ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59162— 2020

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 6

Обеспечение информационной безопасности при использовании беспроводных IP-сетей

(ISO/IEC 27033-6:2016, NEQ)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 ноября 2020 г. № 1038-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 27033-6:2016 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей» (ISO/IEC 27033-6:2016 «Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 Федеральное агентство по техническому регулированию и метрологии не несет ответственности за патентную чистоту настоящего стандарта. Патентообладатель может заявить о своих правах и направить в национальный орган по стандартизации аргументированное предложение о внесении в настоящий стандарт поправки для указания информации о наличии в стандарте объектов патентного права и патентообладателе

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В современном мире большинство коммерческих и государственных организаций обладают собственными информационными системами, оснащенными сетевыми соединениями одного или нескольких типов:

- внутри организации;
- между разными организациями;
- между организацией и широким кругом лиц.

В условиях быстрого развития общедоступных сетевых технологий (в частности, сети Интернет), обеспечивающих существенные коммерческие возможности, организации все чаще реализуют электронный бизнес в глобальном масштабе и предоставляют общедоступные онлайн-сервисы. Возможности включают в себя как просто обеспечение более дешевой передачи данных и использование сети Интернет в качестве среды передачи данных, так и более сложные услуги, предлагаемые Интернет-провайдером (ISP). При этом на каждом конечном узле доступа к полнофункциональным системам электронной торговли и доставки услуг с использованием веб-приложений могут использоваться относительно недорогие локальные точки подключения. Помимо этого, новые технологии, такие как интеграция данных, голоса и видео, расширяют возможности удаленной (дистанционной) работы, что позволяет персоналу в течение значительных периодов времени работать дистанционно. Эти технологии могут поддерживать связь посредством использования средств удаленного доступа к сетям организации и сообществ, а также получать необходимую информацию и услуги для поддержки своей работы.

Хотя подобная среда обеспечивает для бизнеса существенные преимущества, она добавляет новые риски безопасности, которыми необходимо управлять. Поскольку деятельность организации сильно зависит от использования информации и соответствующих информационных сетей, утрата конфиденциальности, нарушение целостности и доступности информации и услуг могут оказать существенное негативное влияние на работу организации. В предотвращение появления новых рисков безопасности информации необходимо устанавливать требования по защите сетей и связанных с ними информации и информационных систем. Другими словами, внедрение и поддержание соответствующей безопасности сети абсолютно необходимы для успеха деловой деятельности любой организации.

Поэтому отрасли телекоммуникаций и информационных технологий ищут экономически эффективные комплексные решения безопасности, направленные на защиту сетей от вредоносных атак и непреднамеренных неправильных действий, а также удовлетворяющие требованиям в отношении конфиденциальности, целостности и доступности информации и услуг. Безопасность сети также имеет важное значение для обеспечения надлежащего учета и использования информации. Функции безопасности, заложенные в продукты[1)], являются критически важными для безопасности сети в целом, включая приложения и сервисы. При этом по мере возрастания числа продуктов, которые объединяются для обеспечения общих решений, их совместимость или ее отсутствие является определяющим фактором успешности решений. Безопасность должна быть не только жизненно важным аспектом для каждого продукта или услуги, но и должна разрабатываться таким образом, чтобы способствовать интеграции функций безопасности в рамках общего решения по обеспечению защиты.

Целью комплекса стандартов ГОСТ Р ИСО/МЭК 27033 является предоставление подробных инструкций по аспектам безопасного контроля, эксплуатации и использования сетей информационных систем и их взаимосвязей. Сотрудники организаций, ответственные за информационную безопасность в целом и за безопасность сетей в частности, должны иметь возможность адаптировать материалы настоящего стандарта к требованиям своих организаций. Основными задачами частей ГОСТ Р ИСО/МЭК 27033 являются:

- ГОСТ Р ИСО/МЭК 27033-1 направлен на определение и описание концепций, связанных с безопасностью сети и предоставление рекомендаций по менеджменту безопасности сети. Стандарт содержит общий обзор безопасности сети и связанных с ней определений, рекомендации по идентификации и анализу рисков безопасности сети, кроме того, определение требований безопасности сети. В нем также рассказывается о том, как добиться хорошего качества специализированных архитектур безопасности, а также об аспектах рисков, дизайна и управления, связанных с типичными сетевыми

[1)] В настоящем стандарте под «продуктом» следует понимать «изделия/средства (программные, технические или программно-технические)».

сценариями и областями сетевых технологий, которые подробно рассматриваются в последующих частях ГОСТ Р ИСО/МЭК 27033;

– часть, определяющая, каким образом организации, используя при необходимости последовательный подход к планированию, проектированию и реализации безопасности сети с применением моделей/систем, должны добиваться требуемого качества специализированных архитектур безопасности сети, а также проектирования и реализации, которые обеспечат уверенность в безопасности сети, соответствующей их среде деятельности, приведена в [1]. В данном контексте термины «модель/система» используются для общего представления структуры и функционирования специализированной архитектуры и проекта безопасности. Данный стандарт предназначен для всего персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры безопасности сети (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за безопасность сети);

- ГОСТ Р ИСО/МЭК 27033-3 направлен на определение конкретных рисков, методов проектирования и вопросов, касающихся мер обеспечения ИБ, связанных с типовыми сетевыми сценариями. Данный стандарт предназначен для персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры безопасности сети (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за безопасность сети);

- часть, направленная на определение конкретных рисков, методов проектирования и вопросов, касающихся меры обеспечения информационной безопасности информационных потоков между сетями с использованием шлюзов безопасности, приведена в [2]. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию шлюзов безопасности (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за безопасность сети);

- часть, направленная на определение конкретных рисков, методов проектирования и вопросов, касающихся мер обеспечения информационной безопасности соединений, установленных с использованием VPN, приведена в [3]. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности виртуальных частных сетей (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за безопасность сети);

- настоящий стандарт направлен на определение конкретных рисков, методов проектирования и вопросов, касающихся мер обеспечения ИБ беспроводных сетей и радиосетей. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности беспроводных сетей и радиосетей (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за безопасность сети).

Следует подчеркнуть, что комплекс стандартов ГОСТ Р ИСО/МЭК 27033 предоставляет дополнительные детализированные рекомендации по реализации мер обеспечения безопасности сети, определенных в базовом стандарте ГОСТ Р ИСО/МЭК 27002.

Следует отметить, что настоящий стандарт не является справочным или нормативным документом для регулирующих и законодательных требований безопасности. Хотя в нем подчеркивается важность этих оказывающих влияние факторов, они не могут быть сформулированы конкретно, так как зависят от страны, вида основной деятельности и т. д.

Если не указывается иное, приводимые в настоящем стандарте требования применимы к действующим в настоящее время и (или) планируемым сетям, но в тексте настоящего стандарта будут применены только термины «сеть» или «сети».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 6

Обеспечение информационной безопасности при использовании беспроводных IP-сетей

Information technology. Security techniques. Network security. Part 6. Securing wireless IP network access

Дата введения — 2021—06—01

1 Область применения

В настоящем стандарте описаны угрозы, требования к информационной безопасности (ИБ), меры по контролю и проектированию систем безопасности, связанные с беспроводными сетями. Настоящий стандарт содержит рекомендации по выбору, реализации и мониторингу мер по обеспечению безопасности обмена информации через беспроводные сети. Информация, содержащаяся в настоящем стандарте, предназначена для использования при пересмотре технической архитектуры/вариантов проектирования безопасности, а также при выборе и документировании предпочтительной технической архитектуры/проектирования безопасности и связанных с ними мер обеспечения ИБ.

В целом настоящий стандарт будет способствовать всестороннему определению и реализации мер безопасности для беспроводной сетевой среды любой организации. Он предназначен для пользователей и разработчиков, ответственных за реализацию и функционирование технических мер и средств контроля для обеспечения безопасности беспроводных сетей.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27033-1 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепция

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального органа исполнительной власти в сфере стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 27000, ГОСТ Р ИСО/МЭК 27033-1, а также следующие термины с соответствующими определениями:

3.1 **точка (беспроводного) доступа** (access point, wireless access point): Устройство или оборудование, позволяющие беспроводным устройствам подключаться к проводной сети.

Примечание — Подключение использует беспроводную локальную сеть (WLAN) или соответствующий стандарт.

3.2 **(беспроводная) базовая станция** (base station, wireless base station): Оборудование, обеспечивающее соединение между мобильными или сотовыми телефонами и базовой коммуникационной сетью.

3.3 **Bluetooth:** Стандарт беспроводной технологии для обмена данными на короткие расстояния.

Примечание — «Bluetooth» — торговая марка, принадлежащая Bluetooth SIG.

3.4 **базовая сеть** (core network): Часть мобильной телекоммуникационной сети, которая подключает сеть доступа к коммуникационной сети большего охвата.

Пример: Интернет и прочие сети общего доступа являются примерами сетей большего охвата.

3.5 **фемтосота; домашняя сота; малая сота** (femto cell; home cell; small cell): Маломощная и миниатюрная базовая станция (3.2) сотовой связи.

Примечание — Фемтосоты обычно используются для обслуживания небольшой территории (офиса небольшой организации или дома).

3.6 **усиление защиты** (hardening): Процесс повышения защищенности системы и сокращения ее уязвимостей.

Примечание — Как правило, процесс усиления защиты обычно включает в себя удаление ненужного программного обеспечения, ненужных имен и логинов пользователей, а также отключение или удаление ненужных служб.

3.7 **межмашинная коммуникация** (machine to machine): Технология, позволяющая как беспроводным, так и проводным системам связываться с другими устройствами того же типа.

3.8 **отношение мощностей; отношение сигнал/шум** (power ratio, signal-to-noise ratio): Величина, используемая для сравнения требуемого уровня сигнала с уровнем фонового шума.

Примечание — Определяется отношением мощности сигнала к мощности шума.

3.9 **сеть радиодоступа** (radio access network): Часть системы мобильной связи, в которой реализована технология радиодоступа, например, WCDMA или LTE, обеспечивающая доступ устройств конечных пользователей к *базовой сети* (3.4).

Примечание — Сеть радиодоступа находится между устройством конечного пользователя и базовой сетью.

3.10 **контроллер радиосети** (radio network controller) Компонент мобильной сети, который управляет базовыми станциями, взаимодействует с базовой сетью (3.4) и выполняет функции управления радиоресурсами и мобильностью в сети.

3.11 **Wi-Fi:** Технология беспроводных локальных сетей, позволяющая электронным устройствам подключаться к сети, в основном используя диапазоны 2,4 ГГц и 5 ГГц.

Примечания

1 «Wi-Fi» является торговой маркой Wi-Fi Alliance.

