Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. 2023, № 2, с. 72-85.

Поступила: 03.08.2023
Окончательный вариант: 21.09.2023

УДК 519.816

Классификация угроз и уязвимостей в беспроводных сетях

Милосердов А.О.

milosalex@list.ru
УлГУ, Ульяновск, Россия

В статье представлен обзор и анализ материалов, который может быть полезен разработчикам беспроводных сетей на этапе проектирования и эксплуатации в области обеспечения безопасности. Подробно рассмотрены и классифицированы виды уязвимостей сетей, возможные угрозы, атаки, нарушения целостности передаваемых сообщений. Эти данные позволяют на предварительном этапе рассмотреть возможные опасные ситуации с нарушениями целостности безопасности, провести необходимое моделирование развития их вариантов, оценки рисков и предусмотреть меры по защите и безопасности при эксплуатации построенной сети, а также совершенствовать имеющиеся.

***Ключевые слова**: беспроводная сеть, безопасность, угроза беспроводным сетям, уязвимость беспроводных сетей, классификация*

Введение

Беспроводная связь является наиболее перспективной на данный момент времени так как позволяет с меньшими затратами обеспечивать передачу данных на расстояния до нескольких километров без использований проводов и большого количества оборудования, что и отличает ее от проводной связи.

Проектирование беспроводной сети состоит из семи этапов [10]. Одним из основных является этап обеспечения безопасности будущей сети. Задача обеспечения безопасности решается путем не только сравнительного анализа эффективности использования методов и средств защиты беспроводной сети, но и задач, связанных с процессами моделирования ситуаций и событий, которые возможны при действиях множества агрессивных внешних факторов, учета уязвимостей сетей и разнообразных атак.

Технология обеспечения безопасности беспроводной сети отличается от других особенностями угроз, уязвимостей, рисков и способов решения задачи безопасности прежде

всего тем, что среда передачи данных расширяет спектр угроз и уязвимостей из-за чего, повышается количество способов доступа к каналам связи.

Для успешного решения задачи обеспечения безопасности беспроводной сети, необходимо провести анализ всех возможных ситуаций, которые могут привести к нарушению целостности передаваемых сообщений, классифицировать виды угроз, уязвимостей с точки зрения их важности и актуальности, а также возможностей нанесения ущерба.

Классификация позволяет упорядочить и систематизировать указанную информацию, задействованные объекты, сгруппировав их по определенным признакам и критериям, выявить закономерности и взаимосвязи между объектами, что позволит использовать оценочные данные по возникающим опасным ситуациям для принятия решений и созданию превентивных мероприятий по защите сетей на предварительных этапах их проектирования [14].

К сожалению, по теме данной публикации, работы носят характер решения отдельных задач по безопасности в конкретных ситуациях, мало материалов по связности уязвимостей, угроз и возможных атак, и средств их противодействия, которые обеспечивают единство проблемы решения безопасности беспроводных сетей [11].

Целью работы является разработка классификации угроз и уязвимостей в беспроводных сетях на основе которой можно определять классы возможных атак и виды защиты от них.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ существующих угроз и уязвимостей в беспроводных сетях;
2. Разработать классификации уязвимостей и угроз в беспроводных сетях.

1. Виды угроз беспроводных сетей

ГОСТ Р 56545-2015 определяет угрозу безопасности информации как совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Описание угроз и мер безопасности в беспроводных сетях описаны в ГОСТ Р ИСО/МЭК 27033-3-2014.

Рассмотрим угрозы, которые присуще большинству технологий беспроводной передачи данных.

1. Обнаружение сети через другие устройства или программы. Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumber. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Информация о степени защиты сети является очень ценной, она позволяет определить злоумышленнику дальнейший ход действий [7].

2. Подслушивание. Атакующий пассивно следит за коммуникацией в сети с целью захвата данных, передающихся по сети, и перехвата учетных данных проверки подлинности (пассивная) [8].

