РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ЦИФРОВЫЕ РЕШЕНИЯ

РусКрипто

Возможности использования российских криптографических стандартов в протоколах динамической маршрутизации телекоммуникационного оборудования отечественных производителей

Додонов Александр Сергеевич | Начальник управления интеграции

Основные ВЫЗОВЫ в области обеспечения информационной безопасности в отрасли связи Российской Федерации:

РусКрипто

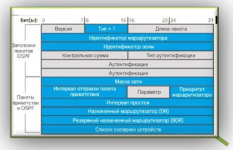
- Рост значимости угроз информационной безопасности и ущерба от их реализации на фоне совершенствования методов и технологий осуществления компьютерных атак
- Рост количества инцидентов информационной безопасности, в том числе скоординированных специальными службами иностранных государств, экстремистскими и террористическими организациями
- Использование иностранных криптографических стандартов

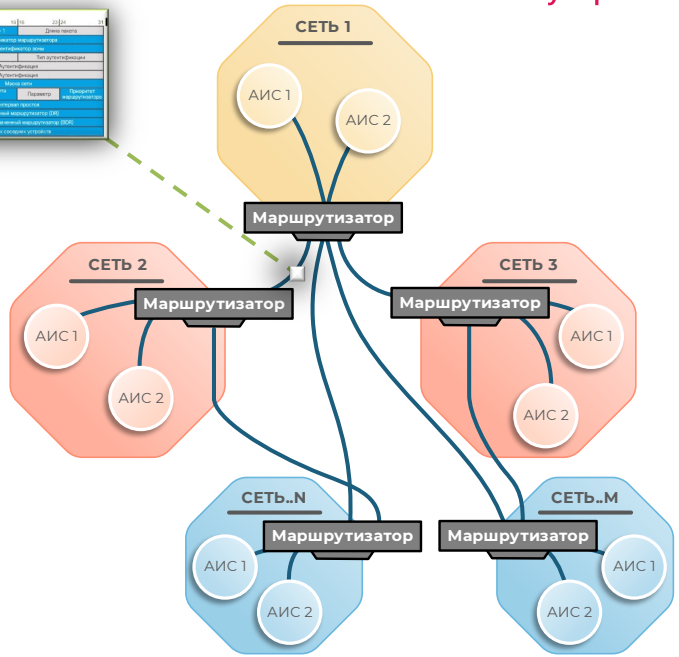
Построение сетей с использованием динамической маршрутизации

РусКрипто

Стандартные протоколы динамической маршрутизации:

- BGP
- OSPF
- RIP
- EIGRP
- IS-IS и др.





В сети происходит постоянный обмен маршрутной информацией:

- Появление новых узлов в сети
- Нарушения в работе линий связи и ввод их в эксплуатацию после устранения неисправностей
- Сообщения о подключенных и доступных сетях
- Синхронизация таблиц маршрутизации

