Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Сетевая безопасность нового поколения – ответы на вызовы времени

Василий Широков, к.т.н.

Октябрь, 2013

Защита информации в ГосИС

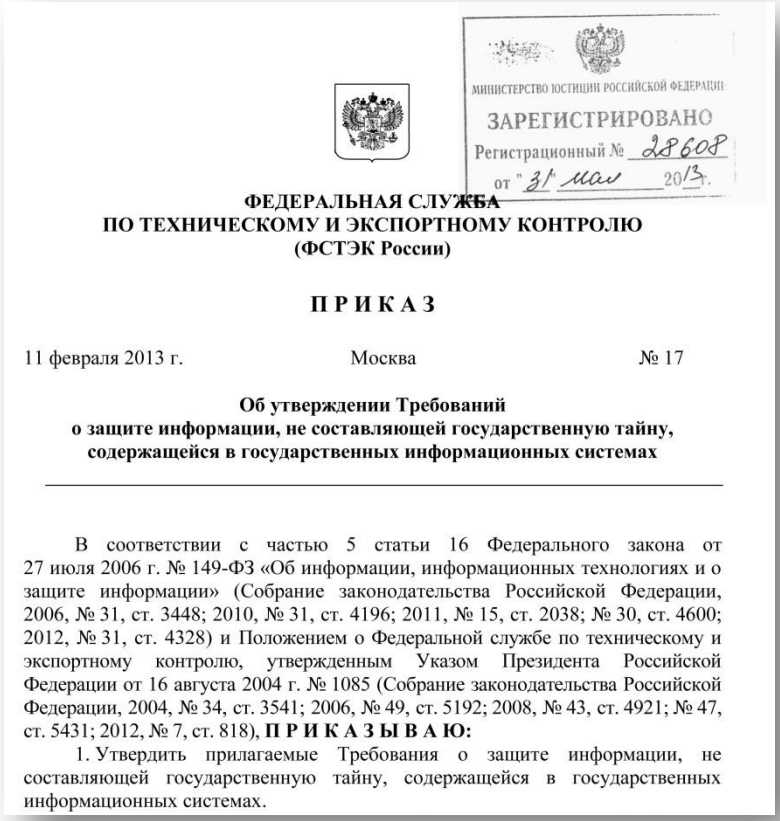
Новый СТР-К

ФСТЭК России. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

4 класса защищенности (К1 – К4)

В информационных системах 1 класса защищенности (К1) обеспечивается нейтрализация (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;

в информационных системах 2 класса защищенности (К2) - нарушителя с потенциалом не ниже среднего;



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 28608
от "31" мая 2013.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

11 февраля 2013 г. Москва № 17

Об утверждении Требований
о защите информации, не составляющей государственную тайну,
содержащейся в государственных информационных системах

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818), **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемые Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Меры по защите ГосИС

ФСТЭК России. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

- обеспечение доверенной загрузки;
- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- **управление доступом** субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- **регистрацию событий безопасности**;
- обеспечение целостности информационной системы и информации (включая **антивирусную защиту**, **обнаружение вторжений**);
- защиту **среды виртуализации**;
- защиту технических средств;
- защиту информационной системы, ее средств и систем связи и передачи данных (в том числе **защиту периметра , контроль использования мобильного кода** и **защиту от отказа в обслуживании**).

Защита персональных данных

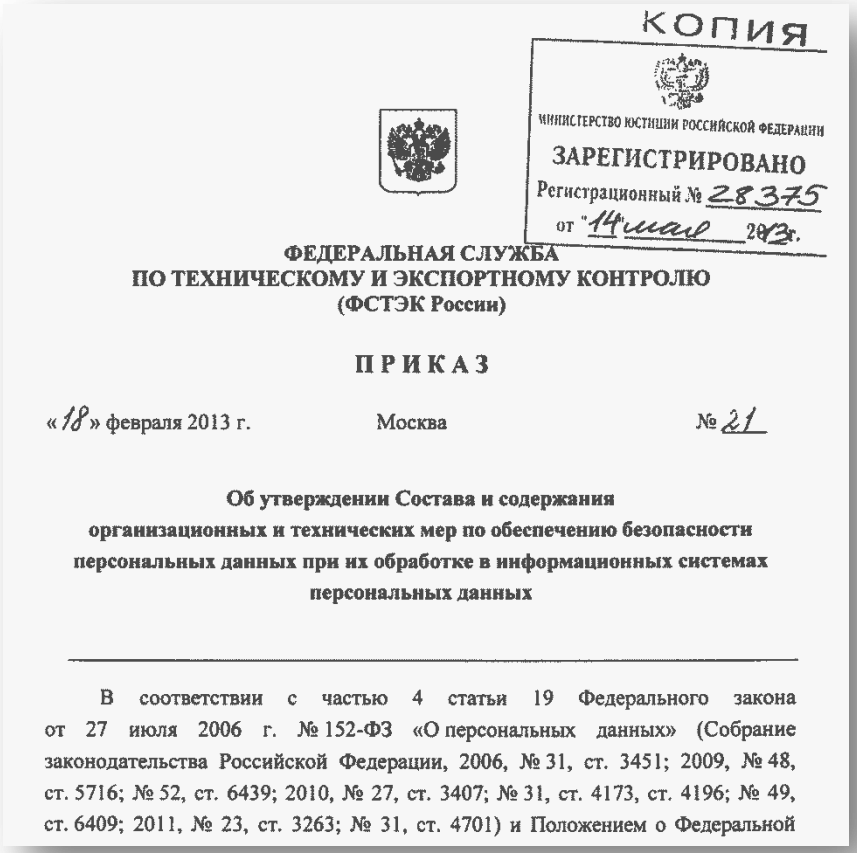
Защита информации в ИСПДн

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработки в ИСПДн»

4 уровня защищенности персональных данных (УЗ1-УЗ4)

Для всех уровней защищенности ИСПДн требуется:

использование средств защиты информации, **прошедших процедуру оценки соответствия** требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.



КОПИЯ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от "14" мая 2013г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной

Меры по защите ИСПДн

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработки в ИСПДн»

- обеспечение доверенной загрузки;
- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- **управление доступом** субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- **регистрацию событий безопасности**;
- обеспечение целостности информационной системы и информации (включая **антивирусную защиту**, **обнаружение вторжений**);
- защиту **среды виртуализации**;
- защиту технических средств;
- защиту информационной системы, ее средств и систем связи и передачи данных (в том числе **защиту периметра , контроль использования мобильного кода** и **защиту от отказа в обслуживании**).

ФСТЭК. Информационное сообщение

ФСТЭК России. «Информационное сообщение по вопросам защиты информации и обеспечения безопасности ПД при их обработке в ИС в связи с изданием приказов [17 и 21]»

1 **Как определить класс защищенности ГосИС, если в ней обрабатываются персональные данные?**

В случае, если уровень защищенности персональных данных выше, чем класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности.

2 **Продолжает ли действовать СТР-К?**

СТР-К применяется в качестве методического документа при реализации мер в целях защиты от утечки по техническим каналам.

Иные положения СТР-К могут применяться в части, не противоречащей Требованиям приказа No 17.

Best Practices: Защита S2S

1. **Защита периметра -** межсетевое экранирование по классу МЭ3 плюс NAT, плюс резервирование
2. **Обнаружение вторжений –** профили защиты системы предотвращения вторжений (класс, не ниже 4-го) и Anti-bot функционал
3. **Антивирусная защита -** профили защиты средств антивирусной защиты (класс, не ниже 4-го) плюс Anti-spam и email security. Отдельная задача - DLP
4. **Контроль использования мобильного кода -** контроль приложений (Web 2.0) плюс URL-фильтрация
5. **Защита среды виртуализации –** защита гипервизора, сети передачи данных, гостевых операционных систем, управления виртуальной инфраструктурой
6. **Защита от отказа в обслуживании -** профили защиты в настоящий момент готовятся

Что делать и как защищать?