3. Аномалия типа "отказ в обслуживании" DoS (от англ. Denial of Service) является, как правило, сетевой атакой, проводимой злоумышленником в отношении сетевого объек-

та, чье функционирование он желает нарушить (например, замедлить или прекратить). Наиболее характерным проявлением DoS является "затопление" или flooding канала связи или конкретного сетевого устройства огромным количеством сетевых пакетов. В зависимости от типа пакетов, это может привести к перегрузке канала и, как следствие, невозможности прохождения по нему легитимного трафика, либо к повышенной загрузке устройства (заполнению доступного объема оперативной памяти и загрузке ресурсов процессора). [18]

4. Глушение клиентской станции. Глушение в сетях происходит тогда, когда преднамеренная или непреднамеренная интерференция превышает возможности отправителя или получателя в канале связи, таким образом, выводя этот канал из строя. Атакующий может использовать различные способы глушения. Также глушение могут использовать для отказа в обслуживании клиента, чтобы ему не удавалось реализовать соединение. Более изощренные атаки прерывают соединение с базовой станцией, чтобы затем она была присоединена к станции злоумышленника [2].

5. Глушение базовой станции. Такое глушение лишает пользователей доступа к услугам. Многие устройства, такие как радиотелефоны, системы слежения и микроволновые печи, могут влиять на работу беспроводных сетей и глушить беспроводное соединение. Чтобы предотвратить такие случаи непреднамеренного глушения, прежде чем покупать дорогостоящее беспроводное оборудование, надо тщательно проанализировать место его установки. Такой анализ поможет убедиться в том, что другие устройства никак не помешают коммуникациям [2].

6. Угрозы криптозащиты. В беспроводных сетях применяются криптографические средства для обеспечения целостности и конфиденциальности информации. Однако взлом злоумышленниками системы безопасности сети приводят к нарушению коммуникаций и злонамеренному использованию информации. Например, протокол безопасности технологии Wi-Fi – WEP, который использует простой ключ, который может быть получен перебором [2].

7. Анонимность атак. Беспроводной доступ обеспечивает полную анонимность атаки. Без соответствующего оборудования в сети, позволяющего определять местоположение, атакующий может легко сохранять анонимность и прятаться где угодно на территории действия беспроводной сети. В таком случае злоумышленника трудно поймать и еще сложнее передать дело в суд [7].

8. Физическая защита. Угроза доступа к авторизированным устройствам злоумышленников. Например, для доступа к сети по технологии Wi-Fi устройства такие, как ноутбуки и телефоны имеют небольшой размер. Незаконно завладев устройством атакующий, имеет физический доступ и может заменить программное обеспечение или украсть учетные данные, такие как статические ключи. [6].

9. Внедрение несанкционированных точек доступа. В роли таких точек выступают отдельные аппаратные или программные точки доступа. Пользователь, подключаясь к такой

точке доступа, предоставляет злоумышленникам все свои передаваемые данные. Так же такая точка может прослушивать сеть с целью перехвата всего трафика [7].

10. Уязвимость самих сетей и устройств. Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации [12]. Уязвимости присущие беспроводным сетям, неотделимы от них и обуславливаются недостатками процесса функционирования, свойствами архитектуры сети, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения. Во всех сетях и устройствах есть свои уязвимости. Каждая их них представляет угрозу обхода безопасности в беспроводных сетях. Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

11. Утечка данных из проводной сети. Если точка доступа настроена в режим моста, то она может передавать широковещательный трафик из проводной сети. К тому же любая беспроводная сеть рано или поздно перейдет в проводную, и на нее будут действовать угрозы присущие проводным сетям.

12. Подозрительный трафик. Если в нерабочее время сети может наблюдаться трафик в сети, это свидетельствует о проблемах с безопасностью. Специалистам необходимо проверять такой трафик.

13. Нарушение работы. Окружающая электромагнитная обстановка может стать причиной для нарушения функционирования сети [1].