Принцип работы протокола динамической маршрутизации в сетевом оборудовании

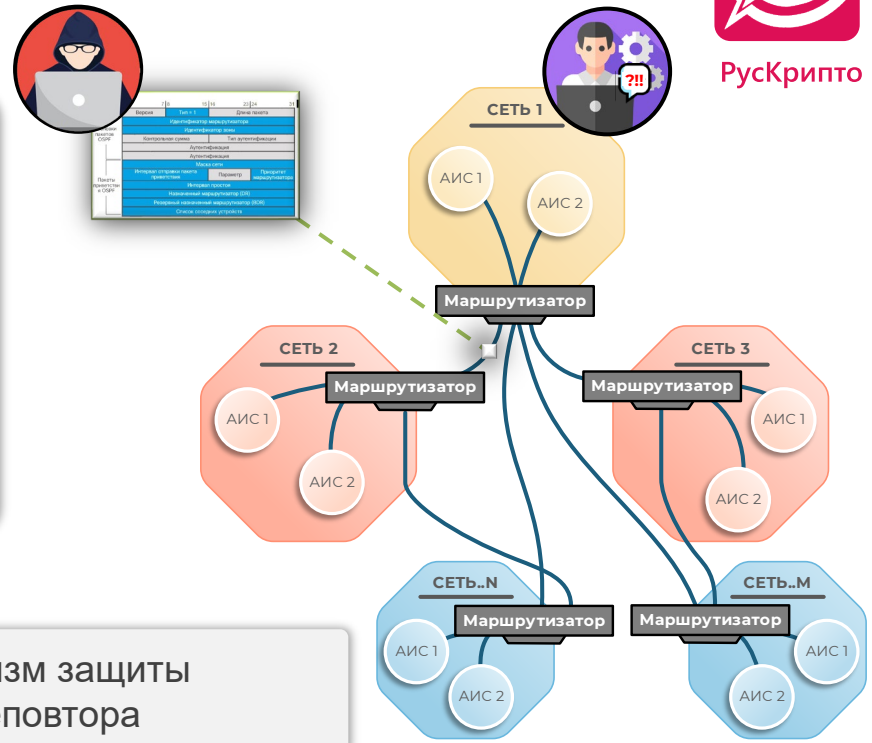
РусКрипто

Атаки на протоколы динамической маршрутизации

РусКрипто

Служебные сообщения протокола динамической маршрутизации могут быть:

- Удалены (заблокированы)
- Модифицированы
- Отправлены повторно
- Созданы ложные служебные сообщения



- Проверка целостности сообщений
- Механизм защиты от переповтора
- Аутентификация (подтверждение подлинности отправителя и принадлежности сообщения отправителю)

Сравнение защищенности протоколов

РусКрипто

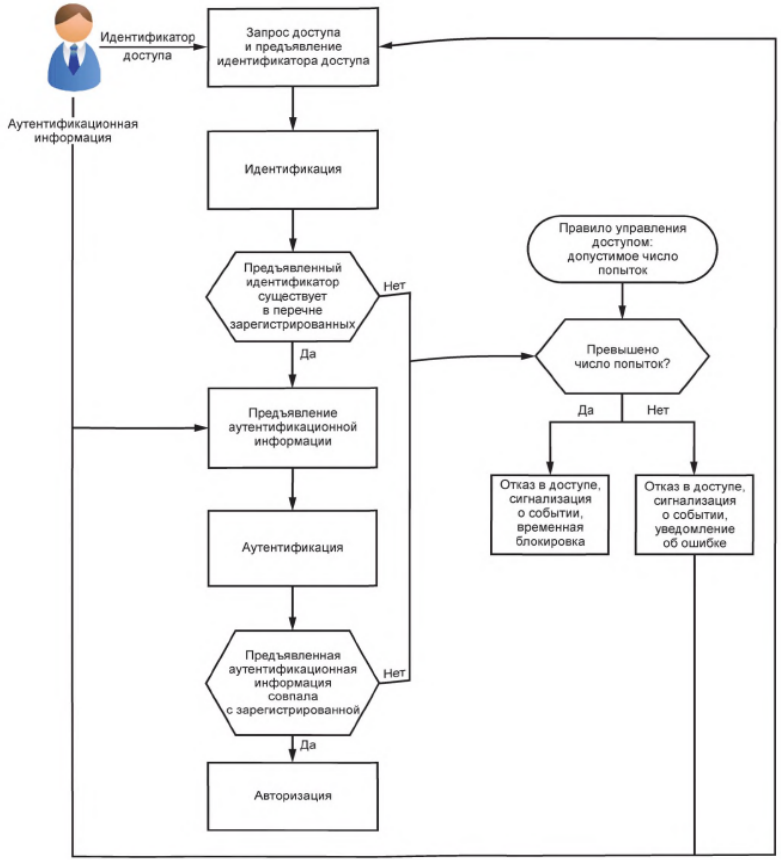
Протокол	Защита от переповтора сообщений	Режимы аутентификации	Общий уровень защиты	Возможность интеграции механизмов
OSPF	+	пароль	-	**да**
		MD5 (HMAC-MD5)	низкий	
BGP	- (+TCP)	TCP MD5 (HMAC-MD5)	низкий	**нет** (только на уровне TCP)
		TCP-AO (HMAC-SHA)	средний	
IS-IS	-	пароль	-	**да**
		MD5 (HMAC-MD5)	низкий	
		CRYPTO (HMAC-SHA)	низкий	
LDP	+ (+TCP)	TCP MD5 (HMAC-MD5)	низкий	**да**
		TCP-AO (HMAC-SHA)	средний	
		hello-msg (HMAC-SHA)	средний	

