elibrary.ru/item.asp?id=36351318 (accessed: 15.06.2022) (in Russian). – EDN YMJXCX.

[14] Muhammad Imran Tariq. Wireless Security and Threats. Conference: 11th Islamic Countries Conference on Statistical Sciences (ICCS-11) At: Lahore, Pakistan. Volume: 21, 2011. URL: https://www.researchgate.net/publication/236585512_Wireless_Security_and_Threats (accessed: 18.06.2022).

[15] Andysah Putera Utama Siahaan. The Weakness of Wireless Networks. Conference SEMILOKA, 2011. URL: https://www.researchgate.net/publication/304425433_The_Weakness_of_Wireless_Networks (accessed: 18.06.2022).

[16] Cesar H. Tarazona T. Amenazas informáticas y seguridad de la información. URL: https://core.ac.uk/display/230095193?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1 (accessed: 18.06.2022).

Поступила в редакцию – 07 сентября 2022 г. Окончательный вариант – 01 ноября 2022 г.
Received – September 07, 2022. The final version – November 01, 2022.