Для каждой задачи можно найти отдельное решение[1]

- **Ошибки администрирования**
- **Возможность обхода**
- **Сложное управление**
- **Высокая стоимость**

[1] И даже некоторые из них будут сертифицированы

1 Защита периметра

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработки в ИСПДн»

1. **Управление (фильтрация, маршрутизация,контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами**
2. **Использование отказоустойчивых технических средств**
3. **Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы**
4. **Контроль использования технологий мобильного кода [Web 2.0], технологий передачи речи и видеоинформации [технологии контроля VoIP и др]**
5. **Разбиение информационной системы на сегменты и обеспечение защиты периметров сегментов информационной системы**

2 Обнаружение вторжений, AV

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн ...»,
«Профиль защиты систем обнаружения вторжения уровня сети 4»

1. **Обнаружение вторжений с использованием сигнатур уязвимостей и эксплойтов**
2. **Выявление аномалий сетевого трафика**
3. **Анализ протоколов сетевого уровня [и уровня приложений]**
4. **[Возможность блокировки трафика с учетом географического расположения атакующего]**
5. **Реализация антивирусной защиты [потоковый антивирус]**
6. **Обнаружение и реагирование на поступление в ИС незапрашиваемых электронных сообщений [анти-спам]**
7. **Контроль содержания информации , передаваемой из ИС и исключение неправомерной передачи информации из ИС [DLP-решения]**
8. **Контроль ошибочных действий пользователей по ... Передаче персональных данных и предупреждение пользователей об ошибочных действиях**

Требуемые меры сетевой защиты

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработки в ИСПДн»

Firewall

IPsec VPN и Mobile Access

IPS и Anti-Bot

URL filtering и Application control

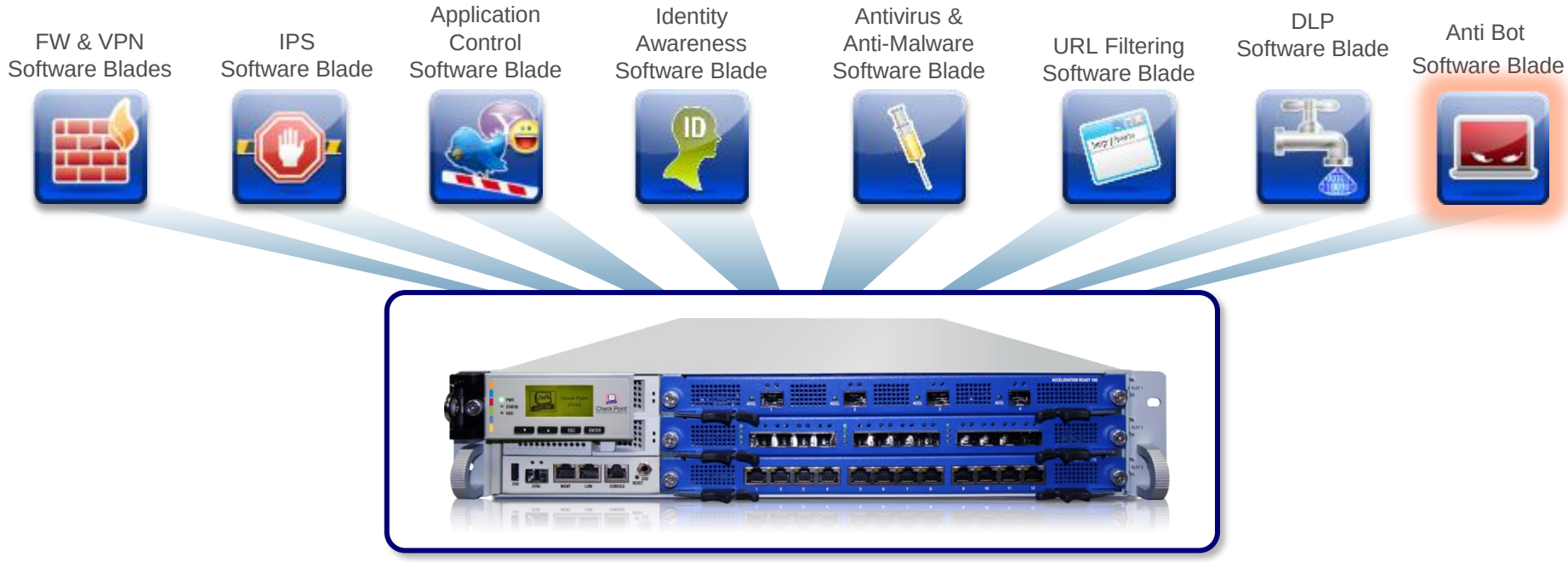
Antivirus & anti-malware и Anti-spam & email security

Data loss prevention

Реализация мер защиты

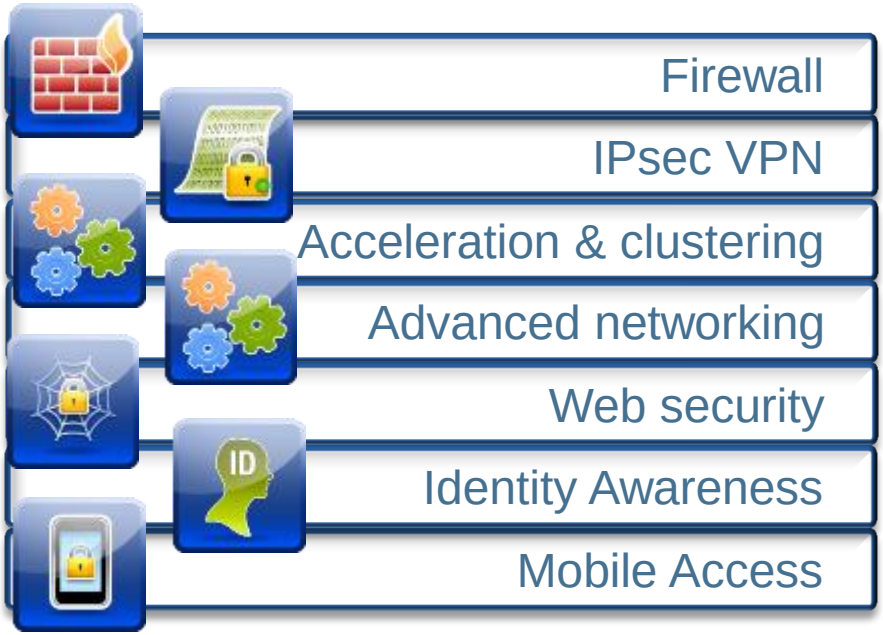
Комплексность

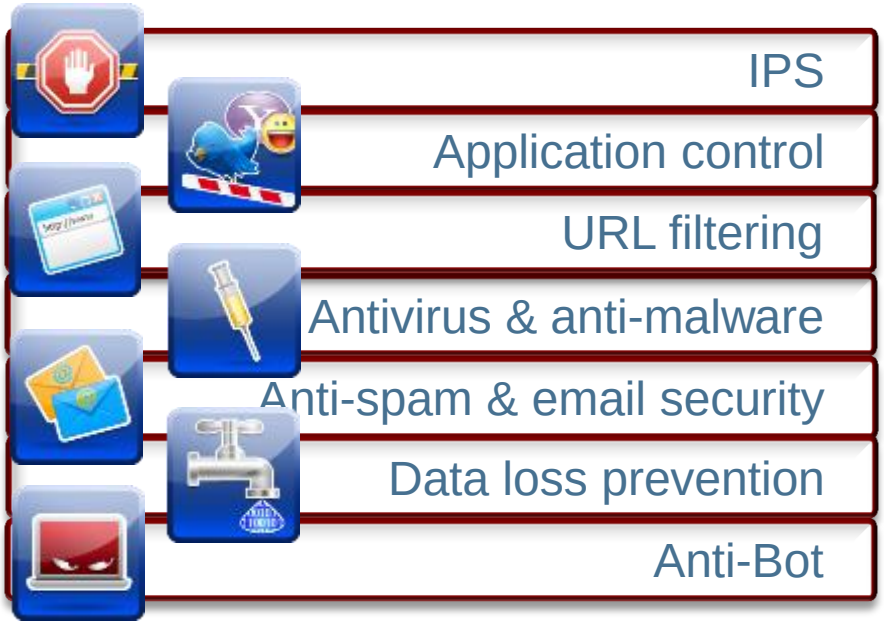
Для обеспечения ИБ требуется согласованное применение всех доступных правовых, организационных и технических мер, перекрывающих в совокупности **все существенные каналы реализации угроз ИБ**. Система ИБ должна строиться с учетом не только известных атак и каналов утечки информации, но и с учетом возможности появления принципиально новых атак и путей реализации угроз безопасности



