DCRYPT XG

ВЫСОКОПРОИЗВОДИТЕЛЬНОЕ ШИФРОВАЛЬНОЕ СРЕДСТВО

Шарапов Илья,
технический директор ООО «ТСС»

Москва, 2019

О КОМПАНИИ

ТСС - РАЗРАБОТЧИК СОВРЕМЕННЫХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ПРОГРАММНЫХ И АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПАНИЯ ОСНОВАНА В **2009** ГОДУ

ШТАТ БОЛЕЕ **50-ТИ** (90% - R&D) ЧЕЛОВЕК В 3-Х ОФИСАХ (**5-ТИ** ДО КОНЦА ГОДА)

ОСНОВНОЙ ПРОФИЛЬ – РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СХЕМОТЕХНИЧЕСКИХ И КОНСТРУКТОРСКИХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

СОЗДАНО НЕСКОЛЬКО ДЕСЯТКОВ АППАРАТНЫХ МОДУЛЕЙ, БОЛЕЕ **20-ТИ** ЗАКОНЧЕННЫХ ПРОГРАММНЫХ ПРОДУКТОВ

РЕАЛИЗОВАНО БОЛЕЕ **200** ПРОЕКТОВ

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

Банк России

ЗАЩИТА КАНАЛОВ СВЯЗИ МОСКОВСКОГО РЕГИОНА

ИСПОЛЬЗУЮТСЯ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛОВ СВЯЗИ В ОТКАЗОУСТОЙЧИВОМ КЛАСТЕРНОМ ИСПОЛНЕНИИ

ЗАЩИЩЕНО БОЛЕЕ **32-Х** ОБЪЕКТОВ

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

ЗАЩИТА ВЫСОКОСКОРОСТНЫХ КАНАЛОВ СВЯЗИ НА СКОРОСТИ **40 ГБИТ/С** МЕЖДУ **ЦОД** И **РЦОД** ГРИНАТОМ.

ИСПОЛЬЗУЮТСЯ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛОВ СВЯЗИ В ОТКАЗОУСТОЙЧИВОМ КЛАСТЕРНОМ ИСПОЛНЕНИИ.

ВНЕДРЕНА **СОВ** НА РЯДЕ ОБЪЕКТОВ.

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

ЗАЩИТА **28-МИ** ЦЕНТРОВ **ЕС ОРВД** И **10-ТИ** УКРУПНЕННЫХ ЦЕНТРОВ.

ИСПОЛЬЗУЮТСЯ **МЭ**, **СОВ**.

ОСУЩЕСТВЛЯЕТСЯ ВНЕДРЕНИЕ **СКЗИ** НА КАНАЛАХ СВЯЗИ.

ФУНКЦИОНИРУЕТ В ОФИСНОЙ И ТЕХНОЛОГИЧЕСКОЙ СЕТИ.

