



# DCRYPT XG

**ВЫСОКОПРОИЗВОДИТЕЛЬНОЕ ШИФРОВАЛЬНОЕ СРЕДСТВО DCRYPT XG И ДРУГИЕ ПРОДУКТЫ КОМПАНИИ ТСС ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

---

**Шарапов Илья,**

Москва, 2020

№ п/п	Название продукта	Назначение	Целевые функции	Архитектуры процессоров и ОС
1	<p>Система контроля и разграничения доступа в средствах вычислительной техники</p> <p><b>МКСЗ Diamond ACS</b></p>	<p>Защита от НСД</p>	<p>Средство вычислительной техники</p>	<p>Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) - Linux</p>
2	<p>Многофункциональный комплекс сетевой защиты</p> <p><b>Diamond VPN/FW</b></p> <p>с функциями МЭ, СОВ и СОА</p>	<p>Многофункциональный комплекс сетевой защиты</p>	<p>МЭ, СОВ, СОА</p>	<p>Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) - Linux</p>
3	<p>СКЗИ Dcrypt</p>	<p>Средство криптографической защиты информации</p>	<p>КриптоАРМ, АП VPN, Криптографические библиотеки</p>	<p>Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) - Linux, аппаратные модули расширения</p>

№ п/п	Название продукта	Назначение	Целевые функции	Архитектуры процессоров и ОС
4	UTM Diamond	Шлюз безопасности (UTM)	АП VPN, МЭ, СОВ	Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) – Linux
5	NGFW «Diamond Endpoint Protection»	Межсетевой экран следующего поколения	АП VPN, МЭ, СОВ, Антивирус, Антиспам, DPI	Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) – Linux



Банк России



**ЗАЩИТА КАНАЛОВ СВЯЗИ МОСКОВСКОГО РЕГИОНА**



**ИСПОЛЬЗУЮТСЯ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ  
ЗАЩИТЫ КАНАЛОВ СВЯЗИ В ОТКАЗОУСТОЙЧИВОМ КЛАСТЕРНОМ  
ИСПОЛНЕНИИ**



**ЗАЩИЩЕНО БОЛЕЕ 32-Х ОБЪЕКТОВ**



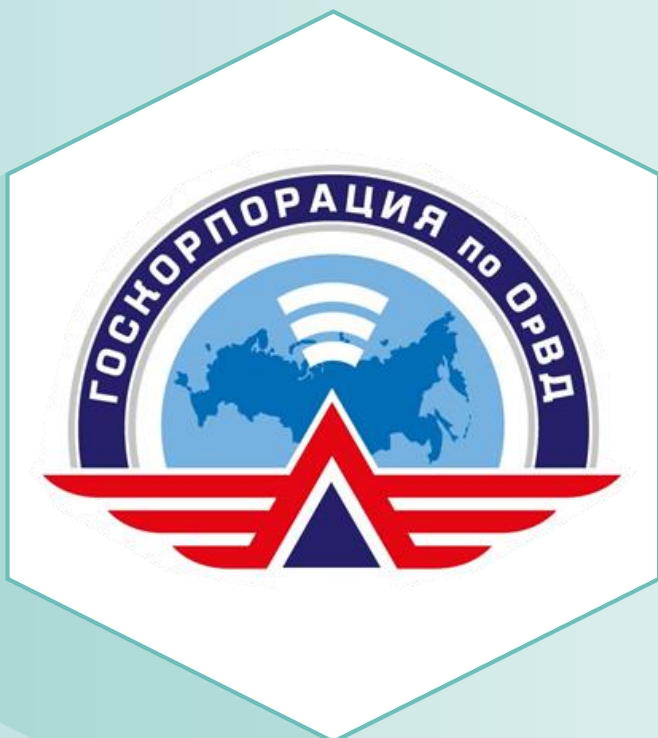
**ЗАЩИТА ВЫСОКОСКОРОСТНЫХ КАНАЛОВ СВЯЗИ  
НА СКОРОСТИ 40 ГБИТ/С МЕЖДУ ЦОД И РЦОД ГРИНАТОМ.**



**ИСПОЛЬЗУЮТСЯ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ  
КАНАЛОВ СВЯЗИ В ОТКАЗОУСТОЙЧИВОМ КЛАСТЕРНОМ  
ИСПОЛНЕНИИ.**



**ВНЕДРЕНА COB НА РЯДЕ ОБЪЕКТОВ.**



**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.**



## Dcrypt (классы защиты КС1, КС2, КС3)

Программный (ОС Windows, Linux)

Программно-аппаратный

Аппаратная платформа с архитектурой процессора **Intel x86**

Аппаратная платформа с архитектурой процессора **RISC (ARM)**

Скорость шифрования:

**От 100 Мбит/с до 35 Гбит/с**  
Задержка **~2 мс**

Скорость шифрования:

**От 10 Кбит/с до 200 Мбит/с**  
**(в будущем до 10 Гбит и выше)**  
Задержка **~2 мс**

Скорость шифрования full-duplex:

- **100 Гбит/с уровень L2/L3**
- **40 Гбит/с уровень L2/L3**
- **25 Гбит/с уровень L2/L3**
- **10 Гбит/с уровень L2/L3**

