Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Стандартизация IPlir: итоги и перспективы развития

Шемякина Ольга,
Системный аналитик, АО «ИнфоТеКС»

Протокол IPlir

- Протокол безопасности сетевого уровня
- Криптографическая защита IP-пакетов
- Создание VPN
- Различные варианты взаимодействия
- Без установления соединения
- Имеет статус рекомендаций по стандартизации

Р –20

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.034-2020

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол безопасности сетевого уровня

Издание официальное

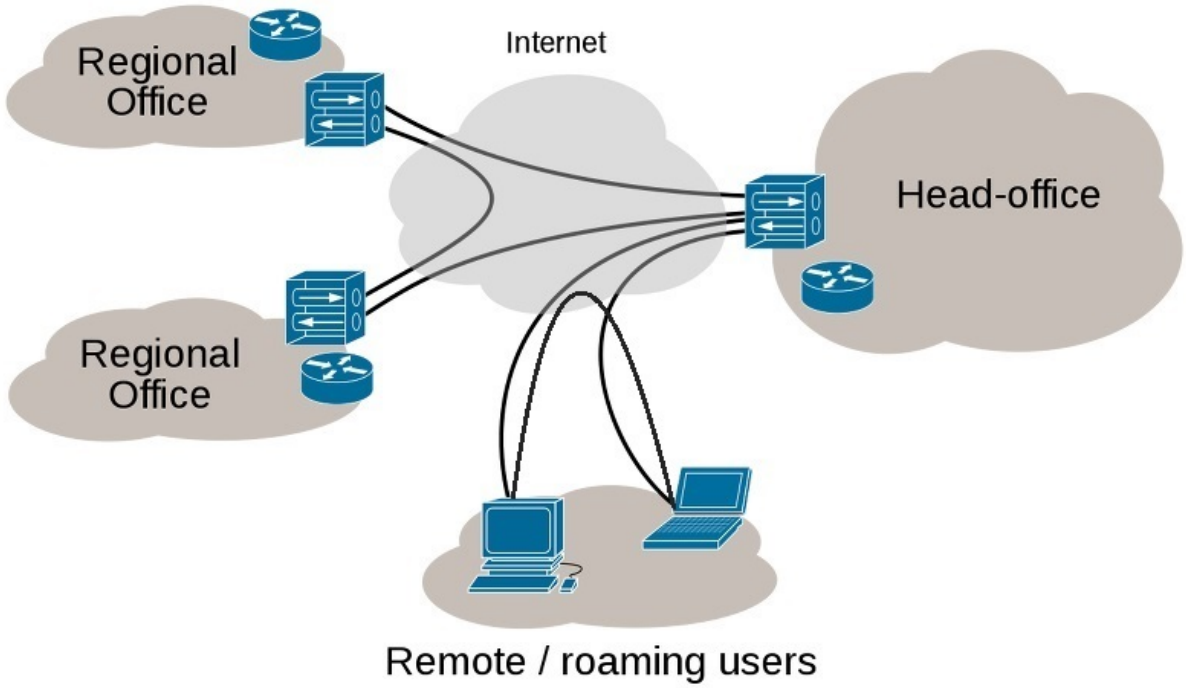
Москва
Стандартинформ
2020

Защита IP-пакетов

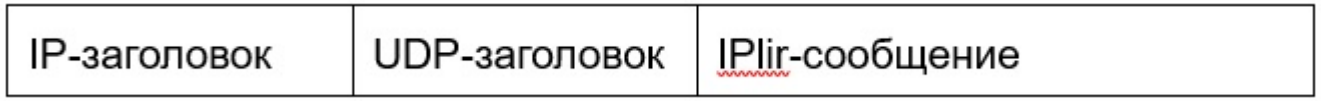
- Имитозащита
- Опциональная конфиденциальность
- Возможность организации защиты от повторов:
  - Номера пакетов
  - Метки времени
  - Случайные числа

Варианты взаимодействия

- Два оконечных узла
- Оконечный узел – шлюз безопасности
- Два шлюза безопасности