ЗАКАЗЧИКИ

ВСЕГО БОЛЕЕ **200** КЛИЕНТОВ

85% - ГОСУДАРСТВЕННЫЕ КОРПОРАЦИИ И ГОСОРГАНЫ

15% - КРУПНЫЕ И СРЕДНИЕ КОММЕРЧЕСКИЕ СТРУКТУРЫ

中国建设银行 China Construction Bank

СК

РусГидро

ДЕПАРТАМЕНТ ЖИЛИЩНОЙ ПОЛИТИКИ И ЖИЛИЩНОГО ФОНДА ГОРОДА МОСКВЫ

ЗАКАЗЧИКИ

ТСС

РОСРЕЕСТР
Федеральная служба государственной регистрации, кадастра и картографии

МРСК СЕВЕРНОГО КАВКАЗА

КОМИТЕТ ПО АРХИТЕКТУРЕ И ГРАДОСТРОИТЕЛЬСТВУ ГОРОДА МОСКВЫ

САЛЮТ®

ДЕПАРТАМЕНТ ГОРОДСКОГО ИМУЩЕСТВА ГОРОДА МОСКВЫ
ЖИЛИЩНЫЕ ВОПРОСЫ

АГРОХИМТЕКС

мбки Межрегиональное БЮРО кредитных историй

Департамент здравоохранения города Москвы

МегаФон

ФЕДЕРАЛЬНАЯ СЛУЖБА ФИНАНСОВО-БЮДЖЕТНОГО НАДЗОРА

РОСКОМНАДЗОР

ITC

Коммерсантъ
картотека

ЗАКАЗЧИКИ

ТСС

СЕРТИФИКАЦИЯ

СКЗИ «Dcrypt 1.0» **Исполнения 2, 4, 7-9, 11, 13-19, 21**	**СКЗИ «Dcrypt 1.0 v.2»** **Исполнения 1-6, 16-21, 31-36**	**СКЗИ «Dcrypt 1.0 v.2»** **Исполнения 50, 51 и 52**	**МКСЗ «Diamond VPN/FW»**
Сертификат соответствия Рег. № СФ/124-3284 от 18.01.2018 г. действителен до 31.12.2019 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3517 от 08.11.2018 г. действителен до 15.11.2021 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3738 от 26.08.2019 г. действителен до 23.08.2022 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия № 4066 от 24.01.2019 г., действителен до 24.01.2024 г., выдан ФСТЭК России в системе Сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00
Сертификат соответствия Рег. № СФ/124-3297 от 29.12.2018 г. действителен до 31.12.2019 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3518 от 08.11.2018 г. действителен до 15.11.2021 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3739 от 26.08.2019 г. действителен до 15.11.2021 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	**СКРД «Diamond ACS»**
Сертификат соответствия Рег. № СФ/124-3298 от 29.12.2018 г. действителен до 31.12.2019 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3519 от 08.11.2018 г. действителен до 15.11.2021 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия Рег. № СФ/124-3740 от 26.08.2019 г. действителен до 23.08.2022 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001	Сертификат соответствия № 2130 от 08.07.2010г., действителен до 08.07.2019г., выдан ФСТЭК России в системе Сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (срок поддержки – до 2119 года)

Dcrypt XG. Целевые функции и назначение

СКЗИ Dcrypt 1.0 v.2
исп. 50, 51 и 52

T

Основная функция – защита трафика на канальном уровне.

L2

Скоростное шифрование пользовательского потока производится на уровне Ethernet (L2),
при этом защищается не только тело данных кадра, но и поля MAC-адресов и поле EtherType.

DTLS

Шифратор использует схему открытого распределения ключей по собственному протоколу DTLS.

Dcrypt XG. Варианты внедрения

- Защита каналов передачи данных между ЦОД
- Защита магистральных каналов сервис-провайдеров
- Защита магистральных каналов системообразующих предприятий
- Защита каналов сетей хранения данных (Fiber-channel)

Dcrypt XG. Стандарты и требования

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ DCRYPT 1.0 V.2 ИСП. 50, 51 И 52 (УСЛОВНОЕ ОБОЗНАЧЕНИЕ DCRYPT XG)

ГОСУДАРСТВЕННЫЕ СТАНДАРТЫ

ГОСТ 28147-89
Алгоритм криптографического преобразования

ГОСТ Р 34.10-2012
Процессы формирования и проверки электронной подписи при установлении соединения

ГОСТ Р 34.11-2012
Функция хэширования

СКЗИ Dcrypt 1.0 v.2 исп. 50, 51 и 52

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

Требования к средствам криптографической защиты

Требования к средствам электронной подписи

Специальные требования к средствам криптографической защиты

Dcrypt XG. Целевые функции и назначение

ПРОГРАММНО-АППАРАТНЫЙ ШИФРАТОР

АП «VPN»

DCRYPT XG

СКЗИ Dcrypt 1.0 v.2 исп. 50, 51 и 52

- Защита каналов связи посредством протокола защищенного обмена по сети по схеме DTLS
- Шифрование данных
- Вычисление имитовставки для данных
- Вычисление значения хэш-функции для данных

Dcrypt XG. Шифровальное средство

DCRYPT

Dcrypt XG (классы защиты **КС1**, **КС2** и **КС3**)