Аутентификация в протоколах динамической маршрутизации

РусКрипто

**ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения»*

Механизм аутентификации по ГОСТ Р 58833-2020



- ✓ Проверка целостности сообщений
- ✓ Идентификация субъекта доступа
- ✓ Доверие к сообщению и аутентификация субъекта доступа

РусКрипто

Формат записи аутентификационной информации

РусКрипто

- ✓ На основе симметричных криптографических алгоритмов ГОСТ Р 34.13-2015 (алгоритм Магма (ГОСТ Р 34.12-2015) – размер 8 байт)
- ✓ На основе симметричных криптографических алгоритмов ГОСТ Р 34.13-2015 (алгоритм Кузнечик (ГОСТ Р 34.12-2015) – размер 16 байт)
- ✓ На основе односторонних хэш-функций Р 50.1.113-2016 (алгоритм Стрибог (ГОСТ Р 34.11-2012) – размер 32 байта)

Структура записи аутентификационной информации содержит необходимые атрибуты (поля) для реализации:

- ✓ защиты от переповтора сообщений
- ✓ контроля целостности сообщений и аутентификации отправителя
- ✓ реализации плавной смены ключей аутентификации

Результат работы «Маршрут-Аутентификация-2024»

РусКрипто

Выполнен анализ существующих механизмов взаимной аутентификации в протоколах динамической маршрутизации (ДМ)

- Существующие механизмы аутентификации в протоколах ДМ используют иностранные стандарты криптографических алгоритмов
- Большинство протоколов ДМ поддерживают возможность интеграции новых механизмов аутентификации

Разработаны механизмы аутентификации на основе российских стандартов криптографических алгоритмов для протоколов ДМ

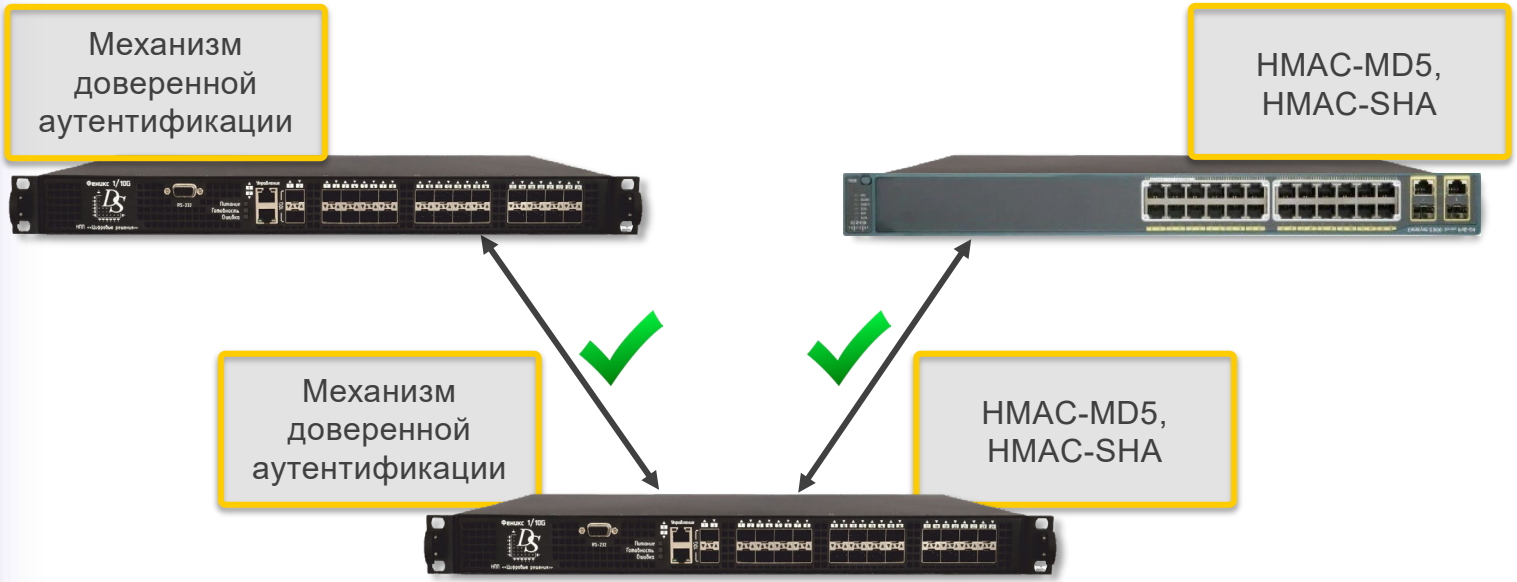
- Использование в механизме аутентификации только отечественных стандартов и методических рекомендаций
- Реализация разработанных механизмов аутентификации в программных библиотеках под ОС Linux с использованием компилятора gcc