Системность

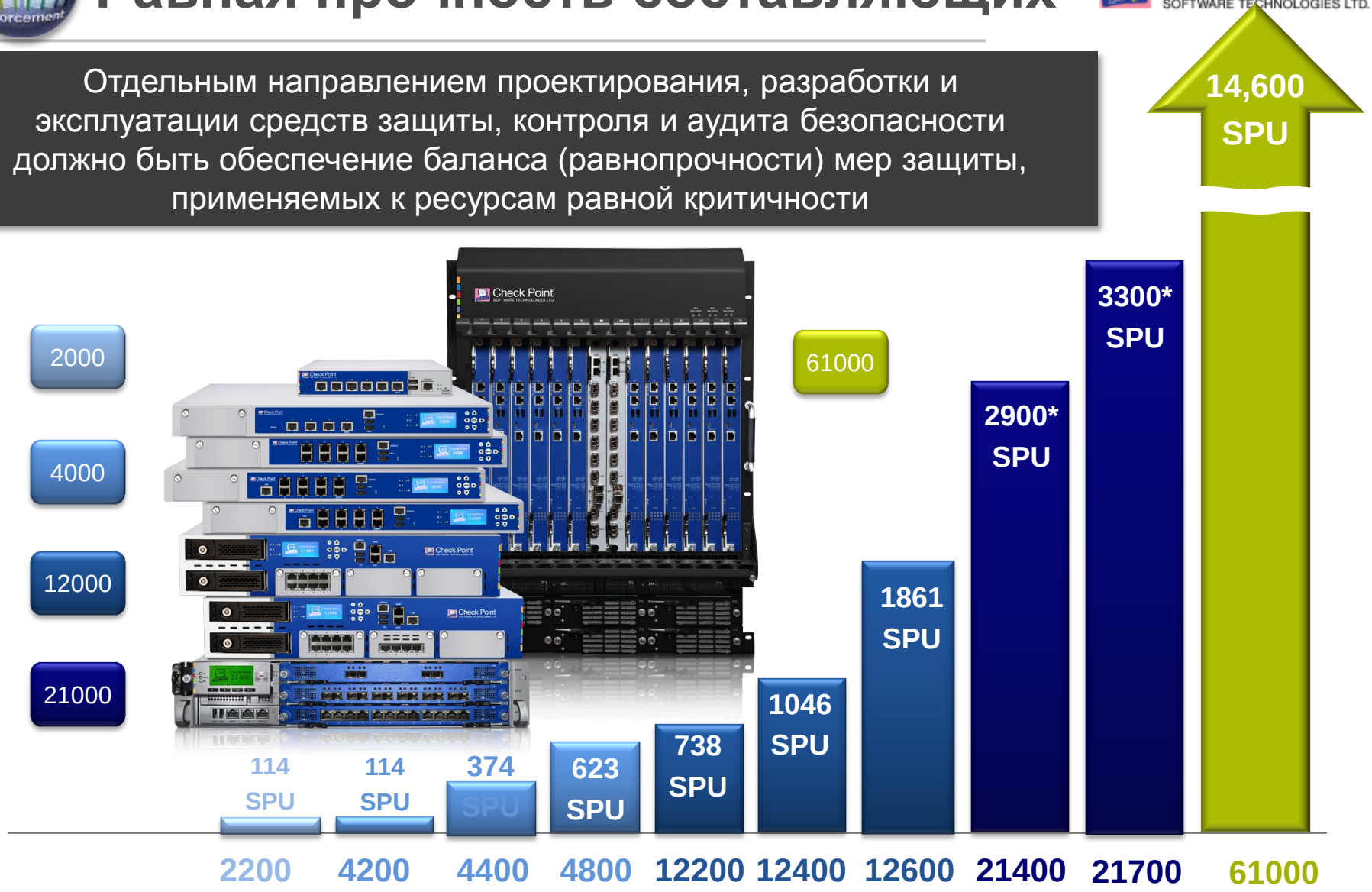
Реализация защиты информации должна быть **научно обоснована и базироваться на системном подходе**, *учитывающем все факторы, оказывающие или могущие оказать влияние на информационную безопасность организации. Также должны учитываться характер, возможные объекты и направления атак, каналы утечек информации и пути проникновения потенциальных нарушителей к информационным ресурсам (модель угроз!).*





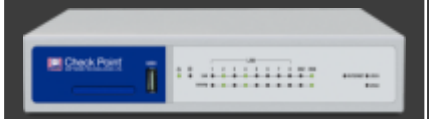
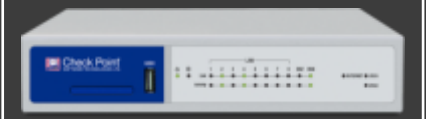
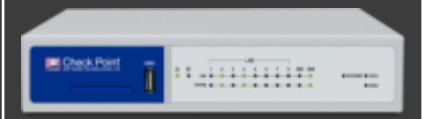
Равная прочность составляющих

Отдельным направлением проектирования, разработки и эксплуатации средств защиты, контроля и аудита безопасности должно быть обеспечение баланса (равнопрочности) мер защиты, применяемых к ресурсам равной критичности



* With Security Acceleration Module

Семейство 1100 Appliances

	 1120 Appliance	 1140 Appliance	 1180 Appliance
Max Firewall Throughput	750 Mbps	1 Gbps	1.5 Gbps
Max VPN Throughput (AES)	140 Mbps	175 Mbps	220 Mbps
Max IPS Throughput (Default/Recommended profile)	360/50 Mbps	500/67 Mbps	720/100 Mbps
Max Antivirus Throughput	50 Mbps	67 Mbps	100 Mbps
Price	Starting at $599	Starting at $899	Starting at $1699

Доступны 4 варианта исполнения

1. Wired
2. Wired + Wireless
3. ADSL
4. ADSL + Wireless

ГОСТ на SG 21700

21700

Datacenter-grade security appliance (3551 SPU/110 Gbps[1]) with high port density, low latency and acceleration options

GOST Performance Tests

	Test Configuration	Test Name	R75.45.VS GOS TXL
64-bit	Set 1 -TCP and UDP With CoreXL	FW GOST VPN Packet Rate (64 bytes), PPS (IKE PSK, Site Key)	660,000
		FW GOST VPN throughput (1452 bytes), Mbps (IKE PSK, Site Key)	**3,814**
		GOST Maximum connections rate - 5 sec. (IKE PSK, Site Key)	45,000
		GOST Max concurrent connections	12,295,319
		IPS Blend, IPS Recommended Mbps	1,687

Параметры встраивания Крипто-Про

	GOST VPN
Алгоритмы шифрования	ESP_GOST-4M-IMIT / ESP_GOST-1K-IMIT (ГОСТ 28147-89 режим гаммирования + ГОСТ 28147-89 режим имитовставки)
Алгоритмы согласования ключей	VKO ГОСТ Р 34.10-2001 (RFC 4357)
Методы аутентификации IKE	GOST-IKE-PSK, GOST-IKE-SIGNATURE
Используемое СКЗИ	КриптоПро CSP 3.6.1
Встраивание СКЗИ	В соответствии с драфтами документов Технического комитета по стандартизации «Криптографическая защита информации» (ТК26) ФАТРМ
Формирование сессионных ключей	Средствами КриптоПро CSP 3.6.1
Поддержка резервирования	Да, режимы HA и LS
Синхронизация параметров туннелей в кластерном VPN-решении	Да, в защищенном (зашифрованном) виде
PFS	Да

