Title

Обеспечение безопасности устройств Инфинет

Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

Пройти сертификационный экзамен

Содержание

Введение

Появление информационных технологий изменило сферы жизни человека, сделав информацию одним из самых ценных ресурсов. Наряду с другими ресурсами, информация представляет ценность для владельца и может стать причиной споров и конфликтов. Именно поэтому, одним из вопросов, связанных с информацией, является обеспечение её безопасности. Развитие информационных систем и накопление больших объёмов данных привело к необходимости комплексного подхода к обеспечению безопасности технических систем.

Документ описывает средства обеспечения информационной безопасности в сетях, построенных с использованием устройств Инфинет. Возможности их применения зависят от семейства беспроводных устройств, поэтому в конце каждого из разделов документа вы найдёте ссылки на техническую документацию для каждого из описываемых средств.

Терминология

- Информация - сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством.
- Информационная безопасность (ИБ) - защищённость информации и инфраструктурных составляющих от воздействий, которые могут нанести ущерб субъектам информационных отношений.
- Техническая политика предприятия - совокупность технических решений, обязательных для применения в технических системах предприятия. Техническая политика включает в себя требования к монтажу, эксплуатации и конфигурации устройств. Необходимо выполнять периодическую актуализацию документа и контролировать его выполнение.
- Угроза - потенциальная возможность нарушения информационной безопасности.
- Атака - попытка реализации угрозы. Атака может быть как злонамеренной, так и нет.
- Злоумышленник - лицо или группа лиц, производящие атаку.
- Эшелон - преграда на пути атаки, реализованная в рамках политики ИБ.
- Риск - вероятность наступления той или иной угрозы.
- Зона ответственности - сегмент сети, за эффективное функционирование которого отвечает определённый субъект. В качестве субъекта может выступать как конкретный человек, так и организация.
- Внутренний сегмент сети - сегмент сети, находящийся в зоне ответственности нашей организации.
- Внешний сегмент сети - сегмент сети, находящийся в зоне ответственности сторонней организации или клиента. Поскольку внешний сегмент сети находится под управлением сторонней организации, поэтому стык внутреннего и внешнего сегментов сетей является источником угроз ИБ.

Характеристики информации

В информационной системе должны быть применены меры обеспечения безопасности информации в соответствии с политикой ИБ, действующей в компании. Политика ИБ должна включать в себя подходы к обеспечению следующих свойств информации:

- Доступность - возможность получения доступа к информации за приемлемое время.
- Целостность - непротиворечивость информации, её актуальность.
- Конфиденциальность - невозможность получения несанкционированного доступа к информации.

Политика информационной безопасности должна предусматривать меры по обеспечению каждого из базовых свойств информации. Нарушение описанных свойств информации ведёт к издержкам, которые могут носить финансовый, репутационный и др. характер. Следует помнить, что реализация политики ИБ является бесконечным процессом, требующим периодического пересмотра мер и контроля за их выполнением.

Организация ИБ должна иметь многоуровневый характер и не ограничиваться только техническими решениями. Помимо технических должны быть предусмотрены законодательные, административные и процедурные меры.

Сценарии использования оборудования Инфинет

Меры по обеспечению ИБ обусловлены не только семейством применяемых устройств Инфинет, но и сценарием их использования (рис. 1а-г). Мы рассмотрим несколько сценариев, в которых беспроводные устройства объединяют сегменты сети, относящиеся к разным зонам ответственности, каждый из которых характеризуется определённым набором угроз:

- объединение внутренних сегментов сети;
- объединение внутреннего и внешнего сегментов сетей;
- объединение внутреннего сегмента сети и сети интернет.

Используемые меры защиты должны соответствовать существующим рискам, архитектура решений по обеспечению ИБ не должна быть избыточной. Например, фильтрация внешних подключений должна выполняться на стыке со сторонним оператором связи, а не на всей цепочке промежуточных узлов.

Требования по обеспечению физической безопасности и безопасности в радиоканале одинаковы для всех рассматриваемых сценариев и подробно представлены в соответствующих разделах. Для конфигурации устройств можно сформулировать следующие общие требования ИБ:

- управление устройством извне должно быть ограничено с помощью "белых" списков;
- работа служебных сетевых протоколов должна быть ограничена внутренним сегментом сети;
- на стыке зон ответственности должен быть организован эшелон безопасности для защиты внутреннего сегмента от вредоносного трафика.

Объединение внутренних сегментов сети

Сценарий объединения двух сегментов сети, находящихся в одной зоне ответственности, является простейшим (рис. 1а). Устройства играют роль моста, следовательно, являются простым соединителем в структуре LAN. поэтому основные средства обеспечения защиты информации размещаются на границах левого и правого сегментов.

Рисунок 1а - Радиоканал, объединяющий два внутренних сегмента

Объединение внутреннего и внешнего сегментов сетей

В сценарии объединения двух сетей, находящихся в разных зонах ответственности, функции информационной безопасности возложены на радиоустройство, расположенное на стыке двух сегментов. Частным случаем внешнего сегмента сети является сеть клиента, которому предостав ляется услуга передачи данных. В таких сценариях должна быть обеспечена фильтрация как входящего, так и исходящего трафика.

Рисунок 1б - Радиоканал, объединяющий внутренний и внешний сегменты

Рисунок 1в - Радиоканал, объединяющий внутренний и внешний сегменты

Объединение внутреннего сегмента сети и сети интернет

Сценарий с нахождением беспроводного устройства на стыке внутреннего сегмента сети и сети интернет является частным случаем сценария, рассмотренного выше. Отличием является отсутствие эшелонов безопасности устройства со стороны подключения к сети Интернет, что является причиной большого количества рисков.

Рисунок 1г - Радиоканал, объединяющий внутренний сегмент сети и сеть интернет

Таблица применимости средств обеспечения ИБ в различных сценариях

Обеспечение ИБ достигается выполнением мероприятий, описанных в разделах и подразделах ИБ:

Раздел ИБ	Подраздел ИБ	Применимость
Физическая безопасность	Все	ВСЕ СЦЕНАРИИ
Безопасность в радиоканале	Все	ВСЕ СЦЕНАРИИ
Управление устройством	Аутентификация	ВСЕ СЦЕНАРИИ
	Методы доступа	LAN - СТОРОННЯЯ LAN LAN - WAN
	Интерфейс управления	ВСЕ СЦЕНАРИИ
	Ограничение доступа	LAN - СТОРОННЯЯ LAN LAN - WAN
	Восстановление доступа	ВСЕ СЦЕНАРИИ
Передача данных	Общие рекомендации	ВСЕ СЦЕНАРИИ
	Настройка передачи данных	ВСЕ СЦЕНАРИИ
	Настройка сетевых протоколов	ВСЕ СЦЕНАРИИ
Инфраструктура	Мониторинг	ВСЕ СЦЕНАРИИ
	Хранение истории	ВСЕ СЦЕНАРИИ
	Технический учёт	ВСЕ СЦЕНАРИИ

Физическая безопасность

Физический уровень является фундаментом информационной безопасности, поэтому обеспечение физической безопасности устройств является приоритетной задачей при реализации технической политики предприятия. Обеспечение физической безопасности подразумевает

комплексный подход и включает несколько компонентов:

- выбор площадки для установки оборудования;
- организация вспомогательной инфраструктуры объекта;
- монтаж оборудования;
- эксплуатация объекта.

Объект связи, включающий в себя беспроводные устройства, состоит из трёх основных элементов (рис. 2):

- Высотная часть: место размещения беспроводных устройств, например, крыша здания, мачта, телекоммуникационная башня.
- Кабельная трасса: путь прохождения кабелей, соединяющих высотную часть и оборудование, размещённое в помещении.
- Помещение: оборудование, размещённое в помещении, и точки подключения к инфраструктуре. Инфраструктура может включать в себя каналы передачи данных, электропитание, климатические системы и т.д. Оборудование должно быть размещено в стойке или телекоммуникационном шкафу, которые могут размещаться в выделенном помещении или быть совмещены с высотной частью объекта.

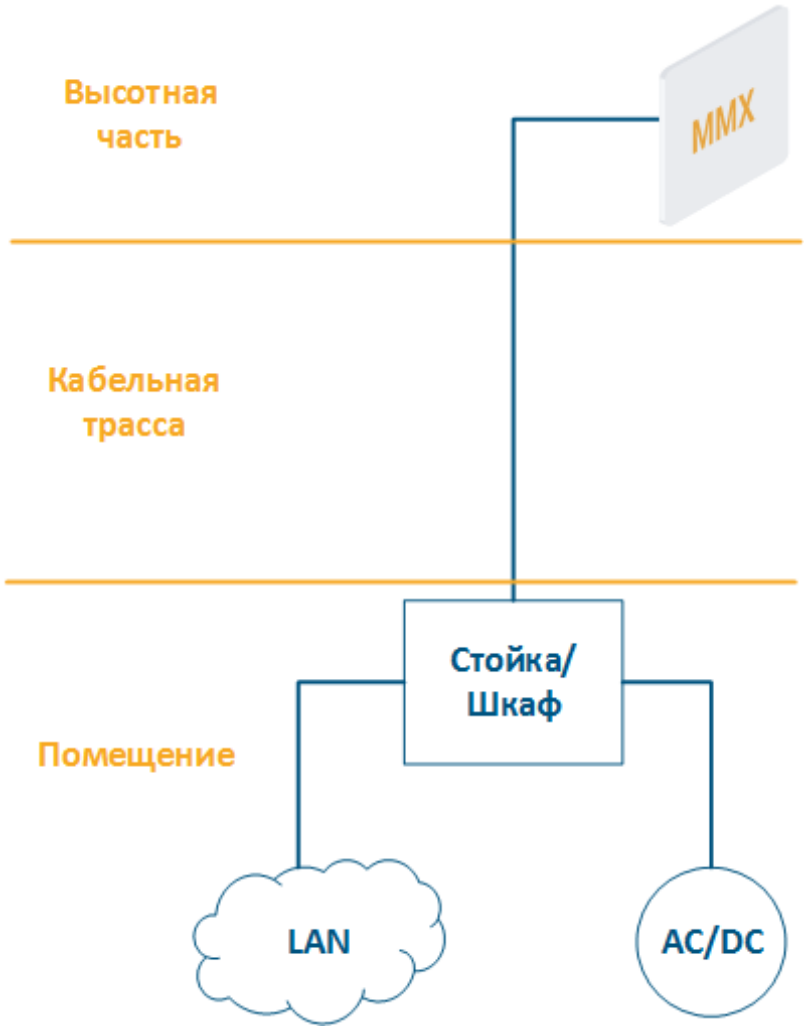

Рисунок 2 - Структурная схема объекта связи

Выбор площадки для установки оборудования

Площадка для размещения оборудования должна отвечать требованиям технической политики предприятия и предусматривать развитие объекта связи. При выборе площадки следует обратить внимание на следующие аспекты:

- Доступ на объект является важным фактором, влияющим на время восстановления связи и удобство обслуживания оборудования на объекте. Доступ на объект должен быть ограничен по времени и по спискам сотрудников. Списки доступа должны поддерживаться в актуальном состоянии. Отсутствие актуальных списков доступа может быть использовано, например, уволенным сотрудником, имя которого не было своевременно исключено из этих списков. Также следует обращать внимание на наличие охраны и замков в местах размещения оборудования для предотвращения несанкционированного доступа.
- Наличие выделенного помещения. Оборудования передачи данных и точки подключения к инфраструктуре рекомендуется размещать

в выделенном помещении, закрытом от воздействия внешних факторов. Например, это может быть помещение с отдельным входом и доступом отдельных сотрудников предприятия или машинный зал, в котором размещается оборудование сторонних компаний.
- Кабельная трасса. Площадка должна отвечать требованиям по прокладке кабельной трассы и доступу к ней на этапе эксплуатации. Соблюдение общих требований при прокладке кабелей является важным фактором снижения рисков, связанных с нарушением доступности каналов связи, которое может быть вызвано повреждением кабеля или ошибками подключения.
- Электропитание. На площадке должна присутствовать возможность подключения к сети стабильного электропитания (ЭП). В соответствии с технической политикой предприятия, может быть организована резервная линия ЭП или система бесперебойного обеспечения электричеством. Источники тока должны быть независимыми, т.е. должны отсутствовать единые точки отказа. Для систем резервного ЭП рекомендуется реализовывать схемы автоматического переключения между источниками, что позволит избежать перерыва связи при отказе основного источника ЭП.
- Заземление. Корректное заземление позволяет существенно снизить вероятность выхода беспроводных устройств из строя в случае электромагнитных наводок или удара молнии.
- Климатические системы. Надёжная работа сетевого оборудования зависит от внешних условий эксплуатации: устройство гарантированно функционирует в установленном диапазоне значений температуры, давления и влажности. Влияние среды носит случайный характер, поэтому, для поддержания стабильной работы, заданный диапазон климатических условий должен быть создан искусственно, для чего на объекте рекомендуется установить кондиционер и обогреватель с возможностью их автоматического включения/отключения. Применение климатических систем в высотной части невозможно, поэтому для надёжной работы в суровых условиях рекомендуется использовать устройства семейств InfiLINK 2x2 / InfiMAN 2x2 с расширенным температурным диапазоном. Такие устройства снабжены встроенным обогревателем, который включается при снижении температуры окружающей среды ниже установленного порога.
- Каналы связи. Сетевая доступность объекта может быть увеличена за счёт организации резервных каналов связи. Каналы связи должны быть независимыми, т.е. не иметь единых точек отказа, например, в качестве основного может использовать проводной канал связи, а в качестве резервного - беспроводной. Схемы организации отказоустойчивых схем автоматического резервирования и агрегации каналов связи с использованием устройств Инфинет представлены в статье "Агрегация каналов, балансировка и резервирование". В сценариях с подвижными объектами используется другая схема резервирования канала связи, представленная в статье "Организация связи с подвижными объектами".

