НОРСИ-ТРАНС
Закрытое Акционерное Общество

Российские разработки средств шифрования алгоритмами ГОСТ

Докладчик: Сметанин Андрей Михайлович
Отдел внедрения СОРМ
a.smetanin@norsi-trans.ru
+79852736104

Нормативное регулирование устройств криптографической защиты (ЦЛСЗ ФСБ России):

- Приказ ФСБ РФ № 182 от 23 марта 2016.
- Статья 12 ФЗ РФ от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Постановление Правительства РФ № 313 от 16 апреля 2012 (В редакции Постановления Правительства Российской Федерации от 18.05.2017 г. № 596).
- Статья 28 ИЗВЕЩЕНИЕ по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети «Интернет» ФСБ РФ от 18 июля 2016.
- Приказ ФСБ РФ № 66 от 9 февраля 2005 года.

Классы сертификации: Требования ФСБ РФ к СКЗИ

- Постановление правительства РФ № 1119 от 1 ноября 2012 утверждает требования к защите ПДн в ИСПДн согласно 19 статье ФЗ РФ № 152 от 27 июля 2006 года. Согласно пункту 6 устанавливаются уровни угроз: Угрозы 1-го, 2-го и 3-его типа
- Согласно пунктам с 8 по 12 устанавливаются уровни защищённости систем: Уровни защищенности с 1 по 4.
- Согласно Приказа ФСБ РФ №378 СКЗИ делятся на пять классов (КА, КВ, КС3, КС2, КС1) и их применение зависит от уровня защищённости системы и типа угроз:

	4 уровень	3 уровень	2 уровень	1 уровень
угрозы 1 типа	-	-	КА	КА
угрозы 2 типа	-	КА, КВ	КВ	КВ
угрозы 3 типа	КА, КВ, КС3, КС2, КС1	КС3, КС2, КС1	КС3, КС2, КС1	-

Классы сертификации: Требования ФСТЭК для МЭ

Согласно информационному сообщению «Об утверждении Требований к межсетевым экранам» Информационное сообщение ФСТЭК России от 28 апреля 2016 г. N 240/24/1986 МЭ делятся по типам объектов оценки:

- МЭ типа «А»
- МЭ типа «Б»
- МЭ типа «В»
- МЭ типа «Г»
- МЭ уровня промышленной сети (тип «Д»)

Шесть классов защиты межсетевых экранов.

Области применения МЭ.

Виток-МЭ4

- ❑ Функциональность
- ❑ Регистрация и учет фильтруемых пакетов
- ❑ Краткая спецификация
- ❑ Энергоэффективность, компактность и стабильность

Технические характеристики:

- Максимальная пропускная способность, Гбит/с: 480;
- Количество параллельных сессий: не ограничено;
- Количество правил таблиц фильтрации – на устройство: до 3072;
- Количество правил таблиц фильтрации – на порт ввода/вывода: до 256;
- Встроенные порты ввода/вывода: 12 портов 1GbE/10GbE (SFP+);
- Дополнительные порты ввода/вывода: 12 портов 1GbE/10GbE (SFP+);
- Встроенные порты управления: 2 порта 10/100/1000MbE UTP;
- Масштабируемость: поддерживается;
- Дополнительный источник питания: поддерживается.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3258

Выдан 5 ноября 2014 г.
Действителен до 5 ноября 2017 г.

Настоящий сертификат удостоверяет, что **межсетевой экран «Виток-МЭ4»** с **установленным программным обеспечением NS_FW, Version 2.0.35** (партия из 100 (ста) экземпляров продукции с серийными №№ с 77НТ-ВитМЭ4-00001 по 77НТ-ВитМЭ4-00100, маркированных знаками соответствия с № И 459314 по № И 459413) производства ЗАО «НОРСИ-ТРАНС», является программно-техническим средством защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей и соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 4 классу защищённости при выполнении ограничений по эксплуатации, указанных в формуляре НИКА.466533.093.ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведённых испытательной лабораторией ЗАО «Научно-производственное предприятие «Безопасные информационные технологии» (аттестат аккредитации от 11.09.2003 № СЗИ RU.473.Б022.047) – техническое заключение от 23.09.2014, и экспертного заключения от 30.09.2014 органа по сертификации ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 13.05.2003 № СЗИ RU.1190.Б032.056).

Заявитель: ООО «ЦИТ-2007»
Адрес: 105187, г. Москва, ул. Щербаковская, д. 53, корп. 4
Телефон: (495) 963-5150

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящего документа, указанного в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «Научно-производственное предприятие «Безопасные информационные технологии».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

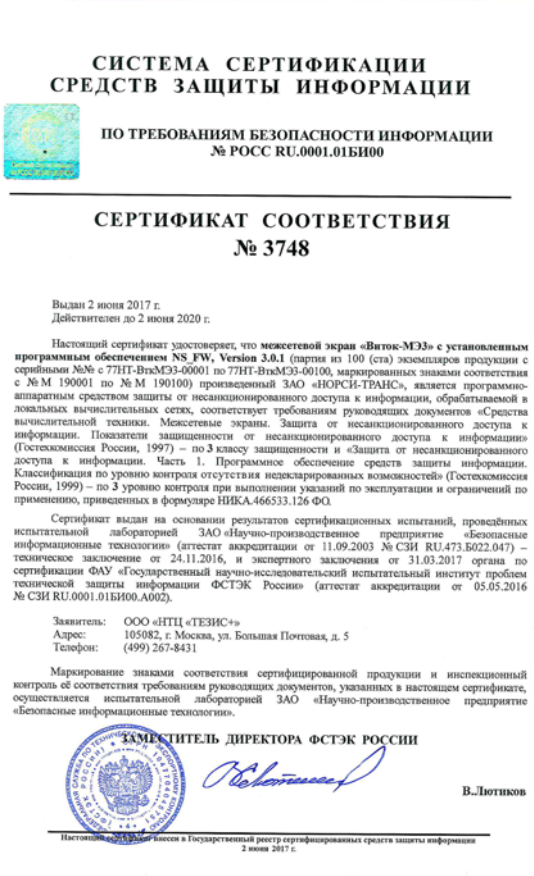
А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 5 ноября 2014 г.