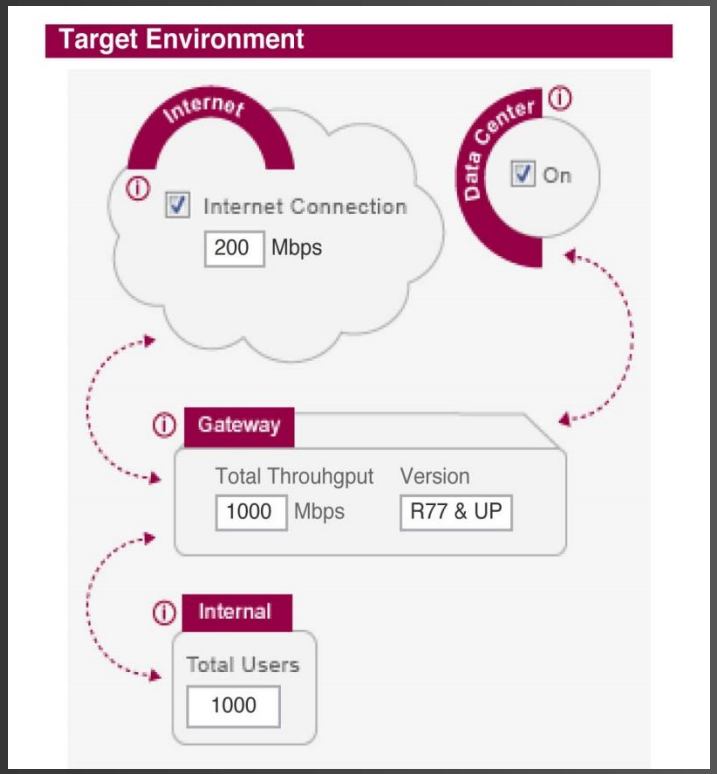
Семейство 21000 Appliances

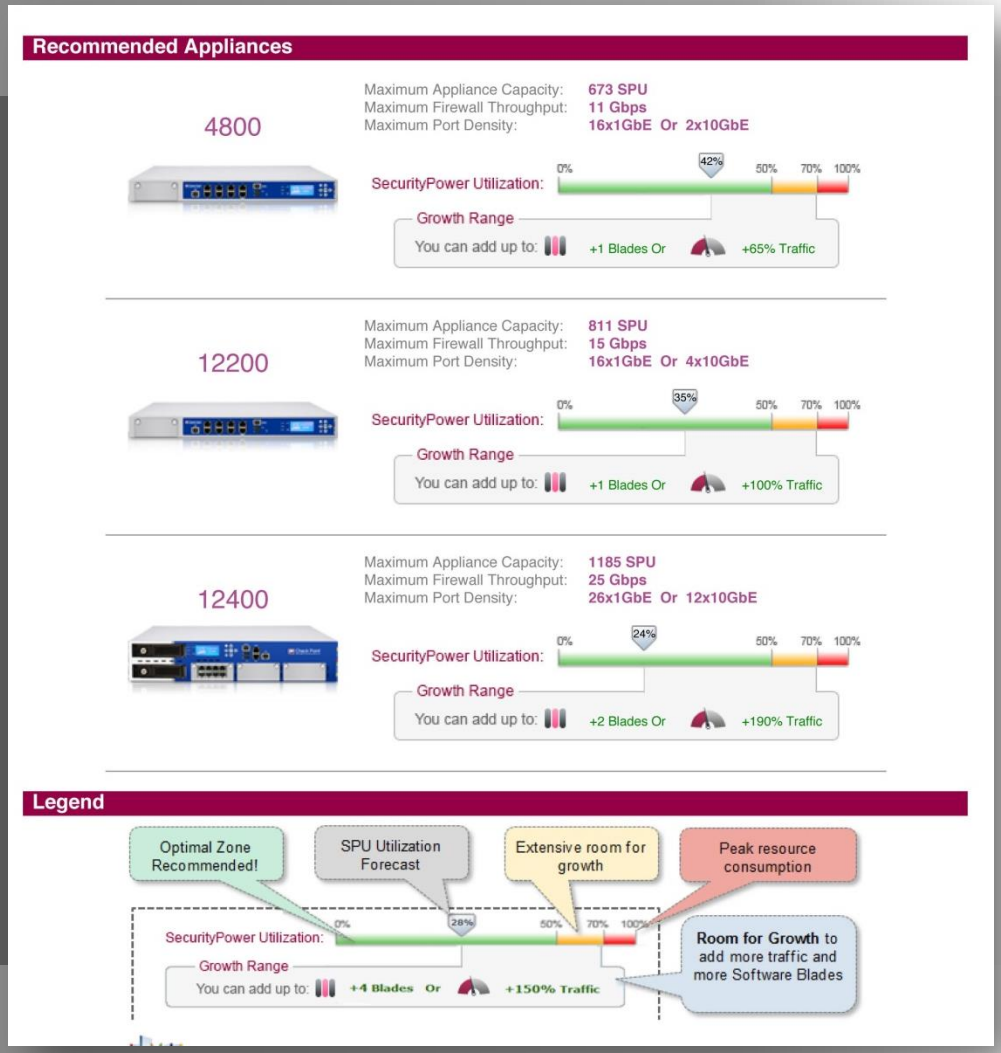
GAiA	 21400 Appliance	 21600 Appliance	 21700 Appliance
Firewall Throughput (Production Performance / 1518 byte UDP)	17/50 Gbps	21/75 Gbps	25/78 Gbps
Max VPN Throughput (AES)	7 Gbps	8.5 Gbps	11 Gbps
Max IPS Throughput (Default/Recommended profile)	/6.0 Gbps	/6.8 Gbps	25.0/8.0 Gbps
Packet Forwarding	7 Mpps	15 Mpps	18 Mpps
Concurrent Connections	10M	13M	13M

21700 Performance Tests (LAB) RFC 3511, 2544, 2647, 1242

- 78 - 110 1 Gbps of firewall throughput, 1518 byte UDP
- 11 - 50 1 Gbps of VPN throughput, AES-128
- 25 Gbps of IPS throughput, IPS Default profile, IMIX traffic blend
- 8 Gbps of IPS throughput, IPS Recommended profile, IMIX traffic blend
- 6/13 3 million concurrent connections, 64 byte response
- 170,000/300,000 connections per second, 64 byte response

Выбор решения



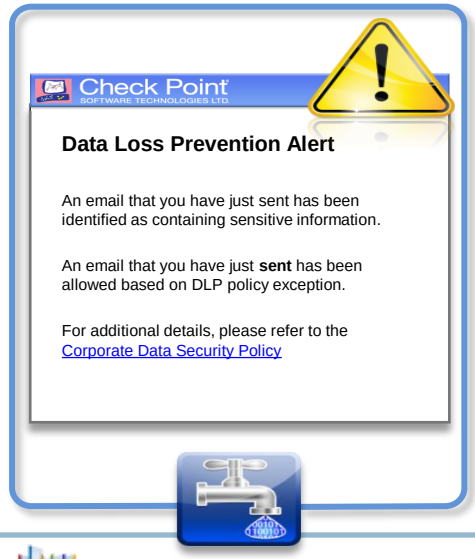


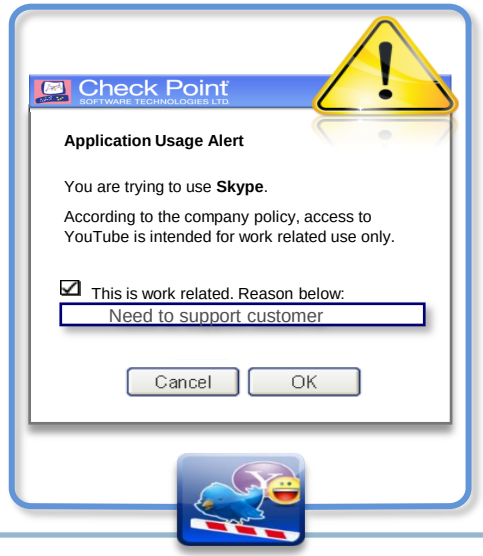
2 Обнаружение вторжений, AV

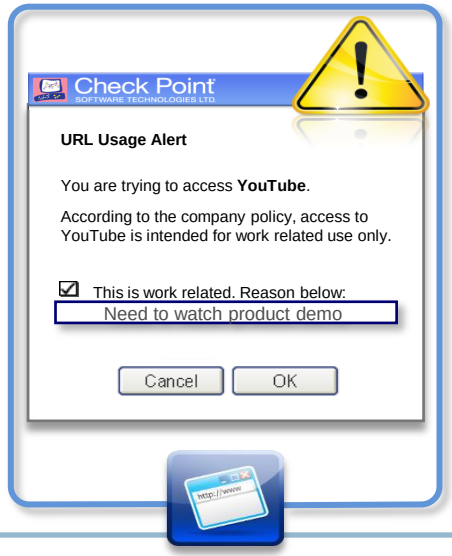
ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн ...»,
«Профиль защиты систем обнаружения вторжения уровня сети 4»

7 **Контроль содержания информации , передаваемой из ИС и исключение неправомерной передачи информации из ИС [DLP-решения]**

8 **Контроль ошибочных действий пользователей по ... Передаче персональных данных и предупреждение пользователей об ошибочных действиях**







