Безопасность беспроводных сетей

Что такое безопасность сети?

- **Безопасность беспроводной сети** - это предотвращение несанкционированного доступа или повреждения компьютеров или данных с помощью беспроводных сетей, в том числе сетей Wi-Fi . Наиболее распространенным типом является безопасность Wi-Fi , которая включает в себя эквивалентную конфиденциальность проводных сетей (WEP) и защищенный доступ Wi-Fi (WPA).

Что такое безопасность сети?

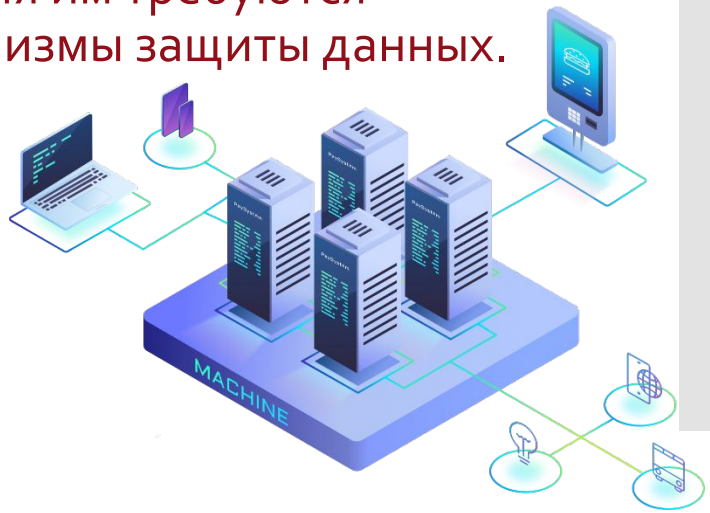
Прочитать и кратко зафиксировать

- Беспроводные локальные сети обеспечивают быстрый и простой доступ между устройствами, очень легко конструируются и реструктуризируются, но отличаются достаточно высокой уязвимостью. Вопрос безопасности Wi-Fi стоит сегодня очень остро. Механизмы аутентификации и шифрования, применяемые в них в настоящее время, крайне несовершенны. Именно поэтому администраторам приходится прибегать к иным инструментам. Пароли, фильтры и другие настройки безопасности беспроводных соединений служат для определенных целей.
- Сетевая безопасность беспроводных сетей — важнейший вопрос, которому следует уделить внимание при их организации. Если вы хотите обеспечить стабильную работу Wi-Fi и защитить данные от несанкционированного доступа, воспользуйтесь Интернет Контроль Сервером. UTM-решение ИКС — это универсальный инструмент, сочетающий в себе функции передовых программных средств, которые позволяют контролировать функционирование любой корпоративной сети.
- Один из первых вопросов, которые необходимо решить IT-специалистам, — это защита беспроводных сетей. Каждый год появляются новые технологии, которые позволяют легко, оперативно передавать трафик между группой абонентов. Параллельно возрастает уязвимость каналов. Сам принцип действия Wi-Fi демонстрирует, насколько легко перехватить ту или иную информацию или осуществить атаку при наличии необходимого оборудования. Главная причина уязвимости беспроводных сетей кроется в обмене пакетами данных посредством радиоволн. Именно эта технология дает злоумышленникам возможность работать в любой точке, где сигнал остается физически доступным.

Прочитать

Политика безопасности беспроводных соединений

- Специфика беспроводных сетей подразумевает, что данные могут быть перехвачены и изменены в любой момент. Для одних технологий достаточно стандартного беспроводного адаптера, для других требуется специализированное оборудование. Но в любом случае, эти угроза реализуются достаточно просто, и для противостояния им требуются эффективные криптографические механизмы защиты данных.



Политика безопасности беспроводных соединений

При построении системы обеспечения безопасности важно определить модель угроз, т. е., решить, чему собственно защита будет противостоять. По сути, в беспроводных сетях угрозы две: несанкционированное подключение и прослушивание, но их список можно расширить, выделив и обобщив к перечисленным в первой главе следующие основные угрозы, связанные с беспроводными устройствами:

- Неконтролируемое использование и нарушение периметра;
- Несанкционированное подключение к устройствам и сетям;
- Перехват и модификация трафика;
- Нарушение доступности;
- Позиционирование устройства.

Если беспроводные сети не используются, то политика безопасности должна включать в себя описание защитных механизмов, направленных на снижение рисков, связанных с несанкционированным использованием радиосетей.

Прочитать

Стандарт ISO/IEC 27001

- Лучшие мировые практики в области управления информационной безопасностью описаны в международном стандарте на системы менеджмента информационной безопасности ISO/IEC 27001 (ISO 27001). ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.
- Стандарт аутентичен ГОСТ РИСО/МЭК 27001-2006. Он устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности, по внедрению мер управления информационной безопасностью и ее контроля.

Стандарт ISO/IEC 27001

Основными преимущества стандарта ISO/IEC 27001:

- Сертификация позволяет показать деловым партнерам, инвесторам и клиентам, что в организации налажено эффективное управление информационной безопасностью;
- Стандарт совместим с ISO 9001:2000 и ISO 14001:2007;
- Стандарт не ставит ограничений на выбор программно-аппаратных средств, не накладывает технических требований на IT-средства или средства защиты информации и оставляет организации полную свободу выбора технических решений по защите информации.
- Понятие защиты информации трактуется международным стандартом как обеспечение конфиденциальности, целостности и доступности информации.