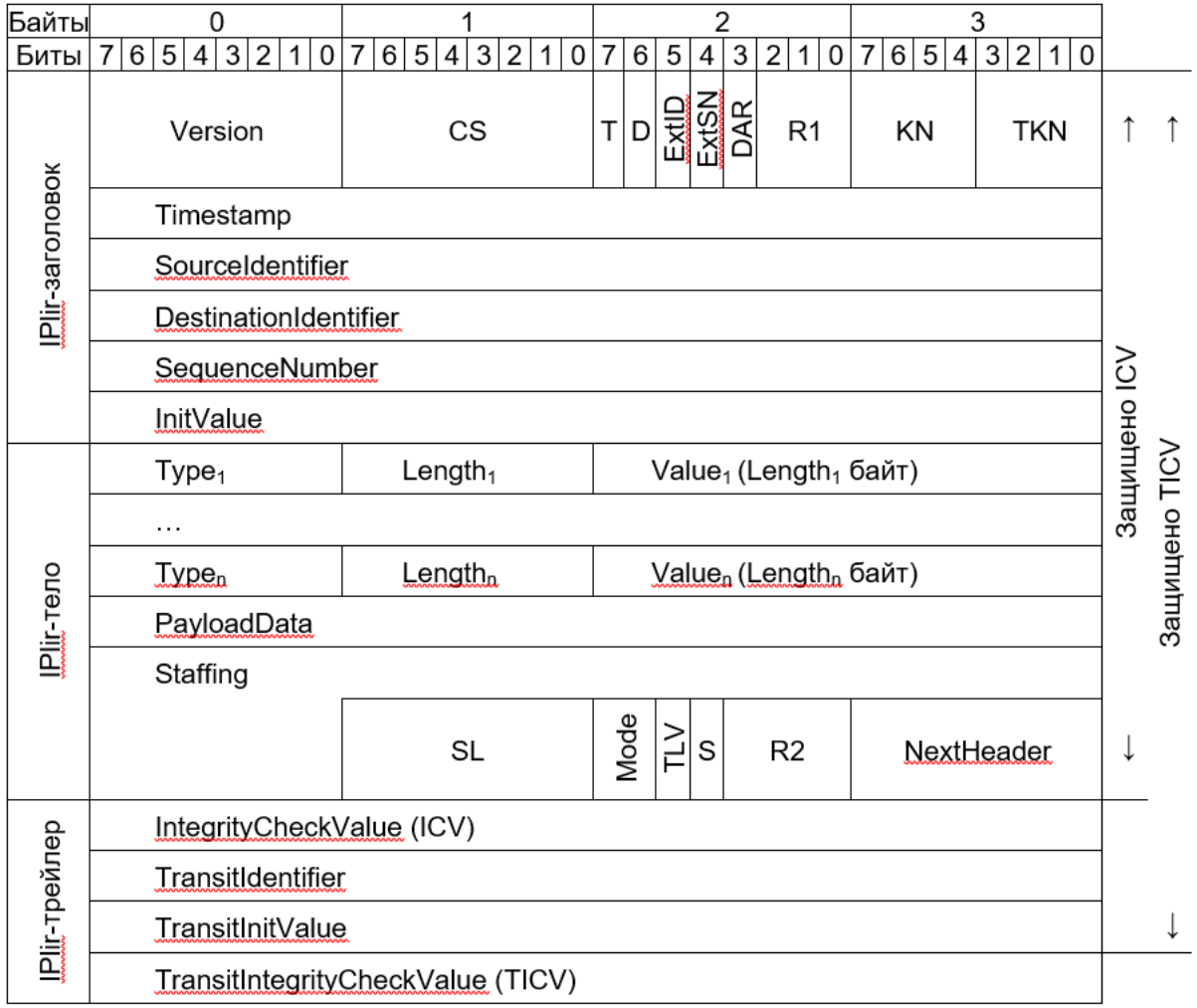
Состав IPlir-пакета



- IP-заголовок стандартный
- Инкапсуляция в UDP опциональна, заголовок стандартный

Состав IPlir-сообщения

- IPlir-заголовок содержит открытую информацию для обработки IPlir-пакета
- IPlir-тело содержит защищенную информацию
- IPlir-трейлер содержит имитовставки и транзитную информацию



Кортежи TLV

- Кортежи (Type, Length, Value) позволяют передавать дополнительную информацию
- IP-адреса используются в режиме «Легкий туннель»