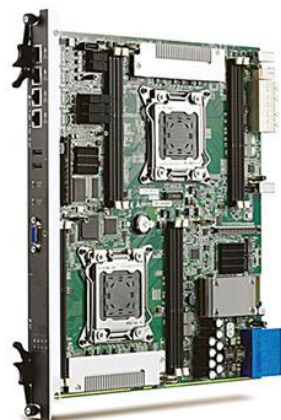
Задержка **~20 мкс**



НАСТОЛЬНОЕ  
ИСПОЛНЕНИЕ



СТОЕЧНОЕ  
ИСПОЛНЕНИЕ



ПРОМЫШLENНОЕ  
ИСПОЛНЕНИЕ



МОБИЛЬНОЕ  
ИСПОЛНЕНИЕ



ИСПОЛНЕНИЕ  
ДЛЯ АСУ ТП





- ПAK Diamond VPN/FW модель 2XXX



- ПAK Diamond VPN/FW модель 5XXX



- ПAK Diamond VPN/FW модель 3XXX/4XXX



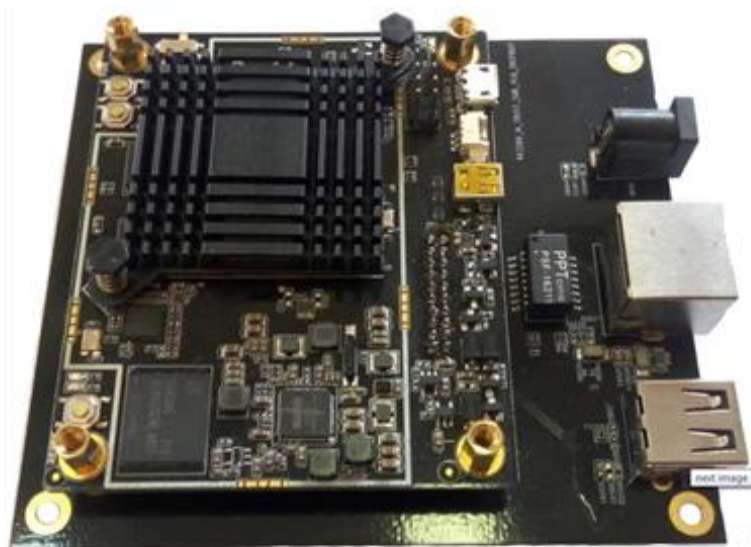
- ПAK Diamond VPN/FW модель 6XXX/7XXX



# ПАК Diamond VPN/FW : для готовых платформ и встраиваемых систем с архитектурой процессора ARM TCC



# ПАК Diamond VPN/FW : для готовых платформ и встраиваемых систем с архитектурой процессора ARM TCC



# ПАК Diamond VPN/FW : для готовых платформ и встраиваемых систем с архитектурой процессора ARM



- Высокопроизводительный опытный образец на базе архитектуры процессора ARM





СКЗИ Dcrypt. Класс  
защиты КС1, КС2, КС3  
и КВ

VPN-построитель

Межсетевой экран L2/L3.  
Тип А, Б и В 4-го класса  
защиты

Система обнаружения  
вторжений.

- ФИЛЬТРАЦИЯ НА L2/L3 ПО ЛЮБЫМ ПОЛЯМ В ЗАГОЛОВКЕ СЕТЕВОГО ПАКЕТА
- ФИЛЬТРАЦИЯ ПО РАСПИСАНИЮ
- СИНХРОНИЗАЦИЯ ПРАВИЛ ФИЛЬТРАЦИИ МЕЖДУ НЕСКОЛЬКИМИ УСТРОЙСТВАМИ
- ЛОГИРОВАНИЕ ПРАВИЛ ФИЛЬТРАЦИИ
- ФИЛЬТРАЦИЯ ПО ДОМЕННОМУ ИМЕНИ
- СОЗДАНИЕ КОНТЕКСТОВ ФИЛЬТРАЦИИ



**DIAMOND**

ПАК Diamond VPN/FW  
с функциями VPN/**FW**/IDS



**DIAMOND**

ПАК Diamond VPN/FW  
с функциями VPN/FW/**IDS**



РАБОТА С ТРАФИКОМ В АКТИВНОМ (СПВ)  
И ПАССИВНОМ (СОВ) РЕЖИМАХ

ОКОЛО 20 000 АКТИВНЫХ СИГНАТУР

ПОДДЕРЖИВАЕТСЯ ВОЗМОЖНОСТЬ НАПИСАНИЯ  
СОБСТВЕННЫХ ПРАВИЛ

МАКСИМАЛЬНАЯ СКОРОСТЬ ДО 50 ГБИТ/СЕК

ЕЖЕНЕДЕЛЬНОЕ ЦЕНТРАЛИЗОВАННОЕ ОБНОВЛЕНИЕ  
СИГНАТУР

## ПОДДЕРЖКА ТЕХНОЛОГИЙ **LAYER2:**

- поддержка Vlan(802.1q);
- поддержка LACP(803.3ad);
- поддержка L2overL3;
- поддержка работы сетевых интерфейсов в режиме bridge;
- поддержка STP.

## ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ:

- поддержка отказоустойчивого кластера;
- синхронизация между группами;
- поддержка нескольких провайдеров;
- поддержка режима bypass;
- резервирование питания.