2 «Wi-Fi» обычно используется в качестве синонима «WLAN», поскольку большинство современных WLAN основаны на стандартах Wi-Fi.

3.12 **беспроводная самоорганизующаяся сеть; сеть Ad-hoc Wi-Fi** (Wi-Fi Ad-Hoc network; wireless ad-hoc network): Децентрализованная беспроводная сеть, не имеющая постоянной структуры.

Примечание — Предопределенную структуру обеспечивают, например, маршрутизаторы в проводных сетях или точки доступа (3.1) в управляемых беспроводных сетях (инфраструктура).

4 Сокращения

В настоящем стандарте применены следующие сокращения:

3G — третье поколение технологии мобильной связи

3GPP — проект партнерства третьего поколения (Third Generation Partnership Project)

4G — четвертое поколение технологии мобильной связи

5G — пятое поколение технологии мобильной связи

BYOD — концепция использования собственных устройств сотрудников (Bring Your Own Device)

DoS — отказ в обслуживании (Denial of Service)

ETSI — Европейский институт по стандартизации в области электросвязи (European Telecommunications Standards Institute)

FTP — протокол передачи файлов (File Transfer Protocol)

HTTP — протокол передачи гипертекста (Hyper Text Transfer Protocol)

IDS — система обнаружения вторжений (Intrusion Detection System)

IEEE — Институт инженеров электроники и электротехники (Institute of Electrical and Electronics Engineers)

IMAP — протокол доступа к электронной почте (Internet message access protocol)

IMEI — международный идентификатор мобильного оборудования (International Mobile Equipment Identity)

IMSI — международный идентификатор мобильного абонента (International Mobile Subscriber Identity)

IP — Интернет-протокол (Internet Protocol)

IPS — система предупреждения вторжений (Intrusion Prevention System)

IPsec — протокол безопасного обмена по протоколу IP (Internet Protocol Security)

ISM — диапазон частот оборудования — промышленность-наука-медицина (Industrial, Scientific and Medical)

ISP — Интернет-провайдер (Internet Service Provider)

LTE — стандарт беспроводной высокоскоростной передачи данных (Long Term Evolution)

MAC — управление доступом к среде (Media Access Control)

MIC — код целостности сообщения (Message Interface Code)

NIC — плата сетевого интерфейса (Network Interface Card)

OBEX — обмен объектами (Object exchange)

PIN — персональный идентификационный номер (Personal Identification Number)

PLMN — наземная сеть мобильной связи общего пользования (Public Land Mobile Network)

POP — почтовый протокол (Post Office Protocol)

RAN — сеть радиодоступа (Radio Access Network)

RBAC — управление доступом на основе ролей (Role Based Access Control)

RFCO — протокол радиосвязи (Radio Frequency Communication)

SAC — Администрация стандартизации Китая (Standardization Administration of China)

SIG — специальная группа интересов (Special Interest Group)

SLA — соглашение об уровне обслуживания (Service Level Agreement)

SIM — модуль идентификации абонента (Subscriber Identity Module)

SNMP — простой протокол сетевого управления (Simple Network Management Protocol)

SMTP — простой протокол передачи почты (Simple Mail Transfer Protocol)

SSH — безопасная оболочка — сетевой протокол (Secure Shell)

SSID — символьное название беспроводной точки доступа (Service Set Identifier)

TCP — протокол управления передачей (Transmission Control Protocol)

UICC — универсальная карта с интегральной схемой (Universal Integrated Circuit Card)

UE — оборудование пользователя (User Equipment)

USB — универсальная последовательная шина Universal Serial Bus

UWB — сверхширокая полоса (Ultra-Wide Band)

VLAN — виртуальная локальная вычислительная сеть (Virtual Local Area Network)

VPN — виртуальная частная сеть (Virtual Private Network)

WAI — инфраструктура аутентификации WLAN (WLAN Authentication Infrastructure)

WAPI — инфраструктура аутентификации и конфиденциальности WLAN (WLAN Authentication and Privacy Infrastructure)

WCDMA — технология радио-интерфейса, использующая широкополосный множественный доступ с кодовым разделением каналов (Wideband Code Division Multiple Access)

WEP — безопасность, эквивалентная проводной сети (Wireless Equivalent Privacy)

WIDS — система обнаружения вторжений через беспроводные сети (Wireless Intrusion Detection System)

WIPS — система предотвращения вторжений через беспроводные сети (Wireless Intrusion Prevention System)

WLAN — беспроводная локальная вычислительная сеть (Wireless Local Area Network)

WMAN — беспроводная сеть масштаба города (Wireless Metropolitan Area Network)

WPA — защищенный доступ в беспроводных сетях Wi-Fi (Wi-Fi Protected Access)

WPAN — персональная беспроводная сеть (Wireless Personal Area Network)

ААА — аутентификация, авторизация и аудит

ДМЗ — демилитаризованная зона

ИБ — информационная безопасность

ИТ — информационные технологии

ПИН-код — персональный идентификационный номер

ПК — персональный компьютер

ДИБ — директор по информационной безопасности

СВЧ — сверхвысокие частоты

ТД — точка доступа

УВЧ — ультравысокая частота

5 Структура

В настоящий стандарт входят следующие разделы:

- основные категории беспроводных IP-сетей и особенности их безопасности (раздел 6);
- угрозы безопасности (раздел 7);
- требования к безопасности (раздел 8);
- меры обеспечения ИБ (раздел 9);
- методы и аспекты проектирования систем безопасности (раздел 10).

6 Основные категории беспроводных IP-сетей и особенности их безопасности

Все больше пользователей услуг связи и устройств обработки данных переходят на беспроводные интерфейсы, позволяющие подключаться к нужным сетям. Имеющие повсеместное распространение беспроводные сети предлагают пользователям преимущества экономичного и постоянного доступа с автоматической настройкой соединения, в качестве альтернативы проводным соединениям. Привлекательность использования беспроводных сетей обусловлена наличием нелицензируемых частотных диапазонов, высокой стоимостью прокладки кабельной инфраструктуры в построенных или старых помещениях, офисах или жилых помещениях, а также гибкостью подключения к сети новых пользователей.

Например, в большинстве стран для подключения к сети Wi-Fi требуется лишь обратиться к Интернет-провайдеру. После чего производится подключение к беспроводной точке доступа или к маршрутизатору, которые и являются приемопередатчиками сигнала. Платы сетевого интерфейса (NIC) обычно входят в состав устройств связи или компьютера, поэтому для подключения к беспроводной сети пользователю нужно всего лишь включить такой интерфейс.

Развертывание мобильных и сотовых сетей сопряжено с куда большими проблемами. В некоторых странах существуют ограничения на частотный диапазон для определенных беспроводных технологий. Процесс планирования, высвобождения и выделения частотного диапазона национальными регулирующими органами может занимать несколько лет. В зависимости от технологии (3G, 4G) ширина необходимой полосы частот может быть различной. Стоимость получения лицензий для поставщиков услуг может быть существенной.

В следующих подразделах приводится описание основных категорий беспроводных IP-сетей с примерами важнейших технологий.

6.1 Персональные беспроводные сети (WPAN)

Персональные беспроводные сети — это небольшие беспроводные сети, требующие минимальной инфраструктуры или не требующие ее совсем. Сети WPAN через беспроводное подключение позволяют связываться и взаимодействовать друг с другом переносным и мобильным компьютерным устройствам, таким как ПК, карманные ПК, периферийное оборудование, мобильные телефоны, пейджеры и потребительская электроника. В качестве примеров технологий WPAN можно привести:

- Bluetooth. Беспроводная технология для обмена данными на коротких расстояниях между стационарными и мобильными устройствами, а также для создания WPAN с беспроводным доступом для небольших переносных устройств с использованием СВЧ-диапазона ISM для промышленного, научного и медицинского оборудования в пределах от 2,4 до 2,485 ГГц. В первой версии Bluetooth максимальная скорость передачи данных составляла около 720 килобит в секунду (кбит/с), а Bluetooth 2.0 поддерживает скорость передачи до 3 Мбит/с. Теоретическая скорость передачи данных по Bluetooth 3.0 ограничена 24 Мбит/с. В Bluetooth реализованы функции обеспечения конфиденциальности, аутентификации и получения ключей на базе блочного шифрования[1)]. Ключи Bluetooth, как правило, генерируются с использованием ПИН-кода Bluethooth, который вводится на обоих устройствах;
- Сверхширокая полоса (UWB). Эта технология широкополосной связи ближнего действия характерна очень низким уровнем мощности и использованием при этом большей части частотного диапазона. В пределах ближнего действия скорость передачи может достигать 480 Мбит/с. При этом поддерживается полный спектр функций WPAN, таких как получение данных с датчиков, точное определение местонахождения и отслеживание. Для аутентификации и установления доверительной связи между двумя UWB-устройствами используется общий универсальный ключ. Безопасность достигается шифрованием конфиденциальной информации, а целостность обеспечивается путем включения кода целостности сообщения (MIC);
- ZigBee. Технология для небольших сетей WPAN, разработанная для недорогих беспроводных сенсорных и управляющих сетей с низким энергопотреблением, таких как системы климат-контроля и освещения зданий. ZigBee представляет возможность безопасной связи с защитой создания и передачи ключей шифрования, фреймов шифрования и управляющих устройств.

6.2 Беспроводные локальные вычислительные сети (WLAN)

Беспроводная локальная вычислительная сеть (WLAN) представляет собой группу узлов в пределах ограниченного географического пространства, способных осуществлять обмен информацией, используя радиосвязь. Как правило, сети WLAN используются устройствами в пределах ограниченного пространства, например, в здании или в комплексе зданий. Такие сети обычно являются расширением существующих проводных локальных сетей для обеспечения повышенной мобильности пользователей. Примерами технологий WLAN являются:

- Wi-Fi — является торговым знаком и представляет собой любой продукт WLAN, работающий по стандартам 802.11[2)] Института инженеров электроники и электротехники (IEEE);
- HiperLAN представляет собой европейскую альтернативу стандартам IEEE 802.11. HiperLAN — это технология цифровой высокоскоростной беспроводной связи в диапазонах 5,15—5,3 ГГц и 17,1—17,3 ГГц, разработанная Европейским институтом по стандартизации в области электросвязи (ETSI);
- WAPI — инфраструктура аутентификации и конфиденциальности WLAN является альтернативой механизму безопасности стандартов IEEE 802.11, разработанной Администрацией стандартизации Китая (SAC).

6.3 Беспроводные сети масштаба города (WMAN)

WMAN — это сети, которые обеспечивают подключение пользователей, находящихся на разных объектах, как правило, в пределах нескольких километров друг от друга. Различные варианты реализации WMAN обеспечивают беспроводной широкополосный доступ для клиентов в городах. Примерами технологий WMAN являются:

---

1) Здесь и далее по тексту под термином «шифрование» понимать алгоритмическое преобразование информации.

2) IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6; 5 и 60 ГГц.

- WiMAX. Технология беспроводной связи, обеспечивающая скорость передачи от 30 до 40 Мбит/с. Обновление 2011 года увеличило возможную скорость для стационарных устройств до 1 Г/с, обеспечивая домашний или мобильный интернет-доступ для целых городов или стран;

- 3G. Третье поколение технологии мобильной связи. Сети 3G поддерживают службы, обеспечивающие передачу данных на скорости не менее 200 кбит/с. Со временем технология 3G обеспечила возможность широкополосного доступа со скоростью до нескольких мегабит в секунду для смартфонов и мобильных модемов, используемых в ноутбуках. Технология 3G находит применение для беспроводной голосовой телефонии, мобильного интернет-доступа, стационарного беспроводного интернет-доступа, видеозвонков и мобильного ТВ;

- 4G. Четвертое поколение технологии мобильной связи. Помимо обычной голосовой связи и прочих услуг 3G, система 4G обеспечивают более высокую скорость мобильного интернет-доступа, например, для ноутбуков с беспроводными USB-модемами, смартфонов и прочих мобильных устройств. Несмотря на то, что стандарт 4G пришел на смену технологии 3G, в процессе перехода с 3G на 4G могут возникнуть значительные трудности из-за недостаточной совместимости. В качестве очевидных областей применения можно указать улучшенный интернет-доступ для мобильных устройств, IP-телефонию, игры, мобильное ТВ с высоким разрешением, видеоконференции, 3D-телевидение и облачные вычисления;

- 5G. Пятое поколение технологии мобильной связи, действующее на основе стандартов телекоммуникаций, следующих за существующими стандартами 4G. Технологии 5G должны обеспечивать более высокую пропускную способность по сравнению с технологиями 4G, что позволит обеспечить большую доступность широкополосной мобильной связи, а также использование режимов прямого соединения между абонентами, сверхнадежные масштабные системы коммуникации между устройствами, а также меньшее время задержки, скорость сети Интернет 1—2 Гбит/с и меньший расход энергии, чем у 4G-оборудования, что благоприятно скажется на развитии интернета вещей.

6.4 Особенности безопасности беспроводных сетей

В беспроводных сетях есть ряд общих проблем безопасности, которые необходимо учитывать и разрешать независимо от типа используемой технологии.

В любой беспроводной сети передача информации может быть обнаружена любым устройством, способным принимать и обрабатывать передаваемые таким образом данные. Поэтому, в отличие от проводной сети, где сигналы передаются только на физически подключенные устройства, в беспроводных сетях, передатчик сигналов может не «знать», какие устройства эти сигналы принимают. Кроме того, доступны технологии, позволяющие создавать помехи для передаваемого сигнала и нарушать работу беспроводной сети, влияя таким образом на качество услуг, предоставляемых сетью. Следовательно, для безопасности сети необходимо, чтобы обеспечивались:

- конфиденциальность: передаваемая информация не должна разглашаться;
- целостность: передаваемая информация не должна изменяться при передаче;
- доступность: услуги сети должны быть доступны;
- аутентификация: подлинность пользователей или объектов, запрашивающих доступ к сети, должна быть подтверждена;
- контроль доступа: доступ к сетям и точкам доступа должен контролироваться;
- подконтрольность: любое нарушение политики должно быть прослежено до конкретного пользователя или субъекта.

Вышеуказанные принципы ИБ применимы для любых сетей. Для беспроводных сетей имеются дополнительные факторы, обусловленные особой средой передачи. Например, гораздо проще задействовать радиочастотное устройство глушения, так как оно не требует непосредственного подключения к кабельной системе здания, чем электронное устройство, создающее помехи в кабельной системе здания. Кроме того, часть устройств, подключенных к сети через беспроводной интерфейс, скорее всего будет иметь соединение с интернетом или через них будет проходить интернет-трафик, следовательно, для этих устройств должны быть рассмотрены и разрешены вопросы ИБ, присущие всем сетям связи, включая и беспроводные сети.

В целях обеспечения соответствия беспроводных сетей принципам ИБ, необходимо понять, каким типам угроз потенциально подвержены беспроводные сети. В разделе 7 рассматриваются угрозы безопасности информации, в том числе и типичные для беспроводных сетей технические угрозы, которые влекут за собой нарушение свойств безопасности информации: конфиденциальности, целостности, до-

ступности, аутентификации, контроля доступа и подконтрольности, при реализации деловой деятельности.

В разделе 8 приводится описание общих требований безопасности для беспроводных сетей и устройств, подключаемых к сети и использующих ее. В разделе 9 описываются общие меры обеспечения ИБ для выполнения требований безопасности в целях предотвращения потенциальных угроз.

В процессе деловой активности в местах, где доступны соответствующие услуги, т. е. дома, на улице, в корпоративной среде, общественных местах и на промышленных объектах, используются многочисленные и разнообразные беспроводные устройства.

При рассмотрении угроз, требований, мер обеспечения ИБ необходимо учитывать поведение пользователей, типы пользовательских устройств, объем и тип используемых информационных ресурсов, и переменную совокупность угроз. Действительно, для организаций и/или предприятий и поставщиков услуг изменившееся поведение пользователей и новые возможности беспроводных устройств требуют оценки новых «беспроводных» угроз безопасности. Такую оценку должны проводить специалисты ИБ, ответственные за внедрение, мониторинг и соблюдение четкой политики использования сети Интернет.

В настоящем стандарте описаны угрозы, требования, меры обеспечения ИБ и методы проектирования, характерные для беспроводных сетей.

7 Угрозы безопасности

7.1 Общая информация

В данном разделе приводится список типичных угроз безопасности, актуальных для беспроводных сетей. Необходимо учитывать, что по мере разработки новых стандартов беспроводной связи будут появляться новые угрозы, а существующие угрозы могут эволюционировать. Для того, чтобы иметь возможность применять новые меры обеспечения ИБ для противодействия потенциальным новым угрозам, поставщики услуг и администраторы беспроводных сетей должны самостоятельно знакомиться с новыми разработками технологий беспроводной связи.

Несанкционированный доступ может привести к раскрытию конфиденциальной информации, модификации данных, отказу в обслуживании и незаконному использованию ресурсов. После того как неавторизованный пользователь получил доступ к сети, мониторинг незащищенных данных может привести к перехвату имен пользователей и паролей, которые затем могут быть использованы для дальнейших атак. Беспроводные сети подвержены всем угрозам безопасности, которые обычно присущи традиционным проводным сетям, но, кроме того, они подвержены угрозам, непосредственно связанным с технологией беспроводного доступа. В самой природе большинства беспроводных сред заложена практическая неосуществимость задачи по ограничению распространения радиосигналов какой-либо контролируемой территорией. Излучаемые сигналы подвергаются тайному перехвату и эксплуатации. В традиционной инфраструктуре проводной связи физическая безопасность на собственном рабочем месте или в помещении поставщика услуг обеспечивает определенную степень защиты сети, поскольку пользователи должны физически подключаться к сети для доступа к ее ресурсам. В беспроводной среде этот способ защиты применяться не может, в связи с чем необходимо пересмотреть весь перечень актуальных угроз.

7.2 Несанкционированный доступ

Беспроводные сети подвержены тем же угрозам несанкционированного доступа, что и проводные сети. Беспроводной доступ к сетям может обуславливать появление новых угроз безопасности в случаях, если общедоступная информация о сети может подсказать направление дальнейших исследований для получения доступа. Например, идентификаторы и настройки беспроводных точек доступа могут быть подсказками для дальнейшего исследования беспроводной сети. Получение доступа к беспроводной сети открывает канал доступа к другим ресурсам этой сети.

Предотвращение доступа к ресурсам не входит в область применения настоящего стандарта.

7.3 Анализ пакетов

Прослушивание соединений незашифрованных беспроводных сетей является простой задачей. Для прослушивания таких беспроводных сетей требуется антенна со стандартными инструментами, а также анализатор трафика (анализатор сетевых пакетов). Анализатор сетевых пакетов — это про-

грамма, с помощью которой сетевой интерфейс переводится в режим прослушивания. Это означает, что интерфейс будет принимать и обрабатывать весь поступающий трафик, а не только тот, который для него предназначен. Анализатор сетевых пакетов предоставляет пользователю все сетевые пакеты в удобном для чтения виде. Весь открытый трафик в текстовом виде легко читается, а для поиска определенных ключевых слов или значений можно применять фильтры. Существует несколько протоколов и сервисов открытого текста. Примерами могут служить протоколы: HTTP, POP, IMAP, SMTP, FTP и ICQ. С помощью анализатора трафика можно получить имена пользователей, пароли и частные данные из почты и сообщений

Для выявления атак, связанных с анализом пакетов, разработаны специальные инструменты. Эти инструменты для выявления анализаторов беспроводной сети обычно отслеживают сетевой трафик или сканируют сетевые интерфейсы в режиме прослушивания. Примерами инструментов для анализа трафика беспроводных сетей (анализаторов пакетов) являются Wireshark и Snoop.

Использование технически сложных антенн в сетях Wi-Fi и других беспроводных сетях (например, Bluetooth) повышает уровень сигнала, но при этом облегчает прослушивание и увеличивает дальность прослушивания. Хотя прослушивание и является пассивным видом деятельности, на его основе могут развиваться другие виды атак, такие как, например, перехват сессии или атака через посредника, при которых происходит перехват и изменение сообщений между пользователем и точкой беспроводного доступа с целью получения несанкционированного доступа к информации или устройству.

На начальном этапе своего развития сотовые и мобильные сети были подвержены прослушиванию. Однако по мере развития сетевых функций и расширения использования этих сетей, что подразумевало передачу через них информации ограниченного доступа, для интерфейсов точек доступа таких сетей были разработаны спецификации шифрования данных.

Однако у нарушителей имеются более простые пути, по сравнению со взломом сложных кодов шифрования. В некоторых случаях многорежимный мобильный телефон может быть переключен на небезопасную устаревшую сеть радиодоступа, что значительно облегчает задачу прослушивания трафика. В некоторых стандартах эта угроза известна как принудительное переключение на устаревшую технологию радиодоступа.

