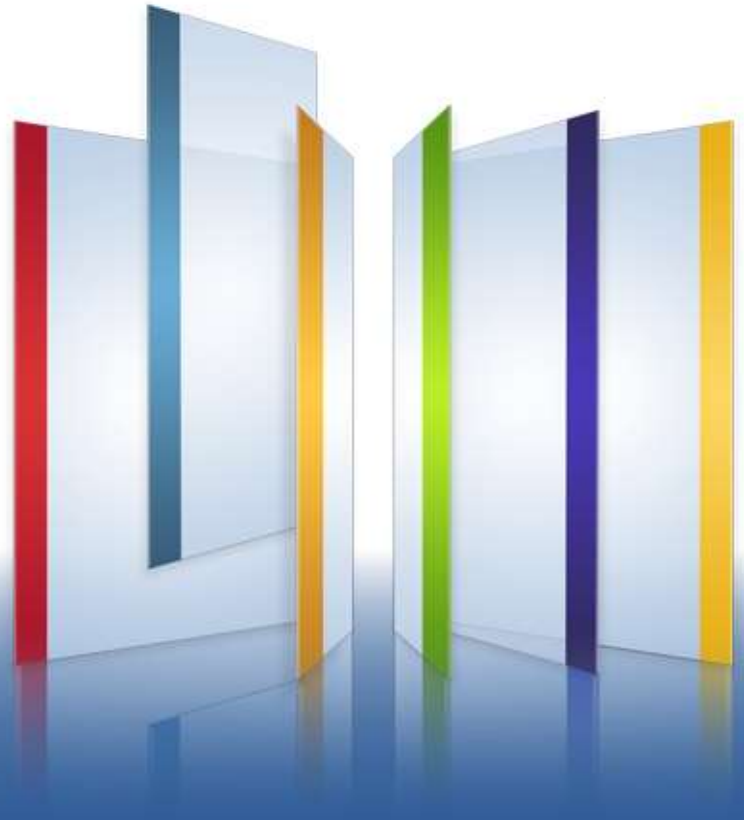
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Сертифицированные продукты Check Point и требования Российского законодательства

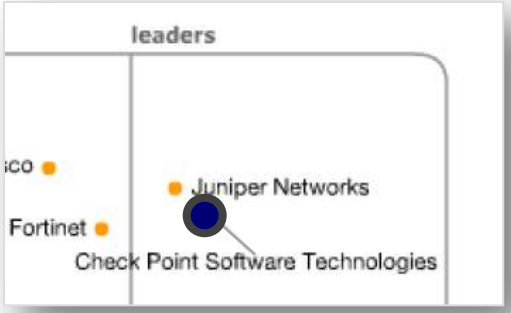


Василий Широков
vshirokov@checkpoint.com
Check Point Software Technologies

Продукты и решения Check Point

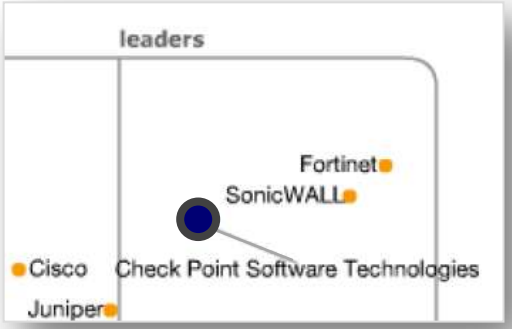
Египет, Шарм-эль-Шейх, Рас Мохаммед

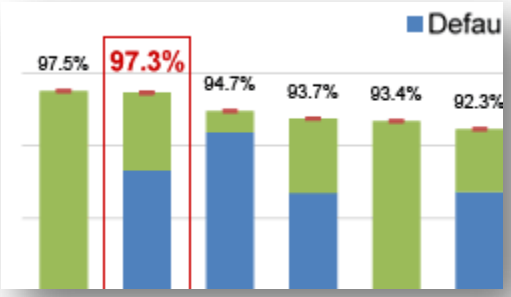
Check Point - лидер рынка



GARTNER (FWs, March 2010): Check Point рассматривается как **лидер для крупных корпораций** потому что … компания побеждает конкурентов благодаря реализованному функционалу и мощной сети продаж

GARTNER (UTMs, October 2010). Check Point UTM-1 признан как продукт, представляющий простое, комплексное решение, обеспечивающее высочайший уровень защиты для малого и среднего бизнеса и удаленных офисов.





January, 2011. NSS Lab. Эффективность Check Point IPS на отличном уровне, обеспечив производительность 2,4 Gbps. При этом Check Point корректно идентифицировал все 100% попыток обхода сенсора

April, 2011. Check Point показал 100% эффективность в тестах NSS Lab по FW, Identity Awareness и Application Control и первым в отрасли получил рейтинг **«Рекомендовано» для Next Generation Firewalls (NGFW)**.