Создан Макет с функциями маршрутизатора

- На базе отечественного коммутатора Феникс-1/10G
- Программная библиотека используется в механизме аутентификации протокола OSPF v2
- Сохранена штатная функциональность коммутатора Феникс-1/10G

Плавная замена оборудования сети передачи данных на ТКО с доверенной аутентификацией в протоколах ДМ

РусКрипто



Реализация разработанных механизмов аутентификации в ТКО с функцией динамической маршрутизации

РусКрипто

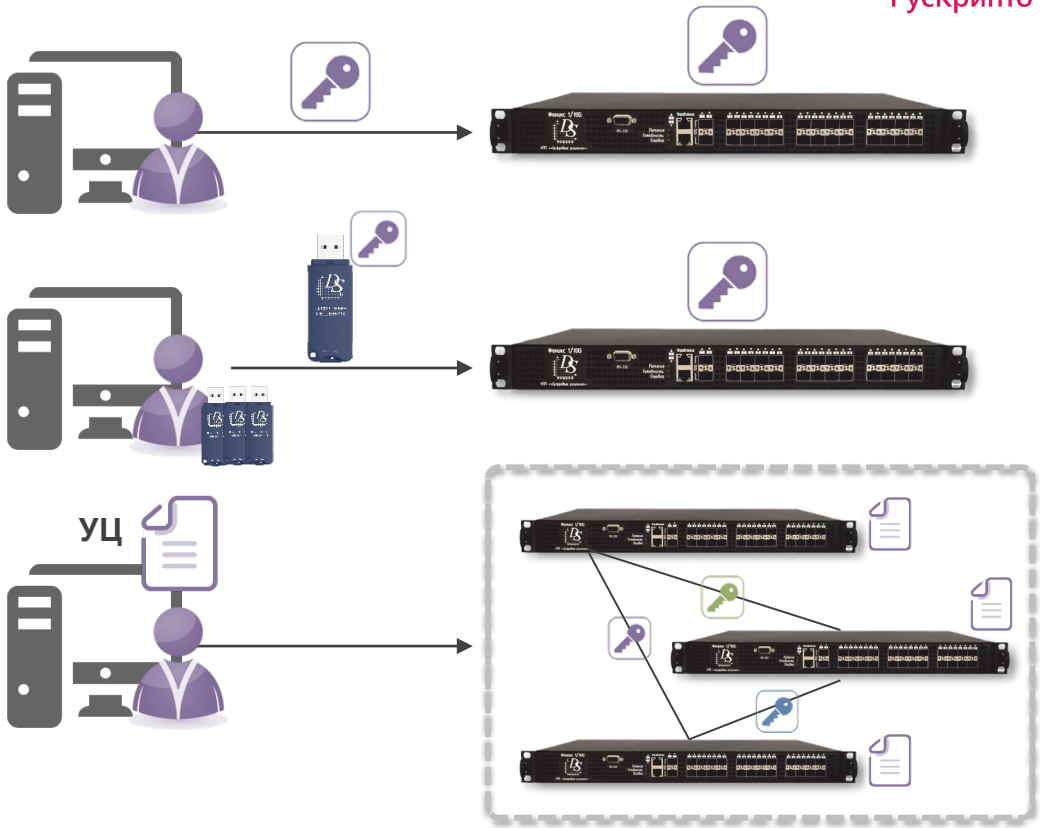
Обеспечение механизмов доверенной аутентификации ключами