14. Система аутентификации. Атакующий пытается украсть учетные данные зарегистрированного пользователя сети. Основными атаками на систему аутентификации являются:

• маскарад (impersonation). Пользователь пытается выдать себя за другого с целью получения привилегий и возможности действий от лица другого пользователя;

• подмена стороны аутентификационного обмена (interleavingattack). Злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика. Существует разновидность атаки подмены: после успешного прохождения аутентификации между двумя пользователями и установления соединения нарушитель исключает какого- либо пользователя из соединения и продолжает работу от его имени;

• повторная передача (replayattack). Заключается в повторной передаче аутентификационных данных каким-либо пользователем;

• отражение передачи (reflectionattack). Один из вариантов предыдущей атаки, в ходе которой злоумышленник в рамках данной сессии протокола пересылает обратно перехваченную информацию;

• вынужденная задержка (forceddelay). Злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;

• атака с выборкой текста (chosen- textattack). Злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах [8].

Классификация угроз безопасности в беспроводных сетях

Рассмотренные выше угрозы можно классифицировать по следующим признакам: характер угрозы, цель реализации угрозы, условие начала процесса реализации угрозы, уровень эталонной модели взаимодействия открытых систем (ISO/OSI), по частоте возникновения, по виду нанесенного ущерба.

Перечисленные признаки играют ведущую роль при оценке опасности и возможности ущерба, выявления причин и следствий, раскрывают достаточно полно картину возникшей ситуации, позволяют построить формальную модель угрозы и провести анализ ее реализации в различных вариантах при проведении имитационного моделирования. Также на базе классифицированных данных имеется возможность создавать сценарии ситуаций с угрозами и проводить анализ на когнитивном уровне с использованием прецедентного подхода.

На основании предложенных признаков составлена классификация угроз безопасности в беспроводных сетях, которая представлена на рис. 1.

Признак **характер угрозы** определяет направление их действий, например, на слабо защищенные места, их связи с видами уязвимостями и возможными последствиями, рисками нарушения целостности и работоспособности, затрачиваемого времени на восстановление сети.

По характеру угрозы можно разделить на пассивные и активные угрозы. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу системы, но могут быть нарушены установленные правила разграничения доступа к данным или сетевым ресурсам. Примером таких угроз является угроза «Подслушивание», «Обнаружение сети через другие устройства или программы», «Подозрительный трафик».

Активная угроза – это угроза, связанная с воздействием на ресурсы системы, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к данным или сетевым ресурсам. В качестве примеров таких угроз можно привести «Отказ в обслуживании», «Глушение базовых станций», «Внедрение несанкционированных точек доступа» [9].

Признак **цель реализации угрозы** несет, прежде всего, значение и объем наносимого ущерба сетям, масштабность события и последствия восстановления после атак.

По цели реализации угрозы могут быть направленны на нарушение конфиденциальности, целостности и доступности информации.

Рис.1. Классификация угроз в беспродных сетях.

Важным признаком угроз является **условие начала процесса реализации угрозы.**

Здесь внимание концентрируется на незавершенности мероприятий по защите сетей, на низкую скорость реагирования, на внезапные атаки, слабость превентивных мер.

Реализация угрозы может начаться лишь при определенных условиях. Среди таких условий выделяют следующие: наступление ожидаемого события на объекте, относительного которого реализуется угроза; отсутствие какого-либо условия. В первом случае злоумышленник осуществляет постоянное наблюдение за состоянием сети, или объектом атаки, и при возникновении определенного события начинает реализацию угрозы. В каче-

стве примера можно привести угрозу нарушения физической защиты. То есть кража устройств, зарегистрированных в сети.

Во втором случае инициатором начала процесса реализации угроз выступает сам атакующий. К ним относятся всевозможные виды атак, например атака «Отказ в обслуживании» [9].