Интегрированные шлюзы для любых задач

Check Point SOFTWARE TECHNOLOGIES LTD.

UTM-1 appliances

- Firewall Blade
- IPsec VPN Blade
- Applic. Control Blade
- Identity Awar. Blade
- IPS Blade
- URL Blade
- AV Blade
- Anti-Spam Blade

- Mobile Access Blade
- Data Loss Prevent. Blade
- Adv. Networking Blade
- Acceler&Cluster Blade
- Web security Blade

Power -1 appliances

- Firewall Blade
- IPsec VPN Blade
- Applic. Control Blade
- Identity Awar. Blade
- IPS Blade
- Adv. Networking Blade
- Acceler&Cluster Blade

- Mobile Access Blade
- Data Loss Prevent. Blade
- Web security Blade
- AV Blade
- URL Blade
- Anti-Spam Blade

IP appliances

- Firewall Blade
- IPsec VPN Blade
- Applic. Control Blade
- Identity Awar. Blade
- IPS Blade
- Adv.Networking Blade
- Acceler&Cluster Blade

- Web security Blade
- Voice over IP Blade

Функционал шлюза безопасности

Check Point SOFTWARE TECHNOLOGIES LTD.

Функцио-нальные Security Blades

Сервисные Security Blades

- Firewall
- IPSec VPN
- Acceleration & clustering
- Advanced networking
- Web security
- New — Identity Awareness
- New — Mobile Access (SSL VPN)
- New — IPS
- New — Application control
- McAfee — URL filtering
- Kaspersky lab — Antivirus & anti-malware
- commtouch® — Anti-spam & email security
- New — Data loss prevention

softwareblades™

Защита конфиденциальной информации

Швейцария, Энгельберг, окрестности

Защита информации при межсетевом взаимодействии

Check Point SOFTWARE TECHNOLOGIES LTD.

ФСТЭК России. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»

5.7.4. Подключение ЛВС к другой автоматизированной системе (локальной или распределенной вычислительной сети) должно осуществляться с использованием МЭ, требования к которым определяются РД Гостехкомиссии России. Например, для защиты АС при ее взаимодействии с другой АС по каналам связи необходимо использовать: **в АС класса 1Г – МЭ не ниже класса 4;**

МЭ Check Point FireWall-1/VPN-1 R65 сертифицирован по **3-му классу защищенности**. Сертификат соответствия для версии R65 HFA50 (для 1Г и К2 ИСПДн) №2119 от 17 июня 2010

5.7.5. Для защиты конфиденциальной информации, передаваемой между АС по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи,а **при использовании открытых каналов связи - сертифицированные ФАПСИ криптографические средства защиты информации**

Используются сертифицированный ФСБ России криптобиблиотеки **КриптоПро CSP 3.6**

Требования ФЗ 152

«Положение о методах и способах защиты информации в информационных системах персональных данных» Приказ ФСТЭК России N 58 от 05.02.2010

Методы и способы… Раздел 4.4

Безопасное межсетевое взаимодействие для информационных систем 1 класса при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования [перечень]

Методы и способы… Раздел 6

Обнаружение вторжений проводится … путем использования в составе информационной системы … средств (систем) обнаружения вторжений

Методы и способы… Раздел 7

Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия НДВ

Новая Зеландия, Окленд, исторический музей

Сертификация Check Point во ФСТЭК

- **Получен сертификат соответствия на Check Point Firewall-1/VPN-1 версии NGX, R65 HFA50 по МЭ3 для 1Г, К2 ПДн**
  - Программное обеспечение на Power-1, UTM-1, IP Appliance, универсальные АП
  - СКЗИ «КриптоПро CSP» версия 3.6
- Сертификация ФСТЭК производства продуктов Check Point Security Gateway R71. Сертификация по требованиям на МЭ по 3-му классу защищенности и ТУ (дополнительно функционал IPS, антивирус)
- Сертификация ФСТЭК на 4 уровень отсутствия НДВ (планируется проведение для R71)
- **Получен сертификат соответствия на Check Point UTM-1 Edge по МЭ4**
- **В процессе сертификации шлюз удаленного доступа Check Point Connectra R66.1 на соответствие МЭ3 и ТУ (партия)**
- **Получено решение на сертификацию клиента безопасности CheckPoint Endpoint Security R73 на соответствие МЭ4 и ТУ (производство)**

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2119

Выдан 17 июня 2010 г.
Действителен до 17 июня 2013 г.