Защита виртуальных сред

5 Защита среды виртуализации

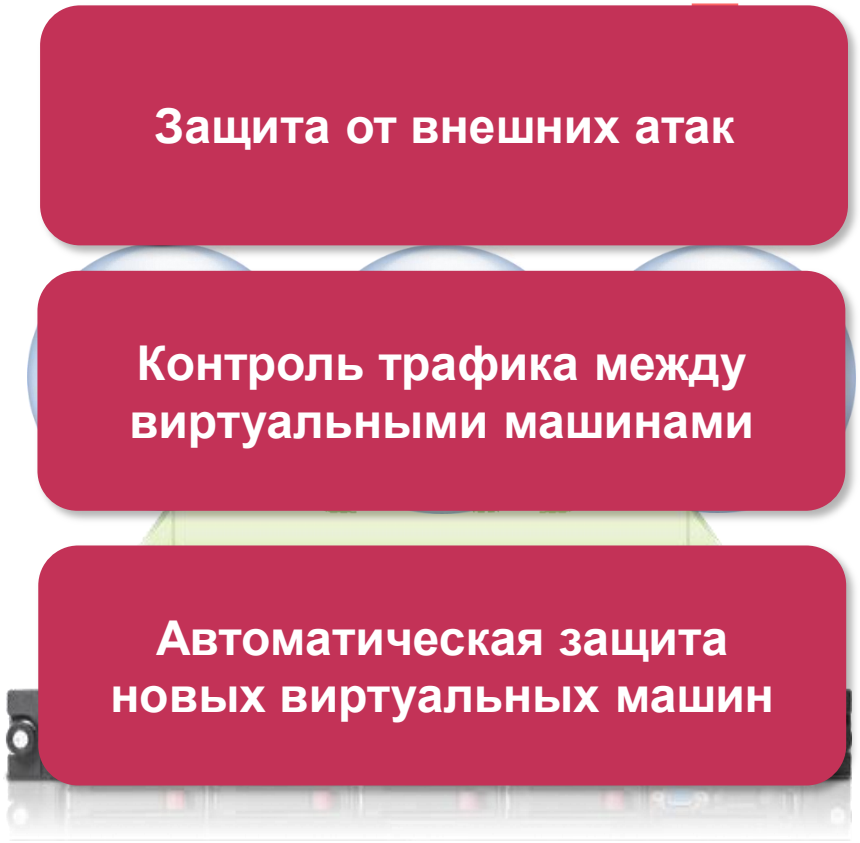
ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработки в ИСПДн»

21.8. Меры по защите среды виртуализации должны исключать несанкционированный доступ к объектам защиты виртуальной инфраструктуры ...,

в том числе к средствам **управления** виртуальной инфраструктурой,

гипервизору, системе хранения, сети передачи данных,

гостевым операционным системам, виртуальным машинам (контейнерам), ...



Управление безопасностью

Управление Политикой Безопасности

Для чего использовать унифицированные средства управления ?

Единая по

Корреляци ТВ

Оперативн
в сложных

Простое м

Оперативное обновление ПО, баз данных и конфигурации устройств

Управление Политикой Безопасности

Для чего использовать унифицированные средства управления ?

- Единая политика управления доступом
- Корреляция событий безопасности с различных устройств
- Оперативное реагирование на распределённые атаки в сложных средах
- Простое масштабирование средств безопасности
- Оперативное обновление ПО, баз данных и конфигурации устройств

7 Управление безопасностью

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн ...», «Профиль защиты систем обнаружения вторжения уровня сети 4»

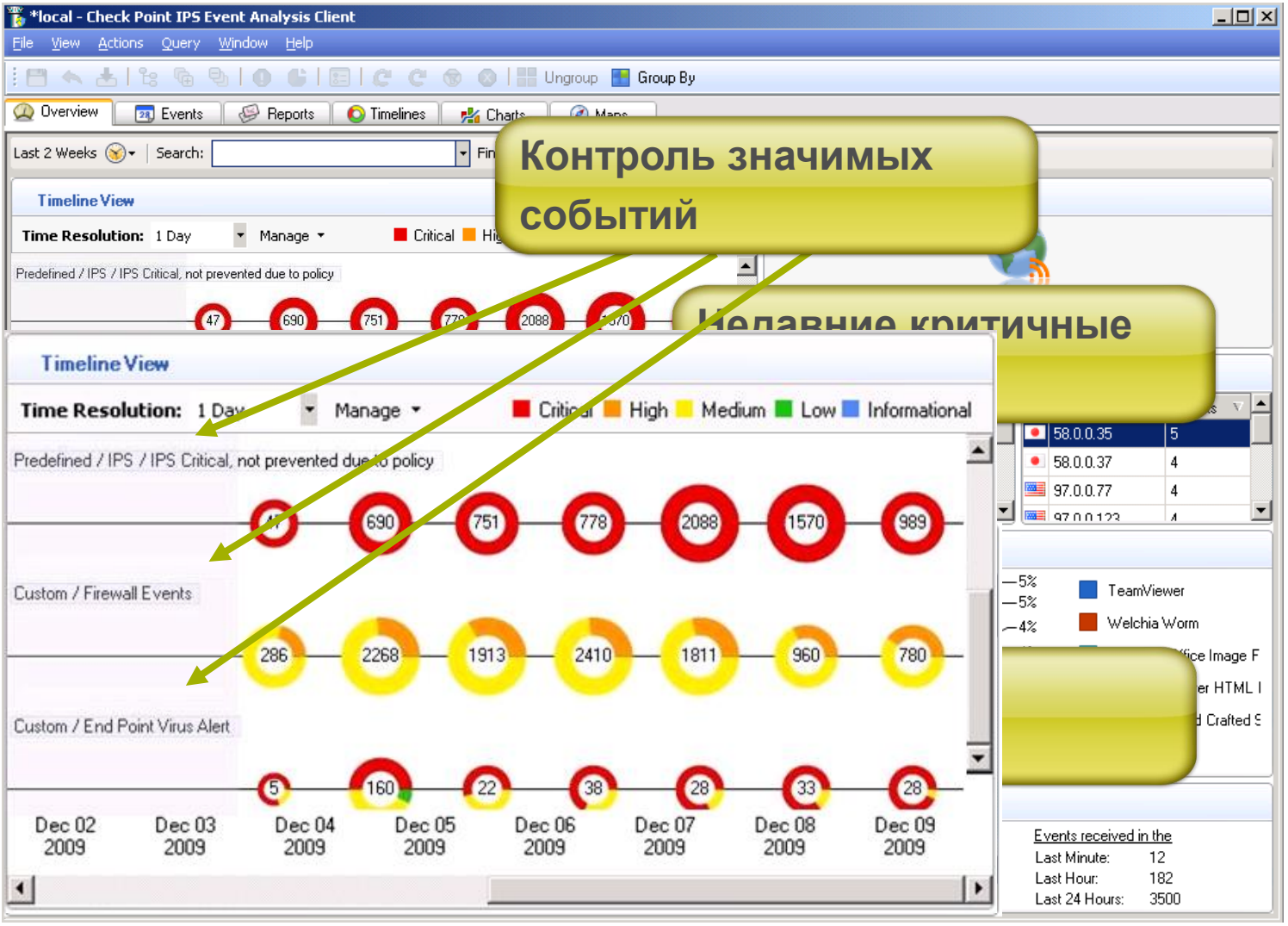
1. **Разделение в информационной системе функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС**
2. **Разделение полномочий и назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС**
3. **Определение событий безопасности, подлежащих регистрации**
4. **Определение состава и содержания информации о событиях безопасности**
5. **Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них**
6. **Обнаружение, идентификация и регистрация инцидентов**
7. **Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них ...**

Централизация и глобальность

Организационные и технические меры ИБ должны подлежать централизации. **Централизация управления** *должна обеспечивать максимальную информированность администраторов ИБ, обоснованность, оперативность и минимальные затраты на координацию решений.*

- Единое централизованное управление политиками безопасности
- Создание и контроль доменов политики из единой консоли
- Централизованный мониторинг и аудит
- Централизованная отчетность о состоянии безопасности сети
- Централизованный провижионинг
- Отдельная политика безопасности для каждого заказчика (домена) и глобальная политика для всех

В центре внимания – системно-значимые события!