Признак **уровень эталонной модели** взаимодействия открытых систем (ISO/OSI), имеет значение для оценки возможных угроз и, прежде всего, для составления их списка, так как удаленную атаку можно ассоциировать с определенным уровнем подели OSI, что позволяет отнести их к известному виду.

По уровню эталонной модели взаимодействия открытых систем (ISO/OSI), можно судить о сложности реализации угрозы. Любой сетевой протокол обмена, как и любую сетевую программу, можно с той или иной степенью точности спроецировать на эталонную многоуровневую модель OSI. И вследствие того, что удаленная атака реализуется какой-либо сетевой программой, ее можно соотнести с определенным уровнем модели ISO/OSI: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной. Кроме того, реализация угрозы может быть совершена на нескольких уровнях, например, как в атаке «Отказ в обслуживании», где атака реализуется на физическом, канальном, сетевом, транспортном и прикладном уровне [18].

Признак **частота возникновения угрозы** связан с ценностью успешных результатов атак со стороны нарушителей, возможностью их прежних неудач, незавершенностью, необходимостью получения дополнительной закрытой информации, в этом случае сеть рассматривается как источник или поставщик важных данных, к которым можно обращаться неоднократно.

По частоте возникновения выделяют два вида таких угроз. Более и наименее частые.

К более частым относятся: «Отказ в обслуживании», «Подслушивание», «Угрозы криптозащиты», «Внедрение несанкционированных точек доступа», «Уязвимость самих сетей и устройств», «Атаки на систему аутентификации» [14, 21].

К менее частым относятся: «Обнаружение сети через другие устройства или программы», «Глушения», «Физические атаки», «Утечка данных из проводной сети».

Признак **вид нанесенного ущерба** можно связать с целями и причинами атак, на основании анализа которых создаются средства для защиты сетей в конкретных условиях.

По виду нанесенного ущерба выделяют три вида ущерба: Полный доступ к сети, кража данных, нарушение нормальной работы сети.

Полный доступ к сети позволяет злоумышленнику завладеть всеми данными или изменить конфигурацию сети. К такому типу ущерба приводят атаки на систему аутентификации и физический уровень.

Кража данных позволяет злоумышленнику завладеть частью данных. К такому типу ущерба приводят угрозы: «Внедрение несанкционированных точек доступа», «Угрозы обхода протоколов криптозащиты».

Нарушение нормальной работы сети замедляет или делает невозможной работу беспроводной сети. В качестве примера можно привести угрозы типа DDos или глушение всей сети или её частей.

2. Виды уязвимостей беспроводных сетей

ГОСТ Р 56545-2015 [4] описывает уязвимость - Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Рассмотрим наиболее распространенные уязвимости, которые присуще большинству технологий беспроводной связи.

1. Уязвимости обусловленные средой передачи данных. Так как среда передачи в беспроводных сетях отличается от проводной, она открывает новые уязвимости и способы доступа к сети.

Информация, циркулирующая в беспроводных сетях подвержена перехвату. Это объясняется тем, что переносчиком информации являются радиоволны. Т.е. Для перехвата информации злоумышленнику достаточно иметь набор устройств, аналогичные комплекту оборудования абонента беспроводной сети [19].

2. Уязвимости системы аутентификации. Основными системами аутентификации в беспроводных сетях являются базовая аутентификация, аутентификация с использованием общих PSK-ключей, аутентификация по стандарту IEEE 802.1x и протоколу EAP.

Уязвимости системы аутентификации складываются из следующих составляющих:

- Уязвимость открытой аутентификации.

Открытая аутентификация, по сути, не является алгоритмом аутентификации в привычном понимании. Точка доступа удовлетворит любой запрос открытой аутентификации. Такой алгоритм аутентификации использовалась в первых системах беспроводного доступа Wi-Fi. Если не использовалось какое-либо шифрование, сеть была уязвима.