## ПОДДЕРЖКА ТЕХНОЛОГИЙ **LAYER3:**

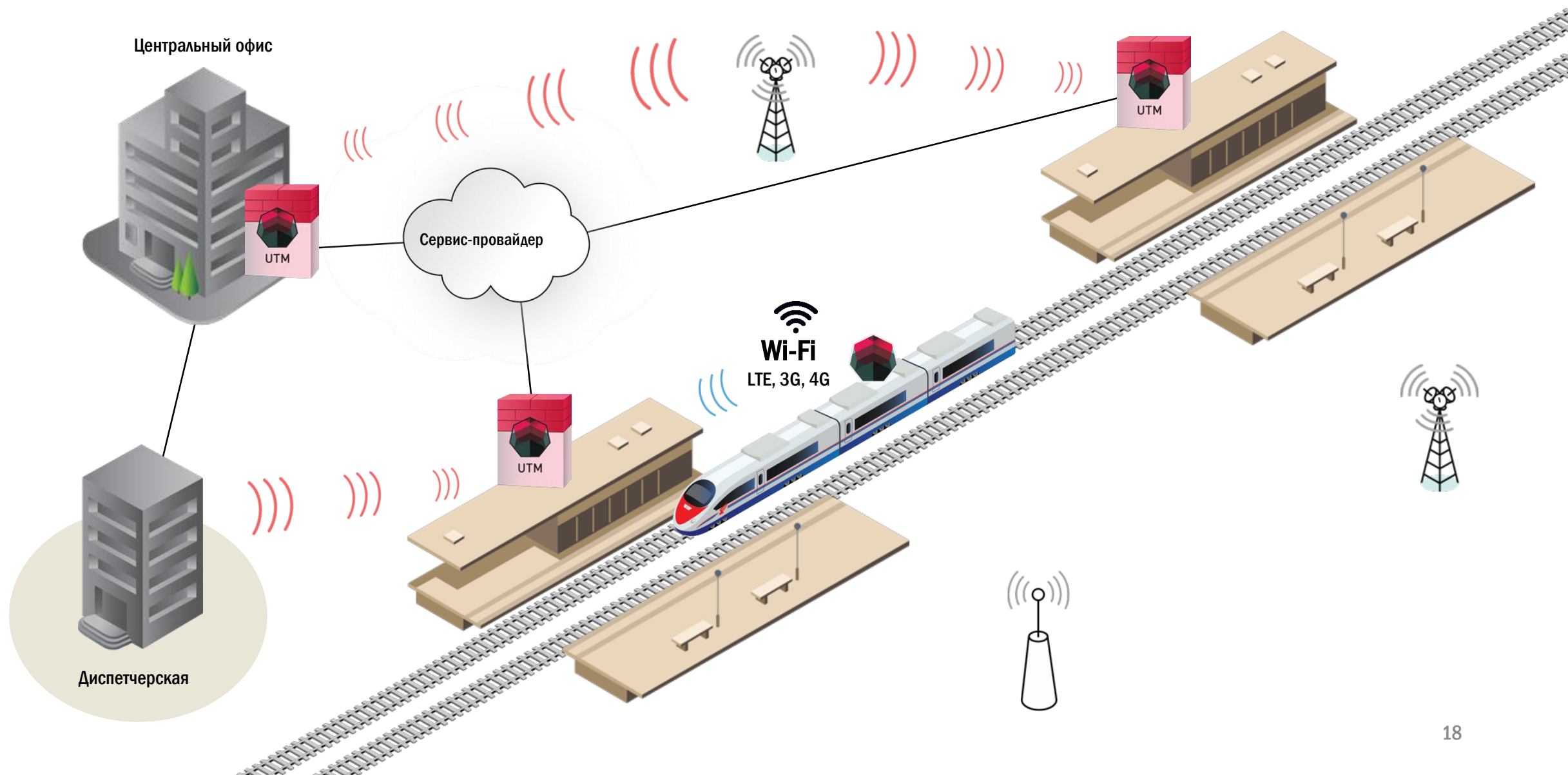
- поддержка статической маршрутизации;
- поддержка динамической маршрутизации (OSPFv2, RIPv2, BGP, IS-IS).



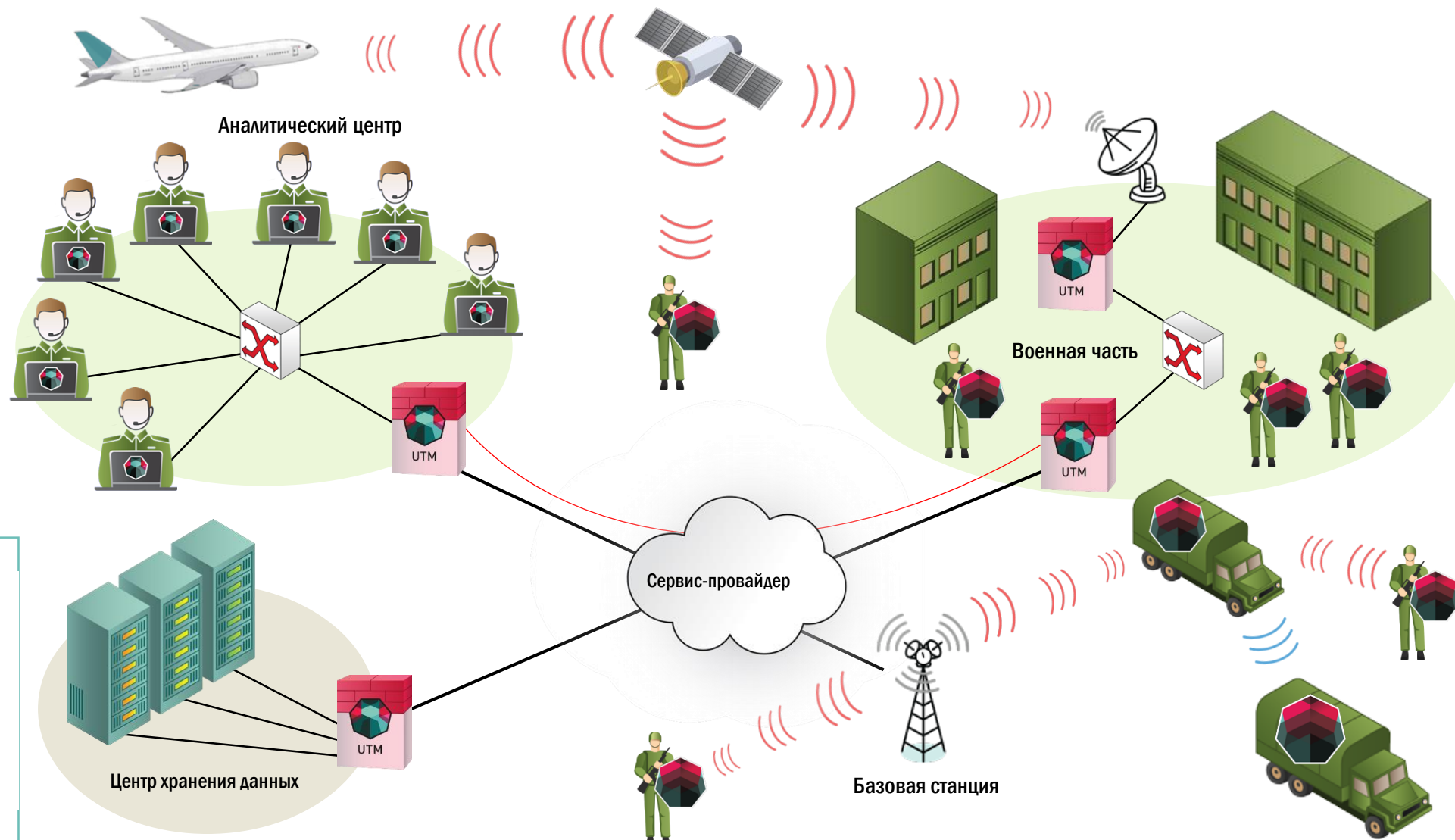
### ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ:

- поддержка DHCP, DHCP Relay, DHCP Client;
- поддержка NTP;
- поддержка SNMP;
- поддержка Rsyslog;
- поддержка Proxy;
- поддержка Link aggregation (Round-robin, Active-Backup, Broadcast, XOR);
- разграничение прав доступа;
- логирование действия пользователей;
- поддержка ролевых политик;
- поддержка балансировки трафика между несколькими провайдерами;
- поддержка скриптов;
- NAT/PAT (Static, dynamic, port-forwarding);
- Backup настроек;
- поддержка совместимости с тонким клиентом.