Поставки с ноября 2019 года **ШАССИ 1U** *1-2 модуля, 2-4 порта*	Поставки с октября 2019 года **ШАССИ 3U** *1-4 модуля, 2-8 портов*	Поставки с декабря 2019 года **ШАССИ 3U** *1-8 модулей, 2-16 портов*
СКОРОСТЬ ШИФРОВАНИЯ **FULL DUPLEX** ***от 100 Гбит/с*** ***до 200 Гбит/с*** Задержка **20 мкс**	СКОРОСТЬ ШИФРОВАНИЯ **FULL DUPLEX** ***от 100 Гбит/с*** ***до 400 Гбит/с*** Задержка **20 мкс**	СКОРОСТЬ ШИФРОВАНИЯ **FULL DUPLEX** ***от 100 Гбит/с*** ***до 800 Гбит/с*** Задержка **20 мкс**

Dcrypt XG. Состав аппаратной платформы

СЕТЕВОЕ УСТРОЙСТВО СО СЛОТАМИ РАСШИРЕНИЯ – **CONTROL PLANE**

АПМДЗ – СЕРТИФИЦИРОВАННЫЙ ФСБ РОССИИ АППАРАТНО-ПРОГРАММНЫЙ МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ (ДЛЯ КС2 И КС3)

АППАРАТНО-ПРОГРАММНЫЕ МОДУЛИ РАСШИРЕНИЯ **Diamond HEM**

Dcrypt XG. Шасси и плотность установки

Шасси 3U, 4 модуля / 8 портов по 100 Гбит/с

Шасси 1U, 1-2 модуля / 2-4 порта по 100 Гбит/с

Шасси 3U, 8 модулей / 16 портов по 100 Гбит/с

Dcrypt XG. Функциональные особенности

ШИФРОВАНИЕ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ **L2**

↓

СОВМЕСТИМОСТЬ С МЛАДШИМИ МОДЕЛЯМИ (начало 2020 года)

↓

ПОДДЕРЖКА **L3** МАРШРУТИЗАЦИИ (май 2020)

↓

ИНТЕГРАЦИЯ **МЭ** И **DPI** (май 2020)

↓

ИНТЕГРАЦИЯ **СОВ**, **СОА** И **АНТИВИРУСА** (август 2020)

DCRYPT XG

Dcrypt XG. Форм-фактор, поддерживаемые протоколы

Diamond HEM выпускается в форм-факторах **PCI-E x16**, **3U blade** и в форм-факторах, предназначенных для установки в шасси сторонних производителей

ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ:

Ethernet 100G (доступен);

Ethernet 40G (декабрь 2019);

FC 16/56 G (декабрь 2019);

10x10G (январь 2020).

Dcrypt XG. Схема испытательного стенда

ПАРАМЕТРЫ ТРАФИКА:

Фрейм 70 байт,

Фрейм 128 байт,

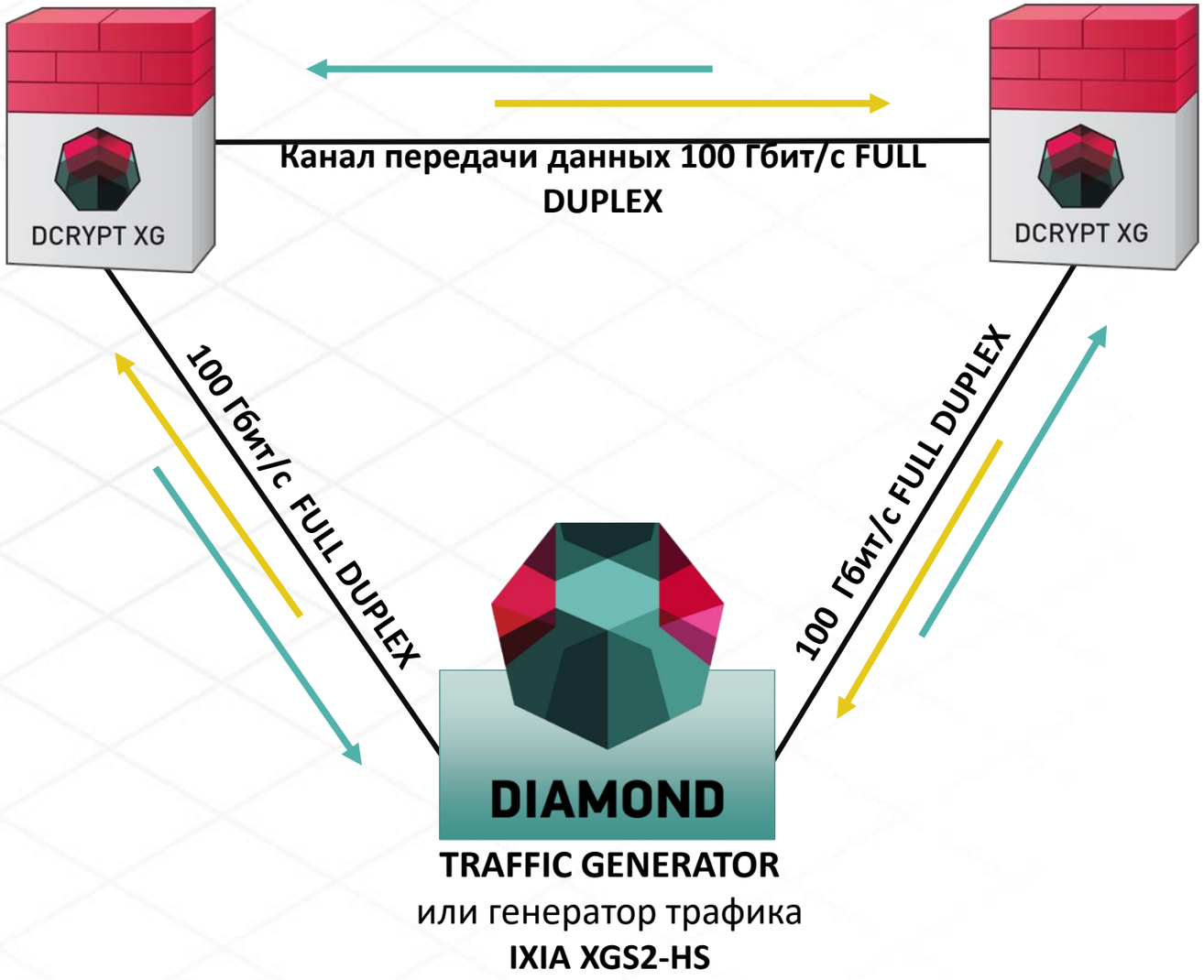
Фрейм 256 байт,

Фрейм 512 байт,

Фрейм 1024 байт,

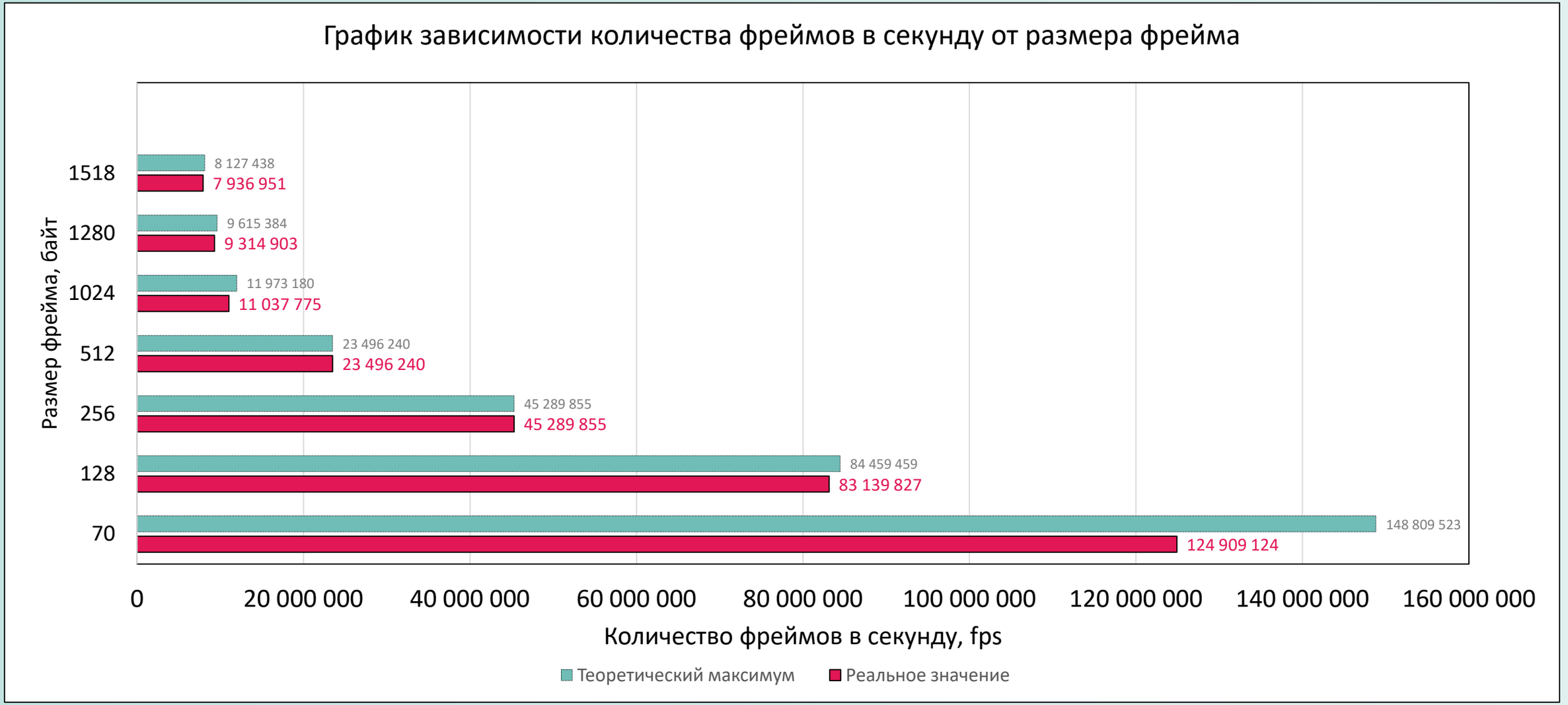
Фрейм 1500 байт,

IMIX



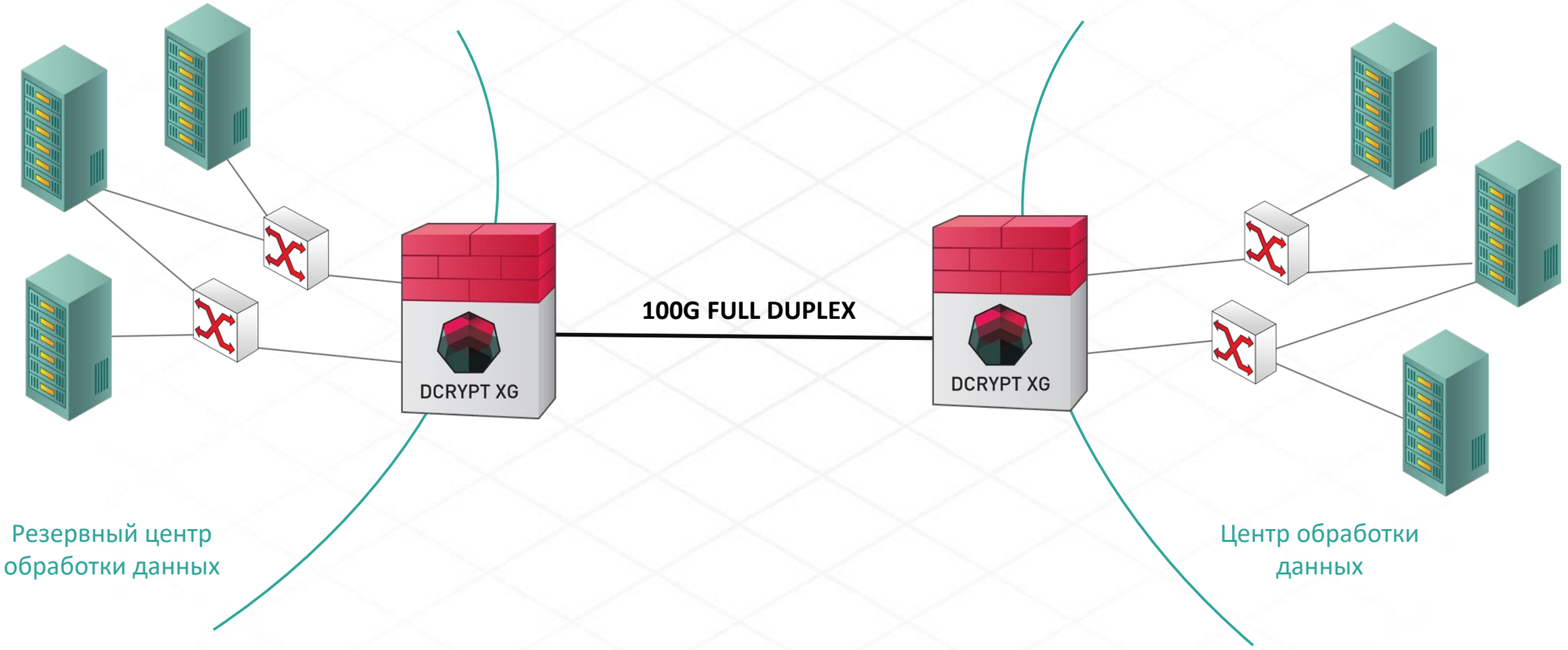
Dcrypt XG. Скоростные характеристики

Dcrypt XG. Скоростные характеристики



Dcrypt XG. Скоростные характеристики

Dcrypt XG. Схема внедрения

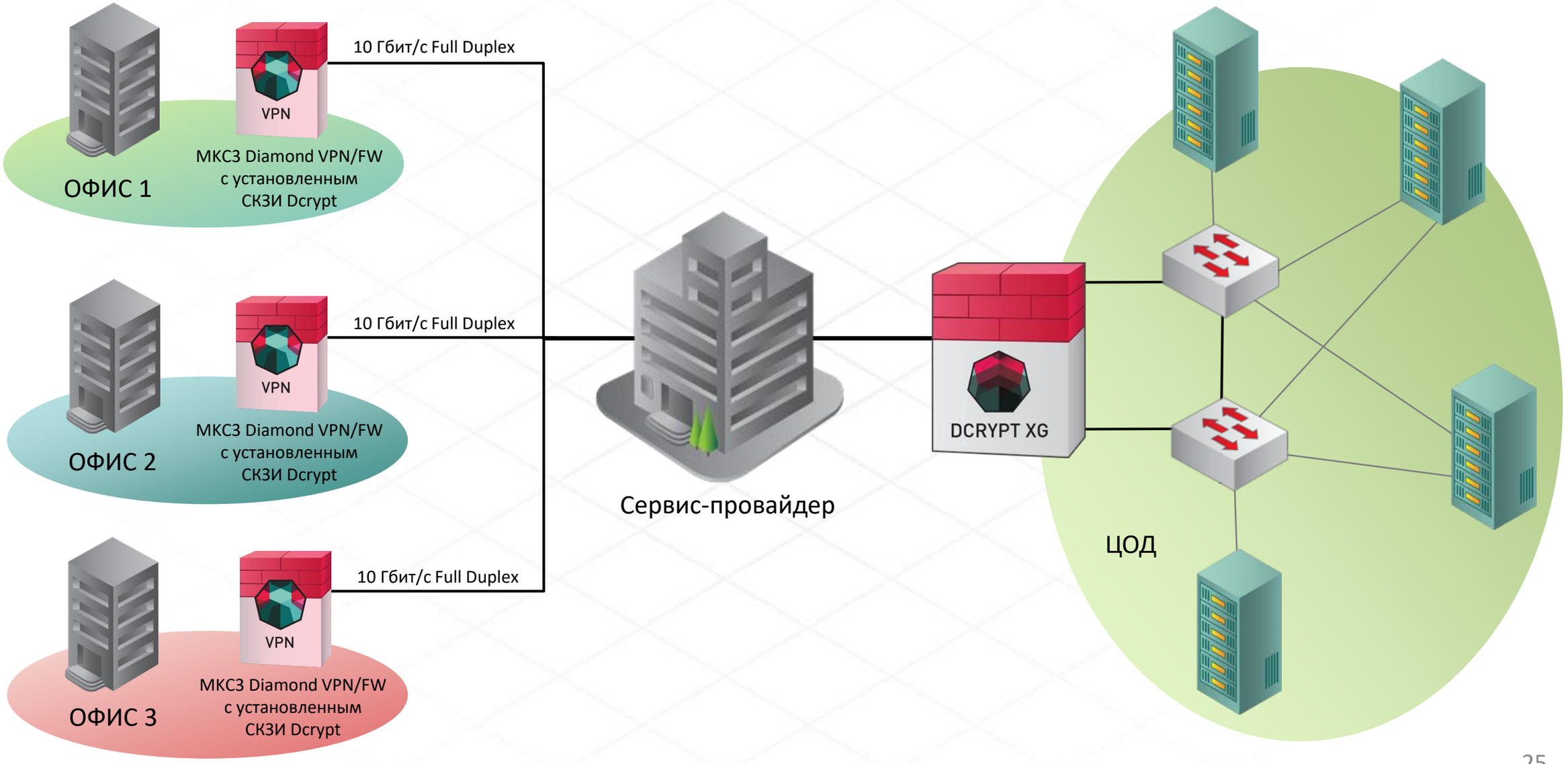


Dcrypt XG. Отказоустойчивость

СОВМЕСТНОЕ РЕШЕНИЕ С ПАРТНЕРОМ НА БАЗЕ ПЛАТФОРМЫ
BAREFOOT TOFINO

1U МОДУЛЬ
ВОЗМОЖНОСТЬ КЛАСТЕРИЗАЦИИ ДО 8, 32 ИЛИ **64** УСТРОЙСТВ
