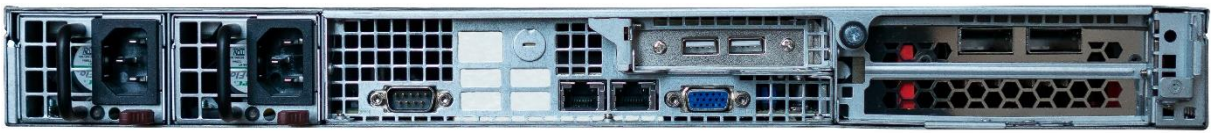
Программно-аппаратный комплекс «Канальный шифратор Dionis-CE»

Изделие «Канальный шифратор Dionis-CE» разработано компанией «Фактор-ТС» и предназначено для криптографической защиты информации, передаваемой по высокоскоростным каналам связи на скорости 100 Гб/с. Изделие содержит плату на базе программируемых логических интегральных схем (ПЛИС), в которой на аппаратном уровне реализованы криптографические алгоритмы ГОСТ, что обеспечивает высокую производительность и минимальную задержку. Плата ПЛИС имеет сетевые порты, обеспечивающие подключение трансиверов по стандарту QSFP28 для приема/передачи кадров Ethernet. Защита информации реализована путем шифрования и имитозащиты данных, содержащихся в кадрах Ethernet. Для защиты канала связи требуется два изделия.



Внешний вид

Технические характеристики

- Форм-фактор 1U для монтажа в стойку 19”.
- Габариты Ш х В х Г (мм) 438 х 44 х 435.
- Электропитание от сети 220-230 В, 50 Гц.
- 2 блока питания с горячей заменой, каждый мощностью 400 Вт.
- 2 сетевых порта 100G QSFP28 для подключения к сети передачи защищаемых данных.
- 2 сетевых порта 1G RJ45 (1000BASE-T) для подключения к сети управления и мониторинга.
- 2 порта USB 2.0 для подключения внешних носителей.
- VGA порт для подключения монитора.
- COM порт для локального доступа к консоли управления.
- Поддержка кадров по стандарту Ethernet IEEE 802.3ba (100-гигабитный Ethernet).
- Поддержка тегированных кадров Ethernet IEEE 802.1q.
- Поддержка кадров длиной до 10000 байт (Jumbo frame).
- Максимальная задержка обработки кадра на одном шифраторе в одном направлении не превышает 0,024 мс.
- Максимальная задержка обработки кадра на двух шифраторах в двух направлениях (Round-Trip Time) не превышает 0,1 мс.
- Скорость шифрования для кадров размером 64 байта, в одном направлении, не менее 60 Гб/с; в двух направлениях одновременно (duplex) не менее 120 Гб/с.
- Скорость шифрования для кадров размером 1518 байт, в одном направлении, не менее 97 Гб/с; в двух направлениях одновременно (duplex) не менее 194 Гб/с.
- Скорость шифрования для кадров размером 10000 байт, в одном направлении, не менее 99 Гб/с; в двух направлениях одновременно (duplex) не менее 198 Гб/с.

Криптографическая защита информации

- Реализованы алгоритмы ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
- Сертификат ФСБ РФ на соответствие требованиям к средствам криптографической защиты информации класса КС3 (№ СФ/124-3960 от 30.12.2020 г действителен до 30.12.2023 г).
- Применяются ключи шифрования парно-выборочной связи, изготавливаемые с использованием сертифицированного СКЗИ «Автоматизированное рабочее место генерации ключей «АРМ ГК-4».
- Ввод ключевой информации со сменных носителей, подключаемых к порту USB. Хранение ключевой информации в памяти устройства.

Обеспечение качества сервиса

- Сохранение тега IEEE 802.1q, включая значения идентификатора VLAN и приоритета (CoS), из заголовка исходного кадра Ethernet.
- Установка/замена тега IEEE 802.1q, включая значения идентификатора VLAN и приоритета (CoS) в заголовке исходного кадра Ethernet.
- Удаление тега IEEE 802.1q из исходного кадра Ethernet.
- Прозрачное (без зашифрования) пропускание кадров указанного типа (EtherType), например, кадров протоколов диагностики канального подключения IEEE 802.3ag (CFM).