7.4 Фальшивая точка беспроводного доступа

Даже если все точки беспроводного доступа Wi-Fi безопасны, любой сотрудник может легко подключить собственную беспроводную точку доступа в своем офисе безотносительно к безопасности. Такое действие эффективно обойдет большинство мер обеспечения ИБ и, возможно, даже вызовет радиопомехи, препятствующие нормальной работе организации или предприятия. Фальшивая беспроводная точка доступа также может быть намеренно установлена скрытно, чтобы предоставить нарушителю легкий доступ к сети как локально, так и удаленно. Нарушитель (также известный как «evil twin») может также заменить существующую беспроводную точку доступа своей точкой, полностью контролируемую им, или даже установить фальшивую беспроводную точку доступа с настройками, аналогичными законной точке доступа, но с более мощным сигналом. После того, как законный пользователь попадает в ловушку и подключается к фальшивой точке доступа, становится возможен сбор информации ограниченного доступа.

В наземных сетях мобильной связи общего пользования (PLMN) гораздо сложнее развернуть «фальшивую» точку радиодоступа или базовую станцию, поскольку обычно существуют физические барьеры или средства защиты, препятствующие таким попыткам. Большая часть оборудования мобильной сети размещается в специальных помещениях или на особых объектах, доступ к которым нарушителям для размещения своего оборудования получить трудно.

Тем не менее, если речь идет о малых сотах для отдельных объектов, домашних сотах или фемтосотах, оборудование может быть установлено в помещении организации или клиента. В таких случаях возможность установки нарушителем собственной базовой станции не исключается. Нарушитель, однако, должен решить задачу проверки подлинности своей базовой станции в сети. Базовые станции централизованно контролируются оператором PLMN, сигналы о любых событиях, связанных с безопасностью и об ухудшении показателей качества связи в сети в зоне действия фальшивой соты, скорее всего, будут отправлены оператору и привлекут его внимание. Поэтому, несмотря на возможность организовать локальную атаку «отказ в обслуживании» (DoS) или бесплатно пользоваться мобильной связью некоторое время, последствия такой атаки через фальшивую точку беспроводного доступа будут ограничены.

7.5 Атака «Отказ в обслуживании»

Суть атаки «отказ в обслуживании» (DoS) состоит в исчерпании ресурсов памяти и (или) вычислительных возможностей жертвы с целью существенного замедления работы или, в идеале, прекращения предоставления ей услуг. Подвергающийся атаке система тратит столько ресурсов на обработку получаемого от нарушителя трафика, что не имеет возможности обрабатывать обычный сетевой трафик.

Результатом DoS-атаки является ухудшение качества или прекращение правомерного доступа к сетевым ресурсам. Из-за открытости носителя, динамически меняющейся топологии, совместно используемых алгоритмов, децентрализации протоколов и отсутствия четкого периметра защиты беспроводная сеть особенно уязвима для DoS-атак, которые и представляют собой острую проблему в современных сетях. Многие из методов защиты, разработанных для проводных сетей, не применимы в мобильной среде беспроводных сетей.

Одним из грубых методов проведения DoS-атаки является создание радиочастотных помех — распространение атакующим устройством электронных сигналов или импульсов в частотном диапазоне беспроводных сетей, находящихся поблизости от такого устройства. Случай, когда радиочастотный сигнал отправляется либо короткими пакетами, либо с перерывами, называют скремблингом, выявить который сетевому оператору сложнее.

Другая разновидность DoS-атаки упоминалась в предыдущем разделе, когда фальшивая точка доступа может вызвать отказ в обслуживании пользователей, пытающихся получить доступ к сети.

При более сложном сценарии нарушитель может многократно отправлять допустимые сообщения на мобильное устройство с ограниченным запасом мощности (например, удаленное устройство, в результате чего такое устройство истощает заряд аккумулятора раньше, чем было запланировано).

Другой разновидностью этого типа атак является fuzzing-атаки, которые заключаются в отправке недопустимых или иных нестандартных сообщений, или данных на устройство и наблюдении за тем, как устройство реагирует. Замедление или прекращение реакции устройства в результате этих атак может послужить основой будущей DoS-атаки.

7.6 Атаки через Bluetooth

В общедоступных источниках описаны многочисленные атаки, в основе которых лежали ошибки реализации или погрешности системы безопасности Bluetooth.

Известны следующие примеры:

a) Bluedumping: атака, основанная на обратном расчете ПИН-кода пользователя, с использованием перехваченного обмена данными между парой устройств;

b) Bluesnarfing: позволяет нарушителю из-за ошибок реализации в протоколе OBEX Push получить через Bluetooth-соединение несанкционированный доступ к персональным данным, таким как телефонная книга и база данных встреч на устройствах: телефонах, настольных ПК, ноутбуках и карманных ПК;

c) Bluebugging: использует скрытые каналы Bluetooth RFCOMM и позволяет нарушителю удаленно управлять большинством функций телефона, в том числе совершать несанкционированные вызовы и включать микрофоны, чтобы превратить телефон в подслушивающее устройство («жучок»);

d) Bluejacking — это атака, использующая недостатки безопасности профиля OBEX на мобильных устройствах с поддержкой технологии Bluetooth, например, мобильных телефонах. Нарушитель начинает атаку bluejacking с отправки несогласованных с получателем сообщений на его устройство с поддержкой Bluetooth. Сами по себе такие сообщения не наносят вреда устройству пользователя, но могут каким-либо образом вовлечь пользователя в обмен сообщениями или побудить его добавить новый контакт в адресную книгу устройства. Атака с отправкой сообщений напоминает спам и фишинг через электронную почту. Bluejacking может нанести вред в том случае, когда пользователь отвечает на сообщение нарушителя;

e) Bluestabbing: нарушитель изменяет имя своего устройства Bluetooth на имя с неправильным форматом, что приводит к сбою других устройств Bluetooth при попытках обнаружить другие находящиеся поблизости устройства;

f) Bluebumping: с использованием методов социальной инженерии, при которой использует тот факт, что парная связь в реальности не удалятся до тех пор, пока оба парных устройства не удаляют соединение. Используя социальную инженерию, нарушитель убеждает жертву осуществить сопряжение с устройством, которое в дальнейшем будет источником атаки. Несмотря на то, что жертва впоследствии

удалит сопряжение со своего устройства, нарушитель этого не сделает, тем оставив скрытую «заднюю дверь» в устройство жертвы;

g) Bluesmacking: результатом запросов неправильного формата будет «ping of death», вызывающий сбой на всех устройствах, на которые отправляются запросы.

7.7 Угрозы в сетях Ad-hoc

Как правило, сеть Wi-Fi создается путем подключения беспроводных устройств к точкам беспроводного доступа или беспроводным маршрутизаторам, однако существует возможность создания сетей Ad-hoc непосредственно между двумя или более устройствами с поддержкой Wi-Fi. Даже если устройства не подключены напрямую друг к другу, они все равно могут быть связаны друг с другом через другой общий компьютер или компьютеры.

В некоторых операционных системах сети Ad-hoc включены по умолчанию. Поэтому любой в непосредственной близости от передающего компьютера может попытаться подключиться к нему и получить доступ к общим документам. Эта проблема особенно актуальна, когда пользователи не используют шифрование при обмене данными через сеть Ad-hoc.

7.8 Прочие угрозы

Кроме перечисленных выше возможны и другие угрозы:

- неправильная маршрутизация/изменение маршрутов сообщений и пакетов;
- перехват международного идентификатора мобильного абонента (IMSI);
- отслеживание оборудования пользователя (UE);
- принудительная передача данных (forced handover);
- угрозы незащищенной начальной загрузки и многоадресной сигнализации в LTE;
- возможное нарушение синхронизации туннелей IPsec, которые обеспечивают конфиденциальность, но не целостность данных.

Среди прочего, следует отметить угрозы для устройств пользователей и хранимой на них информации, например, ключей шифрования и т. д.

8 Требования к безопасности

8.1 Общие положения

Основные требования и меры обеспечения ИБ применимы в равной степени к беспроводным и проводным сетям. Однако для беспроводных сетей должны быть предусмотрены дополнительные требования и меры обеспечения ИБ, которые позволят нейтрализовать угрозы, непосредственно относящиеся к беспроводным сетям (см. раздел 7). В данном разделе рассматриваются такие дополнительные требования. При оценке выполнения основных требований безопасности (см. подразделы 8.2—8.7) необходимо принимать во внимание как сами угрозы, так и их многообразие.

8.2 Конфиденциальность

Для повышения безопасности при отправке информации ограниченного доступа через беспроводные сети требуется обеспечить шифрование данных пользователей, а в некоторых случаях, и шифрование сигналов и данных контроля и управления с целью предотвратить раскрытие или перехват данных во время их передачи. В зависимости от технологии беспроводного доступа могут использоваться различные средства криптографической защиты информации разного уровня сложности, сертифицированные уполномоченным федеральным органом исполнительной власти. Для обеспечения конфиденциальности данных администратор сети должен найти компромисс между криптографической стойкостью шифрования и его влиянием на производительность и пропускную способность сети, управление ключами и удобство использования.

8.3 Целостность

Целостность передаваемых через беспроводные сети данных должна обеспечиваться с помощью соответствующих схем защиты целостности, гарантирующих, что данные пользователя или фактические данные сигнализации, контроля и управления не были изменены или подделаны. В любой беспроводной технологии могут быть использованы различные схемы защиты целостности с использованием средств

защиты информации (в том числе средств криптографической защиты информации разного уровня сложности), сертифицированных уполномоченным федеральным органом исполнительной власти. Администратор сети должен найти компромисс между криптографической стойкостью шифрования и его влиянием на производительность и пропускную способность сети, управление ключами и удобство использования.

8.4 Доступность

Доступность беспроводной сети зависит от ряда факторов, большинство из которых являются общими для всех беспроводных технологий. В их число входят:

- радиочастотные характеристики выбранной технологии (ширина полосы канала, уровень сигнала, полоса частот, модуляция, кодирование и т. д.);
- среда, в которой разворачивается сеть (физическая местность, атмосферная среда);
- производительность сети под нагрузкой и в условиях перегрузки;
- особенности планирования сети (пропускная способность, повторное использование спектра);
- уровень избыточности, заложенный в сеть и в ее компоненты;
- устойчивость сети и ее компонентов к DoS-атакам.

Для обеспечения уровня обслуживания клиентов поставщики сетевых и прочих услуг и организации могут быть связаны нормативно-правовыми актами. В отдельных случаях клиенты могут заключать с поставщиками услуг Соглашения об уровне обслуживания (SLA), что также может влиять на некоторые из перечисленных выше факторов.

8.5 Аутентификация

Идентификация и аутентификация (проверка подлинности) источников данных или участников обмена информацией, администраторов и обслуживающего персонала сетей является основополагающим фактором для безопасности беспроводных сетей. В отличие от проводных сетей, в беспроводных сетях данные передаются через среду, не имеющую четких физических границ.