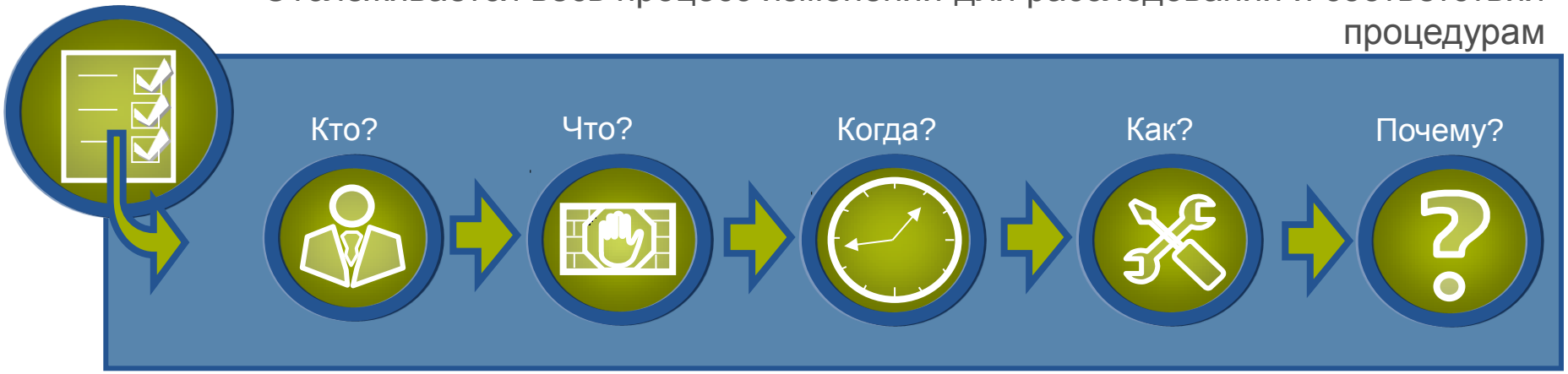


7 Управление безопасностью

ФСТЭК России. «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн ...», «Профиль защиты систем обнаружения вторжения уровня сети 4»

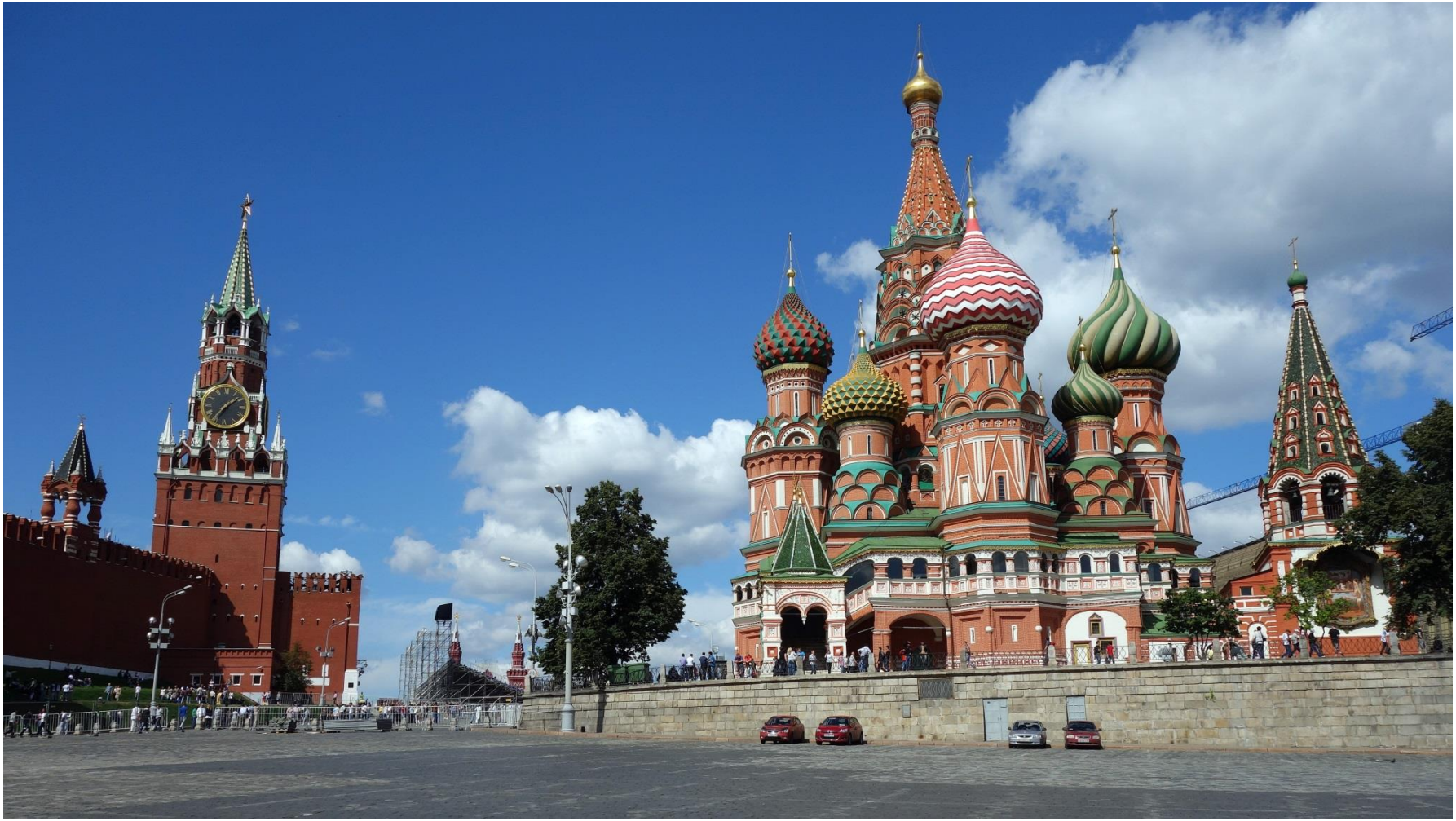
1. **Разделение в информационной системе функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС**
2. **Разделение полномочий и назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС**