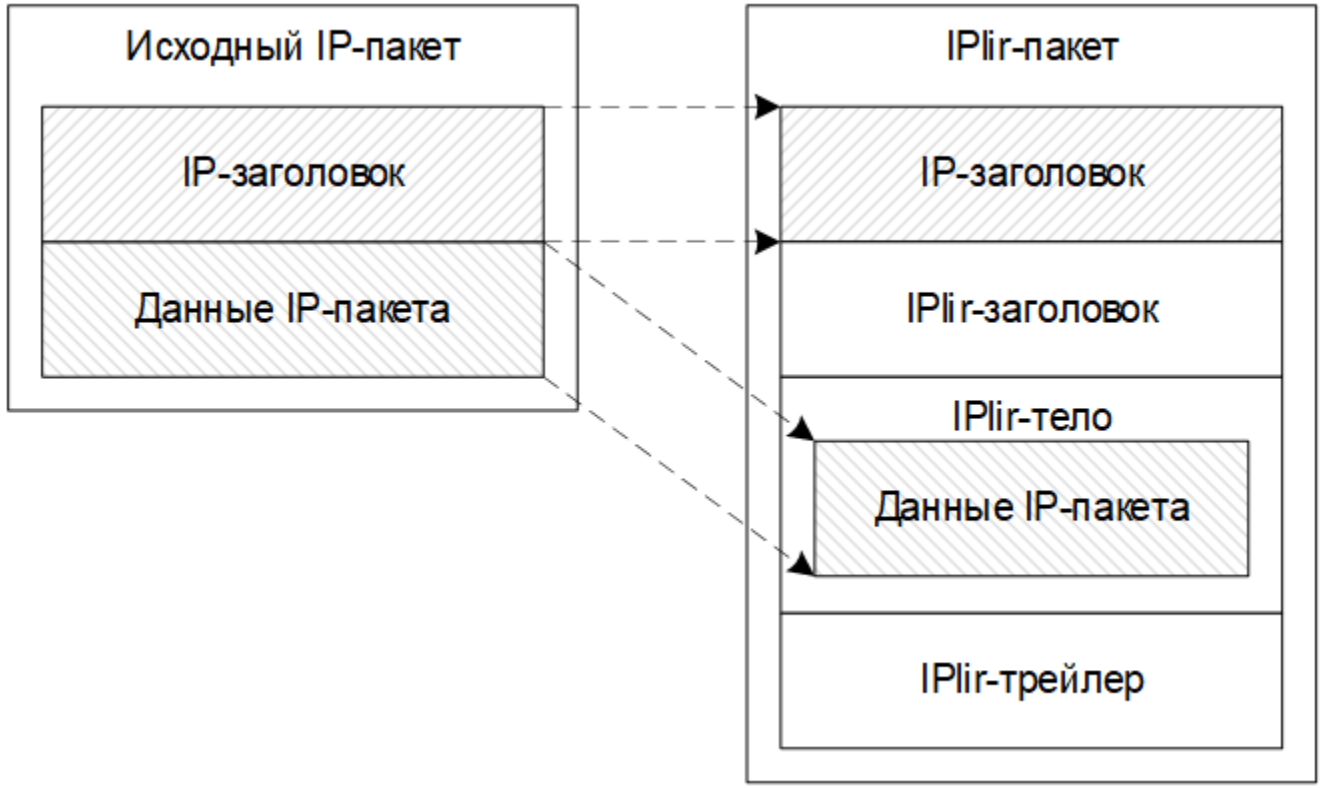
Значение Type	Описание
0	последний кортеж в IPIir-сообщении; может использоваться производителем для собственных нужд
1	пара IPv4 адресов
2	пара IPv6 адресов
3-126	могут использоваться для будущих нужд по согласованию с техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»
127	не используется
128	не используется
129-254	могут использоваться производителем для собственных нужд
255	не используется

Режимы

- Транспортный
- Режим легкого туннеля («легкий туннель»)
- Туннельный (режим «туннель»)