Каждая технология беспроводного доступа может использовать разные схемы аутентификации пользовательских устройств, пытающихся подключиться или получить доступ к сети, с различными собственными специальными протоколами обязательной аутентификации. В большинстве случаев администратор сети не осуществляет контроль такого протокола.

Администратор сети должен найти компромисс между использованием максимально строгой аутентификацией и ее влиянием на производительность, управление ключами или паролями, удобство использования, модель развертывания и т. д.

Например, некоторые стандарты беспроводных сетей определяют несколько алгоритмов шифрования и защиты целостности, которые могут быть использованы между мобильным устройством пользователя и контроллером радиосети. Выбор того или иного алгоритма для конкретной сети осуществляется оператором сети.

В таких мобильных сетях именно оператор принимает решение о способе аутентификации устройств пользователей в сети и аутентификации точек сетевого доступа для устройств пользователей. Соответственно, директор по информационной безопасности (ДИБ) или специалист, отвечающий за информационные технологии сети PLMN должны это принимать во внимание.

8.6 Авторизация

Контроль доступа гарантирует, что доступ к компонентам сети, хранимой информации, потокам информации, услугам и приложениям предоставляется только авторизованному персоналу или устройствам.

Каждая конкретная технология беспроводного доступа определяет свой порядок контроля доступа конечных устройств и точек радиодоступа, что обычно оформляется в виде спецификаций для данных пользователя, данных управления и сигнализации, включая данные управления устройством и компонентом.

Кроме того, поставщики оборудования тоже определяют и реализовывают конкретные схемы управления доступом для точек радиодоступа.

В сетях Wi-Fi контроль над тем, какие пользователи могут входить в сеть, осуществляет ДИБ и/или администратор по информационным технологиям. В сетях PLMN контроль над тем, какие устройства пользователей (определяемые по их идентификатору IMEI) имеют право доступа в сеть, осуществляет

оператор, избавляя руководителя по информационной безопасности и (или) администратора по информационным технологиям от необходимости прямого контроля».

Примечание — По мере все большего распространения технологии фемтосот 3G и 4G администраторы организаций и предприятий получают все больше непосредственного контроля над тем, какие устройства пользователей смогут получать доступ к радиосети.

8.7 Неотказуемость

Необходимо обеспечить неотказуемость действий пользователей беспроводной сети, чтобы гарантировать, что любое нарушение политики безопасности будет отслеживаться вплоть до конкретного пользователя.

Неотказуемость посредством предоставления таких доказательств действий в сети, как подтверждение обязательств, намерений или ответственности, подтверждение происхождения данных, подтверждение права собственности или подтверждение использования ресурса, обеспечивает возможность предотвращения того, что физическое или юридическое лицо будет отрицать выполнение конкретных действий с данными. Неотказуемость обеспечивает свидетельства, которые могут быть представлены третьей стороне и использованы для доказательства определенного события или выполнения каких-либо действий.

Точки доступа Wi-Fi можно настроить для ведения журнала доступа клиентов. Информацию журнала можно использовать для устранения неполадок, мониторинга производительности сети и для анализа инцидентов. Информация о событиях, таких как неудачные попытки клиентов входа в сеть, ошибки аутентификации, история ассоциации клиентов обеспечивают возможности администратора сети упреждать возможные нарушения безопасности, а также идентифицировать клиентов, ответственных за определенные действия.

9 Меры обеспечения информационной безопасности

9.1 Общая информация

При оценке рисков ИБ, актуальных для сети, следует иметь в виду, что перечисленные в разделе 7 специфические для беспроводных сетей угрозы дополняют и усиливают общие для всех сетей угрозы, такие как несанкционированный доступ, компрометация хранимых данных или вредоносное программное обеспечение. В разделе 8 перечислены требования безопасности именно для беспроводных сетей, но на самом деле они являются основополагающими для всех сетей. Таким образом, во многих случаях меры безопасности, перечисленные в разделе 9, применимы ко всем типам сетей доступа, например, усиление защиты ТД. Одной из целей раздела 9 является выявление отличий применения мер обеспечения ИБ к беспроводным сетям от применения в любых других сетях.

Для каждого актуального риска безопасности необходимо проверить каждый защищаемый компонент, чтобы определить, является ли риск значимым, влияет ли он на актив или сеть, а также в зависимости от приоритета выяснить, какие из доступных мер обеспечения ИБ можно применить для снижения этого риска. Большинство рисков могут быть смягчены при условии использования более чем одной меры обеспечения ИБ. Например, для защиты от вредоносного воздействия применяются и контроль доступа, и аутентификация. Именно на этапе оценки рисков/управления рисками проекта принимаются решения по выбору мер обеспечения ИБ или количеству уровней защиты.

Как и для любой другой коммуникационной сети, ключевой стратегией безопасности для беспроводных сетей является многоуровневая защита.

Некоторые из ключевых общих мер обеспечения ИБ применимы и к беспроводным сетям:

- усиление защиты оборудования;
- устранение уязвимостей путем обновления программного обеспечения оборудования;
- система управления информацией, построенная на основе оценки рисков безопасности, связанных с защищаемыми элементами;
- обучение операторов;
- информирование конечного пользователя.

Далее приводится описание мер обеспечения ИБ, относящихся к беспроводным сетям. Необходимо иметь в виду, что не все из них будут применимы ко всем без исключения беспроводным технологиям.

9.2 Контроль и реализация шифрования

Мерой обеспечения ИБ, реализация которой позволит сохранить свойства безопасности информации, такие как конфиденциальность и целостность, является шифрование данных. Шифрование данных, передаваемых через радиоинтерфейсы беспроводных сетей, рекомендуется практически для всех вариантов развертывания. Как правило, стандарты беспроводной связи дают подробное определение типов шифрования для данных пользователей, данных сигнализации/управления, а также, в некоторых случаях, для данных управления устройствами и оборудованием.

При выборе параметров шифрования для используемых беспроводных технологий сотрудник ИБ, руководствуясь соответствующими стандартами безопасности, должен учитывать следующие аспекты:

- какие алгоритмы шифрования данных доступны? Какие алгоритмы шифрования данных реализованы в оборудовании и (или) сети и в устройствах конечных пользователей? Какие из них сертифицированы уполномоченным федеральным органом исполнительной власти?;
- должен ли конечный пользователь иметь возможность выбирать тип шифрования, либо он должен быть жестко задан администратором сети?;
- использование надежного шифрования желательно, но необходимо соотнести его с производительностью сетевого интерфейса, производительностью устройств конечного пользователя и доступной пропускной способностью интерфейса;
- каким образом конечный пользователь проинформирован об уровне шифрования его данных, то есть о безопасности его данных;
- необходимо понимать процедуру управления ключами шифрования. Разворачивается ли инфраструктура открытых ключей? Будет ли беспроводная сеть располагать собственным локальным центром сертификации или будет использоваться открытый и/или корневой центр сертификации? Чем более автоматизирован процесс управления ключами, тем удобнее для пользователей;
- местные законы некоторых юрисдикций определяют разрешенные и запрещенные типы шифрования;
- необходимый тип шифрования может также определяться соглашением об уровне обслуживания (SLA);
- возможность взаимодействия с другими (беспроводными) сетями. Например, если будет происходить переключение устройств конечных пользователей в другую сеть, то будет ли эта сеть поддерживать тот же уровень шифрования, что и исходная сеть?;
- обратная совместимость с различными версиями устройства/оборудования. В некоторых случаях более ранние версии пользовательских устройств могут не поддерживать используемый уровень шифрования.

Стандарты безопасности беспроводной сети могут определять механизм шифрования данных только для каждого транзитного участка или для интерфейса, например, радиоинтерфейса. При изучении вопроса о шифровании данных специалист по ИБ должен провести анализ сквозных потоков данных. В некоторых случаях имеет смысл рассмотреть возможность использования сквозного безопасного туннеля или VPN-соединения.

В дополнение к сквозным потокам данных необходимо учитывать шифрование данных, хранящихся в точках беспроводного доступа и конечных устройствах. Это шифрование, в целом, должно соответствовать передовым рекомендованным практическим методам хранения конфиденциальных данных.

Специалист по ИБ должен быть осведомлен обо всех ставших известными проблемах алгоритмов шифрования. Как правило, такие проблемы становятся общеизвестными в отрасли информационных и коммуникационных технологий. Однако важно, чтобы со всеми поставщиками систем были заключены соглашения о раскрытии уязвимостей, что позволит руководителю по ИБ своевременно получать информацию о проблемах. Это особенно актуально, если уязвимость связана с реализацией алгоритма, а не с его теоретическими характеристиками, поскольку уязвимости подобного типа реже становятся общедоступными.

9.3 Оценка целостности

Для защиты сетей от атак, связанных с перехватом управления сессией, атак через посредника, атак с репликацией сообщений в беспроводных интерфейсах используются встроенные механизмы проверки целостности, представляющие собой основу защиты от таких атак. Стандарты беспроводной

связи, как правило, определяют метод проверки целостности. Некоторые из них поддерживают несколько вариантов, выбор из которых должен сделать специалист по ИБ.

В подразделе 9.2 перечислены соображения по шифрованию данных, которые могут в равной степени применяться для оценки целостности.

При изучении специалистом по ИБ механизмов обеспечения целостности данных необходимо учитывать данные пользователей, передаваемые контрольные данные, а также данные, относящиеся к управлению, такие как информация о загрузке и обновлении программного обеспечения, о загрузке конфигурации.

По мере того, как атаки становятся все более изощренными, могут быть выявлены слабые места в механизмах целостности данных и их конкретных реализациях. Специалист по ИБ должен постоянно поддерживать уровень своей компетентности в области стандартов безопасности беспроводной связи, а также должен быть осведомлен обо всех известных взломах и уязвимостях.

9.4 Аутентификация

Для защиты от угроз несанкционированного доступа к сети, точке доступа или данным, внедрения фальшивых точек доступа и атак через посредника в стандартах беспроводных технологий определены механизмы аутентификации различной степени сложности, начиная с аутентификации по паролю, аутентификации с использованием разделяемых, закрытых или открытых ключей и заканчивая более сложными сочетаниями методов. Специалист по ИБ должен рассмотреть не только процедуру аутентификации конечного пользователя в сети доступа, но и процедуры аутентификации устройств конечного пользователя, процедуры проверки подлинности точек доступа или промежуточных шлюзов со стороны устройств конечного пользователя, а также порядок взаимной аутентификации точек доступа или проверки их подлинности базовой сетью. В целом все эти аспекты большинства беспроводных технологий определены в соответствующих стандартах безопасности.