Настоящий сертификат удостоверяет, что **межсетевой экран «Check Point FireWall-1/VPN-1 версии NGX, R65 HFA 50»** (партия из 200 (двухсот) экземпляров продукции (серийный номер: CPMP-CERT-R65HFA50, номера комплектов с № 0001 по № 0200, маркированных знаками соответствия с № Г 152240 по № Г 152439 соответственно) производства компании Check Point Software Technologies Ltd., является программным 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 защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) - по 3 классу защищенности, и может использоваться при

Система сертификации ФСТЭК

Сертификация Check Point Security Gateway R71 на соответствие МЭ3 и ТУ

Санкт-Петербург, городовой

Управление доступом посредством контроля сетевого трафика методами фильтрации сетевых пакетов (в том числе Stateful Inspection);

Управление доступом мобильных и удаленных пользователей к различным ресурсам сети (в том числе, web-приложениям и ресурсам, а также разделяемым файлам и электронной почте) в зависимости от результата их аутентификации (в версии R75);

Обнаружение и предотвращение сетевых атак (вторжений), обеспечивающее целостность внутренних приложений сети

Управление доступом с удаленных рабочих станций посредством блокирования доступа с устройств, не прошедших проверку политики доступа (в версии R75);

Защита от вирусов и вредоносных программ посредством обнаружения и уничтожения вирусов, шпионского ПО и иных вредоносных программ

Работы по сертификации шлюза безопасности Check Point Security Gateway R71.20 начались в апреле 2011 года (сертификация производства)

Система сертификации ФСТЭК

Сертификация Check Point Endpoint Security R80 на соответствие МЭ4 и ТУ

Санкт-Петербург, городовой

Управление доступом посредством контроля сетевого трафика методами фильтрации сетевых пакетов (модуль Firewall and Security Compliance Verification)

Управление доступом к внешним устройствам и портам компьютера (модуль Media Encryption and Port Protection)

Управление доступом пользователей к Интернет-ресурсам (модуль WebCheck) путем виртуализации браузера, средств антифишинга и обнаружения сайтов с вредоносным кодом

Анализ защищенности рабочей станции посредством проверки наличия актуальных обновлений ПО до предоставления доступа к сети (модуль Firewall and Security Compliance Verification)

Защита от вирусов и вредоносных программ посредством обнаружения и уничтожения вирусов, шпионского ПО и иных вредоносных программ (модуль Anti-Malware and Program Control)

Работы по сертификации клиента безопасности Check Point Endpoint Security R80 начинаются в Q3 2011 года (сертификация производства)

ТЗ на встраивание ГОСТ в удаленный доступ

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point Mobile Access Blade, Remote Access technologies

Check Point
SOFTWARE TECHNOLOGIES LTD.

Встраивание КриптоПро TLS (SPLAT) в Mobile Access Blade (Native SSL VPN)

SNX туннелирование должно защищаться SSL VPN GOST, если того требует политика

Поддержка многопоточности в Mobile Access Blade при реализации SSL VPN GOST

Встраивание КриптоПро TLS (Win, iOS, …) в клиентскую технологию удаленного доступа – Check Point Remote Access module (“Endpoint Connect”)

Встраивание SSL VPN GOST технологии в **Endpoint Security**

Встраивание SSL VPN GOST технологии в **Mobile Client**

Встраивание SSL VPN GOST технологии в **ABRA**

Новая Зеландия, Ваитомо

Встраивание СКЗИ от Крипто-Про

Швейцария, Энгельберг, Альпийский экспресс

Встраивание криптобиблиотек (СКЗИ)

Check Point SOFTWARE TECHNOLOGIES LTD.

ФСБ России. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных»

5.1. Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы)

5.2. Встраивание криптосредств класса КС1, КС2 или КС3 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России

Новая Зеландия, озеро Вакатипу

Проверка корректности встраивания

ФСБ России. «Средство криптографической защиты информации «КриптоПро CSP». Версия 3.6. Формуляр

Если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации

При организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ

При организации криптографической защиты информации ... при выполнении заказов для государственных нужд

При использовании библиотек класса КС1, КС2 проверка корректности встраивания со стороны ФСБ России требуется только при поставках в органы исполнительной власти, при выполнении госзаказов или если это явно требуется в ТЗ на СКЗИ

Работы по корректности встраивания планируются компанией Check Point после завершения сертификации СКЗИ КриптоПро R3.6.1

Новая Зеландия, вблизи Квинстауна

Встраивание СКЗИ КриптоПро CSP 3.6

1. Используется комбинированное преобразование ESP, включающее режим имитовставки для обеспечения целостности потока данных

2. Процедуры согласования ключей использует соответствующий требованиям Российского законодательства алгоритм VKO ГОСТ Р 34.10-2001 (RFC 4357), вместо традиционного (и не соответствующего криптостойкости ГОСТ) алгоритма Диффи-Хеллмана.