Отслеживается весь процесс изменений для расследований и соответствия процедурам



Изготовлено в Израиле

Локализовано для России

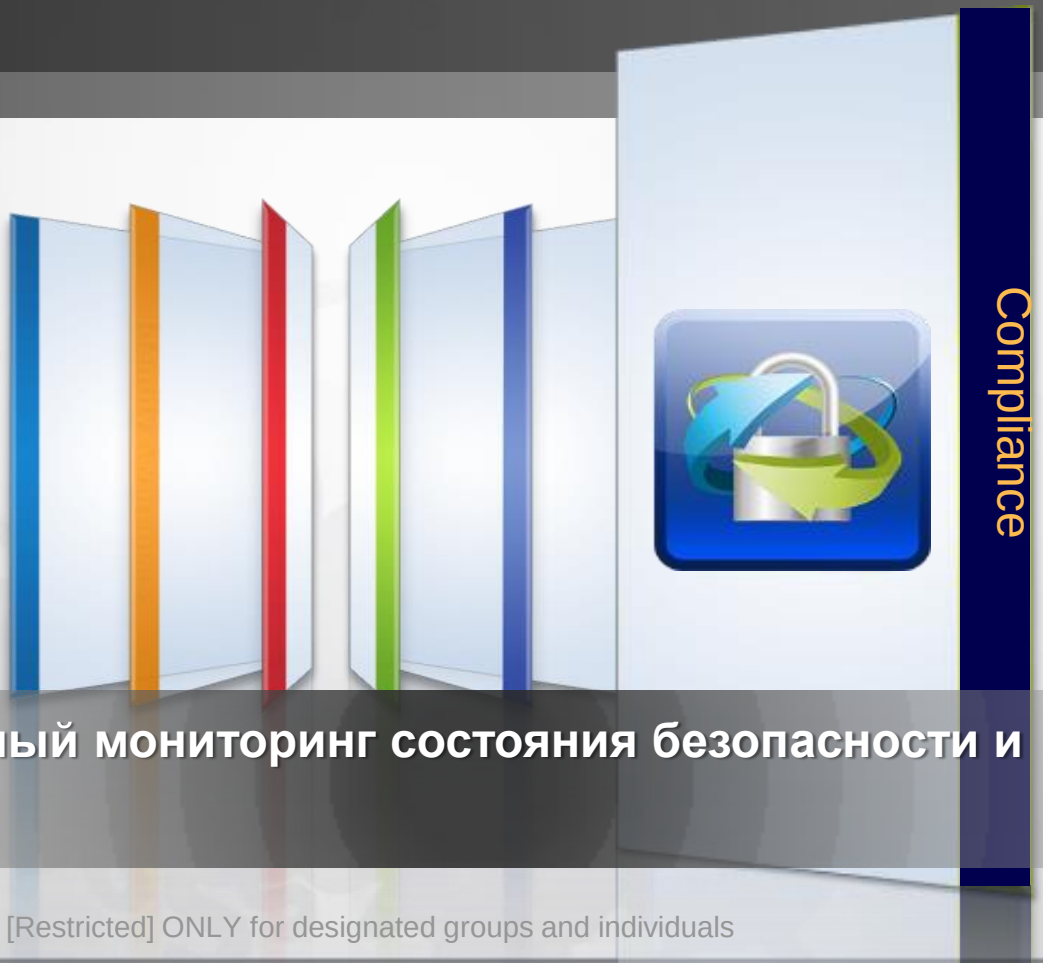


Производство и сертификация

Compliance Software Blade

Check Point представляет

Compliance Software Blade



Автоматизированный мониторинг состояния безопасности и compliance

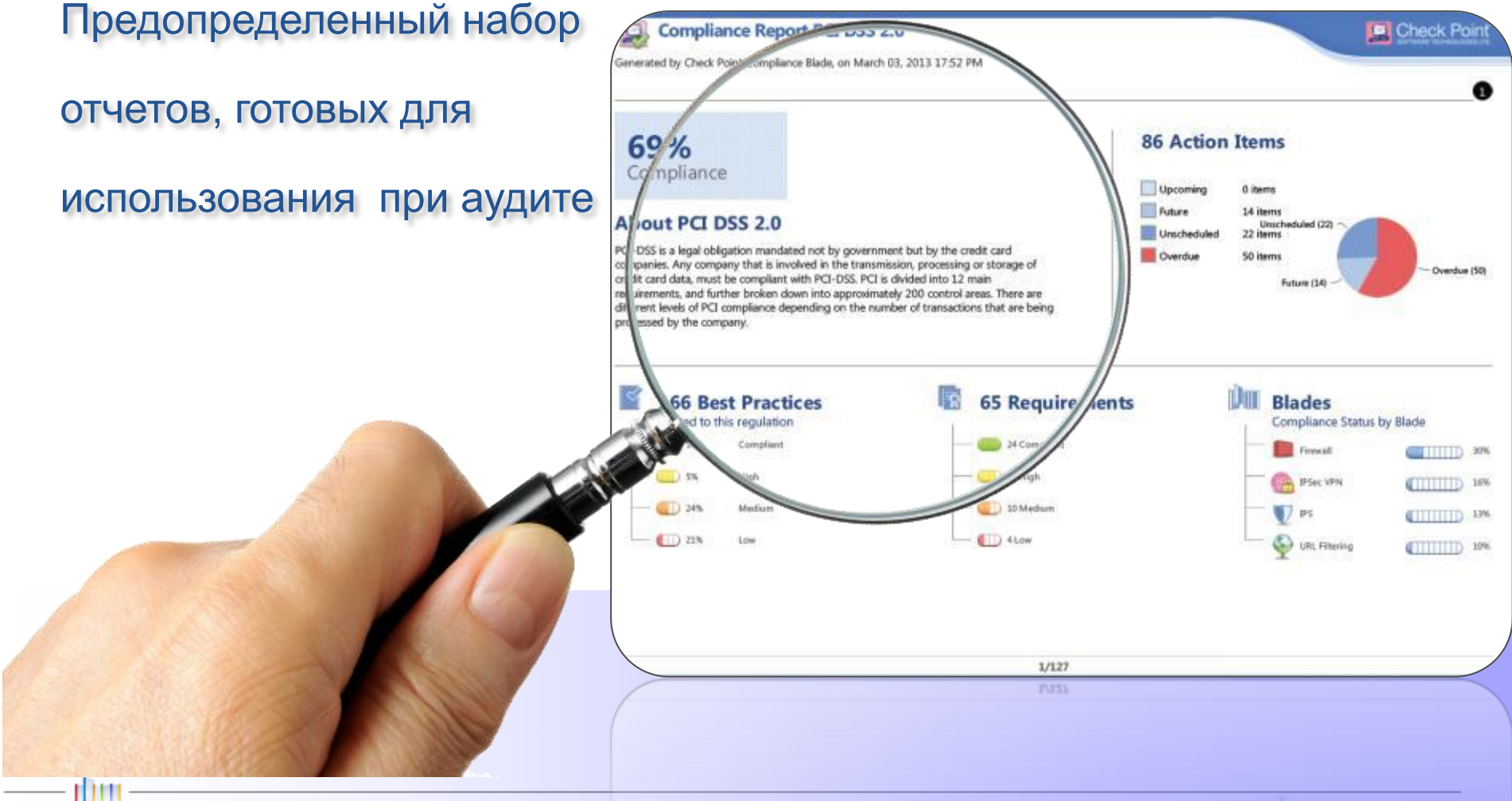
Библиотека лучших практик по безопасности