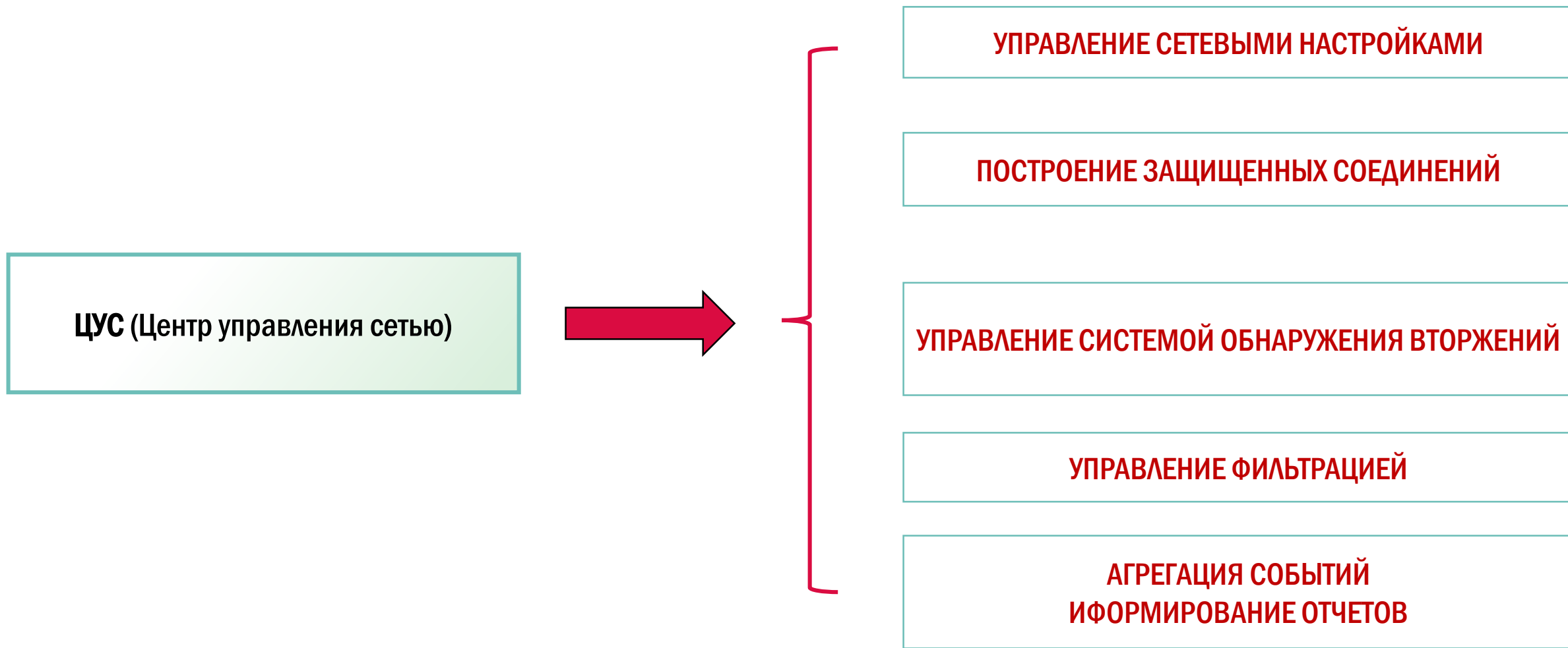
# СКЗИ Dcrypt: схема применения для подвижного ж/д-состава