Специалисту по ИБ необходимо обратить внимание на следующие аспекты:

- перечень методов (механизмов) аутентификации, предусмотренных для данной технологии беспроводной связи соответствующими стандартами безопасности, с конкретизацией интерфейсов, для каждого механизма, включая радиоинтерфейс обмена данными и интерфейс для управления и контроля устройств и/или точек доступа. Необходимо учесть, что для всех интерфейсов рекомендуется взаимная аутентификация;
- механизмы аутентификации, реализованные в оборудовании сети и в устройствах конечных пользователей. Некоторые устройства и/или оборудование точки доступа могут не поддерживать последнюю версию стандарта или поддерживать не все параметры безопасности;
- параметры, доступные сетевому администратору для выбора и настройки механизма аутентификации;
- предпочтительно использовать наиболее надежный механизм аутентификации, но необходимо оценить его с точки зрения удобства для пользователя, управляемости с точки зрения сетевого администратора, а также затрат на реализацию;
- управление учетными данными аутентификации должно быть четко определено;
- среди прочих аспектов управления учетными данными для проверки подлинности необходимо рассмотреть следующее. Как обрабатываются неудачные попытки аутентификации? Как происходит аннулирование/восстановление прав? Как истекает срок действия полномочий? Эти аспекты нужно рассматривать как с позиции пользователей, так и с позиции функций контроля и менеджмента;
- в беспроводных технологиях типов 2G/3G/4G/5G в устройствах конечных пользователей используются карточки SIM/UICC, которые либо выдаются оператором PLMN, либо могут быть встроены в устройство их производителями. Специалист по ИБ должен понимать суть взаимоотношений всех задействованных в таком случае сторон. Руководитель по ИБ также должен понимать механизмы физической безопасности, используемые для защиты учетных данных на устройствах конечных пользователей или в контроллерах, таких как защищенные от несанкционированного доступа интегральные схемы, доверенные среды и т. п.;
- местные законы некоторых юрисдикций определяют разрешенные и запрещенные типы механизмов аутентификации;
- необходимый тип аутентификации может также определяться соглашением об уровне обслуживания (SLA);

- возможность взаимодействия с другими (беспроводными) сетями; например, если будет происходить переход устройств конечных пользователей в другую сеть, будет ли эта сеть поддерживать тип аутентификации, аналогичный исходной сети? Как правило, у специалиста по ИБ нет возможности изменять параметры операционного взаимодействия или управлять ими, однако специалист должен быть осведомлен о возможностях различных технологий обеспечения безопасности беспроводной связи;

- обратная совместимость с различными версиями устройств и оборудования.

9.5 Контроль доступа

9.5.1 Общие положения

Современные решения в системах безопасности беспроводных сетей основаны на использовании распространенных механизмов управления доступом, таких, например, как управление доступом на основе ролей (RBAC), функции контроля доступа к файловой системе, межсетевые экраны, обнаружение вторжений. Их можно интегрировать в отдельный продукт или создать на их основе внешний уровень защиты. Они в полной мере применимы к беспроводным сетям, однако существуют и специфические механизмы, определенные в стандартах безопасности беспроводной связи и дополняющие традиционные средства управления доступом.

Специалисту по ИБ необходимо получить ответы на следующие вопросы:

- какие механизмы контроля доступа определены соответствующими стандартами безопасности беспроводной связи для выбранной беспроводной технологии;

- какие механизмы контроля доступа реализованы в оборудовании сети и в устройствах конечных пользователей? Некоторые устройства и/или оборудование ТД могут не поддерживать последнюю версию стандарта или поддерживать не все параметры безопасности;

- какие параметры доступны сетевому администратору для выбора и настройки механизма контроля доступа?;

- местные законы некоторых юрисдикций определяют разрешенные и запрещенные типы механизмов контроля доступа;

- совместимость с другими (беспроводными) сетями;

- как правило, у специалиста по ИБ нет возможности изменять параметры операционного взаимодействия или управлять ими, однако специалист должен быть осведомлен о возможностях различных технологий обеспечения безопасности беспроводной связи;

- обратная совместимость с различными версиями устройств и оборудования;

- для обнаружения несанкционированного доступа в беспроводную сеть и предотвращения последующего воздействия такого нарушения безопасности необходимо создать соответствующую систему обнаружения и предотвращения вторжения в беспроводную сеть.

9.5.2 Контроль разрешений

Одним из примеров контроля разрешений является фильтрация по MAC-адресам, реализованная в системах IEEE 802.11, в которых возможность подключения к беспроводной сети предоставляется только клиентам, MAC-адреса которых удовлетворяют условию фильтрации. Однако, следует отметить, что этот механизм сам по себе не обеспечивает эффективную защиту, поскольку нарушитель имеет возможность маскироваться под доверенного клиента беспроводной сети. Тем не менее этот механизм является примером одного из уровней защиты системы.

В стандартах мобильных сетей в качестве критерия допуска в сеть используется идентификатор оборудования пользователя. Таким образом, если международный идентификатор мобильного оборудования (IMEI) пользователя находится в черном списке оператора, доступ в сеть ему предоставлен не будет.

9.5.3 Сетевой контроль

Анализ множества стандартов беспроводных технологий показывает, что протоколы данных пользователей и протоколы управления отдельно определены и во многих случаях реализуются тоже отдельно. При таком определении и реализации стандарта обеспечивается логическое разделение протоколов, что само по себе обеспечивает возможность контроля доступа.

В стандартах 4G LTE содержатся рекомендации по использованию протокола IPsec для защиты передачи не шифрованных данных управления при пересечении границы сети и переходе из одного

домена безопасности в другой (в незащищенную сеть). Мобильные операторы могут опционально использовать такую же возможность и для данных пользователей.

9.6 Устойчивость к атакам «Отказ в обслуживании»

Типичные механизмы предотвращения или нейтрализации атак отказа в обслуживании варьируются от использования методов защиты исходных программ, тестирования и анализа исходного кода, тестирования на наличие уязвимостей до применения сетевых или серверных систем обнаружения и предупреждения вторжений (IDS/IPS) для обнаружения аномальной активности в трафике IP или трафике приложений. Эти методы применимы ко всем сетям, использующим информационные и коммуникационные технологии.

Радиочастотные помехи, которые могут создаваться нарушителем или случайно, присущи только беспроводным сетям. Чтобы гарантировать обнаружение и регистрацию в журнале таких событий руководитель по ИБ должен обеспечить в сети установку соответствующего оборудования для мониторинга сети.

Специфические для беспроводных протоколов DoS-атаки могут быть выявлены системами обнаружения аномалий. Руководитель по информационной безопасности должен быть осведомлен о том, какое оборудование развернуто в сети, каковы возможности оборудования для мониторинга, и, кроме того, должен знать о новых или изменившихся угрозах в этой области.

9.7 Использование демилитаризованной зоны

Поскольку беспроводные сети могут подвергаться атакам через радиоинтерфейс, то рекомендуется подключать их к безопасной внутренней сети через сеть так называемой демилитаризованной зоны (ДМЗ).

Беспроводная сеть ДМЗ должна быть отделена от защищенной сети межсетевым экраном, который в целях безопасности по заданным правилам ограничивает трафик, поступающий из беспроводной сети в защищенную сеть.

Примером ДМЗ является беспроводная гостевая сеть как часть общей сети организации и/или корпоративной сети.

9.8 Менеджмент уязвимостей посредством безопасных конфигураций и усиления устройств

Рекомендуется внедрить программу менеджмента сетевых уязвимостей. Периодическую оценку уязвимости приложений и инфраструктуры можно выполнять при помощи инструментов сканирования уязвимостей беспроводных систем. Обнаруженные уязвимости могут устраняться путем установки исправлений («патчей») для приложений, операционных систем или устройств либо с помощью безопасных конфигураций и усиления устройств.

9.9 Постоянный мониторинг беспроводных сетей

Беспроводная сеть должна быть интегрирована с системой мониторинга безопасности предприятия. Для периодического или непрерывного мониторинга с целью выявления угроз могут использоваться инструменты менеджмента инцидентов и событий безопасности, а также корпоративные средства обнаружения атак и утечек данных.

10 Методы и аспекты проектирования систем безопасности

10.1 Общая информация

Данный раздел представляет собой общее руководство по проектированию и развертыванию беспроводных сетей. В разделе намеренно не приводится подробная информация о безопасности протоколов или интерфейсов технологий беспроводной связи, поскольку их описание содержится в соответствующих стандартах беспроводных технологий. Одним из наиболее распространенных является семейство стандартов беспроводных сетей [4]. Список технологий беспроводной связи, описываемых в этом разделе настоящего стандарта, не является исчерпывающим, поскольку еще до публикации настоящего стандарта появятся новые стандарты и их варианты, которые в перспективе смогут превзойти по функциональности или заменить рассматриваемые здесь технологии.

В процессе планирования безопасной беспроводной сети, чтобы убедиться в том, что ДИБ, архитектор информационных систем или сети способны проанализировать и безопасно развернуть новые технологии, можно воспользоваться следующими базовыми проверками:

- проведение оценки рисков при использовании новых беспроводных технологий;

- в рамках разработки стандарта беспроводной связи и, в частности, раздела безопасности, организация по разработке стандартов, как правило, выполняет описание и анализ связанных с технологией угроз и определяет контрмеры для снижения последствий любых воздействий. Меры снижения последствий либо оформляются в виде рекомендаций, либо включаются непосредственно в спецификацию стандарта;

- руководитель и специалист по вопросам безопасности должны знать о конкретных угрозах, связанных с предлагаемой беспроводной технологией;

- необходимо, чтобы в организации была реализована политика безопасности беспроводной сети, в которой конкретно определены следующие аспекты:

а) аутентификация пользователя беспроводной сети;

б) контроль доступа к беспроводной сети как сотрудников, так и гостей или лиц, не являющихся сотрудниками;

в) как сотрудники на работе получают доступ к другим беспроводным сетям, не контролируемым организацией;

г) кто уполномочен разрешать подключение точек доступа к сети организаций.

В политику безопасности беспроводных сетей могут также быть включены аспекты безопасности использования сотрудниками собственных устройств (BYOD), даже если домены безопасности собственных устройств сотрудников не относятся исключительно к беспроводной технологии. Политика безопасности беспроводной сети должна охватывать все беспроводные технологии, которые развернуты в сети предприятия или организации.

10.2 Сети Wi-Fi

10.2.1 Общая информация

Wi-Fi представляет собой совокупность компонентов беспроводной локальной вычислительной сети (WLAN), в основе которой лежат стандарты беспроводной связи серии 802.11 Института инженеров электроники и электротехники (IEEE) (см. [4]).

В данном подразделе содержится общая информация о принципах и методах, связанных с сетями и оборудованием Wi-Fi.