250 Лучших практик по безопасности

360° Visibility соответствия требованиям

Compliance Reports

Предопределенный набор отчетов, готовых для использования при аудите

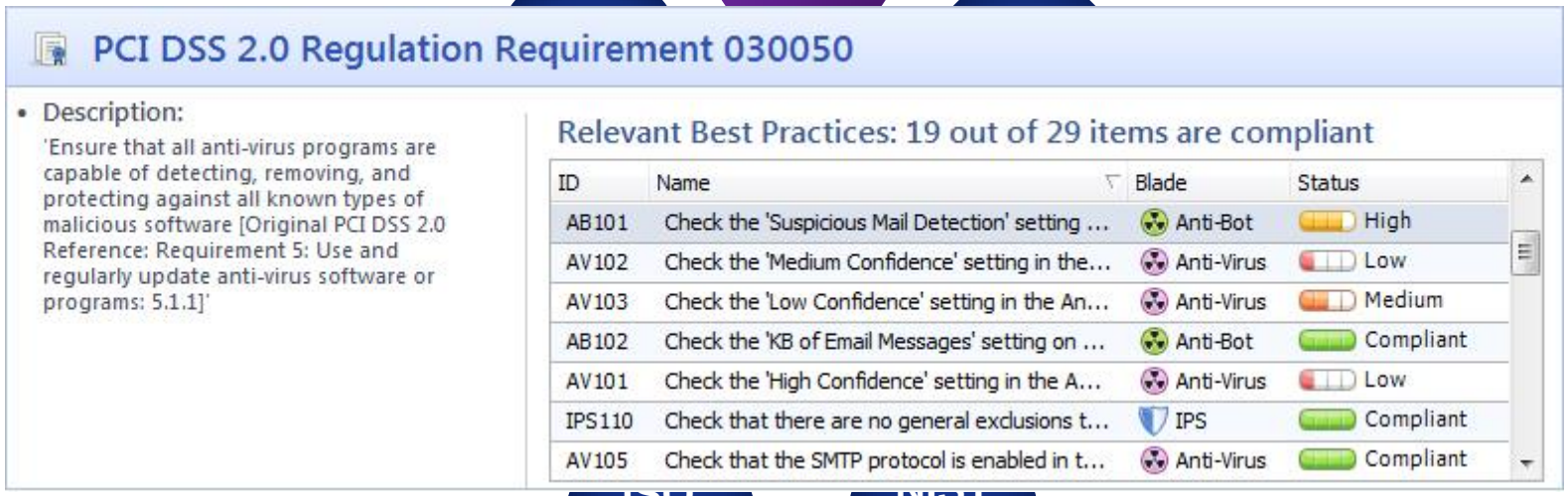


From Regulatory Requirements to Best Practices

PCI-DSS

ISO 27002

NIST 800-41



Translated Into

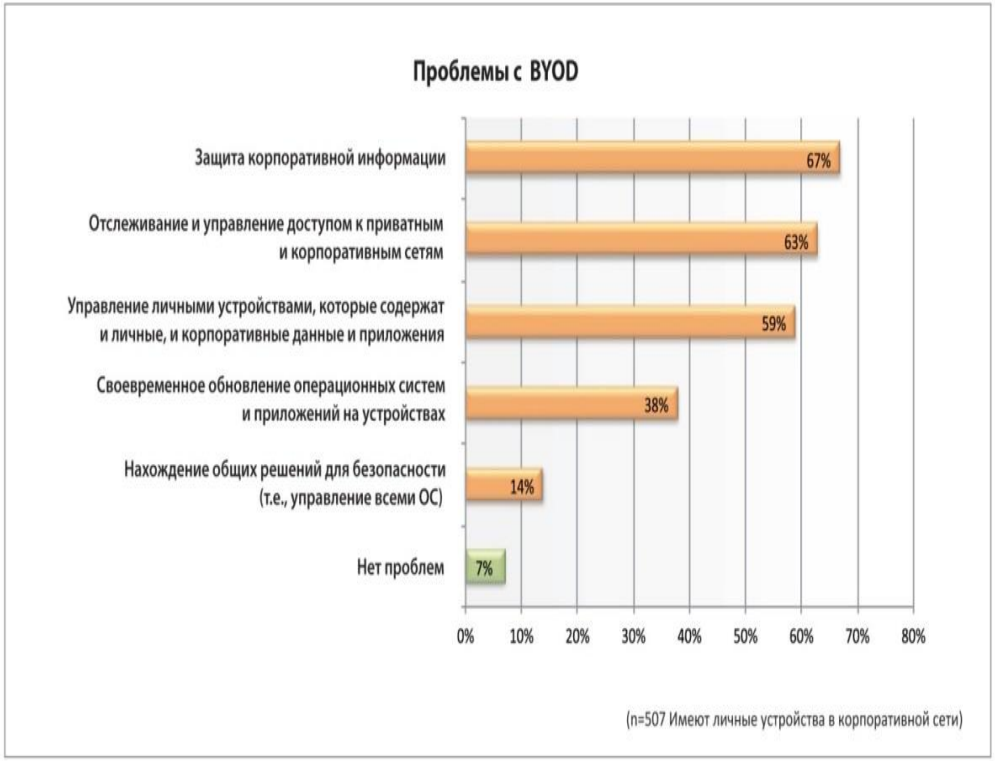
Actionable Security Best Practices

Защита мобильных устройств

Влияние мобильных устройств на информационную безопасность: опрос IT-профессионалов

1. **BYOD быстро растёт и затрагивает предприятия любых масштабов**
2. **Корпоративная информация на мобильном устройстве – более ценное имущество, чем само мобильное устройство**
3. **Инциденты мобильной безопасности обходятся дорого, даже малому и среднему бизнесу.**

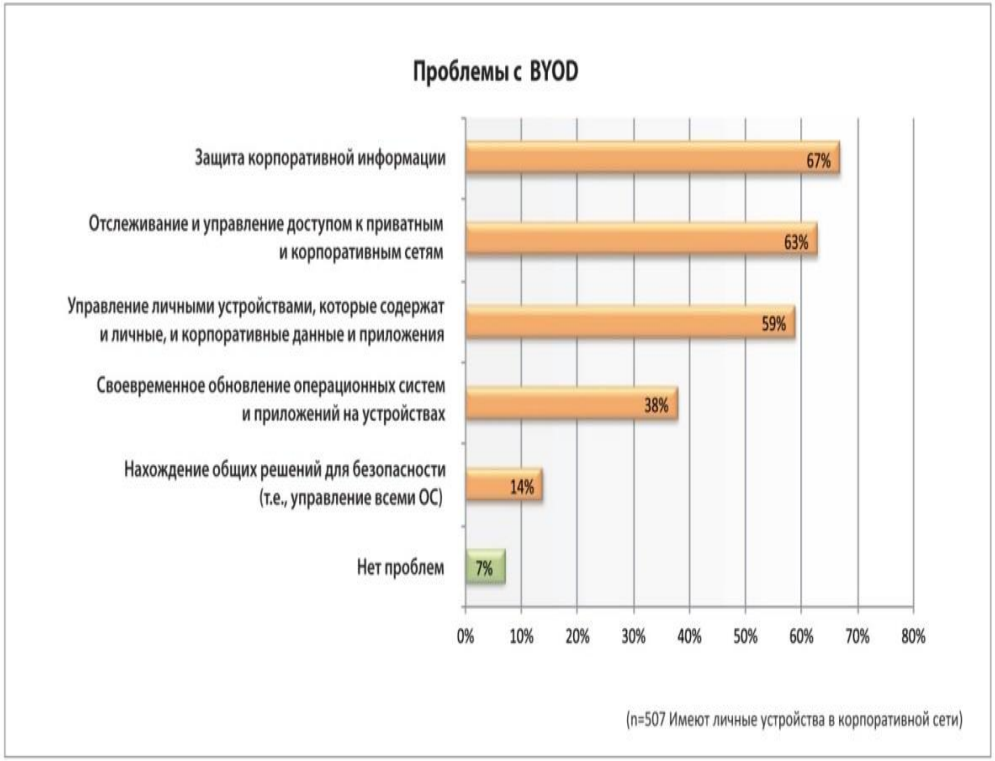
Данный доклад, выполненный при поддержке Check Point, основан на глобальном опросе 790 IT-профессионалов, проведённом в США, Канаде, Великобритании, Германии и Японии.



Безопасность мобильных устройств

Влияние мобильных устройств на информационную безопасность: опрос IT-профессионалов

1. **63% не управляют корпоративной информацией на личных устройствах**
2. **93% сталкиваются с проблемами, внедряя политики касательно BYOD**
3. **Защита корпоративной безопасности упоминается как главная проблема BYOD (67%)**



Данный доклад, выполненный при поддержке Check Point, основан на глобальном опросе 790 IT-профессионалов, проведённом в США, Канаде, Великобритании, Германии и Японии.

Mobile
VPN

Check Point Mobile VPN

client for iOS

Полнофункциональный VPN

Check Point™
SOFTWARE TECHNOLOGIES LTD.

Check Point Mobile VPN

Check Point SOFTWARE TECHNOLOGIES LTD.

Обеспечивает простой и защищенный доступ
с любого бизнес-приложения на вашем iOS

- **Полнофункциональный VPN клиент**
- **Поддержка Office Mode**
- **Работа в фоновом режиме**
- **VPN по запросу**
- **Поддержка сертификатов**

Check Point mobile®

Secure Business Mail

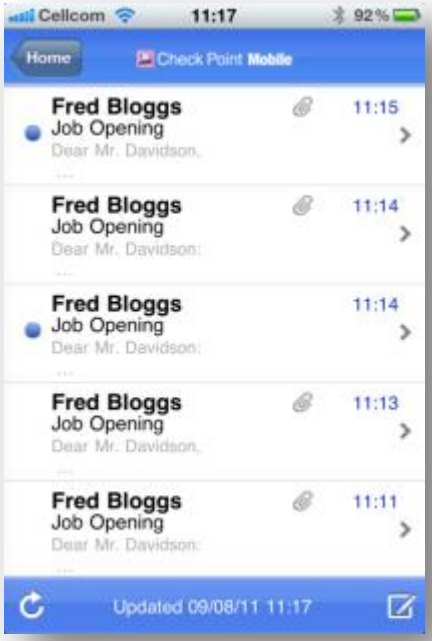
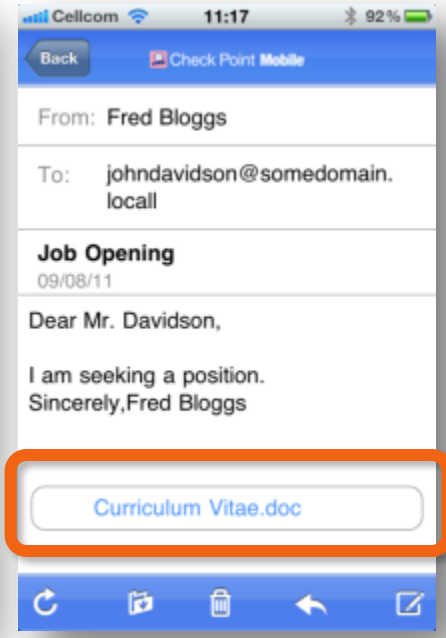
Sandbox Protection

Bring Your Own Device

Check Point™
SOFTWARE TECHNOLOGIES LTD.

Corporate Mail Security

Check Point SOFTWARE TECHNOLOGIES LTD.

Pin Code	Secure Access	Mail	Sandbox
			
Защищенный доступ по pin-коду	Защищенный доступ к Web порталу, почте и календарю	Native и простой почтовый клиент	Все присланные документы открываются в «песочнице»

Планы и перспективы