ПРОГРАММИРУЕМАЯ ЛОГИКА ПЕРЕКЛЮЧЕНИЯ КАНАЛОВ **BYPASS**
ВОЗМОЖНОСТЬ ЛЮБОЙ БАЗОВОЙ **МАНИПУЛЯЦИЕЙ ТРАФИКА**

Dcrypt XG. Схема внедрения 2020г.



Dcrypt XG. Сравнение с конкурентами

	Компания	ТСС		Thales e-Security	Gemalto Inc.	Инфобезопас-ность
						
№	Модель / Спецификация	МКСЗ Diamond VPN/FW с СКЗИ Dcrypt	Dcrypt XG	Datacryptor 5000	SafeNet Carrier Ethernet Encryption	Квазар
1.	Реализация	Программно-аппаратная (Intel/ RISC)	Аппаратная	Аппаратная	Аппаратная	Аппаратная
2.	Скорость шифрования (full-duplex)	от 10 Мбит/с до 16 Гбит/с	10, 40, 100 Гбит/с-Ethernet, 56 Гбит/с-Fiber Channel	100 Мбит/с, 1 Гбит/с, 10 Гбит/с	10 Мбит-1 Гбит/с Ethernet, 10 Гбит/с, 100 Гбит/с (10 x 10 Гбит/с), 100 Гбит/с	10 Гбит/с
3.	Вносимые задержки	1,5 - 2 мкс	20 мкс	от 40 до 4 мкс	<2 мкс	Нет данных

Dcrypt XG: Сравнение с конкурентами

	Компания	ТСС		Thales e-Security	Gemalto Inc.	Инфобезопас-ность
						
№	Модель / Спецификация	МКСЗ Diamond VPN/FW с СКЗИ Dcrypt	Dcrypt XG	Datacryptor 5000	SafeNet Carrier Ethernet Encryption	Квазар
4	Консоль управления	Многоуровневая централизованная система управления (ЦУС)		Нет	SafeNet Crypto Command Center	Нет
5	Уровень протокола	L2, L3, L4	L2	L2	L2	L2
6	Криптографические стандарты	ГОСТ 28147-89 с учетом рекомендаций ГОСТ Р34.12-2015 («Магма»), ГОСТ Р34.13-2015	ГОСТ 28147-89 с учетом рекомендаций ГОСТ Р34.12-2015 («Магма»), ГОСТ Р34.13-2015	AES-GCM AES-CBC (256-bit)	RSA-2048, ECC P-256	ГОСТ Р34.12-2015 («Магма»), ГОСТ Р34.13-2015
7	Форм-фактор	1U, настольные исполнения	1U/3U	1U/2U	3U	1U

Спасибо за внимание!

Адрес: Москва, 105187, ул. Борисовская, д.1, офис 900.
Телефон, факс: +7 (495) 120-12-84.
E-mail: info@tssltd.ru.