Стандарт ISO/IEC 27001

На основе данного стандарта могут быть сформулированы рекомендации для снижения вероятности нарушения политики безопасности беспроводной сети в организации:

- Обучение пользователей и администраторов. ISO|IEC 27001 A.8.2.2. В результате обучения пользователи должны знать и понимать изложенные в политике ограничения, а администраторы должны иметь необходимую квалификацию для предотвращения и обнаружения нарушений политики;
- Контроль подключений к сети. ISO|IEC 27001 A.11.4.3. Уровень риска, связанного с подключением несанкционированной точки доступа или клиента беспроводной сети, можно снизить путем отключения неиспользуемых портов коммутаторов, фильтрации по MAC-адресам (port-security), аутентификации 802.1X, систем обнаружения атак и сканеров безопасности, контролирующих появление новых сетевых объектов;
- Физическая безопасность. ISO|IEC 27001 A.9.1. Контроль приносимых на территорию устройств позволяет ограничить вероятность подключения к сети беспроводных устройств. Ограничение доступа пользователей и посетителей к сетевым портам и слотам расширения компьютера снижает вероятность подключения беспроводного устройства;
- Минимизация привилегий пользователя. ISO|IEC 27001 A.11.2.2. Если пользователь работает на компьютере с минимально необходимыми правами, то снижается вероятность самовольного изменения настроек беспроводных интерфейсов;
- Контроль политики безопасности. ISO|IEC 27001 6, A.6.1.8. Средства анализа защищенности, такие как сканеры уязвимостей, позволяют обнаруживать появление в сети новых устройств и определить их тип (функции определения версий ОС и сетевых приложений), а также отслеживать отклонения настроек клиентов от заданного профиля. Техническое задание на проведение работ по аудиту внешними консультантами должно учитывать требования политики в отношении беспроводных сетей;

Стандарт ISO/IEC 27001

- Внутренний и внешний аудит. ISO|IEC 27001 6, A.6.1.8. При проведении работ по оценке защищенности должны учитываться требования политики в отношении беспроводных сетей. Более подробно возможный состав работ по оценке защищенности WLAN описан в последней глава данной книги;
- Разделение сетей. ISO|IEC 27001 A.11.4.5. В связи со спецификой беспроводных сетей желательно выделять точки беспроводного доступа в отдельный сетевой сегмент с помощью межсетевого экрана, особенно когда речь касается гостевого доступа;
- Использование криптографических средств защиты. ISO|IEC 27001 A.12.3. Должны быть определены используемые протоколы и алгоритмы шифрования трафика в беспроводной сети (WPA или 802.11i). При использовании технологии 802.1X определяются требования к протоколам ЭЦП и длине ключа подписи сертификатов, используемых для целей;
- Аутентификация. ISO|IEC 27001 A.11.4.2. Должны быть определены требования к хранению данных аутентификации, их смене, сложности, безопасности при передаче по сети. Могут быть явно определены используемые методы EAP, методы защиты общего ключа сервера RADIUS;
- Контроль изменений в информационной системе. ISO|IEC 27001 A.12.5.1. Должны учитываться в ИС беспроводные технологии;
- Допустимость использования программного и аппаратного обеспечения. ISO|IEC 27001 A.12.4.1 В этом разделе рассматриваются требования к точкам доступа, беспроводным коммутаторам и клиентам беспроводной сети;

Решения для обеспечения безопасности беспроводных сетей

- Важным элементом безопасности любой сети, не только беспроводной, является управление доступом и конфиденциальностью. Одним из надежных способов управления доступом к WLAN является аутентификация, позволяющая предотвратить доступ несанкционированных пользователей к передаче данных через точки доступа. Действенные меры управления доступом к WLAN помогают определить круг разрешенных клиентских станций и связать их только с доверенными точками доступа, исключая несанкционированные или опасные точки доступа.

Решения для обеспечения безопасности беспроводных сетей

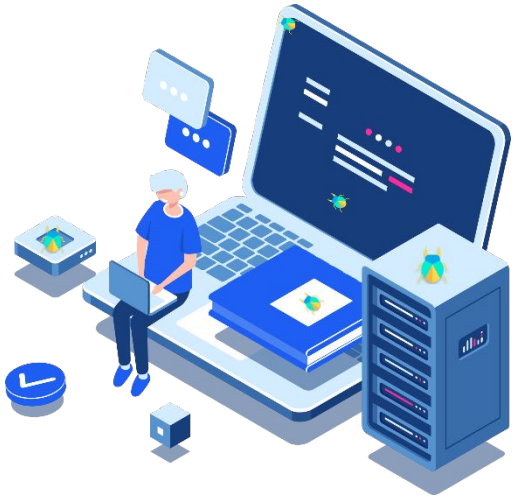
На сегодняшний день компании, использующие сети WLAN, внедряют четыре отдельных решения для безопасности WLAN и управления доступом и конфиденциальностью:

- - Открытый доступ;
- - Базовая безопасность;
- - Повышенная безопасность;
- - Безопасность удаленного доступа.

Прочитать

Необходимость защиты беспроводной сети

- Несмотря на то, что в большинстве компаний уже развернуты те или иные беспроводные сети у специалистов обычно возникает много вопросов по поводу безопасности выбранных решений, а руководители компаний, избегающие внедрения беспроводных технологий, беспокоятся об упущенных возможностях повышения производительности труда и сокращения инфраструктурных расходов.
- В дальнейшем мы поговорим о методах защиты, и типов угроз.



РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ

1. Конспект
2. Выполнить до 10.12 до 18:00