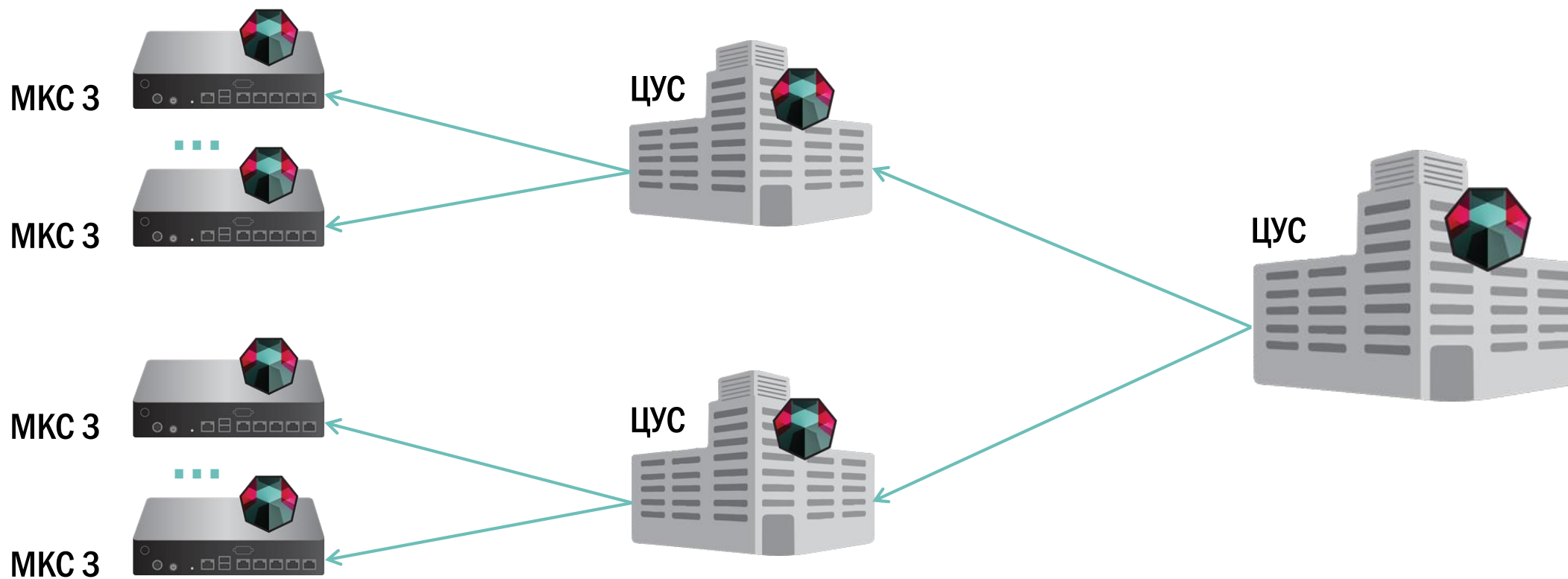


# СКЗИ Dcrypt: возможная схема управления войсками



**СКОРОСТЬ ШИФРОВАНИЯ FULL-DUPLEX:**  
*От 100 Кбит/с до 100 Гбит/с*  
*Задержка не более 2мс*

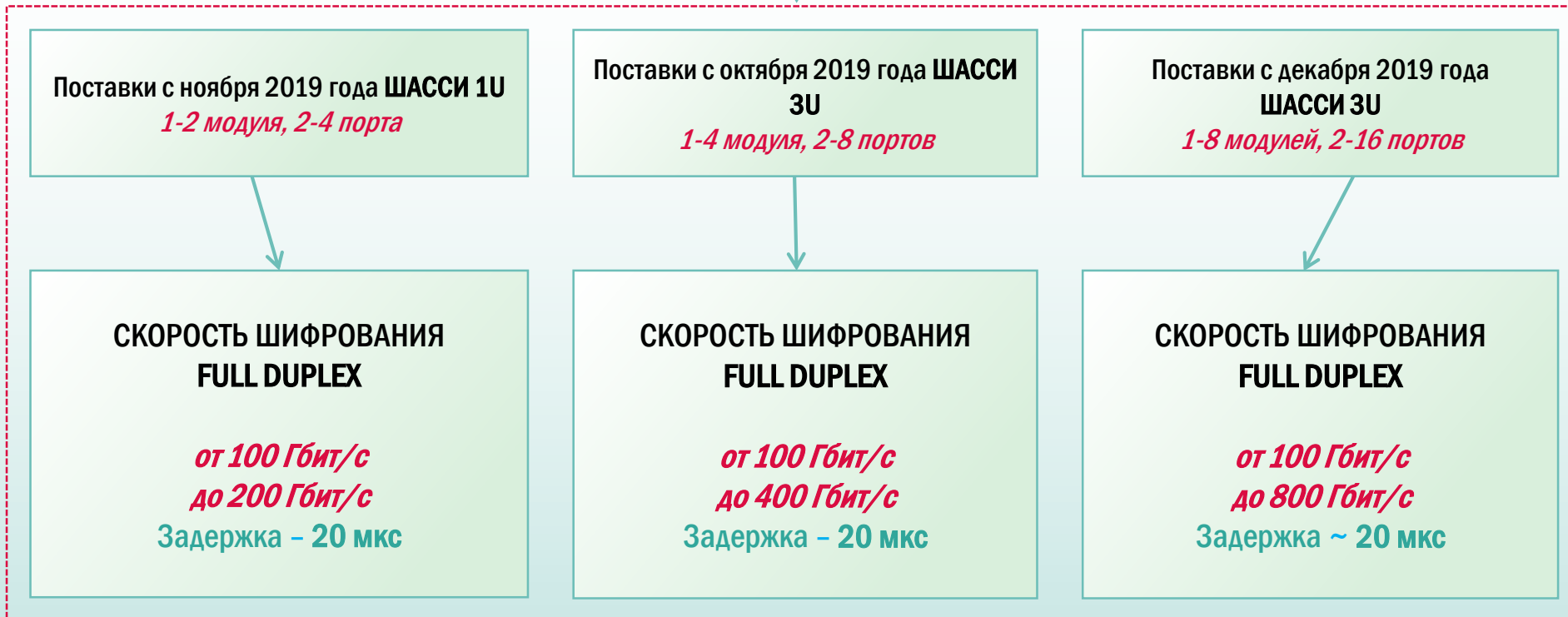




- Возможность одновременной работы нескольких тысяч устройств под управлением одного ЦУС;
- Возможность создания иерархий ЦУС;
- Возможность ведения и совместного использования политик безопасности разного уровня абстракции.