Организация вспомогательной инфраструктуры объекта

Важным фактором при выборе площадки является возможность установки элементов вспомогательной инфраструктуры, которая позволит повысить доступность системы связи. Примерами вспомогательной инфраструктуры являются системы видеонаблюдения и сигнализации. Сигнализация позволит оперативно зафиксировать несанкционированный доступ на объект, а система видеонаблюдения будет полезна в расследовании инцидентов.

Монтаж оборудования

При выполнении монтажных работ на площадке следует руководствоваться общими требованиями и технической политикой предприятия. Некачественно выполненные монтажные работы могут стать причиной нарушения доступности всего сетевого объекта, восстановление которой может потребовать больших временных и финансовых ресурсов.

В целях обеспечения физической безопасности необходимо выполнить следующие настройки беспроводного устройства:

- отключение световых индикаторов на корпусе устройства повысит его скрытность;
- неиспользуемые порты беспроводных устройств могут быть использованы злоумышленником для получения доступа к сети, поэтому д ля исключения возможности несанкционированного подключения рекомендуется отключать неиспользуемые сетевые интерфейсы;
- модели устройств, основанные на аппаратной платформе H11, поддерживают функцию PoE-out на порту Eth1. Этим может воспользоваться злоумышленник, непосредственно подключившись к порту устройства и запитав стороннее оборудование. Если функция PoE-out не используется, необходимо убедиться в том, что её поддержка отключена.

Эксплуатация объекта

Контроль качества монтажных работ выполняется на этапе приёмки объекта в эксплуатацию. Процедура приёмки должна быть построена в соответствии с технической политикой предприятия.

Обеспечение информационной безопасности является непрерывным процессом, требующим контроля и реакции на выявленные и появляющиеся угрозы, поэтому необходимо проводить профилактическое обслуживание объектов связи. В зависимости от требований, закреплённых в компании, и специфики сетевого объекта список профилактических мероприятий может отличаться. Общий набор регулярных работ включает:

- осмотр объекта связи с составлением списка отклонений от требований технической политики;
- приборка на объекте;
- периодическое тестирование резервных систем: для каналов связи - плановые работы с отключением основного канала, для систем электропитания - плановые работы с отключением основного источника (дополнительно, для источников бесперебойного питания, тестирование ёмкости батарей).

Реализация средств обеспечения физической безопасности для семейств устройств

Список мероприятий

Мероприятия по обеспечению физической безопасности

Мероприятие / Интерфейс	InfiLINK 2x2 и InfiMAN 2x2		InfiLINK XG и InfiLINK XG 1000		Vector 5
	Web	CLI	Web	CLI	Web
Монтаж устройств	Установка InfiNet Wireless R5000		Установка		Установка устройств
Управление световой индикацией	-	Общие команды	-	Общие команды	-
Управление статусом интерфейсов	Настройки сети	Команда ifconfig (настройка интерфейсов)	Раздел Коммутатор	Команда ifconfig (настройка интерфейсов)	Настройка коммутации
Управление PoE-out	Настройки сети	Команда ifconfig (настройка интерфейсов)	-	-	-
Управление обогревателем	-	Специальные команды	-	-	-

Безопасность радиоканала

Беспроводная передача данных выполняется в общей среде, что позволяет злоумышленникам организовывать атаки различных видов. Рассмотренные ниже средства обеспечения безопасности должны применяться комплексно, поскольку мероприятия, направленные на борьбу с одной угрозой, могут быть не эффективны против другой.

Частотные настройки

Частотный ресурс является ограниченным, поэтому процесс распределения частот между беспроводными системами должен рассматриваться комплексно. Сторонние беспроводные системы, работающие на тех же или смежных частотах, могут оказывать влияние на радиоканал (рис. 3). Как правило, такое влияние не является злонамеренным, однако оно должно рассматриваться как угроза доступности, поскольку его результатом является невозможность функционирования канала связи. Нашей задачей является поиск и выбор частотного канала, свободного от помех. При этом, мы должны помнить, что помеха может отсутствовать на этапе монтажа, но появиться уже в процессе эксплуатации беспроводной системы.

Снизить риски, связанные с угрозами данного типа, можно следующими способами:

- Поиск источников помех: устройства семейств InfiLINK 2x2 и InfiMAN 2x2 позволяют получить MAC-адреса систем, работающих в выбранном частотном канале, с помощью утилиты "Radio scanner", что позволяет выявить источник помехи и принять решение о мерах по исключению его влияния на канал связи.
- Ручное сканирование спектра: предварительное радиообследование территории, в которой будет развёрнута система связи, выполненное вручную. Выбор частотного канала системы осуществляется с учётом данных сканирования. Устройства Инфинет позволяют оценить состояние спектра с помощью встроенной утилиты "Спектроанализатор".
- Автоматическое сканирование спектра: радиообследование территории, в которой развёрнута система связи, выполняемое автоматически с заданной периодичностью. Выбор частотного канала системы осуществляется с учётом данных сканирования и может быть автоматически изменён. В устройствах Инфинет реализована поддержка технологии DFS и iDFS (см. Динамический выбор частоты), которые предназначены для сканирования спектра в автоматическом режиме.

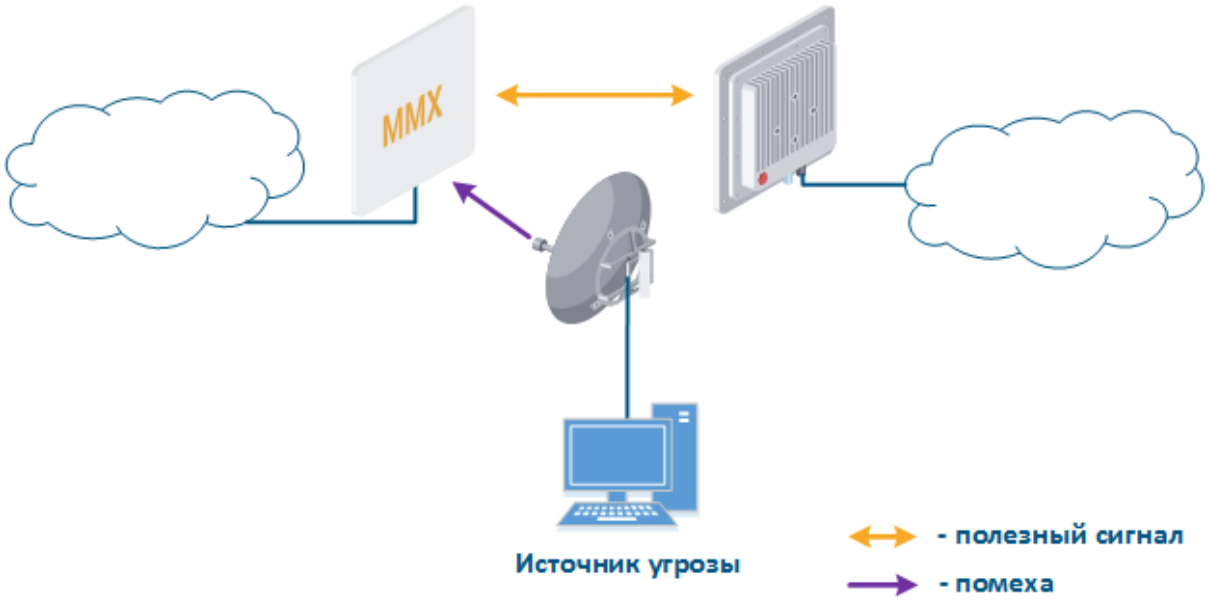

Рисунок 3 - Пример угрозы в частотном канале системы

Даже при согласованном распределении частотных каналов может сохраняться проблема взаимного влияния. Причиной этому служит внеполосное излучение: спектр излучения не является идеальным прямоугольником. Он имеет боковые полосы, которые оказывают влияние на соседние частотные каналы. Ниже представлены спектры систем связи (рис. 4 а-б), использующих соседние частотные каналы: в первом случае (рис. 4а) мощность излучения систем равна и влияние источника угрозы ниже чувствительности системы связи, во втором случае (рис. 4б) мощность излучения источника угрозы выше, чем системы связи и уровень боковой полосы выше чувствительности, что окажет влияние на систему связи в виде помехи.

Снизить влияние сторонней системы связи на используемые частотные каналы поможет функция автоматической регулировки выходной мощности (АТРС). При возникновении помех устройства с активной функцией АТРС увеличат мощность излучения, сохранив производительность канала связи.

Бюджет канала связи, помимо мощности излучения, зависит от используемой модуляционно-кодовой схемы: схемы высших порядков более требовательны к параметрам канала связи, поэтому их использование невозможно при низком уровне сигнала и высоком уровне помех. Таким образом, выбор модуляционно-кодовой схемы является компромиссом между производительностью и надёжностью канала связи. Использование функции автоматического контроля скорости передачи данных (АМС) позволяет выбирать модуляционно-кодовую схему в соответствии с текущими параметрами радиоканала и менять её в соответствии с обстановкой в эфире. Это позволяет повысить надёжность и доступность информации, сохраняя работоспособность канала связи даже в условиях сильных помех.

Подробно частотные характеристики сигналов рассмотрены в онлайн-курсе "Основы беспроводных сетей".

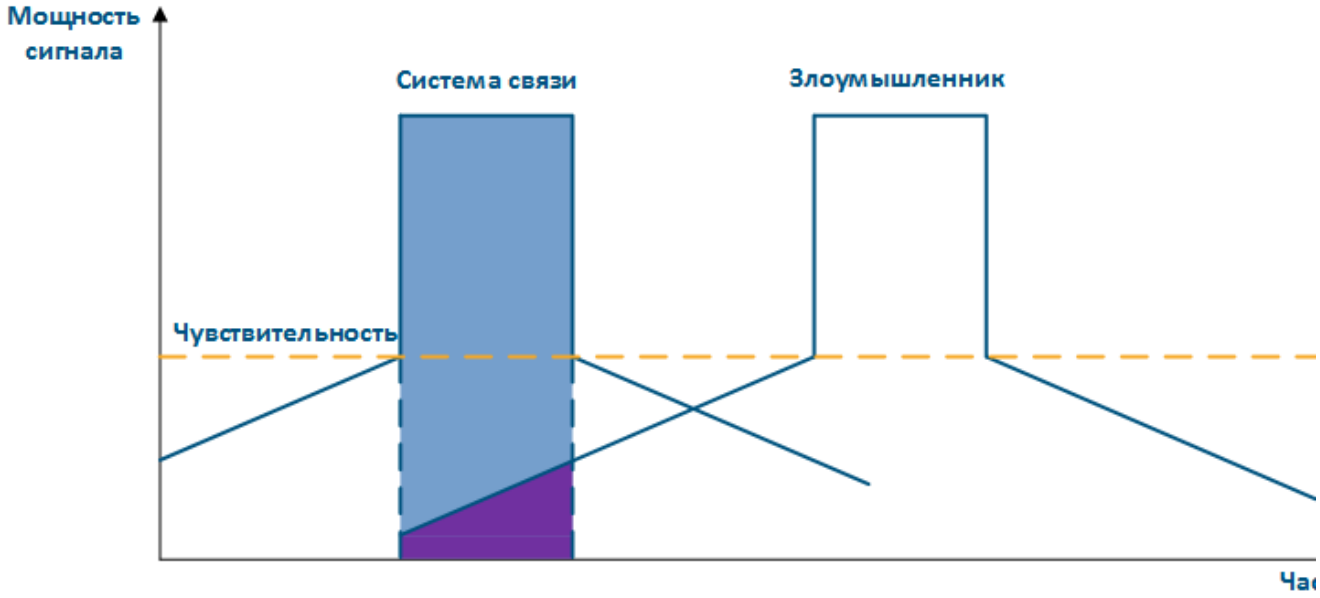

Рисунок 4а -Пример влияния соседнего частотного канала на систему связи

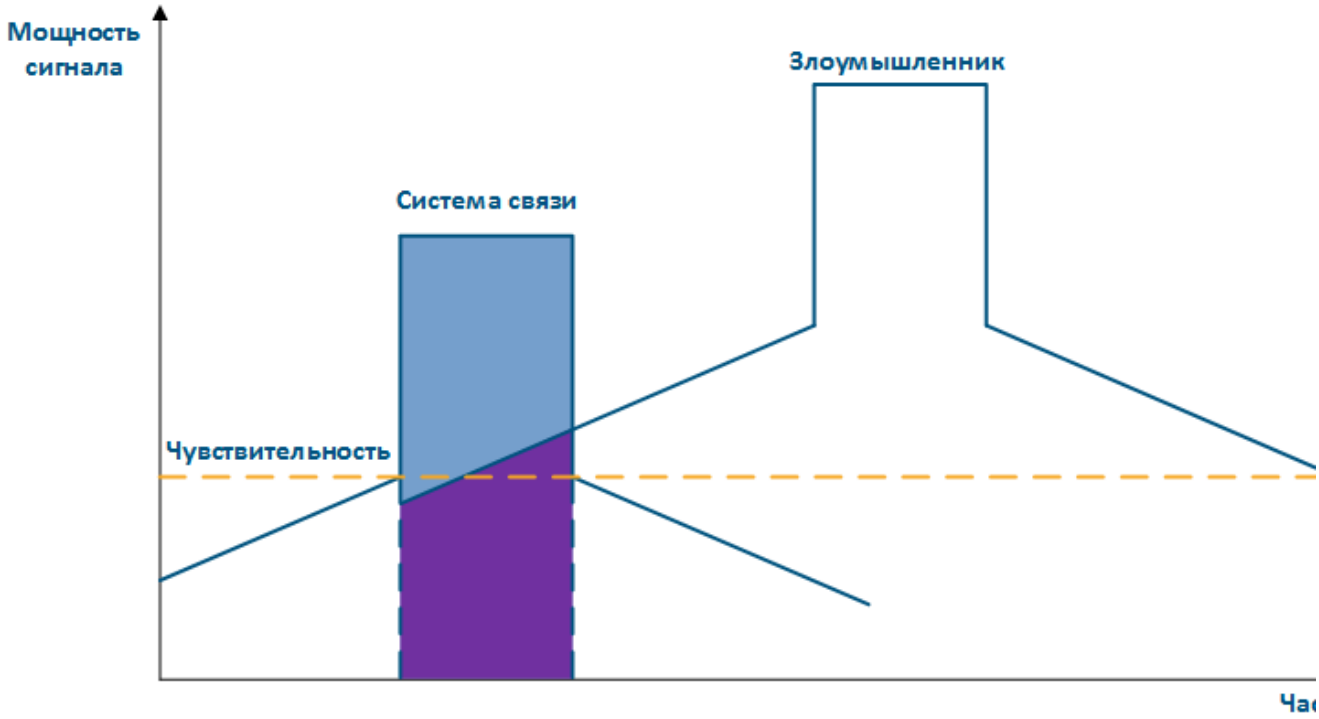

Рисунок 4б - Пример влияния соседнего частотного канала на систему связи

Настройки аутентификации

Популярными сценариями нарушения конфиденциальности и целостности информации в радиоканале являются атаки типа "человек посередине" (MITM - Man in The Middle). Рассмотрим примеры атак такого типа:

- Перехват данных (рис. 5а): в зоне покрытия системы связи злоумышленник устанавливает устройство, принимающее все передаваемые сигналы. Все беспроводные системы используют общую среду передачи данных, поэтому устройства принимают данные независимо от того, указаны ли они в качестве адресата. Далее устройство обрабатывает кадр на канальном уровне, если является его получателем, или отбрасывает, если не является. Злоумышленник может прикинуться одним из адресатов и получить доступ ко всем сообщениям, наравне с легальным адресатом.
- Ретрансляция данных (рис. 5б): частный случай сценария "Перехват данных", в котором злоумышленник использует ретранслятор вместо пассивного приёмника. Такой вариант атаки, например, применим для каналов "точка-точка" с узкой диаграммой направленности, для которых не подходит схема из сценария "Перехват данных".
- Подмена данных (рис. 5в): частный случай сценария "Ретрансляция данных", в котором злоумышленник подменяет данные при ретрансляции. В таком сценарии, помимо нарушения конфиденциальности, нарушается целостность данных.

Рисунок 5а - Перехват данных

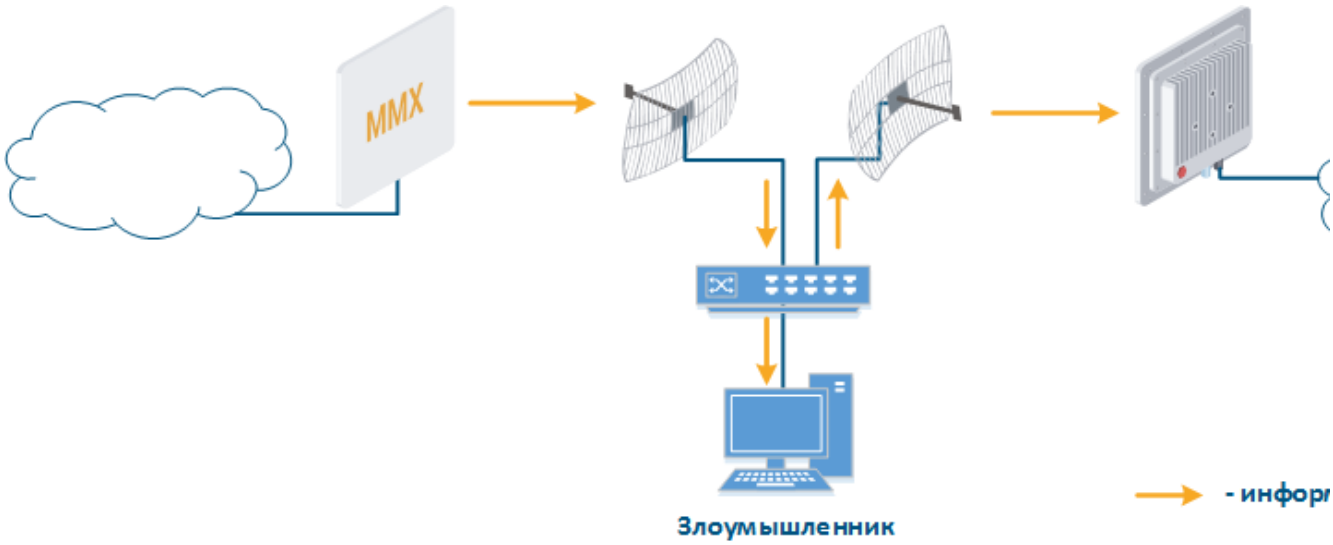

Рисунок 5б - Ретрансляция данных

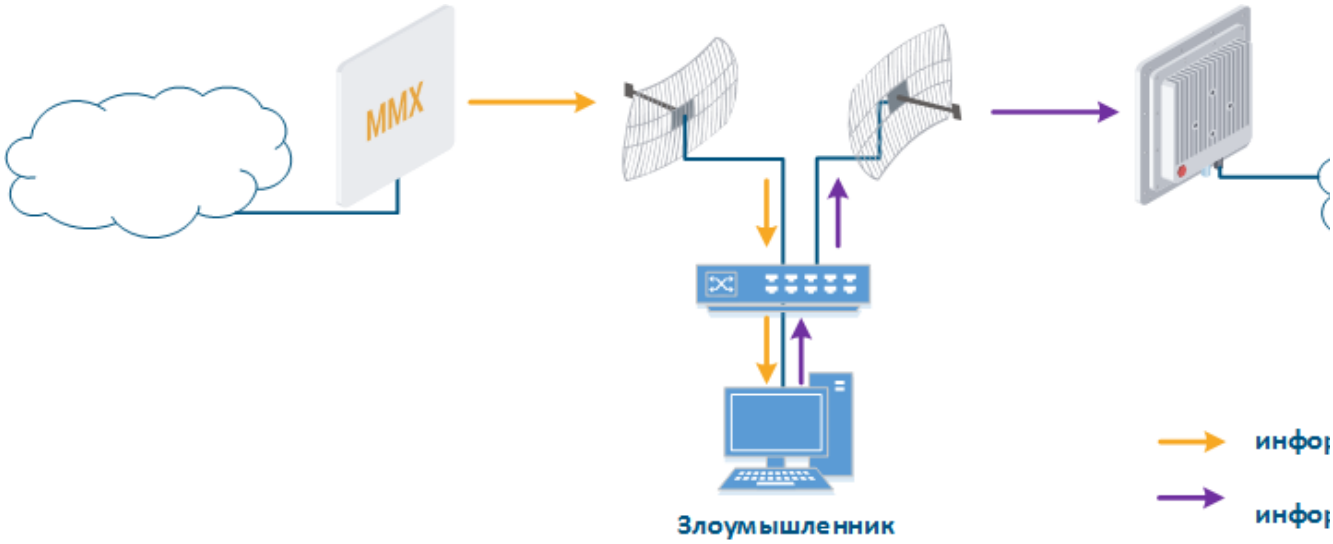

Рисунок 5в - Подмена данных

Наравне с атаками MITM возможны сценарии получения несанкционированного доступа к ресурсам через подключение к радиосети. Рассмотрим примеры атак такого типа:

- Подключение злоумышленника к сети предприятия (рис. 6): злоумышленник, имеющий абонентское устройство, может установить его в зоне действия базовой станции. После установки канала связи с сектором базовой станции, злоумышленник может получить доступ к сети предприятия и реализовать атаки, направленные на нарушение целостности, доступности и конфиденциальности. Злоумышленник сможет установить канал связи с сектором базовой станции только при условии использования беспроводного устройства Инфинет.

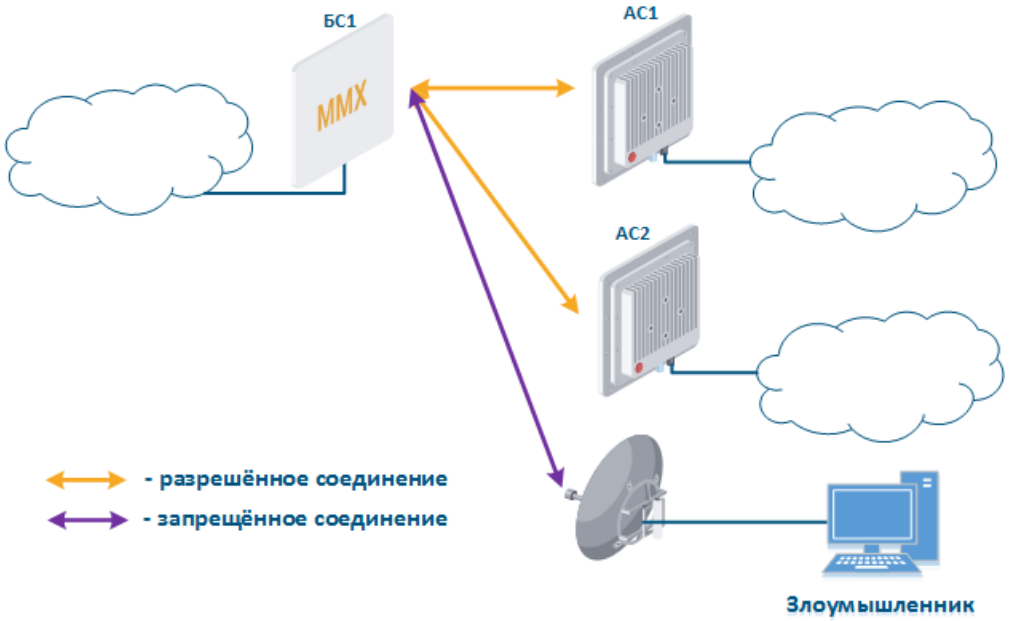

Рисунок 6 - Подключение злоумышленника к сети предприятия

- Подмена сектора базовой станции (рис. 7а,б): злоумышленник устанавливает сектор базовой станции, к которой подключается абонентская станция. После подключения злоумышленник получает несанкционированный доступ к данным, источником которым является абонентская станция, и сегменту сети за абонентской станцией. Рассмотрим пример реализации такой атаки в сценариях с организацией связи для подвижных объектов (см. Организация связи с подвижными объектами). Между АС и БС1 организован радиоканал (рис. 7а), при этом АС установлена на движущемся объекте, поэтому при отдалении от БС1, АС разрывает канал связи и начинает поиск сектора базовой станции, с которым можно установить соединение (рис. 7б). Злоумышленник установил сектор базовой станции на пути следования АС, между БС1 и БС2, поэтому после отключения от БС1, АС устанавливает связь с сектором злоумышленника. Реализация атаки такого типа возможна только в случае пренебрежения настройками безопасности.

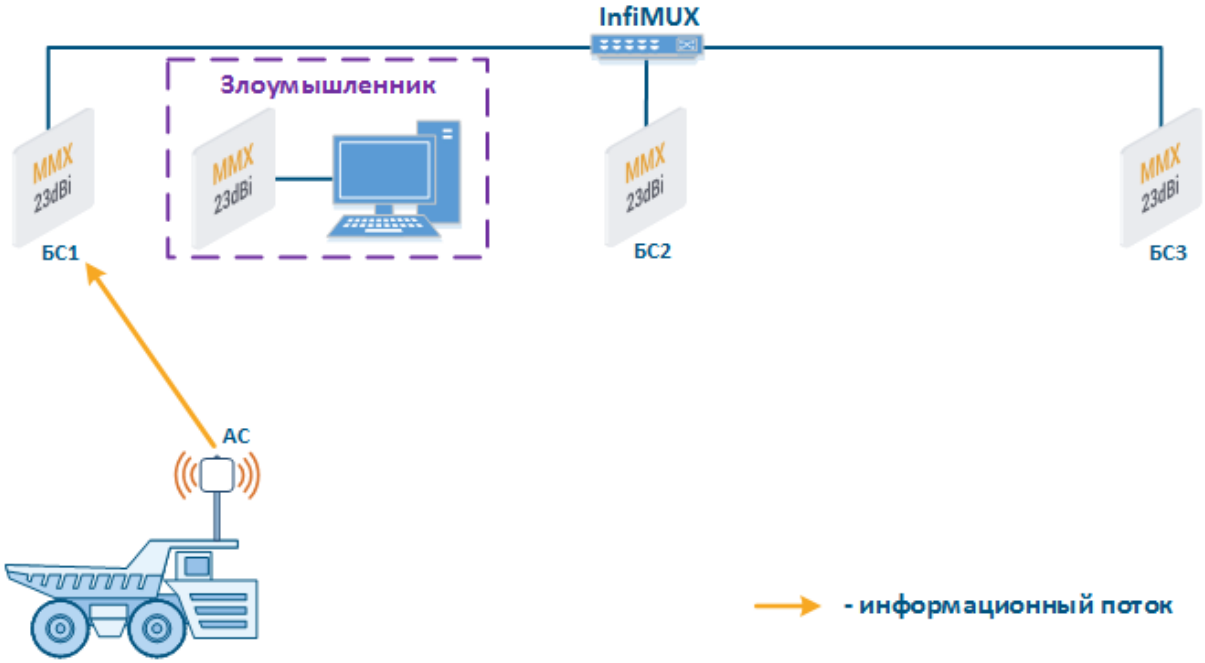

Рисунок 7а - Подключение абонентской станции к сектору базовой станции предприятия