РусКрипто

Текущий уровень –
прямое подключение к ТКО

Ближний уровень –
с ключевого носителя

Достижимый уровень –
через УЦ



Автоматизированная система формирования и администрирования сертификатов безопасности для механизмов доверенной аутентификации

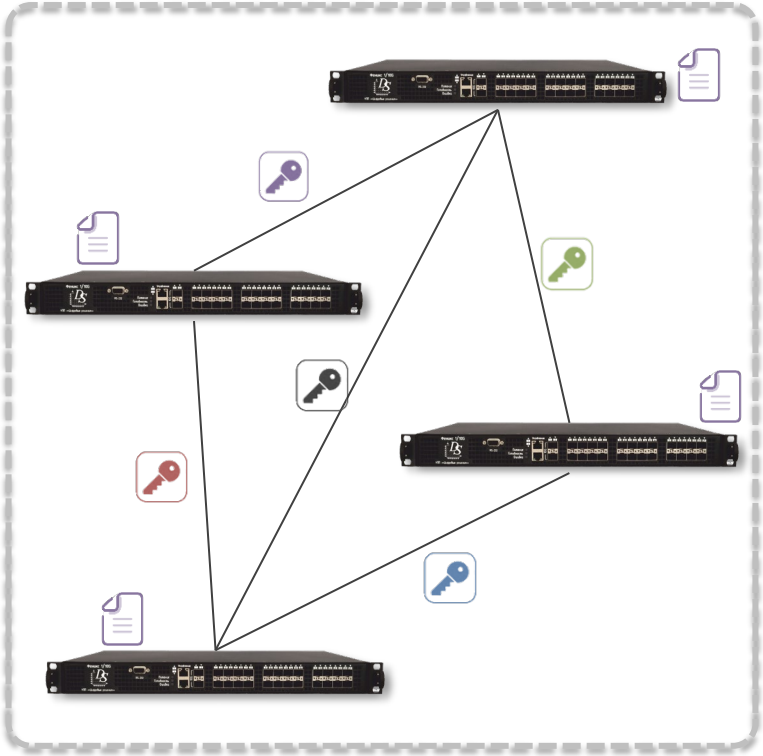
РусКрипто

Ручное распределение сертификатов безопасности

АРМ формирования сертификатов

Автоматизированное распределение сертификатов безопасности на основе удостоверяющего центра (УЦ)

УЦ



Преимущества сертификатов безопасности

РусКрипто

Формирование уникальных ключей аутентификации (КА) между парами ТКО на основе сертификатов безопасности (СБ)

Ввод ключей	ввод текстовой строки	ввод КА с КН (КМА)	ручной ввод СБ	автоматическая работа с УЦ
первичный ввод	вручную	вручную	вручную	вручную
периодическое обновление	вручную	вручную	вручную СБ (КА новый из СБ)	автоматически
добавление нового ТКО	добавление КА для всех соседей	добавление КА для всех соседей	добавление СБ для всех соседей	добавление СБ только для УЦ

ЦИФРОВЫЕ РЕШЕНИЯ

РусКрипто

СПАСИБО ЗА ВНИМАНИЕ