Сеть Wi-Fi — это группа из двух или более беспроводных сетевых устройств в ограниченной географической области, которые обмениваются данными по радиосвязи. Основными компонентами сети Wi-Fi, соответствующей [4], являются клиентские устройства, такие как ноутбуки, планшеты и смартфоны, а также точки доступа (AP), которые логически связывают клиентские устройства с распределительной сетью, как правило, инфраструктурой проводной сети организации. Некоторые сети Wi-Fi также используют беспроводные коммутаторы, которые выполняют роль ретрансляторов между точками доступа и распределительной сетью.

Семейство стандартов [4] определяет технологию беспроводного обмена данными с полудуплексной модуляцией, в котором используется один и тот же базовый протокол. К первоначальной версии [4] было применено более десятка различных дополнений и корректировок спецификаций, предусматривающих поддержку различных частот передачи и других механизмов безопасности.

Механизмы безопасности сетей Wi-Fi определены в [4] и включают в себя функции аутентификации клиентских устройств на точках доступа, точек доступа на устройстве, шифрование пользовательских данных и защиту их целостности. Следует отметить, что не каждый из стандартов [4] определяет все функции безопасности.

Отделы ИБ организации отвечают за контроль конфигурации безопасности подведомственной им инфраструктуры.

Сотрудники, использующие другие сети и общественные точки беспроводного доступа, должны быть обеспечены инструкциями по использованию альтернативных механизмов защиты при передаче информации ограниченного доступа, например, VPN.

10.2.2 Аутентификация пользователей

Все пользователи, пытающиеся получить доступ к беспроводной сети, контролируемой или управляемой организацией, должны проходить проверку подлинности. Лишь после этого им может быть предоставлен доступ к сети или точкам гостевого доступа Wi-Fi.

Доступ сотрудников организации к сети должен осуществляться с использованием двухфакторной аутентификации, например, с использованием токена[1)] и ПИН-кода к нему.

Для авторизации гостевого доступа в сеть Интернет должны приниматься в расчет следующие факторы:

- регистрация всех гостевых пользователей беспроводной сети должны производиться под контролем ответственного лица организации;
- для обеспечения неотказуемости следует использовать уникальные гостевые идентификаторы. В тех случаях, когда использование уникальных идентификаторов и паролей нерационально, они могут использоваться совместно (например, при проведении крупных встреч с клиентами);
- срок действия паролей должен отвечать принципу коммерческой целесообразности (до одной недели);
- каждый гостевой пользователь должен быть ознакомлен с правилами предоставления доступа и использования сети.

10.2.3 Конфиденциальность и целостность данных

Данные, получаемые и передаваемые сетью организации, должны шифроваться. Для шифрования передаваемых данных должны использоваться соответствующие криптографические механизмы защиты, в том числе и использование VPN-туннелей с надлежащим шифрованием. Кроме того, для предотвращения приема фальсифицированных пакетов необходима проверка целостности сообщений.

10.2.4 Беспроводные технологии Wi-Fi

На всем оборудовании беспроводной связи, подключаемом к сети организации, должны быть установлены и настроены средства защиты информации в соответствии с политикой безопасности предприятия.

Ввиду общеизвестных проблем безопасности использование алгоритмов шифрования Wired Equivalent Privacy (WEP) или WPA не допускается.

10.2.5 Другие конфигурации Wi-Fi

В отдельных случаях может потребоваться использовать приложения, основанные на беспроводных конфигурациях, не отвечающих вышеизложенным требованиям безопасности. Примером является использование сканеров складских запасов, с аутентификацией AAA.

В таких случаях необходимо проводить оценку рисков безопасности для определения дополнительных мер контроля, таких как:

- регулярная смена паролей разной максимальной длины;
- выделенные SSID;
- ограничение диапазона радиопередачи;
- ограничения доступа к сети путем использования межсетевых экранов TCP или использования изолированной VLAN;
- наличие журналов мониторинга.

10.2.6 Контроль доступа — оборудование пользователя

В целом механизмы контроля доступа для беспроводных сетей должны быть аналогичны используемым для проводных сетей.

Политика безопасности беспроводной сети может конкретно указывать, что сторонние пользователи (гости) не должны иметь доступ к внутренней сети организации через беспроводную сеть.

В некоторых политиках безопасности беспроводной связи может присутствовать запрет на использование сотрудниками организации сетей Wi-Fi в качестве моста к сетевому периметру организации (например, использование Wi-Fi для одновременного подключения к сети LAN организации и внешней сети, не контролируемой данной организацией). Поэтому сотрудникам запрещено включать IP-переадресацию (IP Forwarding), устанавливать беспроводные одноранговые соединения, использовать специальный режим Ad-hoc или устанавливать иные виды маршрутизации.

Беспроводные системы обнаружения/предотвращения вторжений (WIDS/WIPS) могут обеспечить эффективный уровень защиты для борьбы с такими угрозами, как создание фальшивых точек доступа и атака отказа в обслуживании.

[1)] Токен — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т. д. Как правило, это физическое устройство, используемое для аутентификации.

Системы WIDS/WIPS оснащены датчиками, которые сканируют радиочастотный спектр и передают результаты на сервер управления, который после анализа полученной с датчиков информации может предпринимать конкретные действия. Как правило, в состав системы WIDS/WIPS входит и сервер базы данных, используемый в качестве хранилища информации.

10.2.7 Контроль доступа — точка доступа

Для точек доступа необходимо придерживаться следующих рекомендаций по настройке:

- пароль управления точки доступа для администрирования по умолчанию должен быть заменен на надежный пароль — отсутствующее в словарях слово длиной не менее 15 (пятнадцати) буквенно-цифровых символов, содержащее не менее одного цифрового или специального символа;
- для аутентификации администратора точки доступа должна использоваться инфраструктура сетевого устройства AAA;
- удаленное администрирование через беспроводную локальную сеть должно быть отключено, администрирование должно быть возможно только через интерфейсы Ethernet, USB или последовательный порт;
- удаленное администрирование должно осуществляться только с использованием шифрования, можно использовать, например, https/ssh, но http/telnet должны быть отключены;
- для исключения возможности подбора пароля, необходимо изменить все строки имен и паролей протокола SNMP, заданные по умолчанию;
- по возможности во всех точках доступа для сетевого управления должен использоваться протокол SNMPv3;
- при установке точки доступа необходимо провести измерение и определение зон покрытия, которые должны находиться в пределах физически контролируемого периметра. Сеть не должна быть доступна там, где не предусмотрено ее использование, например, на автомобильных парковках. С целью предотвращения несанкционированного доступа следует ограничивать доступность сигнала маршрутизатора конкретной территорией;
- необходимо надлежащим образом обеспечить физическую защиту всех точек доступа, чтобы предотвратить кражу или взлом;
- необходимо изменить SSID (идентификатор набора услуг) с заданного по умолчанию имени сети на собственное имя и разрешить точке доступа транслировать свой SSID;
- точки доступа дают возможность без лишних проблем создать беспроводную сеть с единым SSID с использованием высокочувствительных направленных антенн для ретрансляции сигнала беспроводной связи базовой точки доступа. Каждая точка доступа, контролируемая и управляемая организацией беспроводной сети, должна осуществлять аутентификацию устройств, пытающихся получить к ней доступ;
- беспроводную сеть необходимо отделить от внутренней сети организации и сети «Интернет»;
- для повышения их надежности и безопасности на маршрутизаторах и в точках доступа должны быть установлены последние версии прошивок;
- в идеальном случае для гостевого доступа должна быть предоставлена отдельная сеть.

Для управления точками доступа могут использоваться несколько административных учетных записей с расширенными правами (одна или несколько учетных записей для управления одной точкой доступа), что может представлять проблемы с их управлением и контролем.

Организации и предприятия должны обеспечить наличие механизма управления привилегированными учетными записями.

Организациям необходимо рассмотреть возможность проведения проверок безопасности независимой третьей стороной. Независимый аудитор, специализирующийся на вопросах безопасности беспроводных сетей, может располагать большей информацией об уязвимостях систем и обладать лучшей подготовкой для оценки безопасности беспроводной сети.

10.2.8 Доступность

В основном, средства обеспечения доступности беспроводных сетей, такие как резервные маршрутизаторы, источники питания и пр., те же самые, что и для проводных сетей. В сетях Wi-Fi информация о доступности точек доступа и их алгоритмах шифрования передается на клиентские компьютеры.

Для сетей Wi-Fi могут предприниматься и некоторые дополнительные меры или проверки, такие как:

- проведение на регулярной основе аудита безопасности конфигураций компонентов сети Wi-Fi, например, клиентских устройств и точек доступа, для подтверждения их соответствия минимальным требованиям безопасности или соответствия внутренним стандартам организации по безопасности;

- мониторинг сети Wi-Fi с использованием беспроводных систем обнаружения вторжений и защиты от них, размещенных в различных точках организации для выявления аномального трафика в беспроводной сети.

Вышеуказанные меры предназначены для обнаружения изменений характеристик сети Wi-Fi или клиентских устройств, которые могут предшествовать атакам. Уязвимости сети могут использоваться для снижения уровня ее доступности.

10.2.9 Неотказуемость

Если законодательство или соответствующие нормативные правовые акты позволяют, то должно быть обеспечено централизованное ведение журналов точек доступа, где для действий пользователей и событий, фиксируется следующая информация:

- метки времени;
- MAC-адреса;
- имена пользователей;
- успешные и неудачные события;
- типы событий, например, попытки входа в сеть;
- перезагрузки;
- изменения конфигурации;
- установление и (или) отключение связей, что может означать попытки атаки отказа в обслуживании;
- идентификация фиктивных точек доступа.

Для того чтобы оценить состояние безопасности беспроводной сети, сеть должна периодически сканироваться на наличие неавторизованных точек доступа в помещениях организации.

10.3 Особенности безопасности мобильных систем

Системы мобильной связи, известные также как системы мобильной сотовой связи, обычно включают в себя базовые станции, контроллеры радиосети и интерфейсы или шлюзы базовой сети оператора. Базовые станции поддерживают одну или несколько сот и в совокупности могут покрывать значительные физические пространства. Изначально разработанные в первую очередь для голосовых вызовов, они поддерживают большое число пользователей телефонной связи, переключение с соты на соту при перемещении пользовательских устройств и роуминг с сетями других операторов. Системы мобильной связи, основанные на современных стандартах беспроводной высокоскоростной передачи данных, способны обеспечивать высокоскоростной мобильный интернет-доступ для ноутбуков, смартфонов и других мобильных устройств.

Безопасность для систем мобильной связи определяется стандартами взаимной аутентификации пользовательского оборудования (устройств) в сети, механизмами защиты целостности и конфиденциальности, а также контроля доступа к сети. По мере развития интеграции систем Wi-Fi с системами мобильной связи угрозы безопасности, характерные для такой интеграции, также стали предметами стандартизации.