- Проблемы идентификатора беспроводной сети. Идентификатор ESSID регулярно передается точками радиодоступа и любой сторонний наблюдатель в состоянии определить ESSID с помощью анализатора трафика протокола IEEE 802.11. Некоторые точки радиодоступа позволяют запретить широковещательную передачу ESSID. Однако и в этом случае ESSID можно легко определить путем захвата кадров, посылаемых точками радиодоступа.

- Уязвимость аутентификации с общим ключом. Аутентификация с общим ключом требует настройки у абонента статического ключа для шифрования специального сообщения, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрования его ответа на специальное сообщение и сравнения его с отправленным оригиналом.

- Уязвимость аутентификации по MAC-адресу. Многие стандарты беспроводной связи требуют передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате этого в беспроводной сети, использующей аутентификацию по MAC-адресу, зло-

умышленник может обмануть метод аутентификации путём подмены своего MAC-адреса на легитимный. Подмена MAC- адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика для выявления MAC-адресов легитимных абонентов [19].

3. Уязвимости криптографических протоколов. К ним относятся:

- Проверка целостности данных. Проверка контрольных сум, при подключении устройства передают друг другу сообщения, если контрольная сумма обоих одинакова, то соединение устанавливается. Злоумышленник может нарушить работу проверки целостности данных, и тем самым подключиться к сети.

- Уязвимости алгоритмов шифрования. В криптографических протоколах используются те или иные алгоритмы шифрования, так или иначе у алгоритмов присутствуют уязвимости, если злоумышленнику удается воспользоваться ей, криптографических протоколах становиться бесполезен.

- Вычисление ключевого потока. Злоумышленник может вычислить ключ шифрования проанализировав поток. Это присуще старым криптографическим протоколам.

- Вычисление ключевого потока. Злоумышленник может вычислить ключ шифрования проанализировав ключевой поток. Это присуще старым криптографическим протоколам. Например, в протоколе WEP, из-за особенностей архитектуры безопасности 802.11 взломщик может быстро вычислить ключевой поток, используя слабые места протокола. В протоколе WEP не задан метод вычисления вектора инициализации для каждого пакета и не требуется, чтобы все пакеты имели разные значения вектора инициализации. Из-за этих ограничений многие поставщики реализовали примитивные и предсказуемые алгоритмы вычисления вектора инициализации, что резко уменьшает число уникальных ключевых потоков в сети.

- Получение секретного ключа. В большинстве практических систем беспроводной связи используется один ключ для всей сети. Этот ключ хранится в каждом устройстве в сети. Если взломщик получит секретный ключ для одного устройства, он будет обладать ключом для всех устройств в сети. Но если бы в каждом устройстве хранился уникальный частный ключ, неизвестный другим пользователям сети, то взломщику было бы гораздо труднее вычислить ключевой поток [20].

4. Уязвимости используемого программного обеспечения.

Драйверы и программы беспроводных устройств разрабатываются без надлежащего внимания к безопасности, и новые функции добавляются в спешке ради конкуренции, поэтому код часто изобилует ошибками и небезопасен. В настоящее время существует множество инструментов, позволяющих использовать уязвимость драйверов беспроводных адаптеров [20].

Эти признаки могут дать необходимую информацию для оценки безопасности сетей на предварительном этапе их проектирования, для выявления слабых мест, составления их списка, расчета рисков атак, проведения моделирования возможных ситуаций и состояний корректного их функционирования сетей, выработки мер и эффективного средства противодействия.

Составим классификацию уязвимостей и для этого введем следующие признаки: вид, степень распространения, источник возникновения.

На рис. 2 представлена классификации уязвимостей в беспроводных сетях.

Рис. 2. Классификация уязвимостей в беспродных сетях.

Признак **вид** делится на объективные, субъективные и случайные уязвимости.

Объективные уязвимости основываются на особенностях построения и технических характеристиках оборудования и ПО, применяемых в беспроводных сетях. К ним относятся уязвимости системы аутентификации и криптографических протоколов.

Субъективные уязвимости зависят от действий субъектов (например, разработчиков оборудования и ПО, системных администраторов и пользователей организации). Уязвимости данного типа в большинстве случаев устраняются организационными и программно-аппаратными методами. К ним относятся уязвимости программного обеспечения.

Случайные уязвимости обуславливаются особенностями окружающей объект и среды и непредвиденными обстоятельствами. К ним относятся уязвимости среды передачи данных. [17]

Признак **степень распространения** делится на: повсеместные, распространённые, нераспространённые.

К повсеместным относиться уязвимость среды передачи, так как все беспроводные сети используют одну среду распространения.

К распространённым относятся уязвимости системы аутентификации и криптографических протоколов [13].

К нераспространённым относиться уязвимость программного обеспечения.

Признак **источник возникновения** уязвимостей показывает, в какой момент времени возникает уязвимость. К данной категории относятся: уязвимости, которые закладываются на этапе проектирования (среда передачи); возникающие на этапе реализации (криптографические протоколы); в следствии ошибок эксплуатации.

Классификация уязвимостей программного обеспечения в беспроводных сетях

Уязвимости программного обеспечения в беспроводных сетях можно классифицировать по следующим признакам: Вид и местоположение уязвимости.

На рис. 3 представлена классификация уязвимостей ПО.

Рис. 3. Классификация уязвимостей ПО.

Признак **вид** позволяет разделить уязвимое программное обеспечение по следующим группам:

• Несовместимые ПО, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

• ПО проникновения, некоторое изменение параметров которых позволяет использовать их для проникновения в операционную среду ИС и вызова штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;

• Дыры, фрагменты кода программ, введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;

• Отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т. п.);

• Ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации [17].

Признак **местоположение** позволяет разделить программное обеспечение по следующим группам:

• в микропрограммах, прошивках;

• в средствах ОС, предназначенных для управления локальными ресурсами (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода / вывода, интерфейсом с пользователем и т. п.), драйверах, утилитах;

• в средствах ОС, предназначенных для выполнения вспомогательных функций [17].

Заключение

В статьи проанализированы и описаны самые распространённые угрозы и уязвимости присущие беспроводным сетям, составлены их классификации по предложенным признакам. Они позволяют строить профессиональные базы данных и прецедентов, дополнять информацией онтологии беспроводных сетей, автоматизировать процесс проектирования сетей, облегчать поиск мест возможных утечек информации, строить превентивные системы защиты от атак, несанкционированного доступа и нанесения ущерба при эксплуатации беспроводных сетей.

Список литературы

1. Канатьев К. Н., Большаков В. Н., Куприков О. Д. и др. Анализ угроз безопасности беспроводной сети и разработка оптимальных методов их предупреждения // *Инновации и инвестиции*. 2022. № 3, с. 116-123.
2. Башмаков А. В. Синтез защищенных локальных каналов передачи данных для мониторинга и управления движением судов: автореферат дис. … канд. техн. наук / специальность 05.13.06 "Автоматизация и управление технологическими процессами и производствами (по отраслям)". Санкт-Петербург, 2011. 24 с.

3. ГОСТ Р 56545 -2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016-04-01. М.: Стандартинформ, 2015. 22 с.
4. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016-04-01. М.: Стандартинформ, 2015. 22 с.
5. ГОСТ Р 56546 -2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Введ. 2015-08-19. М.: Стандартинформ, 2015. 17 с.
6. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Введ. 2015-11-01. М.: Стандартинформ, 2012. - 36 с.
7. Капарбек Б., Жалилов Г. Э. Анализ угроз информационной безопасности в беспроводных сетях // *Современные проблемы механики*. 2020, № 39(1), с. 42-49.
8. Качалкова С. В., Трусфус М. В., Мифтахова Л. Х. Анализ рисков и критических угроз в технологии беспроводной связи посредством методологии ETSI // *Вестник Технологического университета*. 2017. Т. 20, № 1, с. 128-131.
9. Чернышева А. Ф., Трубин И. С., Корепанов А. Г., Репкин Д. А. Классификация угроз информационной безопасности в когнитивных сетях связи // *Advanced Science*. 2017. № 4(8), С. 37.
10. Косачев А.С., Пономаренко В.Н. *Анализ подходов к верификации функций безопасности и мобильности.* М.: Триумф, 2004. 101 с.
11. Муханова А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // *Вестник Новосибирского государственного университета. Серия: Информационные технологии*. 2013. Т. 11, № 2, с. 55-72.
12. Новиков А.А., Устинов Г.Н. *Уязвимость и информационная безопасность телекоммуникационных технологий: учеб. пособие для вузов*. М.: Радио и связь, 2003. 296 с.
13. Отчет о безопасность роутеров в 2021 году // Securelist | Аналитика и отчеты о киберугрозах «Лаборатории Касперского» [Электронный ресурс]. URL: https://securelist.ru/router-security-2021/105481/ (дата обращения: 21.08.2023).
14. Соколов, А. В. О классификации, максимально совместимой с нечёткой классификацией // *Автоматизация и современные технологии*. 2013. № 8, с. 37-42.
15. Евглевская Н. В., Зуев А. Ю., Карасенко А. О., Лаута О. С. Сравнительный анализ эффективности существующих методов защиты сетей связи от DDoS-атак // *Радиопромышленность*. 2020. Т. 30, № 3, с. 67-74. DOI 10.21778/2413-9599-2020-30-3-67-74.
16. Чайкин П. В., Шабанов А. В. Применение WPA3 для решения проблем уязвимостей KARCK // *Актуальные проблемы деятельности подразделений УИС : Сборник материалов Всероссийской научно-практической конференции.* В 2-х частях,

Воронеж, 23 мая 2019 года. Том Часть 1. Воронеж: Издательско-полиграфический центр "Научная книга", 2019. С. 253-255.
17. Черемушкин, А. В. Криптографические протоколы: основные свойства и уязвимости // *Прикладная дискретная математика. Приложение*. 2009. № 2, с. 115-150.
18. Шелухин О.И., Симонян А.Г., Иванов Ю.А. Особенности DDoS атак в беспроводных сетях // *T-Comm: Телекоммуникации и транспорт*. 2012. Т. 6, № 11, с. 67-71.
19. Щербаков В.Б., Ермаков С.А., Бочаров М.И. *Анализ и управление рисками беспроводных сетей: учеб. пособие.* Воронеж: ГОУВПО «Воронежский государственный технический университет», 2008. 348 с.
20. Щербаков В.Б., Ермаков С.А. *Безопасность беспроводный сетей: стандарт IEEE 802.11*. М.: РадиоСофт, 2010. 256 с. ISBN 978-5-93274-020-0.
21. Guliyev I. F. ARP attack in Kali linux for pentesting secure transmission of packets // *European Journal of Technical and Natural Sciences*. 2020. No. 1-2, P. 12-15. DOI 10.29013/EJTNS-20-1.2-12-15.
22. IEEE std. 802.11 - 97 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications
23. IEEE Wireless Communication Standards: A Study of 802.11, 802.15, and 802.16, Todor Cooklev, Soflcover, 2004.

Classification of threats and vulnerabilities in wireless networks

Miloserdov, A.O.

milosalex@list.ru

Ulyanovsk State University, Russia

The paper presents a review and analysis of materials that can be useful to developers of wireless networks at the design and operation stage in the field of security. Types of network vulnerabilities, possible threats, attacks, and violations of integrity of transmitted messages are considered in detail and classified. These data allow to consider in advance possible dangerous situations with violation of safety integrity, to carry out necessary modeling of development of their variants, risk assessments and to provide measures for protection and safety in operation of the constructed network, as well as to improve the existing ones.

Keywords*: wireless network, security, threat to wireless networks, vulnerability of wireless networks, classification*