## DCrypt XG (классы защиты КС1, КС2 и КС3)





**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  
NEM**



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



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



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



**ШИФРОВАНИЕ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ L2**

**СОВМЕСТИМОСТЬ С МЛАДШИМИ МОДЕЛЯМИ**

**ПОДДЕРЖКА L3 МАРШРУТИЗАЦИИ**

**ИНТЕГРАЦИЯ МЭ И DPI**

**ИНТЕГРАЦИЯ СОБ, СОА И АНТИВИРУСА**



## ПАРАМЕТРЫ ТРАФИКА:

Фрейм 70 байт,

Фрейм 128 байт,

Фрейм 256 байт,

Фрейм 512 байт,

Фрейм 1024 байт,

Фрейм 1500 байт,

**IMIX**

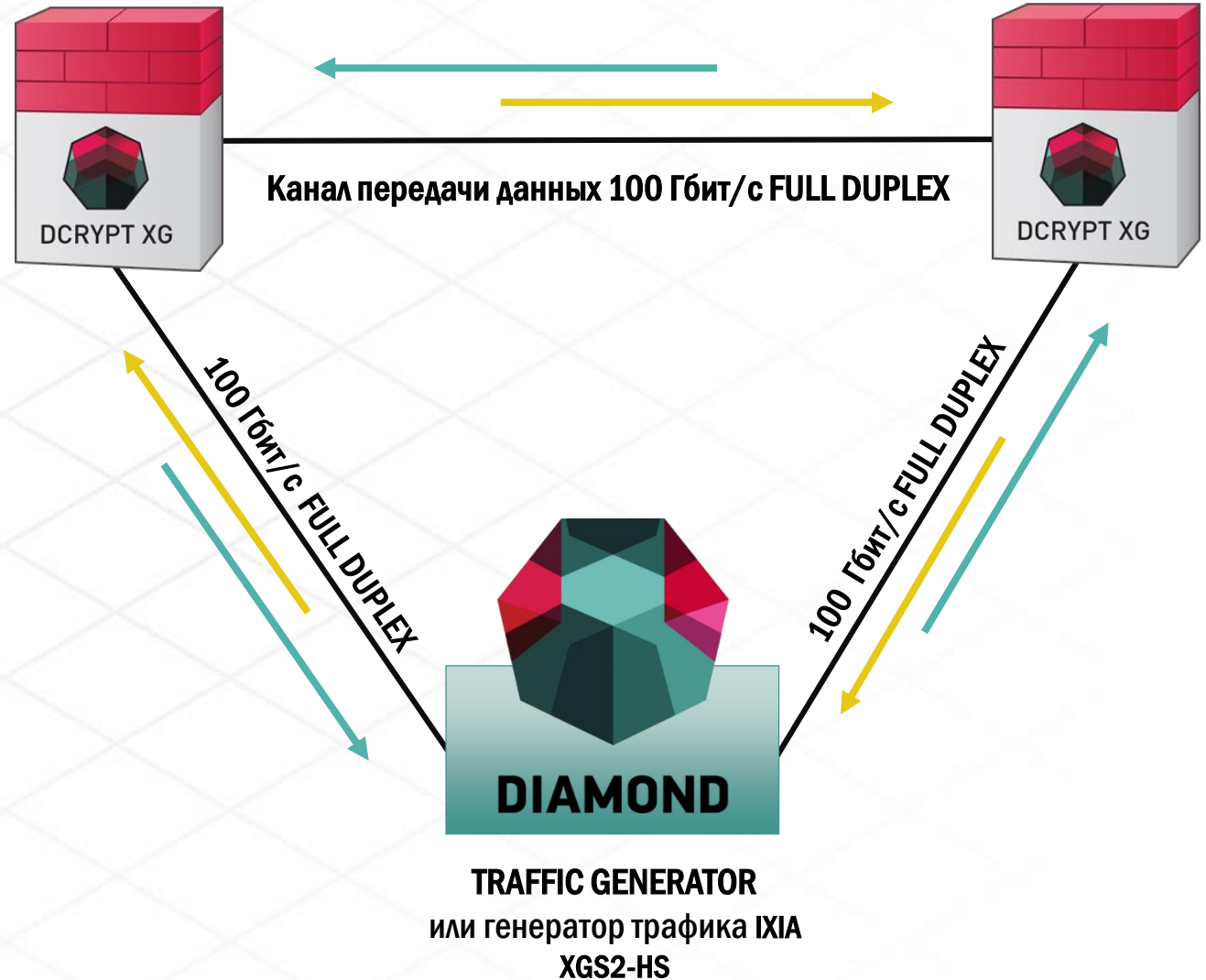
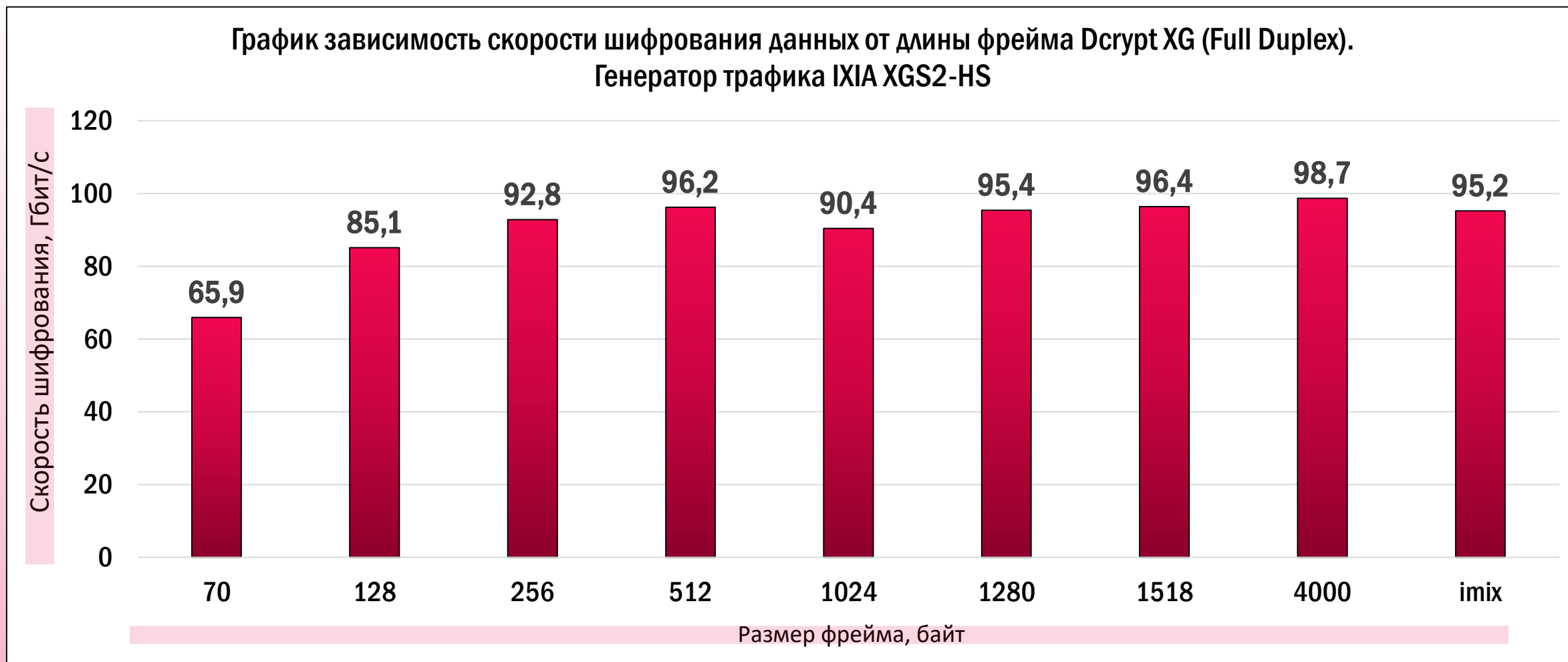


График зависимость скорости шифрования данных от длины фрейма Dcrypt XG (Full Duplex).  
Генератор трафика IXIA XGS2-HS