3. Формирование сессионных ключей осуществляется средствами СКЗИ КриптоПро CSP 3.6, таким образом никакие криптофункции не исполняются средствами продуков Check Point (в режиме ГОСТ IPsec), что также обусловлено задачей корректности встраивания СКЗИ КриптоПро CSP 3.6.

4. Реализовано кластерное VPN-решение, обеспечивающее синхронизацию криптоконтекстов СКЗИ КриптоПро CSP 3.6 (в зашифрованном виде), что обеспечивает оперативное переключение между элементами кластера без пересоздания IPsec туннелей.

Параметры встраивания

Алгоритмы шифрования	ESP_GOST-4M-IMIT (ГОСТ 28147-89 "режим гаммирования" + ГОСТ 28147-89 "режим имитовставки")
Алгоритмы согласования ключей	VKO ГОСТ Р 34.10-2001 (RFC 4357)
Формирование сессионных ключей	Средствами КриптоПро CSP 3.6
Методы аутентификации IKE	GOST-IKE-PSK, GOST-IKE-SIGNATURE
Встраивание СКЗИ	В соответствии с драфтами документов Технического комитета по стандартизации "Криптографическая защита информации" (ТК26) ФАТРМ
Синхронизация криптоконтекстов в кластерном VPN-решении	Да, в защищённом (зашифрованном) виде

Нотификация продуктов CHKP

Новая Зеландия, Квинстаун, озеро Вакатипу

Нотификация продуктов CHKP

Зарегистрирована в реестре "11" июня 2010 г. № RU0000002591

В.К.СВИРИН

М.П. _____ (подпись лица, уполномоченного органа) _____ (Ф.И.О.)

НОТИФИКАЦИЯ
о характеристиках товара (продукции),
содержащей шифровальные (криптографические) средства

1. Наименование товара (продукции) _____

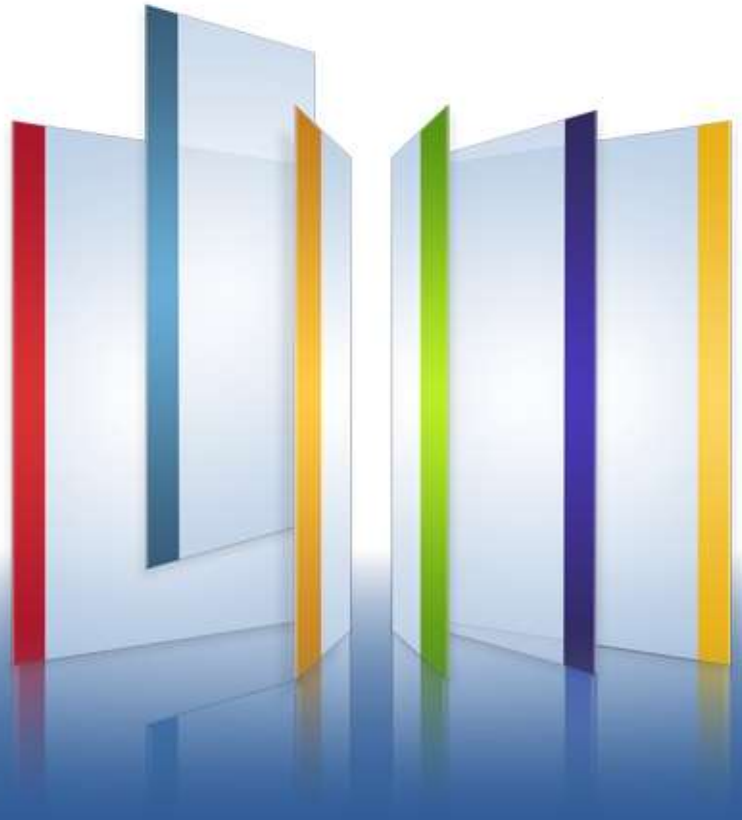
Устройства (аппаратно-программные комплексы) Check Point Power-1 и их модификации:

№ п/п	Каталожный номер, SKU	Краткое описание
1.	CPAP-SG5075-RUS	Устройство Power-1, тип 5075 с ПО SecurePlatform R70.20 и пакетом fw1_HOTFIX_R7020_56BIT_532
2.	CPAP-SG9075-RUS	Устройство Power-1, тип 9075 с ПО SecurePlatform R70.20 и пакетом fw1_HOTFIX_R7020_56BIT_532
3.	CPAP-SG11065-RUS	Устройство Power-1, тип 11065 с ПО SecurePlatform

Нотификация получена на: Power-1, UTM-1, UTM-1 Edge X3, UTM-1 Edge W3, Smart-1, IPS-1, DLP-1 и другие

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Спасибо!



Василий Широков
vshirokov@checkpoint.com
Check Point Software Technologies