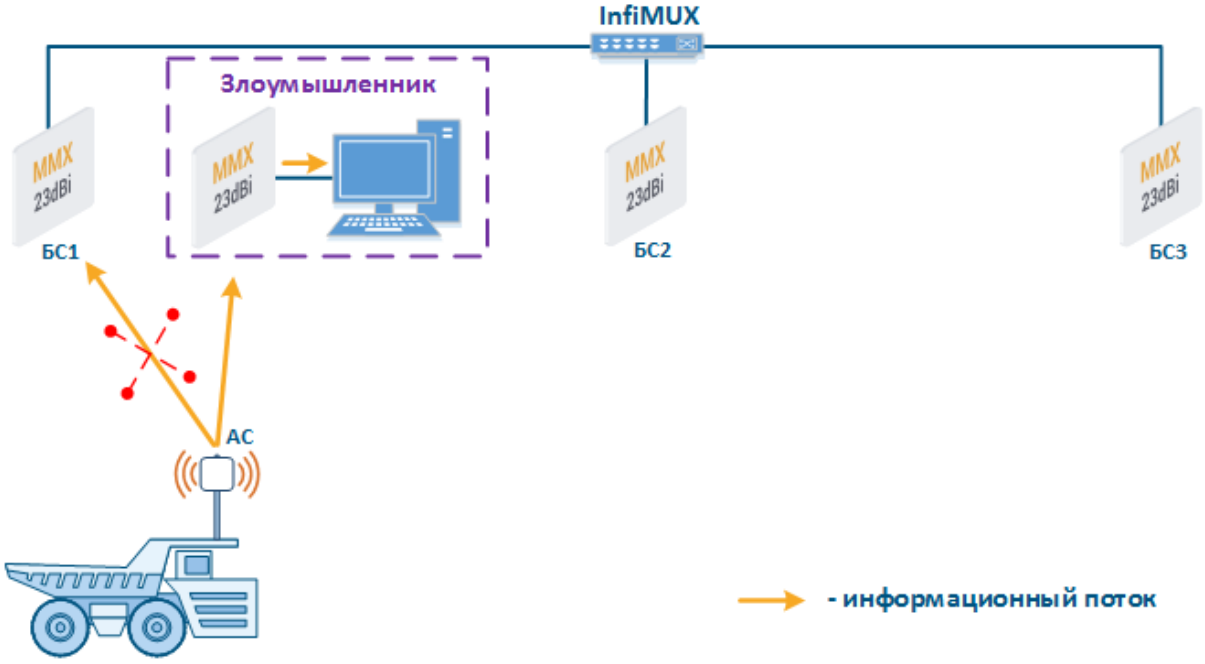

Рисунок 7б - Подключение абонентской станции к сектору базовой станции злоумышленника

Устройства Инфинет используют собственный формат радиокадров, что делает невозможным организацию канала связи между устройствами, работающими по стандартам семейства 802.11, и устройствами Инфинет. Это усложняет реализацию планов злоумышленника, т.к. он будет вынужден использовать устройства Инфинет.

Для противодействия атакам рассмотренного типа должны применяться следующие инструменты:

- Идентификатор канала связи: всегда меняйте значение параметра, установленное по умолчанию, на уникальное.
- Ключ безопасности: устройства смогут установить канал связи, только если у них совпадают идентификатор канала и ключ безопасности, т.е. для снижения вероятности организации канала связи с устройством злоумышленника, на обоих устройствах должны быть установлены ключи безопасности.
- Режим авторизации: устройства семейств InfiLINK 2x2 и InfiMAN 2x2 поддерживают настройку режима авторизации при установлении беспроводного канала связи. К методам, позволяющим ограничить список устройств, с которыми разрешена установка канала связи, мо

жно отнести "статический" и "remote". При статическом методе авторизации указывается список MAC-адресов устройств, с которыми может быть установлен беспроводной канал связи (белый список), либо список адресов, с которыми запрещено устанавливать канал связи (чёрный список). Метод "remote" позволяет централизованно хранить MAC-адреса для белых или чёрных списков и выполнять соответствующие запросы при попытках установления радиоканала. Использование одного из описанных методов авторизации значительно усложнит неавторизованное подключение злоумышленника к сети, т.к. MAC-адрес его устройства будет отсутствовать в списке разрешённых.

- Число каналов связи: на секторе базовой станции может быть установлено пороговое значение числа абонентских станций, которые могут быть подключены к сектору. Рекомендуется установить значение на уровне фактического количества абонентских станций.
- Скрэмблирование: обратимый процесс перераспределения битов данных в соответствии с заданным алгоритмом с целью выравнивания частотного спектра сигнала. Побочным эффектом скрэмблирования является сложность расшифровки перехваченных данных, т.к. злоумышленник должен обладать используемым алгоритмом дескрэмблирования для восстановления исходной последовательности битов. Операции скрэмблирования/дескремблирования потребуют аппаратных ресурсов, поэтому использование данной опции рекомендуется в случаях невысокой аппаратной загрузки устройств.
- Частотная сетка: диапазон поддерживаемых радиомодулем частот может быть осознанно ограничен с помощью частотной сетки на устройствах всех семейств Инфинет. Данное ограничение сужает список частот, которые могут быть установлены в качестве центрально й. Инструмент настройки частотной сетки предназначен для сужения списка разрешённых к использованию частот и его дополнительным эффектом является повышение уровня защищённости устройства от выбора случайного частотного канала в качестве рабочего. Если в конфигурации устройства установлен автоматический выбор центральной частоты, то она будет выбрана в соответствии с частотной сеткой. Кроме того, центральная частота может быть установлена вручную: на устройствах с ролью "Ведущий" центральная частота устанавливается явно, на устройствах с ролью "Ведомый", в зависимости от семейства, либо явно, либо с помощью одного или нескольких радиопрофилей. Если на абонентской станции используется несколько радиопрофилей (см. Организация связи с подвижными объектами), то при подключении к сектору базовой станции будет осуществляться перебор профилей до момента успешного подключения.
- Функция Global: в сценариях организации связи для подвижных объектов опция Global используется для подключения абонентской станции к секторам базовых станций, имеющих связность с ядром сети (см. Организация связи с подвижными объектами). Этот подход может применяться для блокировки подключений абонентских станций к секторам базовых станций, установленными злоумышленниками (рис. 7б): поскольку базовая станция злоумышленника не подключена к ядру сети, то абонентская станция в процессе роуминга будет игнорировать устройство злоумышленника.

Реализация средств обеспечения безопасности радиоканала для семейств устройств

Список мероприятий

Мероприятия по обеспечению безопасности радиоканала

Мероприятие	InfiLINK 2x2 и InfiMAN 2x2		InfiLINK XG и InfiLINK XG 1000		Vector 5
	Web	CLI	Web	CLI	Web
Анализ спектра	Спектроанализатор	Команда muffer	Раздел Спектроанализатор	Команда сканирования радиоспектра	Спектроанализатор
Анализ радиокадров (Radio Scanner)	Состояние устройства	Команда muffer	-	-	-
Включение поддержки технологии DFS	Настройки линка	Команда dfs (Динамический выбор частоты)	Раздел Радио	Команды настройки модема	Настройка радиоканала
Включение поддержки технологии Instant DFS	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	Раздел Радио	Команды настройки модема	-
Просмотр результато вработы DFS/Instant DFS	Вкладка DFS	-	Раздел Instant DFS	Команды настройки модема	-
Автоматическая регулировка мощности излучения	Настройки линка	Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Настройка радиоканала
Автоматическая регилуровка MCS	Настройки линка	Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Настройка радиоканала
Определение идентификатора канала связи	Настройки линка	Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Общие настройки

Определение ключа безопасности канала связи	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	Раздел Радио	Команды настройки модема	Настройки безопасности
Конфигурация режима авторизации	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-
Конфигурация списков для статического режима авторизации	Статические линки	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-
Конфигурация списков для удалённого режима авторизации	-	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-
Определение максимального числа абонентских станций	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-
Управление статусом технологии скрэмблирования	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-
Конфигурация частотной сетки	Настройки линка	Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Настройка радиоканала
Конфигурация центральной частоты (устройства с ролью "Ведущий")	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Настройка радиоканала
Конфигурация центральной частоты (устройства с ролью "Ведомый")	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA Команда rfconfig в версии MINT Команда rfconfig в версии TDMA	Раздел Радио	Команды настройки модема	Настройка радиоканала
Выбор регуляторного домена	-	-	-	-	Общие настройки
Использование функции Global	-	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-

Управление устройством

Получение несанкционированного доступа к интерфейсу управления устройством является серьёзной угрозой, которая может повлечь за собой нарушение всех основных свойств информации, поэтому необходимо уделить внимание тщательной проработке мероприятий по обеспечению безопасности информации и снижения потенциальных рисков.

Аутентификация и авторизация

Внимание!
По умолчанию в конфигурацию устройств Инфинет добавлен один пользователь с административными параметрами и следующими значениями атрибутов:

- логин: любая непустая строка;
- пароль: любая непустая строка.

Поскольку с настройками аутентификации по умолчанию велика вероятность несанкционированного доступа, требуется изменить логин и пароль при первоначальной настройке.

В компаниях может быть организовано несколько линий технической поддержки: в такой схеме часть проблем, не требующих изменения конфигурации беспроводных устройств, может быть решена первой линией технической поддержки. Ресурсы квалифицированных сотрудников второй и третьей линий технической поддержки для решения тривиальных задач использованы не будут. Для реализации описанного сценария в конфигурацию устройства может быть добавлена гостевая учётная запись. Пользователь, получивший доступ к интерфейсу управления с использованием гостевой учётной записи, может использовать утилиты и просматривать статистику интерфейсов, но ему запрещено вносить изменения в конфигурацию.

При эксплуатации сетей с большим количеством устройств рекомендуется использовать централизованное хранение учётных записей. Это позволяет избежать ошибок при блокировании учётных записей, обеспечить единую парольную политику и иметь единый интерфейс для управления учётными записями. Устройства Инфинет поддерживают работу протокола RADIUS, который предназначен для централизованной аутентификации, авторизации и аккаутинга в сетях. В зависимости от возможностей и масштабов сети, база данных учётных записей для работы RADIUS может быть развёрнута на отдельном устройстве, либо совмещена с другим элементов сети.

Алгоритм использования RADIUS-сервера

Алгоритм использования RADIUS-сервера выглядит следующим образом (рис. 8):

1. Запрос на доступ к интерфейсу управления устройством: пользователь пытается получить доступ к интерфейсу управления устройством с помощью одного из протоколов (см. ниже), формируя запрос, в котором передаёт логин и пароль.
2. Формирование запроса серверу RADIUS: устройство принимает запрос от пользователя и формирует запрос серверу в соответствии с протоколом RADIUS.
3. Ответ от сервера RADIUS: сервер RADIUS получает запрос и проверяет наличие и выделенные права для пользователя, учётные данные которого переданы в запросе. Сервер формирует один из двух ответов:
    a. Доступ разрешён: учётная запись присутствует в базе и ей разрешён доступ к интерфейсу управления устройством Slave (рис. 8а).
    b. Доступ запрещён: учётная запись отсутствует в базе, либо данному пользователю запрещён доступ к интерфейсу управления Slave (рис. 8б).
4. Принятие решения устройством: устройство получает ответ от сервера RADIUS и принимает решения об авторизации пользователя с указанной текущей записью. В случае успешной авторизации пользователю демонстрируется интерфейс управления устройством (рис. 8а), в противном случае пользовательское соединение сбрасывается и демонстрируется информационное сообщение.