Система управления и мониторинга

- Управление и мониторинг с помощью интерфейса командной строки. Доступ к интерфейсу командной строки по протоколам SSH и Telnet.
- Ролевая модель аутентификации пользователей с поддержкой ролей привилегированного пользователя (администратора), в рамках которой могут выполняться функции управления (настройка, конфигурирование и т.д.) и непривилегированного пользователя, в рамках которой выполняется контроль функционирования СКЗИ.
- Мониторинг в реальном времени состояния интерфейсов шифратора, загрузки системы и статистики трафика.
- Поддержка внешнего мониторинга работы шифратора по протоколу SNMP.
- Регистрация событий, связанных с настройкой и функционированием шифратора в журналы и экспорт журналов на внешний носитель, подключаемый к порту USB.
- Поддержка отправки журналов по протоколу Syslog.

Дополнительные возможности

- Контроль целостности ПО.
- Контроль функционирования шифратора.
- Средства обновления ПО.

Результаты лабораторных испытаний пропускной способности и задержки по методике RFC 2544

Размер кадра (байт)	**64**	**128**	**256**	**512**	**1024**	**1280**	**1518**	**2048**	**4096**	**8192**	**10000**
Суммарные показатели для прямого и обратного направления трафика (режим duplex)											
Процент утилизации канала	82,44%	90,24%	94,15%	96,88%	98,44%	98,44%	98,83%	99,22%	99,61%	99,61%	99,61%
Скорость на уровне L2 (Гб/с)	125,62	156,1	174,65	186,47	193,11	193,85	195,09	196,52	198,25	198,73	198,82
Скорость (кадр/с)	245 355 514	152 439 426	85 277 612	45 525 434	23 572 572	18 930 588	16 064 580	11 994 624	6 050 154	3 032 444	2 485 272
Потери кадров	0	0	0	0	0	0	0	0	0	0	0
Детализация показателей в одном направлении											
Скорость на уровне L2 (Гб/с)	62,81	78,05	87,32	93,24	96,55	96,92	97,54	98,26	99,13	99,37	99,41
Скорость (кадр/с)	122 677 757	76 219 713	42 638 806	22 762 717	11 786 286	9 465 294	8 032 290	5 997 312	3 025 077	1 516 222	1 242 636
Средняя задержка (мкс)	3,088	3,244	3,481	3,998	5,035	5,54	6,024	7,094	11,192	19,384	23,003
Min задержка (мкс)	3,056	3,208	3,449	3,962	5,004	5,51	5,991	7,057	11,131	19,325	22,958
Max задержка (мкс)	3,136	3,289	3,529	4,05	5,077	5,582	6,071	7,129	11,227	19,438	23,054
Джиттер (мкс)	0,003	0,004	0,003	0,004	0,005	0,005	0,006	0,005	0,007	0,013	0,005

Размер кадра (байт)	**64**	**128**	**256**	**512**	**1024**	**1280**	**1518**	**2048**	**4096**	**8192**	**10000**
Детализация показателей в обратном направлении											
Скорость на уровне L2 (Гб/с)	62,81	78,05	87,32	93,24	96,55	96,92	97,54	98,26	99,13	99,37	99,41
Скорость (кадр/с)	122 677 757	76 219 713	42 638 806	22 762 717	11 786 286	9 465 294	8 032 290	5 997 312	3 025 077	1 516 222	1 242 636
Средняя задержка (мкс)	3,1	3,249	3,485	4,019	5,032	5,549	6,032	7,098	11,192	19,379	23,016
Min задержка (мкс)	3,064	3,208	3,449	3,986	4,996	5,518	5,991	7,065	11,131	19,325	22,974
Max задержка (мкс)	3,144	3,297	3,537	4,058	5,069	5,598	6,079	7,137	11,227	19,43	23,07
Джиттер (мкс)	0,002	0,004	0,003	0,004	0,005	0,005	0,006	0,005	0,007	0,013	0,005

График производительности и задержки по результатам испытаний