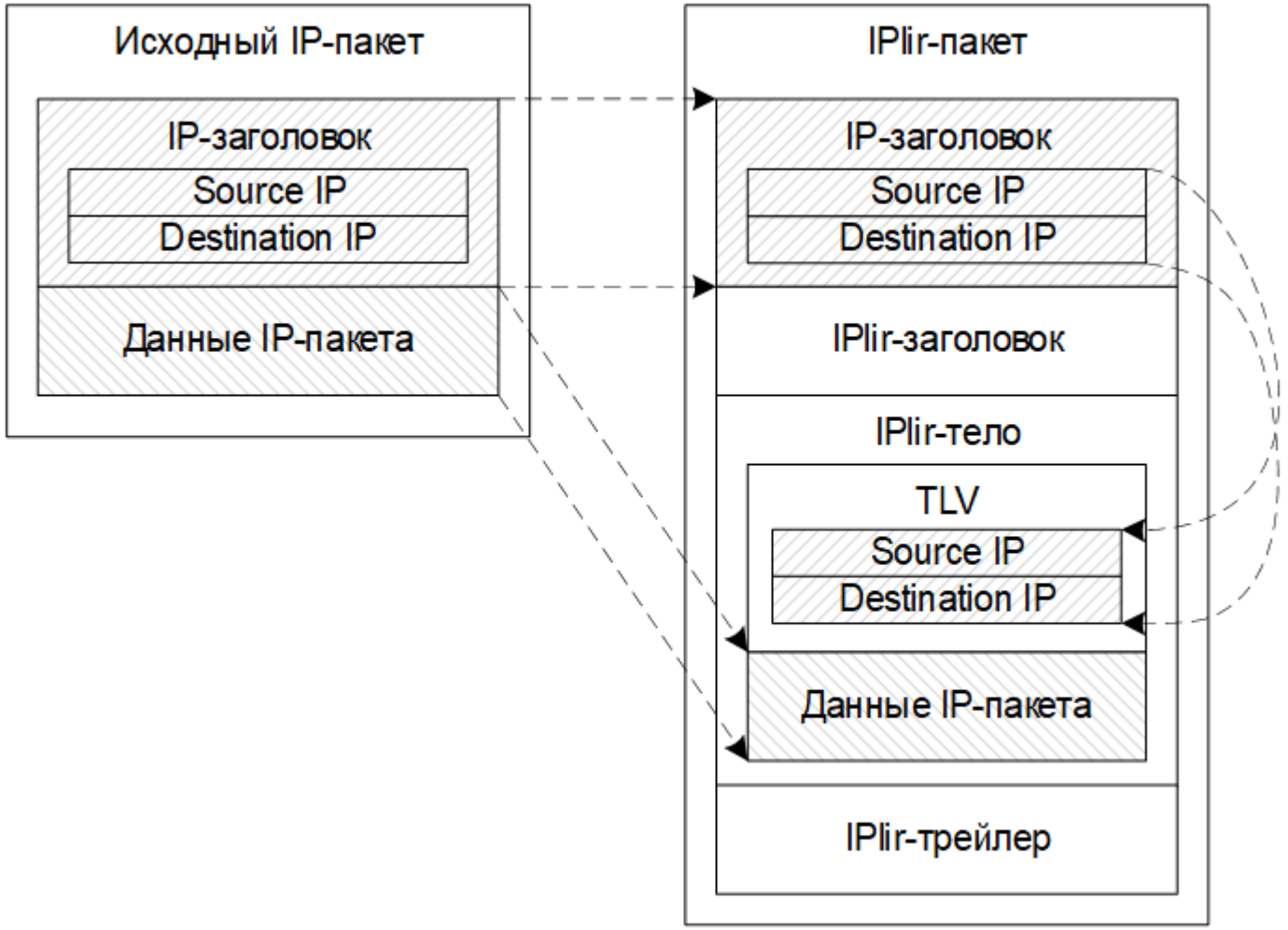
Транспортный режим

- Сохраняется исходный IP-заголовок
- Защищаются только данные IP-пакета



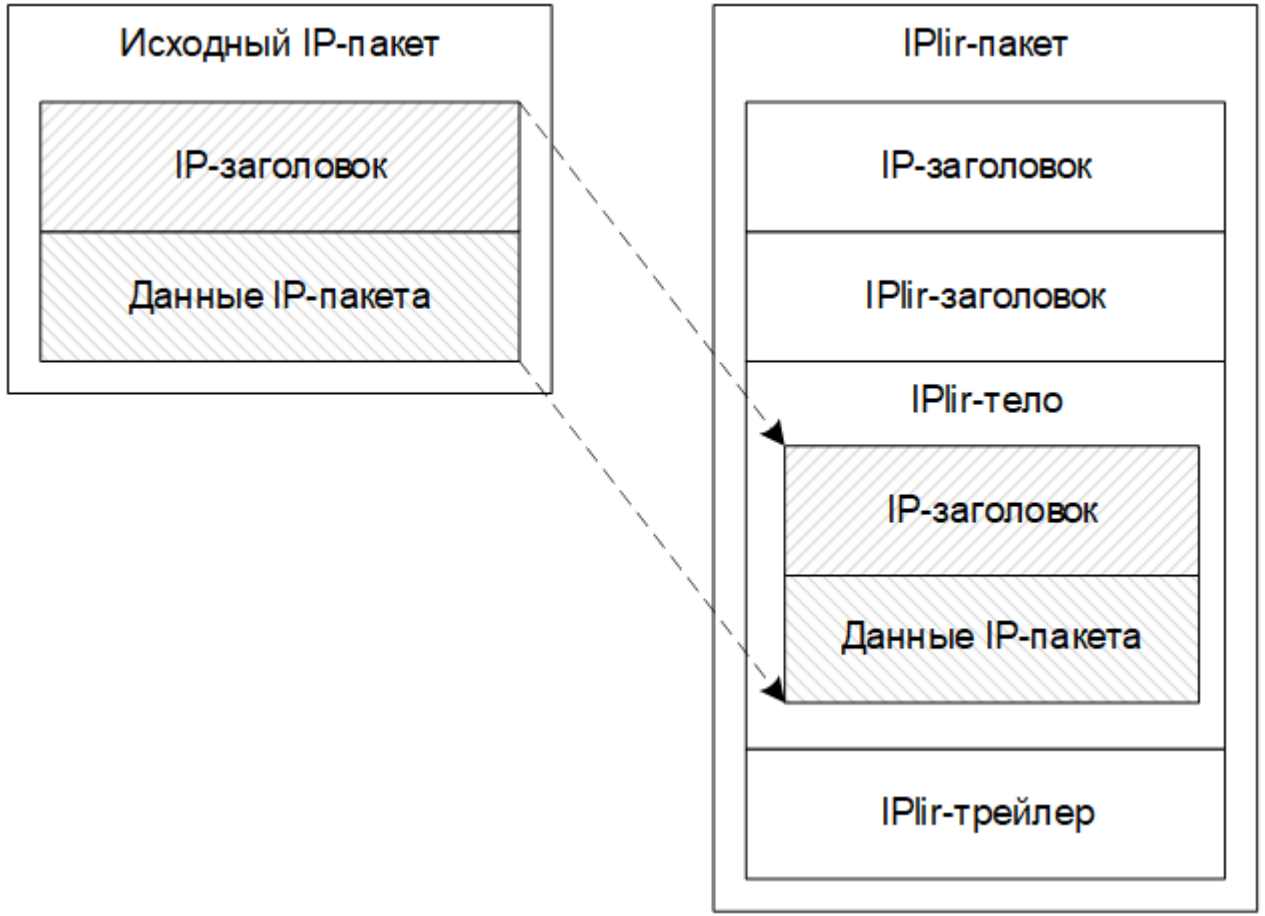
Легкий туннель

- В TLV присутствуют исходные IP-адреса
- Можно менять IP-адреса в заголовке



Туннельный режим

- Защищается весь исходный IP-пакет



Защита от повторов

- SequenceNumber
- InitValue
- Timestamp

Криптографические наборы

- MAGMA-MGM: CS = 1

Параметр	Значение
шифрование	«Магма» в режиме MGM
имитозащита	«Магма» в режиме MGM
длина имитовставки	32 бита
длина синхропосылки	64 бита
производные ключи	«Магма» в режиме CMAC

Криптографические наборы

- KUZN-CTR-CMAC: CS=2

Параметр	Значение
шифрование	«Кузнечик» в режиме CTR
имитозащита	«Кузнечик» в режиме CMAC
длина имитовставки	64 бита
длина синхропосылки	64 бита
производные ключи	«Кузнечик» в режиме CMAC

Особенности IPlir

- Взаимодействие без установления соединения
- Простота
- Распределение парных ключей связи взаимодействующих узлов за рамками протокола
- Режим легкого туннеля с возможностью изменения IP-адресов в заголовке
- Опциональная дополнительная транзитная защита
- Опциональная защита от повторов
- Минимальный набор криптографических алгоритмов

Возможные перспективы

- Создание открытой реализации
- Поддержка новых требований регулятора в новых наборах

Вопросы

Контактная информация

Электронная почта:

Olga.Shemyakina@infotecs.ru

Телефон:

+7 812 383-14-28 (доб. 4910)

Сайт:

infotecs.ru

tc26.ru