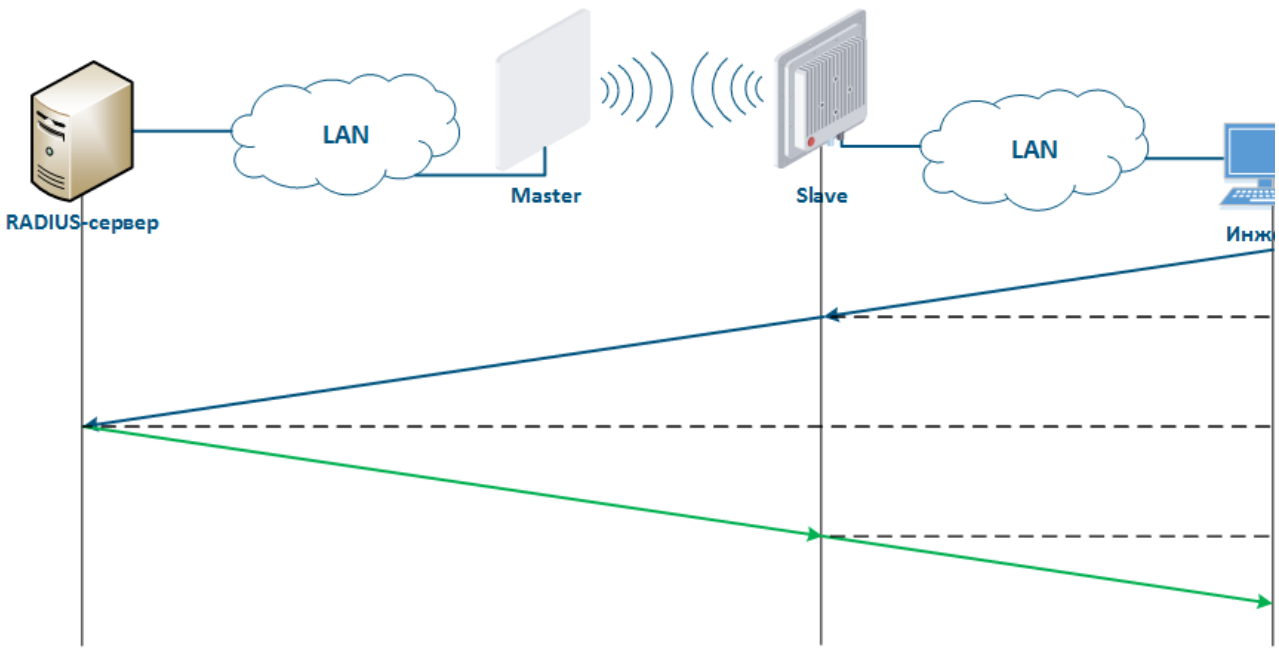

Рисунок 8а - Пример успешного прохождения аутентификации через RADIUS

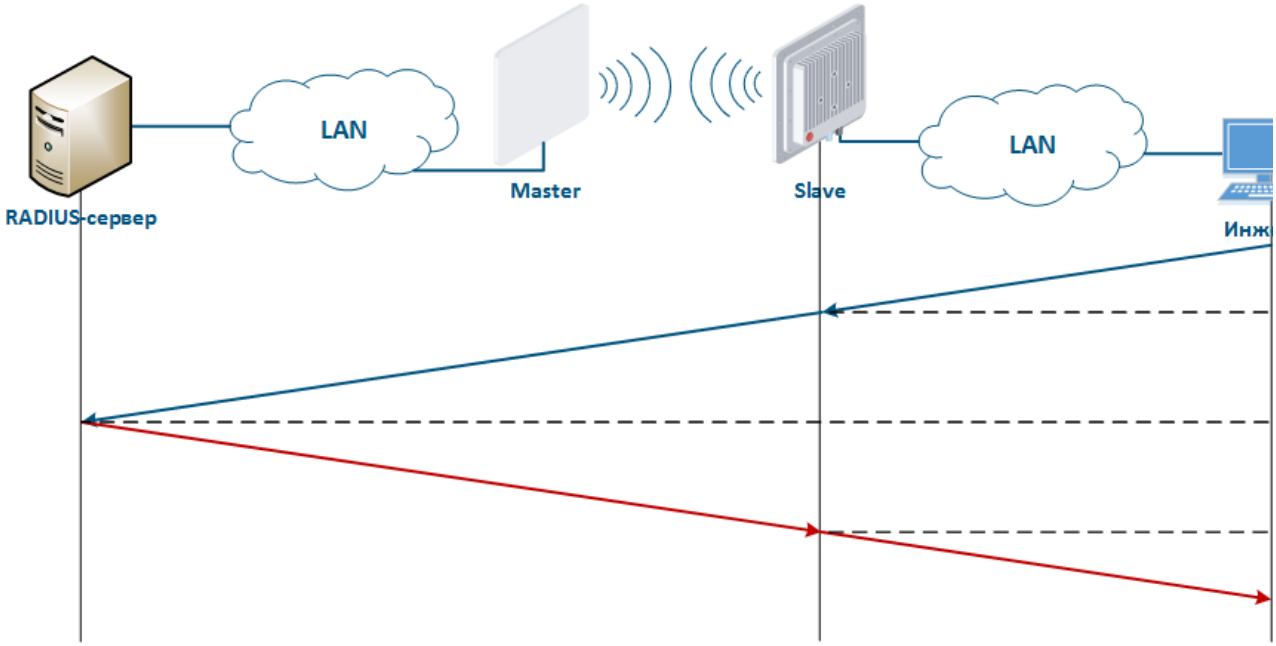

Рисунок 8б - Пример неудачного прохождения аутентификации через RADIUS

Методы доступа

Конфигурация устройств Инфинет может быть выполнена с помощью графического Web-интерфейса или интерфейса командной строки (CLI). Управление некоторыми функциями устройства возможно только с помощью CLI. Доступ к тому или иному интерфейсу осуществляется с помощью различных сетевых протоколов. Неиспользуемые протоколы рекомендуется отключить, тем самым сократив возможности несанкционированного доступа к интерфейсу управления устройством.

Протоколы управления, поддерживаемые устройствами Инфинет, соотносятся с интерфейсами управления следующим образом:

- Web-интерфейс:
  - Протокол HTTP: данные передаются по сети в открытом виде, поэтому злоумышленник, получив доступ к сети, может их перехватить.
  - Протокол HTTPS: данные передаются по сети в зашифрованном виде, поэтому злоумышленник, перехвативший данные, не сможет их расшифровать, не имея соответствующих ключей шифрования При отсутствии особых причин для использования HTTP, должен использоваться протокол HTTPS.
- Интерфейс CLI:
  - Протокол Telnet: данные передаются в открытом виде, поэтому злоумышленник, получив доступ к сетевой инфраструктуре, может перехватить информацию. Использование протокола Telnet допустимо в случае крайней необходимости, когда отсутствует возможность использования SSH.
  - Протокол SSH: данные передаются в зашифрованном виде. В случае, если злоумышленник сможет перехватить служебные сообщения, то, не имея ключей шифрования, он не сможет их расшифровать.

Сетевой интерфейс управления

Сетевой интерфейс управления (mgmt), используемый для доступа к устройству, в разных семействах устройств организован по-разному:

- InfiLINK XG, InfiLINK XG 1000 и Vector 5: выделен внутренний виртуальный интерфейс mgmt для управления устройством, который может быть ассоциирован с IP-адресом.
- InfiLINK 2x2 и InfiMAN 2x2: IP-адрес может быть ассоциирован с виртуальным или физическим интерфейсами, т.е. в роли сетевого интерфейса управления могут выступать интерфейсы различных типов, например eth0, svi100. В конфигурацию могут быть добавлены несколько сетевых интерфейсов управления одного или разных типов.

Помимо выбора интерфейса, с которым будет ассоциирован IP-адрес управления, также существует возможность управления связностью между интерфейсом управления и другими сетевыми интерфейсами. Данный механизм позволяет ограничивать доступ к устройству через проводные или беспроводные интерфейсы, в зависимости от сценария использования оборудования.

На рис. 1 представлены сценарии использования устройств Инфинет. Рассмотрим организацию доступа к сетевому интерфейсу управления устройствами для каждого из сценариев. Для этого дополним схему ПК, подключенных к разным сетевым сегментам, с помощью которых выполняется управление устройствами (рис. 9а-в):

- Объединение двух сегментов локальной сети: доступ к интерфейсу управления устройств должен быть предоставлен пользователям ПК, подключенным к разным сегментам сети (рис. 9а). Беспроводные устройства находятся во внутренней сети и не контактируют с устройствами внешних сетей напрямую. Функцию обеспечения защиты от несанкционированного доступа должны выполнять сетевые элементы, находящиеся на границе внутренней и внешней сетей.
- Объединение сегментов локальной и сторонней сетей: доступ к интерфейсу управления устройств должен быть предоставлен только пользователю ПК, подключенному к локальному сегменту сети (рис. 9б), т.е. необходимо отключить возможность передачи данных между интерфейсом управления и проводным интерфейсом устройства Slave.
- Объединение сегментов локальной сети и сети интернет: доступ к интерфейсу управления устройств должен быть предоставлен пользователю ПК, подключенному к локальному сегменту сети (рис. 9в). Кроме того, доступ может быть предоставлен некоторым пользователям ПК, подключенных к сети интернет. При этом на пограничных устройствах обязательно должна быть настроена фильтрация входящего трафика, которая будет рассмотрена далее.

Рисунок 9а - Радиоканал, объединяющий два сегмента локальной сети

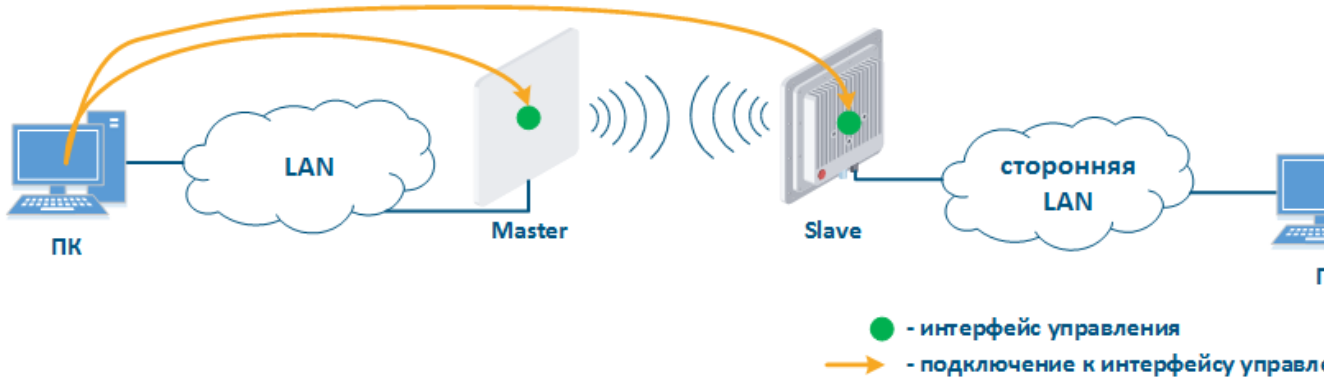

Рисунок 9б - Радиоканал, объединяющий сегменты локальной и сторонней сетей

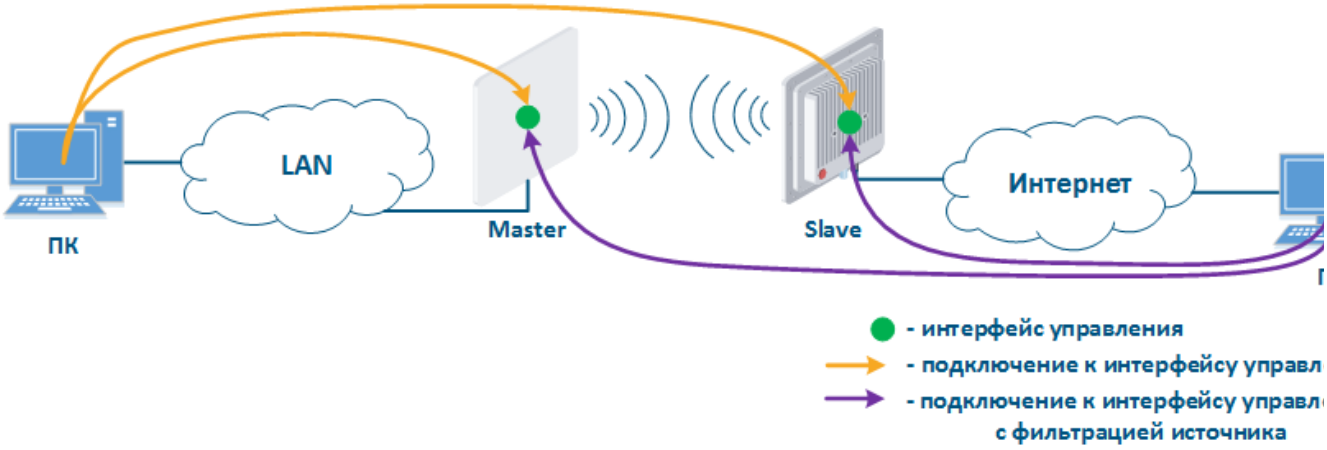

Рисунок 9в - Радиоканал, объединяющий сегменты локальной сети и сети интернет

Мы рекомендуем руководствоваться следующими принципами настройки интерфейса управления:

- В качестве интерфейса управления необходимо использовать виртуальный интерфейс:
  - Устройства семейств InfiLINK XG, InfiLINK XG 1000 и Vector 5: сетевой интерфейс управления mgmt.
  - Устройства семейств InfiLINK 2x2 и InfiMAN 2x2: сетевой интерфейс svi, связанный с группой коммутации управляющего трафика.
- Доступ к интерфейсу управления должен быть разрешён только через сетевые интерфейсы, за которыми расположены ПК инженеров или сервисы, осуществляющие управление устройствами, например, система мониторинга.
- В случае изоляции сетевого трафика с помощью VLAN, должен быть выделен отдельный VLAN для трафика управления, который должен быть ассоциирован с интерфейсом управления.

Ограничение доступа

Устройства семейств InfiLINK 2x2, InfiMAN 2x2 и Vector 5 позволяют создать белые списки доступа. В этом случае доступ к интерфейсу управления будет предоставлен только узлам, адреса которых включены в белые списки.

Восстановление доступа

Восстановление доступа к устройствам Инфинет всех семейств выполняется с помощью утилиты ERConsole (см. скринкаст "Утилита ERConsole"). Использование утилиты полезно в следующих сценариях:

- Ошибка в конфигурации устройства: утилита ERConsole позволяет назначить IP-адрес на интерфейс, либо сбросить устройство к заводским настройкам в ситуации, когда была допущена ошибка в конфигурации и доступ к устройству был утерян.
- Защита от использования устройства злоумышленником: для сброса устройства Инфинет к заводским настройкам требуется ввод заводского пароля, который закреплён за предприятием, которое его приобрело. В случае кражи устройства злоумышленником, он не сможет получить заводской пароль, обратившись в службу технической поддержки, т.к. не является сотрудником предприятия, значит не сможет получить доступ к устройству.

Реализация средств обеспечения безопасности управления для семейств устройств

Список мероприятий

Мероприятия по обеспечению безопасности управления устройством

Мероприятие	InfiLINK 2x2 и InfiMAN 2x2		InfiLINK XG и InfiLINK XG 1000		Vector 5
	Web	CLI	Web	CLI	Web
Смена параметров учётной записи	Системные настройки	Общие команды	Раздел Общие	Общие команды	Настройки безопасности
Создание гостевой учётной записи	-	Общие команды	Раздел Общие	Общие команды	-
Аутентификация через сервер RADIUS	-	Общие команды Процедура аутентификации с использованием RADIUS-сервера	-	Общие команды	Настройки безопасности
Конфигурация протоколов управления	Обслуживание	Команда td (Telnet daemon) Общие команды	Раздел Общие	Команда td (Telnet daemon) Общие команды	Настройки безопасности
Добавление IP-адреса управления	Настройки сети	Команда ifconfig (настройка интерфейсов)	Раздел Сетевой доступ	Команда ifconfig (настройка интерфейсов)	Настройка сетевого доступа
Ограничение доступа к устройству	IP Firewall	Общие команды Команда ipfw (IP Firewall)	-	-	Настройки безопасности
Восстановление доступа к устройству	Emergency Repair Console - утрачен контроль над устройством	Общие команды	Emergency Repair Console - утрачен контроль над устройством		Поиск и устранение неисправностей

Передача данных

Передача данных является основной функцией любого сетевого оборудования. Помимо пользовательских данных, устройства обмениваются служебными сообщениями вспомогательных протоколов, таких как SNMP, LLDP и т.д. Реализация описанных функций содержит в себе потенциальные угрозы, которыми может воспользоваться злоумышленник, что требует кропотливой настройки всех подсистем беспроводных устройств.

Общие рекомендации

Беспроводные системы представляют собой программно-аппаратные комплексы. Следовательно, одним из важнейших требований является своевременная актуализация программного обеспечения. Рекомендуется использовать стабильную версию программного обеспечения и следить за выходом обновлений. Проверить актуальность используемой версии ПО можно непосредственно на устройстве.

Внося изменения в конфигурацию устройств, следует иметь в виду, что механизм применения настроек зависит от того, в каком интерфейсе они применяются:

- Web-интерфейс: изменения, вносимые в разных разделах интерфейса, накапливаются и последовательно вносятся в конфигурацию только после нажатия кнопки "Применить". При перезагрузке устройства, будет выполнена загрузка последней успешно сохранённой конфигурации.
- Интерфейс CLI: при выполнении команда мгновенно добавляется в текущую конфигурацию, но не сохраняется. Для сохранения настроек необходимо выполнить соответствующую команду. При перезагрузке устройства будет выполнена загрузка последней успешно сохранённой версии конфигурации.

В некоторых ситуациях ошибки, допущенные в процессе настройки устройства, могут привести к потере связи с устройством. Независимо от последствий, будет нарушена доступность связи и может потребоваться сброс устройства к заводским настройкам (см. "Восстановление доступа"). Для того, чтобы снизить риск возникновения рассмотренного сценария, рекомендуется использовать отложенную перезагрузку устройства. В этом случае после применения новой конфигурации будет выполнена проверка доступности устройства. Если устройство недоступно, то будет возвращена предыдущая версия конфигурации.

Служебный трафик

По умолчанию коммутация на устройстве настроена таким образом, чтобы данные между проводным и беспроводным интерфейсами не подвергались фильтрации. Такая схема уязвима для большого объёма паразитного трафика, который может занять всю доступную пропускную способность и канал связи фактически станет недоступен для передачи полезного трафика. Пример паразитного трафика - широковещательный шторм, причиной которого может быть ошибка в коммутации устройств, либо действия злоумышленника. Мероприятиями по защите сетевой инфраструктуры от атак подобного типа являются:

- Фильтрация трафика: хорошей практикой является разделение физической инфраструктуры на несколько виртуальных локальных сетей с использованием технологии VLAN. Такой метод позволяет ограничить широковещательные домены, а значит уменьшить влияние шир оковещательного шторма. Это потребует настройки фильтрации трафика разных VLAN на устройствах: на беспроводных устройствах рекомендуется разрешить обработку только тех меток VLAN, которые действительно должны быть переданы через организованный радиоканал и запретить все остальные.
- Протокол STP: протокол покрывающего дерева (Spanning Tree Protocol) предназначен для предотвращения петель на канальном уровне, которые могут быть причиной широковещательного шторма. Кроме того, протокол STP может быть использован для построения схемы автоматического резервирования на канальном уровне в сетях с избыточностью каналов связи.
- Режим маршрутизатора: одним из подходов к снижения влияния широковещательного шторма является уменьшение размера широковещательного сегмента за счёт использования технологии маршрутизации. Маршрутизатор является устройством, разделяющим широковещательные домены, т.е. широковещательный шторм, возникший в одном домене не повлияет на работу устройств в другом. Кроме того, маршрутизация подразумевает передачу пакетов на основе заголовка IP, включающего в себя поле TTL, которое исключает циклическое прохождение пакетов по сети.

Настройка сетевых протоколов

Помимо пользовательского трафика, устройства в сети обмениваются служебными данными с использованием различных протоколов. В процессе обеспечения безопасности необходимо помнить, что любая доступная служба является потенциальной целью злоумышленника.

DHCP

Устройства Инфинет могут быть настроены в качестве DHCP-клиента, DHCP-сервера и DHCP-ретранслятора. Следует иметь в виду, что протокол DHCP поддерживает не только выделение IP-адреса клиенту, но и передачу множества сетевых настроек.

Рассмотрим пример атаки с использованием протокола DHCP (рис. 10): организован канал связи между Master и Slave, на радиоинтерфейсе устр ойства Slave активирован DHCP-клиент, в корпоративной сети установлен DHCP-сервер. Представим, что злоумышленнику удалось подключить

сетевое устройство, на котором настроен сервер DHCP, к корпоративной сети. После установления канала связи Master-Slave, устройство Slave отправляет в сеть широковещательный запрос для получения сетевых настроек от DHCP-сервера. DHCP-серверы, находящиеся в сети, отвечают на запрос от Slave. Если ответ от сервера злоумышленника будет получен первым, то устройство Slave присвоит одному из сетевых интерфейсов предлагаемый адрес и сетевые настройки, которые переданы в этом запросе. Таким образом, злоумышленник может указать своё устройство в качестве маршрутизатора по умолчанию и получить доступ к трафику, передаваемому устройством Slave.

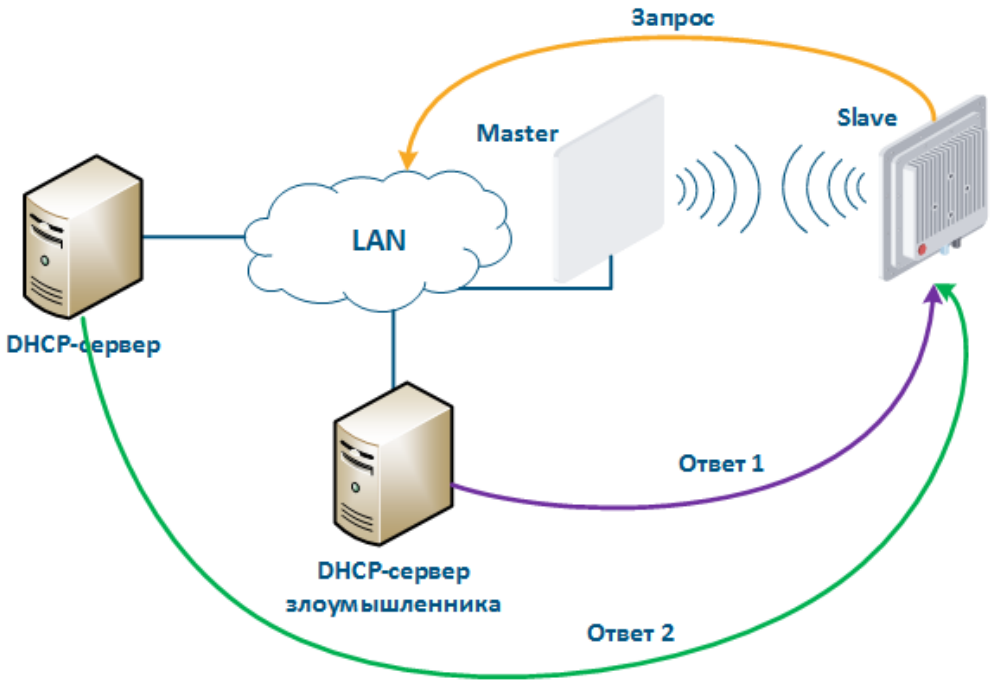

Рисунок 10 - Пример атаки с использованием протокола DHCP

Кроме того, возможна атака, в которой устройство злоумышленника будет выступать в роли DHCP-клиента (рис. 11): в сети установлен DHCP-сервер, функции которого могут быть реализованы на устройствах Инфинет, к сети подключено устройство злоумышленника. В ситуации, когда протокол конфигурация DHCP-сервера не предусматривает средств защиты, злоумышленник сформирует запрос и сервер предоставит устройству сетевые реквизиты. Таким образом, злоумышленник получит доступ к передаваемым по сети данным.

Рисунок 11 - Пример атаки с использованием протокола DHCP

Для того, чтобы повысить безопасность использования протокола DHCP в корпоративной сети рекомендуется реализовать следующие мероприятия:

- Ограничение DHCP-клиентом списка DHCP-серверов: DHCP-клиент позволяет ограничить список серверов, для которых будет формироваться запрос сетевых настроек. В этом случае DHCP-клиент сформирует запросы для указанных DHCP-серверов, а если они не ответят, то сформирует широковещательный запрос.
- Использование ключа безопасности: при аутентификации клиента может быть использован ключ безопасности. Следует иметь в виду, что данная настройка должна быть выполнена как на DHCP-сервере, так и на DHCP-клиенте.
- Фиксация пары "клиент-адрес" в конфигурации DHCP-сервера: конфигурация DHCP-сервера позволяет зафиксировать за клиентами, выделяемые им IP-адреса. Таким образом можно сформировать белые списки устройств, что затруднит действия злоумышленника для получения сетевых реквизитов.
- Использование DHCP Snooping: использование данной технологии позволяет предотвратить получение сетевых реквизитов от DHCP-сервера злоумышленника. Принцип работы весьма прост: порты устройств домена Ethernet, за которыми расположен DHCP-сервер, помечаются как доверенные, остальные - как ненадёжные. Сообщения от DHCP-серверов, пришедшие на вход ненадёжных портов будут отброшены, что делает невозможным получение устройствами-клиентами сетевых реквизитов от сервера злоумышленника.
- Отключение DHCP на неиспользуемых интерфейсах: необходимо тщательно следить за списком интерфейсов, на которых включена поддержка протокола DHCP. На интерфейсах, которые не используются для передачи данных или на которых используется статическая адресация, необходимо деактивировать поддержку DHCP. Эта рекомендация справедлива как для DHCP-клиента, так и DHCP-сервера.
- Отказ от протокола DHCP: следует понимать, что использование протокола DHCP должно иметь ограниченный характер, т.к. возможны сценарии, в которых рекомендуется использовать статическое назначение сетевых реквизитов на соответствующие интерфейсы. Так, например, статические адреса рекомендуется назначать ключевым сетевым элементам, в роли которых могут выступать и беспроводные устройства Инфинет. Это позволит избежать проблем при организации систем технического учёта и мониторинга.

ARP

Поскольку протоколы Ethernet и IP относятся к разным уровням модели сетевого взаимодействия, то необходим инструмент, который будет связывать адреса устройств, используемых в каждом из протоколов. Таким инструментом является протокол ARP и заполняемая им таблица

соответствия адресов. Таблица состоит из записей, в которых MAC-адрес интерфейса сопоставлен с IP-адресом, что используется при передаче IP-пакетов, инкапсулированных в Ethernet-кадры.

Рассмотрим пример атаки с подменой IP-адреса: через радиоканал Master-Slave организован доступ к сети интернет двум клиентам (Клиент 1 и Клиент 2). За каждым из клиентов закреплён IP-адрес, который является идентификатором для назначения тарифного плана. Клиенту с адресом 192.168.0.1 предоставляется пропускная способность 10 Мбит/с, клиенту с адресом 192.168.0.2 - 2 Мбит/с (рис. 12а). В какой-то момент времени Клиент 1 выключает ПК и не пользуется услугами провайдера, в это же время Клиент 2 заменяет свой IP-адрес на IP-адрес 192.168.0.1, закреплённый за Клиентом 1 (рис. 12б). В этом случае Клиент 2 получит доступ в Интернет с большей пропускной способностью, и у Клиента 1, после включения, возникнут проблемы с доступом к сети.

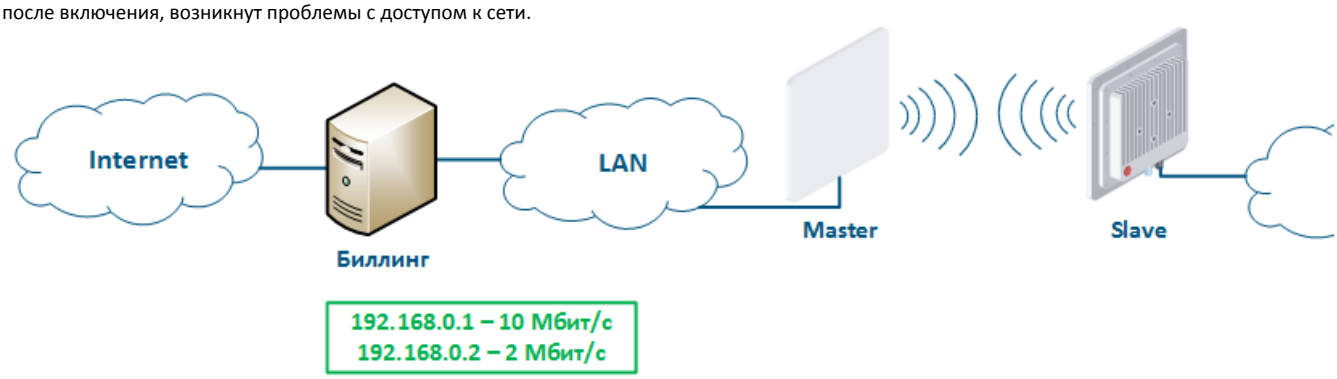

Рисунок 12а - Пример атаки с подменой IP-адреса

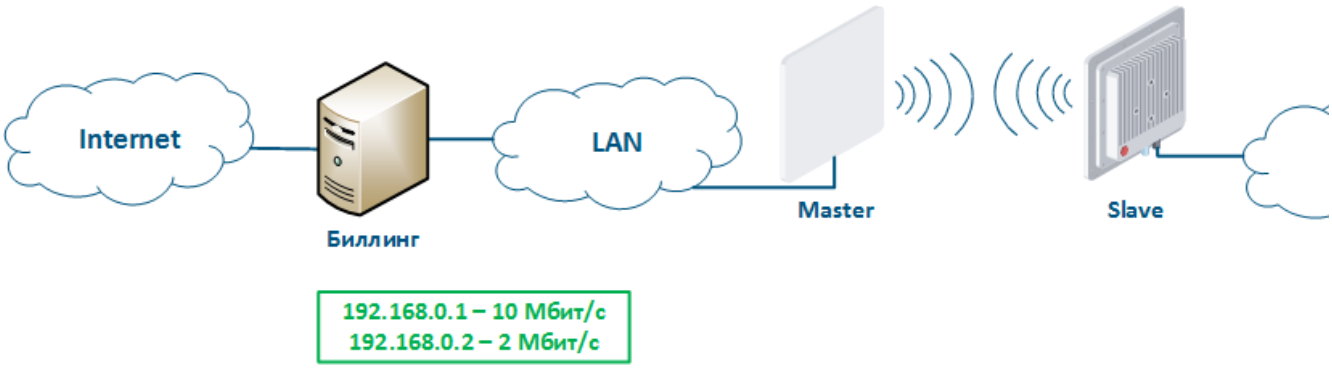

Рисунок 12б - Пример атаки с подменой IP-адреса

Рассмотренный вид атак с подменой IP-адреса можно предотвратить, добавив статическую запись в таблицу соответствия адресов протокола ARP. В этом случае, после смены IP-адреса данные Клиента 2 передаваться не будут, т.к. за адресом 192.168.0.1 будет закреплён MAC-адрес Клиента 1.

LLDP

Протокол LLDP предназначен для обмена справочной информацией об устройстве с непосредственно подключенным к нему устройством. В качестве справочной информации передаётся имя VLAN, MAC-адрес, имя устройства, IP-адрес интерфейса управления и т.д. В случае, если злоумышленник получит физический доступ к устройству и подключится к нему, то, запустив на своём ПК службу LLDP, сможет, обменявшись служебными сообщениями, получить справочную информацию об устройстве (рис. 13). Эти сведения могут облегчить ему задачу по несанкционированному доступу к устройству.

Для того, чтобы предотвратить атаки данного типа, необходимо придерживаться следующих правил:

- Глобальное отключение LLDP: в случае, если использование протокола не предусмотрено технической политикой предприятия, то рекомендуется отключить его работу на всех устройствах сети.
- Отключение LLDP на интерфейсах: если использование протокола LLDP необходимо, то следует разрешить его работу только на тех сетевых интерфейсах, к которым подключены элементы сетевой инфраструктуры.

Рисунок 13 - Пример атаки с использованием протокола LLDP

SNMP

Протокол SNMP был создан как унифицированный протокол для управления сетевыми устройствами и сбора данных об их функционировании. Протокол предусматривает запросы двух типов: запрос GET для получения значения какого-либо параметра и запрос SET для установки параметра в указанное значение. Таким образом, устройства, на которых реализована поддержка SNMP, могут работать в режиме чтения (обрабатывать только запросы GET) и режиме записи (обрабатывать запросы SET и GET). Активация сервера SNMP необходима, как правило, для централизованного управления устройствами с помощью системы мониторинга. Но если сервер SNMP настроен недостаточно надёжно, то им может воспользоваться злоумышленник В этом случае он сможет не только получить информацию о структуре сети, но и изменить конфигурацию устройства (рис. 14).

Для предотвращения несанкционировнного доступа следуйте рекомендациям:

- Использование SNMPv3: по умолчанию на устройствах активирована поддержка SNMPv1 и SNMPv2c, на устройствах создано community с именем "public". Протоколы SNMPv1 и SNMPv2c предусматривают аутентификацию с помощью параметра community, значение которого передаётся по сети в явном виде. В SNMPv3 реализованы как возможность аутентификации, так и шифрования сообщений, кот орое рекомендуется всегда использовать.
- Использование режима чтения: в случае, если не используется режим записи протокола SNMP, то требуется отключить его поддержку. Это снизит возможные последствия в случае несанкционированного доступа.
- Организация списков доступа: устройства Инфинет позволяют создать белые списки доступа к серверу SNMP.

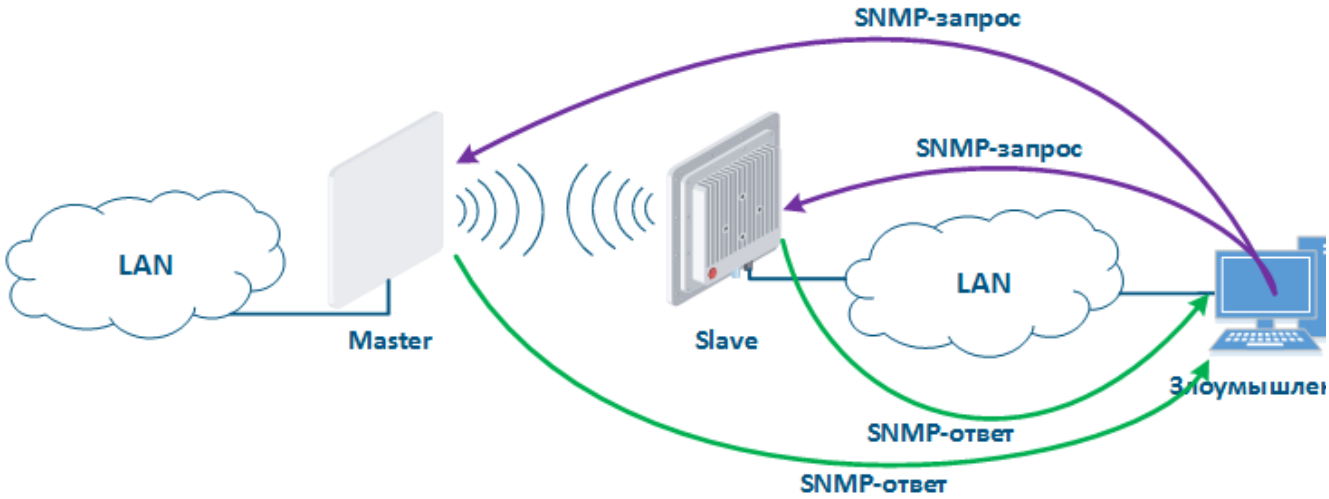

Рисунок 14 - Пример атаки с использованием протокола SNMP

MINT

MINT является фирменным протоколом компании Инфинет, работа которого может быть организована в проводном и беспроводном сегментах. Злоумышленник, получив доступ к области MINT, может скомпрометировать все сетевые устройства, относящиеся к этой области, поэтому при использовании протокола MINT необходимо обратить особое внимание на его настройку.

Рассмотрим пример атаки с использованием протокола MINT: два беспроводных канала связи Master 1 - Slave 1 и Master 2 - Slave 2 объединены в область MINT с помощью интерфейсов PRF (рис. 15а). Злоумышленник, имея физический доступ к сети предприятия, подключается к ней коммутатором InfiMUX, на котором создан интерфейс PRF (рис. 15б). В общем случае, интерфейсы PRF установят между собой каналы связи и все устройства будут объединены в область MINT, поэтому злоумышленник получит информацию об устройствах в этой области и сможет выполнять удалённые команды на них средствами MINT.

Средства защиты от атак подобного типа:

- Использование ключа безопасности: интерфейс PRF представляет собой виртуальный радиоинтерфейс, работающий в проводной среде, поэтому, по аналогии с беспроводным интерфейсом, интерфейс PRF поддерживает возможность установки ключа безопасности. При этом канал связи будет организован между двумя интерфейсами PRF только в том случае, когда их ключи безопасности совпадают.
- Использование пароля для выполнения удалённых команд: одним из удобных инструментов протокола MINT является возможность удалённого выполнения команд на устройстве, находящимся в той же области MINT. По умолчанию удалённое выполнение команд

доступно без указания пароля, поэтому такое поведение необходимо изменить. В этом случае, для удалённого выполнения команд на устройстве потребуется ввести пароль, что ограничит возможности злоумышленника.

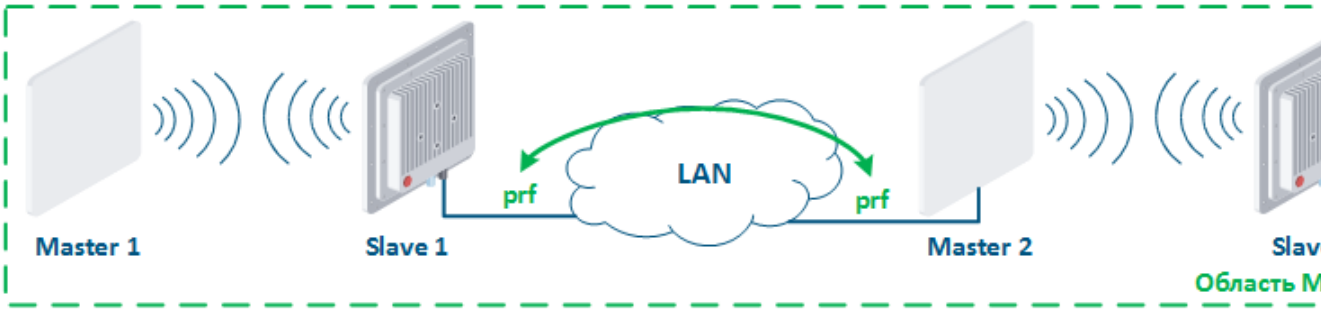

Рисунок 15а - Объединение каналов связи в единую область MINT

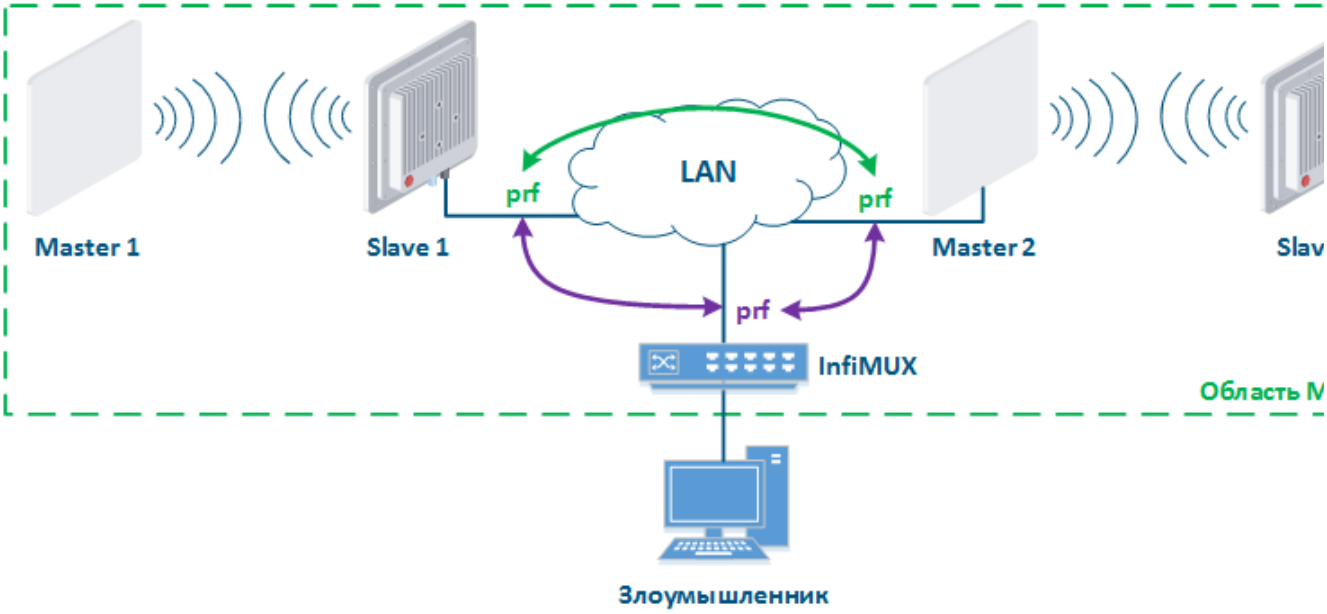

Рисунок 15б - Пример атаки с использованием протокола MINT

Реализация средств обеспечения безопасности передачи данных для семейств устройств

Список мероприятий

Мероприятия по обеспечению безопасности передачи данных

Мероприятие	InfiLINK 2x2 и InfiMAN 2x2		InfiLINK XG и InfiLINK XG 1000		Vector 5
	Web	CLI	Web	CLI	Web
Обновление ПО	Обслуживание	Общие команды	Раздел Обслуживание	Общие команды	Обслуживание
Отложенная перезагрузка	Применение, проверка и предварительный просмотр конфигурации	Общие команды	Проверка и применение настроек	Команды настройки модема	-
Фильтрация трафика	IP Firewall Коммутатор (MAC Switch)	Команда ipfw (IP Firewall) PCAP-фильтры Команда switch	Раздел Коммутатор Коммутация на основе VLAN	Команды настройки коммутатора	Настройка коммутации
Конфигурация STP	Коммутатор (MAC Switch)	Команда switch	-	-	-

Включение режима маршрутизатора	-	Команда route (статические маршруты) Команда arip Команда OSPF Команда ARDA	-	-	-
Конфигурация DHCP-клиента	Настройки сети	Команда dhcpc (DHCP клиент)	Раздел Сетевой доступ	Команда dhcpc (DHCP клиент)	Настройка сетевого доступа
Конфигурация DHCP-сервера	-	Команда dhcpd (DHCP Server)	-	-	-
Конфигурация DHCP-ретранслятора	-	Команда dhcpr (DHCP relay)	-	-	-
Конфигурация ARP	-	Команда arp Команда macf	-	Команда arp	-
Конфигурация LLDP	-	Команда lldp	-	Команда lldp	-
Конфигурация SNMP	Раздел "SNMP"	Команда snmpd (SNMP daemon)	Раздел SNMP	Команда snmpd (SNMP daemon)	Настройка SNMP
Конфигурация MINT	Настройки линка	Команда mint в версии MINT Команда mint в версии TDMA	-	-	-

Инфраструктура

Инфраструктурная безопасность - это важнейший раздел информационной безопасности, которому не всегда уделяется должное внимание. Состав инфраструктуры зависит от технической политики предприятия. В сети должны быть реализованы средства журналирования, мониторинга и технического учёта (ТУ).

Мониторинг

Система мониторинга необходима для централизованного управления устройствами и контроля работы сети. Кроме того, система мониторинга рассылает уведомления инженерам, если значения параметров вышли за рамки разрешённого диапазона. Такие уведомления уменьшают время реакции обслуживающего персонала, благодаря чему минимизируются последствия сбоев и вероятных атак.

Системы мониторинга могут быть интегрированы с системами сигнализации и видеонаблюдения.

Компания Инфинет предоставляет собственную систему мониторинга беспроводных устройств Инфинет - InfiMONITOR. Система мониторинга осуществляет сбор данных следующими способами (рис. 16):

- Поллинг: система мониторинга отправляет SNMP-запросы устройству с указанием параметров, значения которых необходимо получить. Устройство формирует для системы мониторинга SNMP-ответ, где указывает значения запрашиваемых параметров. Опрос параметров устройств ведётся с установленной периодичностью, что гарантирует опрос устройства в заданный интервал.
- Trap-сообщения: устройство отправляет специальное сообщение SNMP Trap серверу мониторинга в случае возникновения события из указанного списка. Отправка SNMP Trap, в отличие от поллинга, инициируется самим устройством и происходит мгновенно, независимо от цикла опроса, однако это потребует дополнительной настройки устройств.

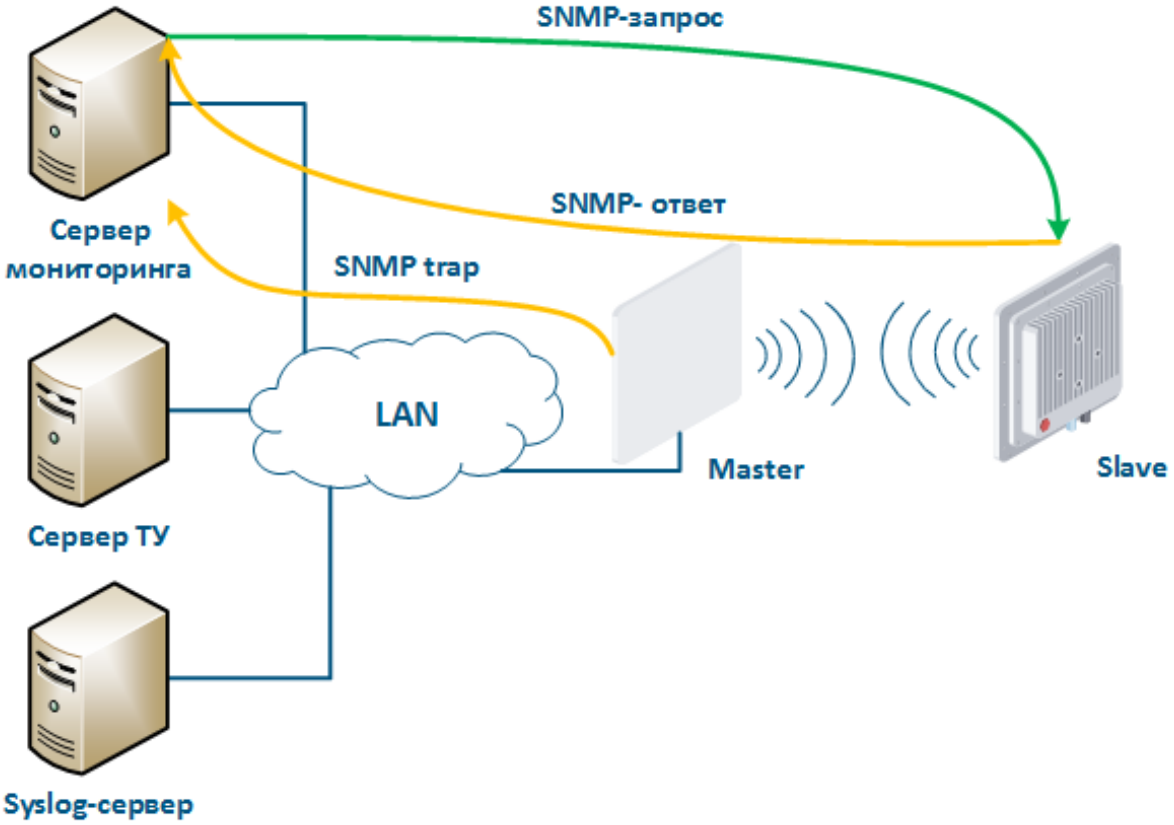

Рисунок 16 - Обмен данными между устройствами и системой мониторинга

Хранение системных журналов

Детальное расследование инцидентов требует анализа системных журналов, зарегистрированных на устройстве. Устройства Инфинет поддерживают логирование событий, однако системный журнал событий не сохраняется после перезагрузки устройства. Кроме того, в крупных сетях удобно иметь централизованное хранилище журнальных файлов, потому что такое хранилище предоставляет интерфейс просмотра журналов всех сетевых устройств, используемые при расследовании инцидентов.

Для этих целей в сети выделяется сервер Syslog. Все журнальные записи одновременно с записью в системный журнал отправляются на сервер Syslog (рис. 17). Это позволяет хранить историю сообщений всех сетевых устройств централизованно и не зависеть от состояния системного журнала непосредственно на устройстве, который может быть очищен при перезагрузке или несанкционированном доступе.

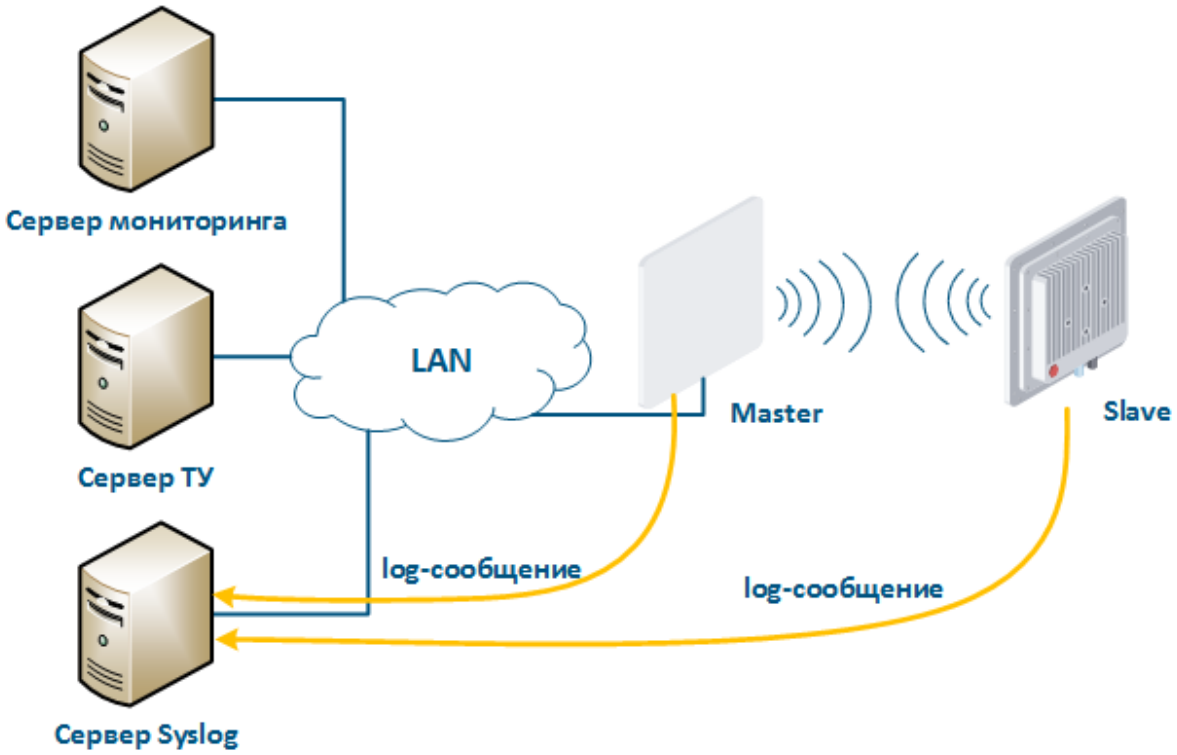

Рисунок 17 - Обмен данными с Syslog-сервером

Технический учёт

Решение эксплуатационных задач требует от инженеров комплексной информации об устройствах для получения доступа на объект, восстановления конфигурации, добавления в систему мониторинга и т.д. Такая информация включает в себя как технические, так и административные аспекты. Для того, чтобы эти данные хранить и иметь к ним доступ, в сети могут быть использованы специализированные системы технического учёта. Системы технического учёта содержат следующую информацию:

- Данные об устройстве: указывается модель устройства, его серийный номер и сетевые реквизиты.
- Данные о площадке: указывается место установки устройства, сведения о доступе на площадку, контактные данные арендодателя и т.д.
- Текстовая конфигурация устройства: хранится история конфигураций, используемых на устройстве. История конфигураций может быть использована для расследования инцидентов и восстановления работы устройства, поэтому сохранение конфигураций должно выполняться с заданной периодичностью. Некоторые системы ТУ могут быть совмещены с системами массовой конфигурации устройств в сети: применение таких систем позволяет иметь унифицированные конфигурации на устройствах, а сеть рассматривается как единое устройство, для которого хранится история изменений.

Реализация инфраструктурных средств обеспечения безопасности для семейств устройств

Список мероприятий

Мероприятия по обеспечению безопасности со стороны инфраструктуры

Мероприятие	InfiLINK 2x2 и InfiMAN 2x2		InfiLINK XG и InfiLINK XG 1000		Vector 5
	Web	CLI	Web	CLI	Web
Использование системы мониторинга InfiMONITOR	InfiMONITOR - Руководство пользователя				
Настройка SNMP	Раздел "SNMP"	Команда snmpd (SNMP daemon)	Раздел SNMP	Команда snmpd (SNMP daemon)	Настройка SNMP
Настройка Trap-сообщений	Раздел "SNMP"	Команда trapd (SNMP traps)	Раздел SNMP	Команда trapd (SNMP traps)	-
Просмотр истории событий	Состояние устройства	Общие команды	Раздел Обслуживание	Общие команды	Обслуживание

	Отправка истории событий на Syslog-сервер	-	Общие команды	-	Общие команды	-
	Управление текстовой конфигурацией	Обслуживание	Общие команды	Раздел Обслуживание	Общие команды	Обслуживание

Дополнительные материалы

Онлайн-курсы

1. Предварительная настройка и установка устройств семейств InfiLINK 2x2 и InfiMAN 2x2.
2. Устройства семейства InfiLINK XG.
3. Vector 5: установка и настройка.
4. Основы беспроводных сетей.
5. Коммутация в устройствах семейств InfiLINK 2x2 и InfiMAN 2x2.

White papers

1. Агрегация каналов, балансировка и резервирование.
2. Организация связи с подвижными объектами.
3. Динамический выбор частоты.

Вебинары

1. Монтаж, грозозащита и заземление оборудования Инфинет.
2. Типовые сценарии настройки коммутации на устройствах Инфинет.
3. Диагностика параметров установленного канала связи InfiLINK 2x2 / InfiMAN 2x2.
4. Решения Инфинет для проектов с подвижными объектами.

Скринкасты

1. "Ввод в эксплуатацию устройств "Инфинет" семейства R5000".
2. "Утилита ERConsole".

Прочее

1. Раздел "Аксессуары" сайта infinet.ru
2. FTP Infinet Wireless
3. Раздел "InfiMONITOR" сайта infinet.ru