ГОСТ 28147-89

Криптошлюз

устройство для шифрации
Ethernet-трафика
и организации VPN

решаемые задачи

аппаратный криптошлюз обеспечивает
одновременную обработку трафика в режимах:

- *шифрование:* прием с защищенного сетевого интерфейса, шифрование, подсчет имитовставки, инкапсуляция и отправка пакетов через открытый сетевой интерфейс,
- *расшифровка:* прием с открытого сетевого интерфейса, деинкапсуляция, расшифрование, проверка имитовставки и отправка пакетов через защищенный сетевой интерфейс.

ключевые особенности

- обеспечивает шифрацию/дешифрацию IP-пакетов и их имитозащиту на скоростях до 20 Гбит/с,
- при шифровании для каждого пакета данных используется уникальная ключевая информация, вырабатываемая из счётчика пакетов и мастер-ключа используемого туннеля,
- для каждого IP-пакета осуществляется выработка ключа шифрования данных и ключа имитозащиты счётчика пакетов.

Обработка шифратором сетевых пакетов подразумевает возможность работы в формате ГОСТ 28147-89:

- MAC-режим выработки имитовставки,
- CFB-режим гаммирования с обратной связью.

ПАРАМЕТРЫ

- установка сетевых интерфейсов – **MAC** и **IP**-адреса, параметры агрегации;
- список защищаемых подсетей для шифрации – до **2 048 маршрутов**;
- список используемых туннелей* – до **512 туннелей**;
- набор ключевой информации – до **512 наборов**, по одному на туннель:

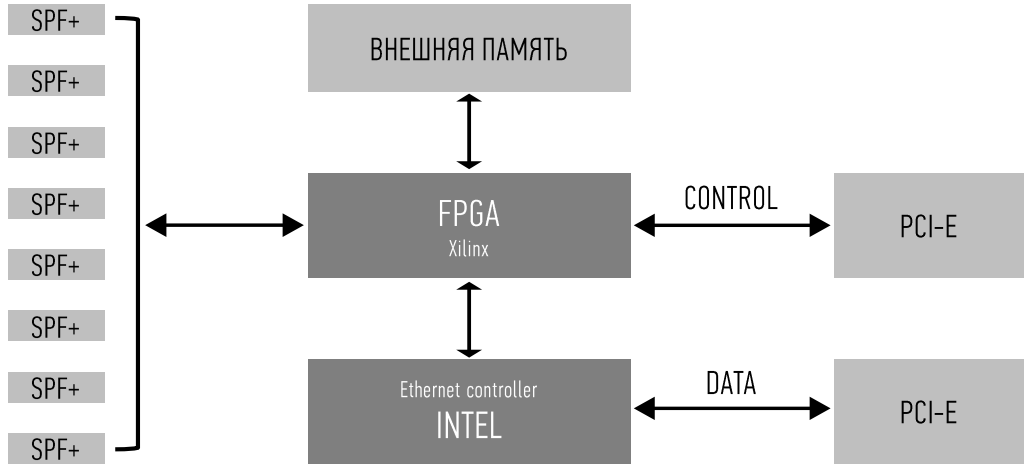
- 256-битный мастер-ключ шифрования,
- 64-битная синхропосылка шифрования,
- 64-битная синхропосылка расшифровки,
- выбор узла замен,
- IP-адрес удаленной точки, которая будет расшифровывать пакеты,
- 32-битный идентификатор туннеля;

- таблица маршрутизации для получателей пакетов – до **128 маршрутов**;
- динамическая таблица MAC-адресов с поддержкой протокола ARP – до **256 записей**.

**связи между двумя защищаемыми подсетями*

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- общая суммарная скорость обрабатываемого потока: **20 Гбит/с** для пакетов размером более 800 байт;
- поддержка **JUMBO**-пакетов – до 4 Кбайт;
- возможность объединения физических портов Ethernet в логические каналы /с поддержкой **LACP** согласно 802.1AX/;
- автономное шифрование и расшифровка пакетов,
- шифрование и расшифровка с дополнительной обработкой в CPU.



интерфейсы и управление

сетевой интерфейс	8 сетевых интерфейсов SFP+ (1, 10 Гбит/с)
интерфейс обмена данными	PCIe 8x
интерфейс управления модуля	PCIe 8x