«Виток-МЭЗ (Firewall)

- ❑ Сертификация
- ❑ Функциональность
- ❑ Энергоэффективность, компактность и стабильность
- ❑ Технические характеристики:

- Максимальная пропускная способность, Гбит/с: 240;
- Количество параллельных сессий: не ограничено;
- Количество правил таблиц фильтрации – на устройство: до 1536;
- Количество правил таблиц фильтрации – на порт ввода/вывода: до 64;
- Встроенные порты ввода/вывода: 24 порта 10GbE (SFP+), 24 порта 1GbE (SFP);
- Встроенные порты управления: 2 порта 10/100/1000MbE UTP;
- Масштабируемость: поддерживается;
- Дополнительный источник питания: поддерживается.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3748

Выдан 2 июня 2017 г.
Действителен до 2 июня 2020 г.

Настоящий сертификат удостоверяет, что **межсетевой экран «Виток-МЭЗ» с установленным программным обеспечением NS_FW, Version 3.0.1** (партия из 100 (ста) экземпляров продукции с серийными №№ с 77НТ-ВткМЭЗ-00001 по 77НТ-ВткМЭЗ-00100, маркированных знаками соответствия с № М 190001 по № М 190100) произведенный ЗАО «НОРСИ-ТРАНС», является программно-аппаратным средством защиты от несанкционированного доступа к информации, обрабатываемой в локальных вычислительных сетях, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 3 уровню контроля при выполнении указаний по эксплуатации и ограничений по применению, приведенных в формуляре НИКА.466533.126 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведённых испытательной лабораторией ЗАО «Научно-производственное предприятие «Безопасные информационные технологии» (аттестат аккредитации от 11.09.2003 № СЗИ RU.473.Б022.047) – техническое заключение от 24.11.2016, и экспертного заключения от 31.03.2017 органа по сертификации ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ООО «НТЦ «ТЕЗИС+»
Адрес: 105082, г. Москва, ул. Большая Почтовая, д. 5
Телефон: (499) 267-8431

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «Научно-производственное предприятие «Безопасные информационные технологии».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
2 июня 2017 г.

Требования ФСТЭК для Систем Обнаружения Вторжений (СОВ)

Требования к системам обнаружения вторжений применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Требования к системам обнаружения вторжений включают общие требования к системам обнаружения вторжений и требования к функциям безопасности систем обнаружения вторжений.

Для дифференциации требований к функциям безопасности систем обнаружения вторжений установлено шесть классов защиты систем обнаружения вторжений.

СОПСА — Система Обнаружения и Предотвращения Сетевых Атак

Алгоритмы шифрования:

- шифрование ГОСТ Р 34.12-2015
- гаммирование ГОСТ Р 34.13-2015
- имитозащита ГОСТ 28147-89

Сравнение характеристик устройств криптозащиты:

- по скорости шифрования трафика
- по числу портов
- масштабирование

Режим	Описание
balance-rr	В этом режиме исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно
balance-xor	В этом режиме для определения подчиненного физического интерфейса, через который отправляется пакет, используется специальная хэш-функция
balance-tlb	В этом режиме ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется выбор интерфейса, через который будет передан пакет, попавший на агрегированный интерфейс
802.3ad	В этом режиме динамическое агрегирование происходит с помощью протокола LACP
active-backup	В этом режиме один из подчиненных физических интерфейсов назначается основным, и все исходящие пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.

Возможность создавать агрегированные интерфейсы. Несколько режимов агрегации.

Режим	Описание
Failover	Передача трафика осуществляется через интерфейс с наивысшим приоритетом (активный), остальные интерфейсы играют роль резервных. При выходе активного интерфейса из строя трафик автоматически станет передаваться через работоспособный резервный интерфейс с наивысшим приоритетом. При восстановлении работоспособности интерфейса с наивысшим приоритетом трафик автоматически станет передаваться через него.
Round-Robin	Исходящий трафик распределяется через все LAG-интерфейсы с использованием циклического планировщика. Данный режим может привести к беспорядочному прибытию IP-пакетов к клиенту.
По протоколу LACP (802.3ad)	Агрегация по протоколу LACP. Выбор интерфейса происходит по специальной формуле, в зависимости от выбранного режима хэширования: • L2 — учет MAC-адресов источника и назначения трафика; • L3 — учет IP-адресов источника и назначения трафика (обычно используется вместе с L2); • L4 — учет номеров портов источника и назначения трафика (обычно используется вместе с L3)
Опция use_flowid	Включение локального вычисления хэш-функции для RSS-хэша на интерфейсе
Опция lacp_fast_timeout	Автоматическая перенастройка значения параметра timeout на 1 секунду (быстрый тайм-аут) для передачи пакетов BPDU.

Приглашаем к сотрудничеству

ЗАО «Норси-Транс»
E-mail: info@norsi-trans.ru *a.smetanin@norsi-trans.ru*
Тел.: +7 495 748 7483; +79852736104.