## График зависимости количества фреймов в секунду от размера фрейма

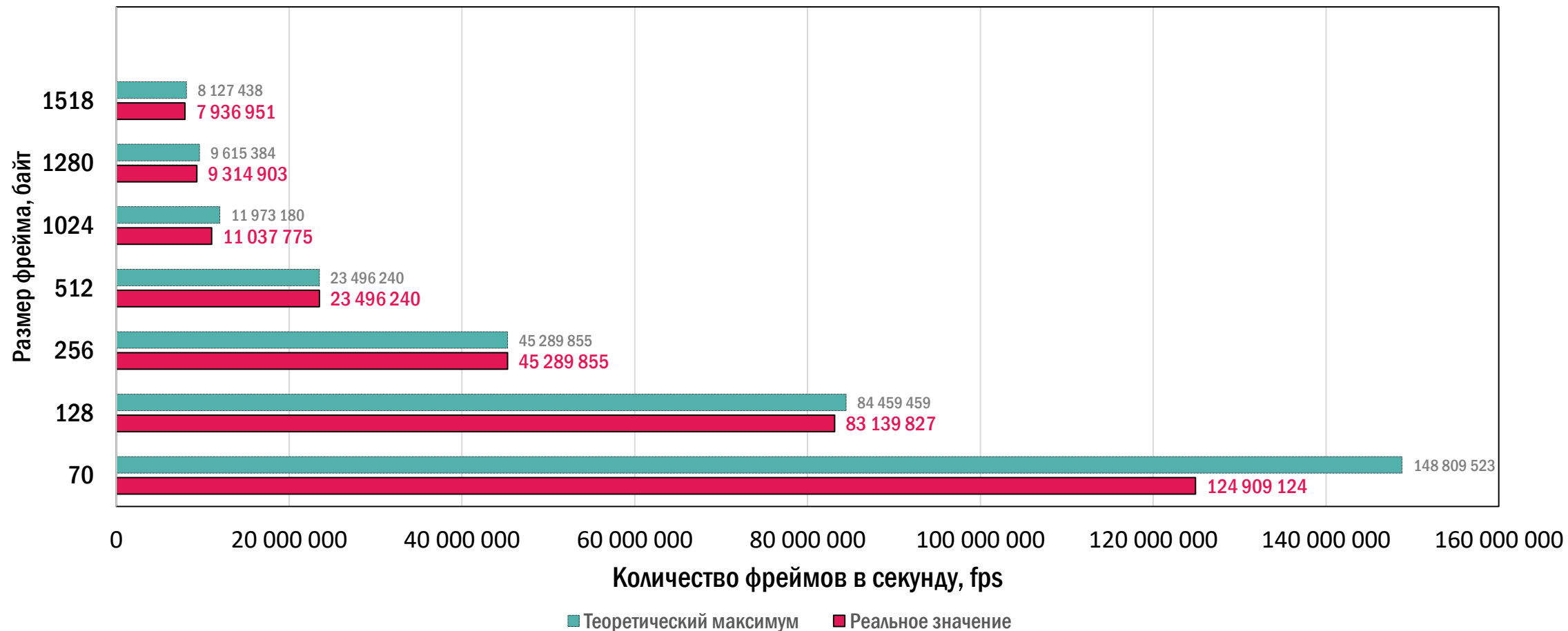
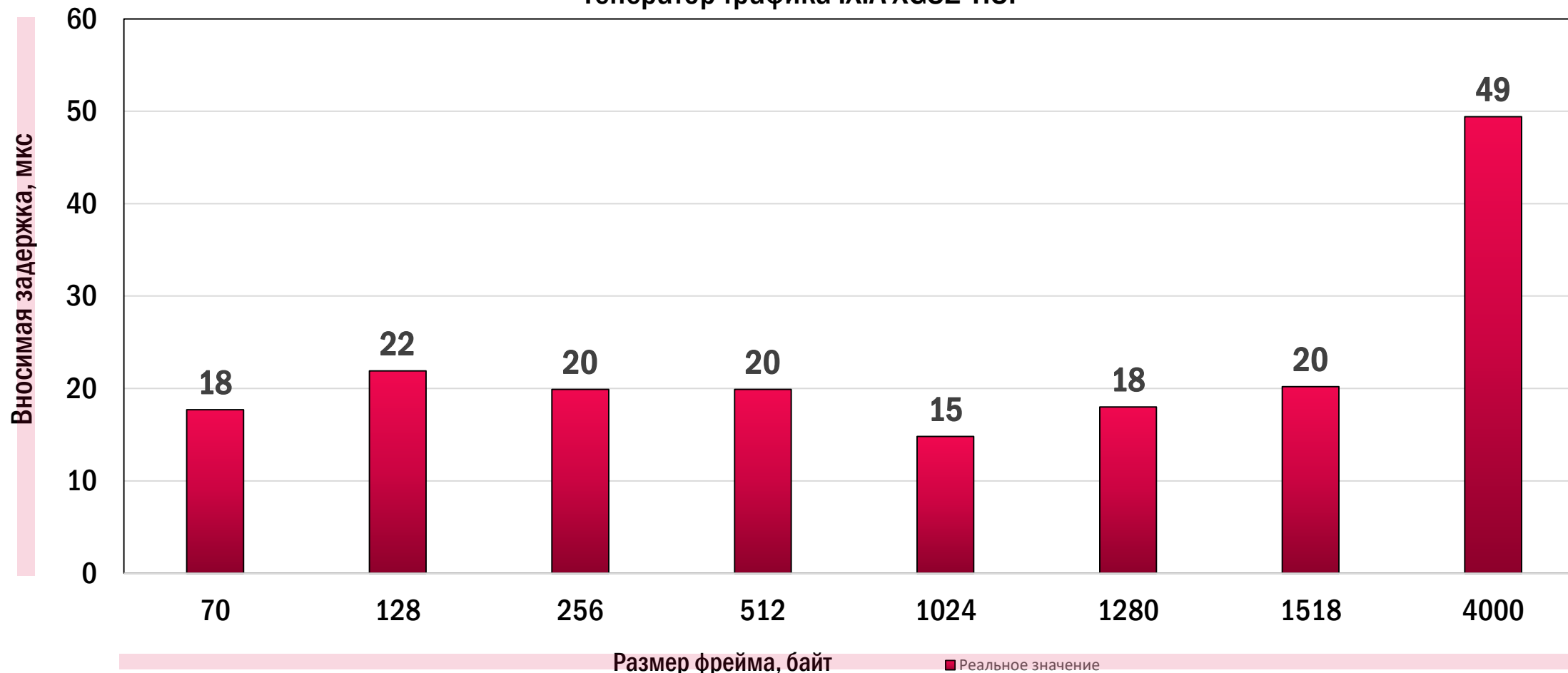
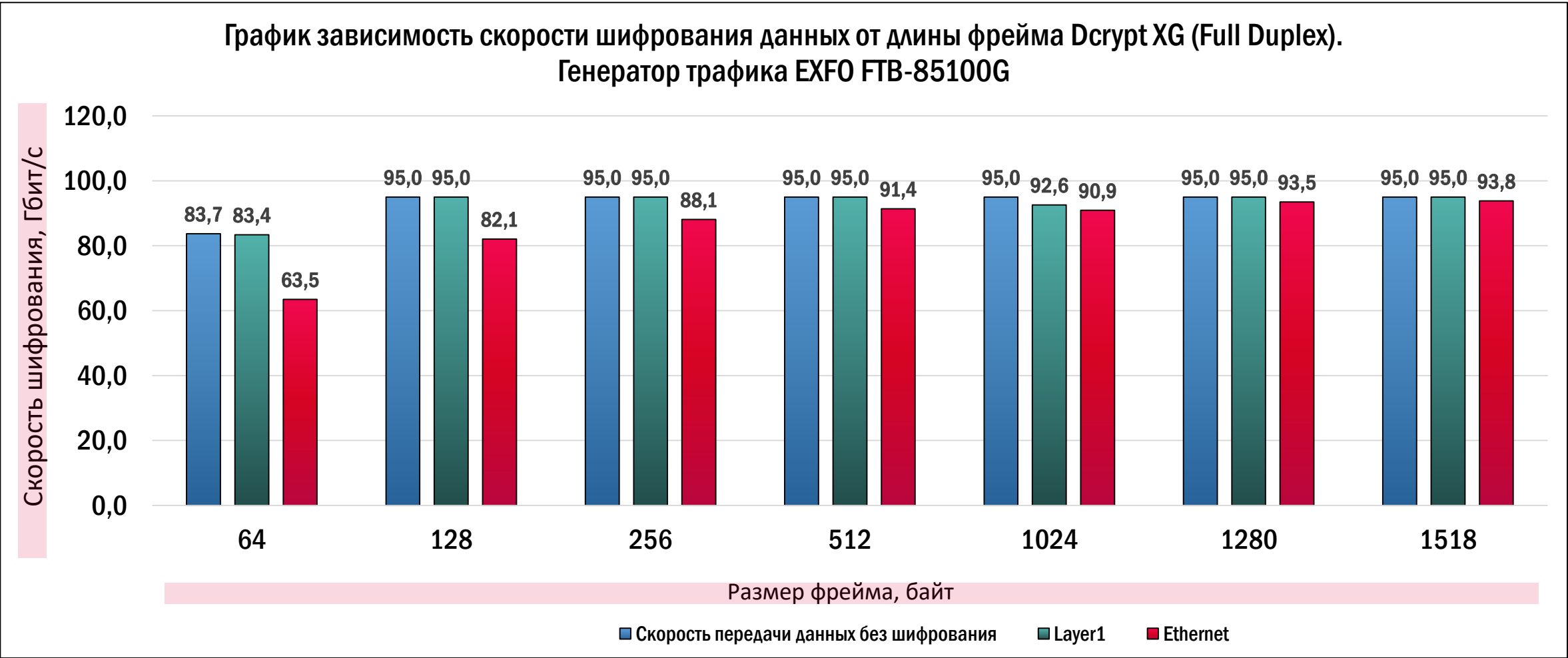


График зависимости вносимой задержки от размера фрейма, мкс.  
Генератор трафика IXIA XGS2-HS.







**СКЗИ «Dcrypt 1.0 v.2»  
Исполнение 50  
Класс защиты КС1**



**СКЗИ «Dcrypt 1.0 v.2»  
Исполнение 51  
Класс защиты КС2**








**СКЗИ «Dcrypt 1.0 v.2»  
Исполнение 52  
Класс защиты КС3**

Сертификат соответствия  
Рег. № СФ/124-3738 от 26.08.2019 г.  
действителен до 26.08.2022 г.,  
выдан ФСБ РФ в системе Сертификации РОСС  
RU.0001.030001

Сертификат соответствия  
Рег. № СФ/124-3739 от 26.08.2019 г.  
действителен до 26.08.2022 г.,  
выдан ФСБ РФ в системе Сертификации РОСС  
RU.0001.030001

Сертификат соответствия  
Рег. № СФ/124-3740 от 26.08.2019 г.  
действителен до 26.08.2022 г.,  
выдан ФСБ РФ в системе Сертификации РОСС  
RU.0001.030001

 <p><b>СКЗИ «Dcrypt 1.0 v.2»</b> Исполнения 1, 3, 4, 6, 18, 21, 31, 33, 34 и 36</p>	 <p><b>СКЗИ «Dcrypt 1.0 v.2»</b> Исполнения 2, 5, 16, 17, 19, 20, 32 и 35</p>	 <p><b>СКЗИ «Dcrypt 1.0 v.2»</b> Исполнения 50, 51 и 52</p>	 <p><b>МКСЗ «Diamond VPN/FW»</b></p>
<p>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</p>	<p>Сертификат соответствия Рег. № СФ/124-3644 от 12.04.2019 г. действителен до 12.04.2022 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001</p>	<p>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</p>	<p>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</p>
<p>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</p>	<p>Сертификат соответствия Рег. № СФ/124-3645 от 12.04.2019 г. действителен до 12.04.2022 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001</p>	<p>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</p>	 <p><b>СКРД «Diamond ACS»</b></p>
<p>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</p>	<p>Сертификат соответствия Рег. № СФ/124-3646 от 12.04.2019 г. действителен до 12.04.2022 г., выдан ФСБ РФ в системе Сертификации РОСС RU.0001.030001</p>	<p>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</p>	<p>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 (дата окончания поддержки – 08.07.2044 г.)</p>





**Спасибо за внимание!**

---

**Адрес: Москва, 105187, ул. Борисовская, д.1, офис 900.**

**Телефон, факс: +7 (495) 120-12-84.**

**E-mail: [info@tssltd.ru](mailto:info@tssltd.ru).**