Используемые сотрудниками организаций или предприятий устройства мобильной связи, как правило, контролируются и поддерживаются поставщиком услуг, что лишает пользователя этих услуг возможности контролировать параметры безопасности, такие как шифрование данных и аутентификация устройств и точек доступа.

Передачи в сети радиодоступа (RAN) могут быть зашифрованы, но гарантии безопасности линии связи на всем ее протяжении нет.

Поскольку сети радиодоступа контролируются операторами, а шифрование на линии связи не гарантировано, то следует рекомендовать конечным пользователям использовать альтернативные механизмы защиты, например, VPN при передаче информации ограниченного доступа.

10.4 Особенности безопасности Bluetooth

Bluetooth — это стандарт беспроводной технологии обмена данными на коротких расстояниях в микроволновом частотном диапазоне в 2,40—2,48 ГГц между фиксированными и мобильными устройствами, а также для создания персональных сетей (PAN).

Стандартизацию Bluetooth осуществляет организация Bluetooth SIG, которая разрабатывает спецификации и руководит квалификационной программой. Все версии стандартов Bluetooth разрабатываются с учетом обратной совместимости. Более поздние версии стандарта обеспечивают улучшение возможностей Bluetooth, более высокие скорости передачи, более быстрое обнаружение устройств и сопряжение, более безопасное сопряжение устройств, поддержку устройств с низким энергопотреблением и безопасные сопряжения с использованием шифрования.

Безопасность Bluetooth соединения «точка-точка» и сети Bluetooth PAN во многом определяется версией стандарта Bluetooth, поддерживаемого или используемого на устройствах. Информация об уязвимостях каждой версии стандарта опубликована в сети Интернет.

Вследствие характерных для протоколов Bluetooth уязвимостей организациям рекомендуется запрещать пользователям передавать конфиденциальные или критически важные данные через устройства Bluetooth.

Для стандарта Bluetooth характерно большинство уязвимостей, которые свойственны беспроводным системам в целом. Передатчик Bluetooth отправляет сигналы через свободное пространство на все приемные устройства, находящиеся в пределах досягаемости сигналов. Кроме того, Bluetooth работает в нелицензированном диапазоне 2,4 ГГц, а передающие и принимающие в этом частотном диапазоне устройства продаются без каких-либо ограничений. Следовательно, неавторизованное устройство мониторинга, которое даже не сопряжено с передатчиком Bluetooth, может перехватывать передаваемую информацию. Такое подслушивающее устройство можно легко скрыть, использовать тайно, и на его развертывание требуется гораздо меньше времени по сравнению с подключением к проводной линии для прослушивания телефонных разговоров.

Основные типы атак при использовании Bluetooth приведены в подразделе 7.6.

Пользователи должны следовать следующим рекомендациям по безопасности:

- активировать функцию Bluetooth только при необходимости;
- использовать наиболее надежный режим Bluetooth;
- располагать сопрягаемые устройства максимально близко друг к другу во время связи через Bluetooth;
- включать возможность обнаружения устройств только в случае крайней необходимости;
- избегать использования слабых фиксированных ключей доступа (по умолчанию производитель, как правило, устанавливает «0000»);
- настраивать устройство и программное обеспечение Bluetooth согласно установленным политикам;
- обеспечивать защиту ПИН-кода от перехвата или взлома;
- обеспечивать защиту устройства, идентификационные данные и ключи;
- в целях обеспечения дополнительных мер безопасности использовать защиту уровня приложений и инфраструктуру открытых ключей;
- разработать рекомендации по конфигурации устройств, политики безопасности и механизмы их реализации при использовании устройств Bluetooth в организации.

10.5 Особенности безопасности других технологий беспроводной связи

Новые технологии беспроводной связи и их модификации будут появляться всегда. Для некоторых из них будут определены новые механизмы безопасности. Рекомендуется всегда выполнять оценку рисков, связанных с передачей информации с использованием конкретной технологии с учетом интеграции беспроводных интерфейсов с остальной информационной инфраструктурой организации. Оптимальным является наличие национального, регионального или международного стандарта, в котором находят отражение описание или определение механизмов безопасности, поддерживаемых данной технологией, анализ связанных с ней угроз, а также рекомендации по ее развертыванию и безопасному встраиванию в информационную инфраструктуру организации. Если механизмы безопасности для данной технологии не существуют или неизвестны, то организация должна принять решение о целесообразности использования такой технологии или о внедрении дополнительных процедур для обеспечения безопасности.

В большинстве организаций совместно используется несколько беспроводных технологий, и пользовательские устройства могут быть одновременно подключены к нескольким беспроводным сетям, таким как сети сотовой связи, сети Bluetooth и Wi-Fi, а в некоторых случаях могут быть подключены также и к проводным сетям. Поэтому при получении беспроводного доступа к клиентскому устройству с множеством подключений у нарушителя появится возможность доступа к ресурсам проводной сети или проведения атаки на них. Организации должны оценить риски, связанные с использованием комбинаций беспроводных технологий, и определить меры по снижению таких рисков. Если для какой-либо сети невозможно снизить риск до приемлемого уровня, то подключения к этой сети могут представлять слишком большой риск для организации и, возможно, должны быть запрещены.

Приложение А
(справочное)

Техническое описание угроз и мер противодействия

А.1 Атака через посредника

При атаке через посредника, также называемой «человек посередине», нарушитель занимает положение между жертвой и ее партнером по связи без их ведома. Весь трафик проходит через нарушителя, который имеет возможность отслеживать его.

При атаке через посредника атакующий маскируется под точку доступа для клиента и под клиента для настоящей точки доступа. Клиент видит точку доступа, которая кажется ему настоящей, и подключается к ней. Через такую фиктивную точку доступа происходит кража MAC-адресов клиентов и связь с настоящей точкой доступа. Весь дальнейший трафик проходит через компьютер нарушителя.

Атаки через посредника известны большинству профессиональных специалистов по обеспечению безопасности. Распространенность такого типа атак несколько снизилась благодаря мерам по обеспечению физической безопасности и сложной, как правило, схеме коммутации двух конечных точек в современных сетях. Однако этот тип атаки переживает возрождение популярности благодаря появлению новых инструментов, облегчающих использование подобного рода уязвимости.

А.2 Перехват сессии

Перехват сессии происходит при получении третьей стороной контроля над сессией. Цель перехвата сессии заключается не в том, чтобы перехватить целиком беспроводное соединение, а в том, чтобы переключить на себя сессию веб-приложения, активированную в беспроводном соединении. Анализ сессии веб-приложения для подготовки к ее перехвату может быть выполнен в процессе атаки через посредника.

Классическая техника получения идентификатора сессии использует маршрутизацию IP-источника. В современной беспроводной среде анализ пакетов возможен путем простого мониторинга беспроводных соединений.

Существует несколько способов решения этой задачи. Сети Wi-Fi могут быть беззащитны от этих действий, поскольку не имеют никаких физических подключений, которые можно изменить. Перехват сессии может использоваться либо только для использования сессии, либо для получения доступа к сети Wi-Fi путем кражи идентификационных данных жертвы. Этот метод может использоваться в тех ситуациях, когда доступ в сеть защищен веб-порталом.

Большинство порталов базируется на списках доступа, содержащих MAC-адреса, и осуществляют проверку подлинности пользователей с использованием имени пользователя и пароля или неким другим похожим способом. После успешной проверки подлинности портал добавляет MAC-адрес клиента в список доступа на определенный период времени. Перехват сессии может использоваться либо только для использования сессии, либо для получения доступа к сети Wi-Fi путем кражи идентификационных данных жертвы. Затем нарушитель под видом точки доступа отправляет жертве сообщение об отключении ее MAC-адреса. Жертва удерживается отключенной посредством DoS-атаки из таких сообщений, а нарушитель маскируется под жертву, изменив свой MAC-адрес на адрес жертвы. После этого он владеет сессией до того момента, когда портал в следующий раз потребует аутентификации.

Несколько проще дождаться, когда жертва выйдет из беспроводной сети, и сразу же подтвердить свою личность, прежде чем портал зарегистрирует неактивность жертвы и деаутентифицирует ее. Комбинация анализа пакетов, ping-запросов и изменения MAC-адреса позволяет это сделать. На большинстве порталов время до ожидания активности составляет несколько минут.

Меры противодействия этой угрозе следующие:

- выбирать подходящую технологию, которая для протокола беспроводного соединения включает в себя криптографический алгоритм и механизм обмена ключами;
- во избежание прослушивания идентификаторов сессии требовать от веб-приложений использования технологии шифрования данных.

А.3 Wardriving

Wardriving — это поиск беспроводных сетей Wi-Fi с использованием оборудования или устройства с возможностями обнаружения Wi-Fi. Исторически этот термин связан с хакерами, которые передвигались на автомобилях в поисках открытых беспроводных сетей, определяемых по идентификатору набора услуг (SSID). SSID не является мерой безопасности. Это не пароль, который пользователи должны знать, чтобы иметь возможность подключиться к беспроводной сети. Любой клиент, который в настройках укажет подключение к любому SSID,

обнаружит и подключится к ближайшей доступной и открытой точке доступа, независимо от используемого SSID. Это связано с тем, что точки доступа транслируют SSID как часть ответа клиентам, посылающим «широковещательный запрос».

В связи с этим, выявить все открытые беспроводные сети на заданной территории не составляет труда. Если владельцы этих открытых беспроводных сетей используют в названиях своих точек доступа беспроводной сети названия своих компаний, то можно составить виртуальную карту всех ресурсов беспроводной сети с указанием принадлежности на этой территории.

Существует множество бесплатных и простых в использовании инструментов с открытым исходным кодом, способных отображать точки беспроводного доступа, которые можно загрузить на портативные устройства. Использование таких инструментов для обнаружения точек беспроводного доступа также называется «Wardriving». Результат работы Wardriving называется «Warchalking», и представляет собой значки, отмечающие обнаруженные беспроводные сети. Вариантами этой угрозы являются Warwalking и Warflying, использующие ту же самую базовую уязвимость беспроводных сетей Wi-Fi.

Библиография

[1] ИСО/МЭК 27033-2:2012 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети

[2] ИСО/МЭК 27033-4:2014 Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности

[3] ИСО/МЭК 27033-5:2013 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем

[4] IEEE 802.11 Рабочая группа по беспроводным сетям (http://ieee802.org/11/)

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030 NEQ

Ключевые слова: методы и средства обеспечения безопасности, безопасность сетей, информационные системы безопасности, беспроводная сетевая среда

Редактор *П.К. Одинцов*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 11.11.2020. Подписано в печать 04.12.2020. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru