



Check Point®
SOFTWARE TECHNOLOGIES LTD.

РЕШЕНИЯ CHECK POINT ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

Дмитрий Кудра | Консультант по безопасности



Индустриальный сектор



Check Point
SOFTWARE TECHNOLOGIES LTD.

ИНДУСТРИАЛЬНЫЙ СЕКТОР

Энергетика



- Энергетика
- Водоснаб.
- Газ
- НПЗ
- Химия

Транспорт



- Управление
- Диспетчерские
- Порты
- Морской транспорт

Производство



- Производство
- Переработка
- Сборка

Оборона



- ВПК

Индустриальные системы под угрозой!

Критичные и индустриальные системы формируют наш современный мир

Как и любые другие IT-системы, они подвержены атакам

Последствия таких атак значительно серьезнее:

Сбои электроэнергии

Наводнения и загрязнения воды

Сбои в транспортных системах

Неисправности производственных процессов

АСУ ТП Факты и реальность



Check Point
SOFTWARE TECHNOLOGIES LTD.

Декабрь 2014

Металлургический завод в Германии был атакован (атака Spear Phishing) – были причинены серьезные повреждения

Декабрь 2015

В Украине зафиксирована первая в истории государства успешная хакерская атака на сеть АСУ ТП. Цель хакеров - «Прикарпатьеоблэнерго». Результат - Блэкаут на территории западной Украине (атака BlackEnergy malware)

И повторная атака 19 января 2016

2015год

Американский центр реагирования на инциденты ICS-CERT, специализирующийся на угрозах для промышленных систем, за 2015 год получил от владельцев АСУ ТП и отраслевых партнеров сведения о **295 инцидентах** нарушения безопасности

Декабрь 2014: Металлургический завод в Германии



Check Point
SOFTWARE TECHNOLOGIES LTD.

Целевая
фишинговая
атака

Вредоносный
код на
множестве
систем

Потеря
контроля над
доменной
печью

Масштабное
разрушение
комбината

https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[Confidential] For designated groups and individuals

Декабрь 2015: Энергетическая компания Украины «Прикарпатьеоблэнерго»



Check Point
SOFTWARE TECHNOLOGIES LTD.

Таргетированная
фишинговая
email атака.
Использование
макросов,
встроенных
в файлы Office

Вредоносное ПО
скомпрометировало
3 региональных
центра управления

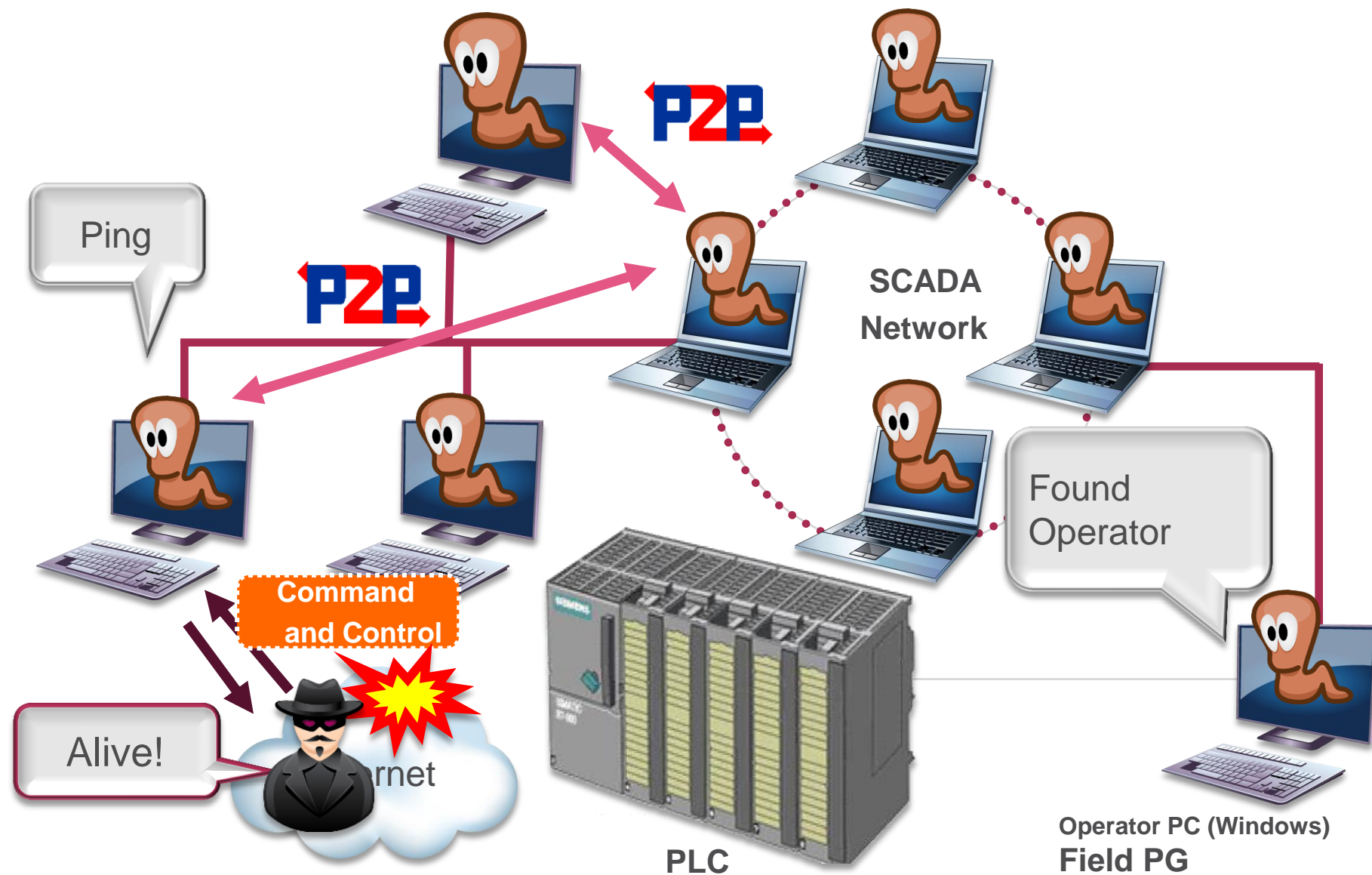
Привело к
деструктивным
последствиям на
подстанциях

В результате
отключения
электроэнергии
сотни тысяч
домов остались
без
электричества

Заражение и контроль



Check Point
SOFTWARE TECHNOLOGIES LTD.



Расположение PLC (Цель)



Check Point
SOFTWARE TECHNOLOGIES LTD.

Водопровод



Трубопровод



Станция очистки воды



PLC

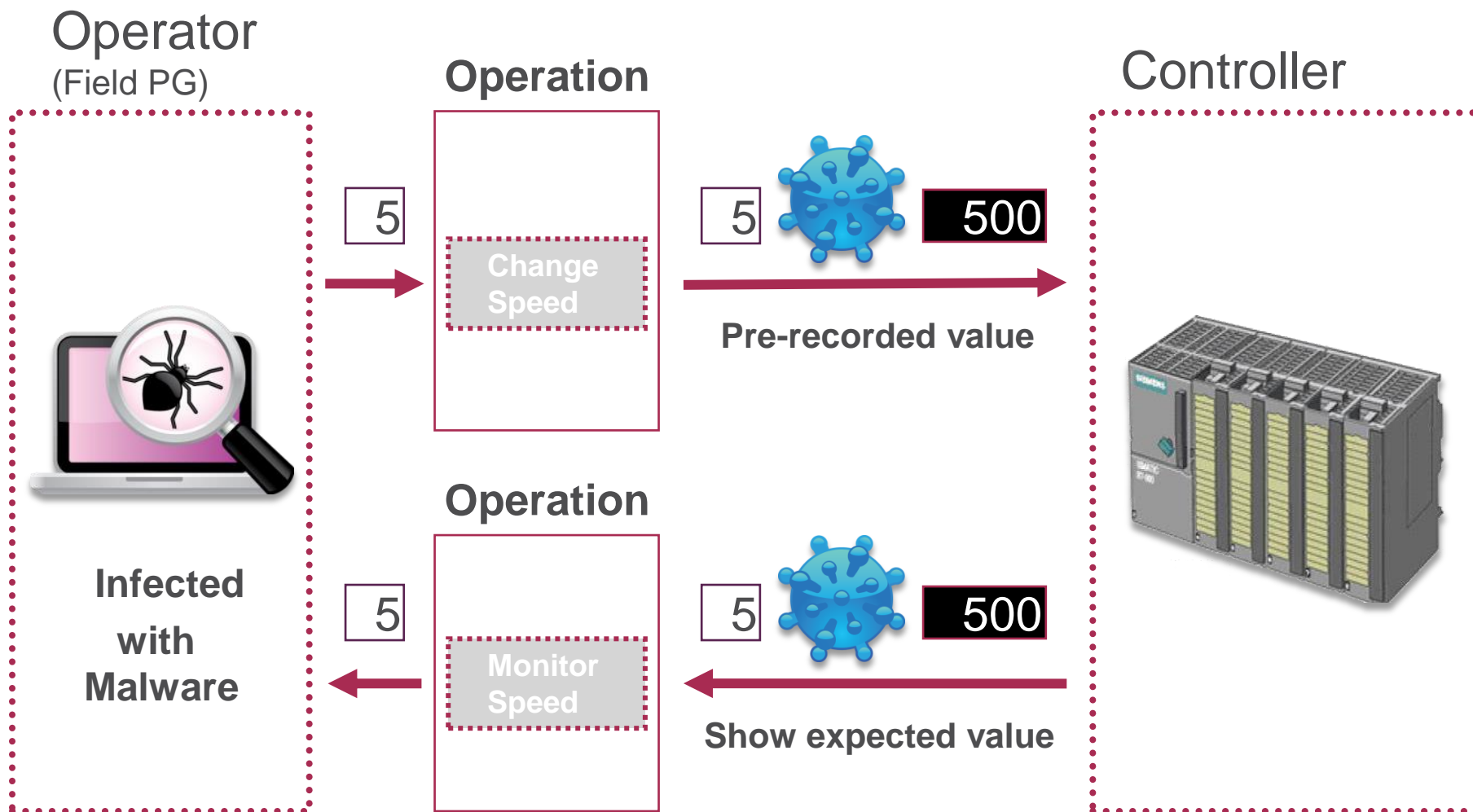


Operator PC (Windows)
Field PG

Internal
Network

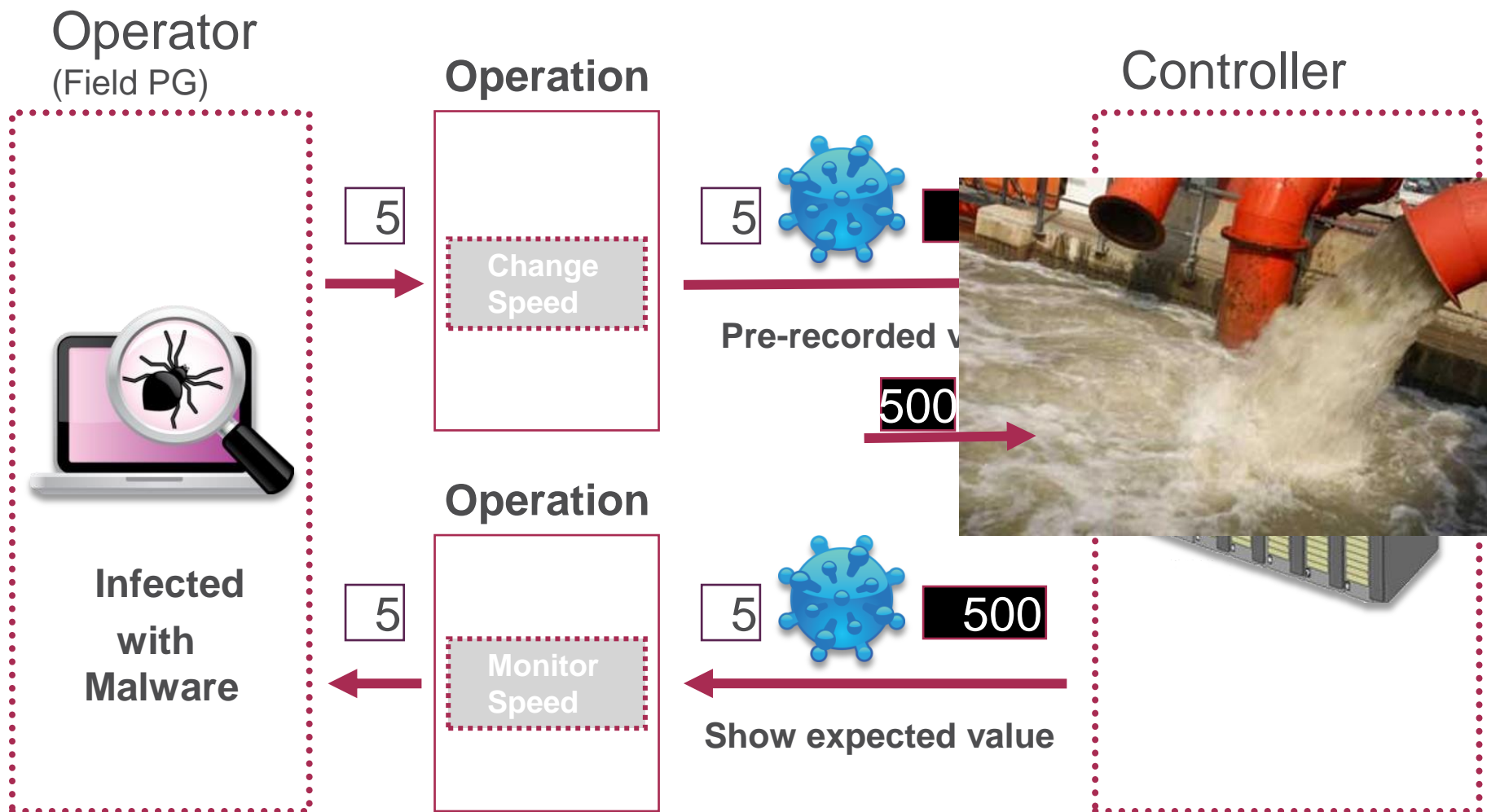


Компрометация PLC Пример (READ/WRITE)





Компрометация PLC Пример (READ/WRITE)



Почему эти атаки возможны?

Устаревшие и необновленные системы

Ошибки в сегментации, подключение технологических сетей к Интернету

Задержки в обслуживании критических систем препятствуют адекватной защите



Требуется специализация на промышленных процессах

УСЛОВИЯ ОКРУЖЕНИЯ

Специализированные протоколы АСУ ТП между машинами операторов и контроллерами

Специализированные системы в условиях непрерывности производства и агрессивной среды

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

Детализация АСУ ТП трафика до уровня команд

Надежная платформа для обеспечения безопасности в тяжелых условиях

Представляем:



Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Решения безопасности для АСУ ТП

CYBER DEFENSE

Специализир
ованная
защита от
SCADA угроз

Обзор и
детальный
контроль SCADA
трафика

Надежные
устройства для
агрессивной
среды

SCADA

Обширная поддержка SCADA/ICS-специализированных протоколов

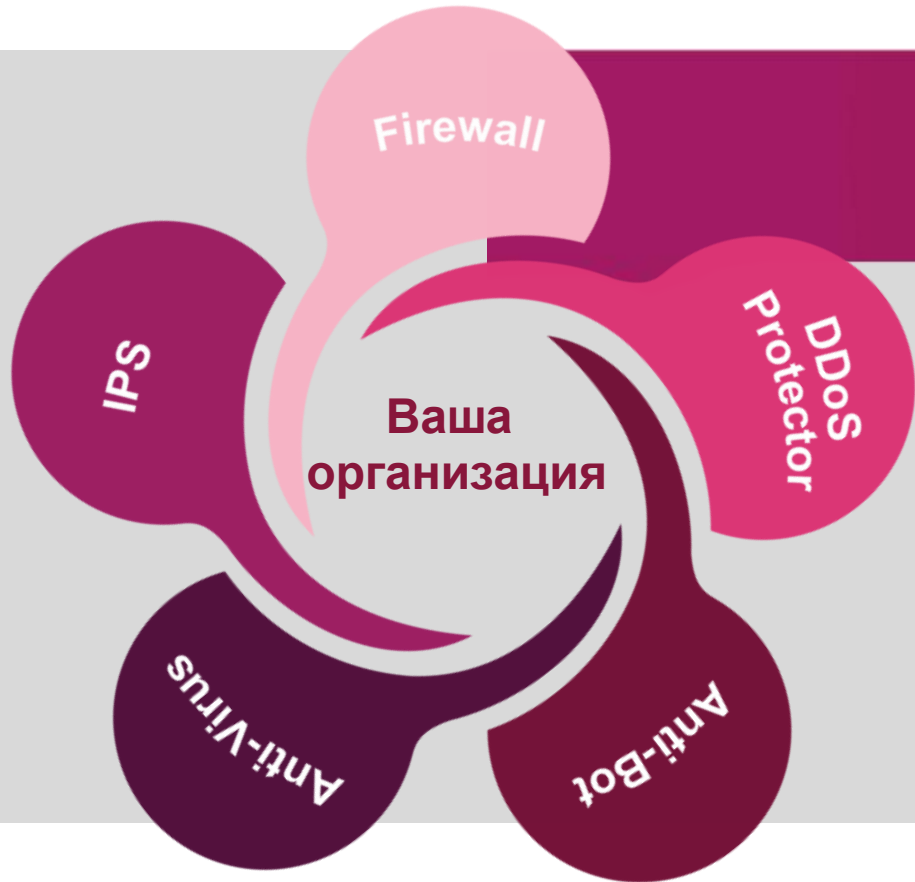


Check Point
SOFTWARE TECHNOLOGIES LTD.



Свыше **720 АСУ ТП** команд
в Check Point Application Control

Комплексная защита от угроз



IPS

Блокирует запусков
эксплойтов и
известных
уязвимостей

NSS Labs
Highest Rating



Защита от SCADA эксплойтов в IPS



Check Point
SOFTWARE TECHNOLOGIES LTD.

Специализированный
набор сигнатур IPS для
SCADA

Используется
занимающий лидирующие
позиции IPS Software
Blade

Решение удовлетворяет
как специфичным для
SCADA, так и обычным,
корпоративным
требованиям к IPS

Встроенная система
анализа и корреляции
событий, поддержка
захвата пакетов

Protection	Severity	Confide...	Perfor...	Release D...	Products	Support
DNP3 abort file function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 assign class function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 server auth challenge response function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 auth error function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 auth file function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 auth reply function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 auth request function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 broadcast	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 close file function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 cold restart function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 confirm function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 delay measure function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 delete file function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 direct operate function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 direct operate no ack function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 disable solution function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 enable solution function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze clear function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze clear no ack function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze no ack function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze time function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 freeze time no ack function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 get file info function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 init app function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 init data function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 Non-Compliant requests	High	Medium...	Medium	5/30/2012	IPS Blade	R75
Non-DNP3 Traffic over DNP3 Port	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 open file function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 operate function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 read function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 record current time function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75
DNP3 save configuration function code	High	Medium...	Medium	5/30/2012	IPS Blade	R75

Устаревшие системы не обновлены



Check Point
SOFTWARE TECHNOLOGIES LTD.

Siemens

Siemens Global

Home > Innovation

ProductCERT Security Alerts

Siemens ProductCERT Security Alerts related to Siemens

2014

- > SSA-831997 (Last Updated: 2014-02-19) ROS-based Devices
- > SSA-654382 (Last Updated: 2013-11-08) ROS-based Devices
- > SSA-724606 (Last Updated: 2013-11-08) S7-1200 PLCs
- > SSA-456423 (Last Updated: 2013-10-17) ROS-based Devices
- > SSA-892342 (Last Updated: 2013-10-17) ROS-based Devices
- > SSA-342587 (Last Updated: 2012-04-30) Architecture

Schneider Electric

Solutions

Support

You are here: Home > Support > Cybersecurity

Operations around the world

- Local operations

Customer Care Centre

- We care!
- Contact

Cybersecurity

- News
- Report an incident

Substitution tool

Counterfeiting

- Counterfeiting
- Definitions
- Report a counterfeit

CAREERS | INVESTORS | ABOUT | CONVERSATIONS

Power and productivity for a better world™ **ABB**

Cyber Security – Alerts & Notifications

ABB is committed to provide customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping our customers minimize risks associated with cyber security.

Recent publications

- 2014-02-19: CMT 1000 Vulnerability bug fix
- 2013-11-08: Remote code execution vulnerability in CAP 501 / CAP 505 / SMS 510
- 2013-11-08: Remote code execution vulnerabilities in MicroSCADA
- 2013-10-17: Advisory for Test Signal Viewer on Windows for Robotics
- 2013-06-18: Security Bulletin for DataManager
- 2012-04-30: Advisory for AC500 web server
- 2012-03-23: Advisory for WebWare Components and Related Product
- 2012-02-28: Buffer Overflow in Robot Communications Runtime on Windows

Date	Product	Vulnerability	Severity
24/01/2014	SCADA Expert Vijeo Citect Vijeo Citect CitectSCADA PowerSCADA Expert PowerLogic SCADA	Unhandled Exception	SEVD 2014-024-02
24/01/2014	SCADA Expert ClearSCADA	File Parsing	SEVD 2014-024-01
15/01/2014	Floating License Manager	Unquoted Service Path	SEVD 2014-015-01

Виртуальный патчинг с около 200 специализированными IDS/IPS сигнатурами



Check Point
SOFTWARE TECHNOLOGIES LTD.

Защищено
Check Point
IPS

Protection	Sever...
Citect SCADA ODBC Overflow Attempt	Medium
Rockwell RSLogix Denial of Service Vulnerability	Critical
SCADA Engine OPC Client Buffer Overflow Vulnerability	High
Schneider Electric UnitelWay Windows Device Driver Buffer Overflow	Critical
Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability	Critical
Siemens Automation License Manager Multiple Vulnerabilities	Critical
ScadaTEC SCADAPhone and ModbusTagServer Buffer Overflow	High
RealWin HMI Service Buffer Overflow 2	High
Automated Solutions Modbus/TCP Master OPC server Modbus TCP Header	High
RealWin INFOTAG/SET_CONTROL Packet Processing Buffer Overflow	High
Unauthorized Miscellaneous Request to a PLC	Critical
Broadcast Request from an Authorized Client	Critical
IGSS SCADARMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Uninitialized Memory Trigger	High
Rockwell RNA Message Negative Header Length	Critical
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High

Политики/Правила на основе Функций и Значений в SCADA командах



Check Point
SOFTWARE TECHNOLOGIES LTD.

- Специализированные Политики и Правила для защиты АСУ ТП
- Правила для АСУ ТП протоколов с учетом направления коммуникации
- Настройка политики до уровня конкретных команд: например, read/write/get

SCADA Application - Modbus

General Properties

Name: Modbus Black

Primary Category: SCADA Protocols

Protocol: Modbus

Unit

☐ Any Unit

☐ Specified Unit ID 0 - 0

Function

☐ Any Function

☒ Standard Function 06: Write Single Register

☐ Any Address

☐ Address Range 0 - 0

☐ Custom Function

Function Range 1 - 1

Value

☐ Any Value

☒ Specified Value 0 - 1500

☐ Allow out of range values

OK Cancel

Протокол

Команда
(Функция)

Разрешенные
значения и
диапазоны

Name	Source	Destination	Applications/Sites	Action
Block High Risk apps	Any	Any	High Risk	Block
Control servers	Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor servers	Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow
Block SCADA traffic	Any	Internal PLCs	SCADA Protocols	Block

Name	Source	Destination	Applications/Sites	Action
Single Point ASDUs	Master	RTU	IEC 60870-5-104 - Single Point Information IEC 60870-5-104 - Single Point Information With Time Tag CP56Time2a	Allow
Double Point ASDUs	Master	RTU	IEC 60870-5-104 - Double Point Information IEC 60870-5-104 - Double Point Information With Time Tag CP56Time2a	Allow
Step Point ASDU	Master	RTU	IEC 60870-5-104 - Step Position Information	Allow
Measured Value ASDU	Master	RTU	IEC 60870-5-104 - Measured Value, Normalized Value	Allow
Any other communication between master and RTU	Master	RTU	Any Recognized	Allow

Firewall



Check Point
SOFTWARE TECHNOLOGIES LTD.

Одно из лучших в
индустрии stateful
inspection и IPSec решений

Поддержка SCADA
протоколов интегрирована
в firewall

Удобный интерфейс
написания политик

Логирование и
оповещение
администраторов для
контроля инцидентов в
реальном времени

No.	Hits	Name	Source	Destination	VPN	Service	Action
Limit Access to Gateways Rule (Rule 1)							
1	<div><div></div><div></div><div></div></div>	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
VPN Access Rules (Rules 2-3)							
Rules for Specific Sites (Rules 4-8)							
4	<div><div></div><div></div><div></div></div>	ICS Control	Internal-net-group	Substation_Zone_3	MyIntranet	TCP DNP3	Session Auth
5	<div><div></div><div></div><div></div></div>	RTU Monitor	Capacity_Reports	Control_Monitoring	MyIntranet	TCP Modbus	accept
6	<div><div></div><div></div><div></div></div>	Outbound HTTP	Remote-2-internal Substation_Zone_3	Any	Any Traffic	TCP http	drop
7	<div><div></div><div></div><div></div></div>	Critical subnet	Corporate-internal-net	Corporate-finance-net Corporate-hr-net Corporate-rnd-net	Any Traffic	Any	accept
8	<div><div></div><div></div><div></div></div>	Tech support	Tech-Support	Remote-1-web-server	Any Traffic	TCP http	accept
Identity Based Access (Rules 9-12)							
9	<div><div></div><div></div><div></div></div>	HR Server Allow	John_Adams_Role HR_Partners_Manage	HR_Server	Any Traffic	Any	accept (display ca
10	<div><div></div><div></div><div></div></div>	Finance Allow	Finance_Users_Role	Finance_Server	Any Traffic	Any	accept (display ca
11	<div><div></div><div></div><div></div></div>	Drop non identified	Any	Finance_Server HR_Server	Any Traffic	Any	drop
12	<div><div></div><div></div><div></div></div>	Internet Access	Guests All_Domain_Users	inet_http_proxy	Any Traffic	TCP HTTP_and_HTTP	accept (display ca
Common Rules - All Sites (Rules 13-19)							
13	<div><div></div><div></div><div></div></div>	Terminal server	Corporate-internal-tern	Any	Any Traffic	Any	Session Auth
14	<div><div></div><div></div><div></div></div>	DNS server	Any	Corporate-dns-ext	Any Traffic	UDP domain-uidn	accept

Обновление сигнатур – Online и Offline



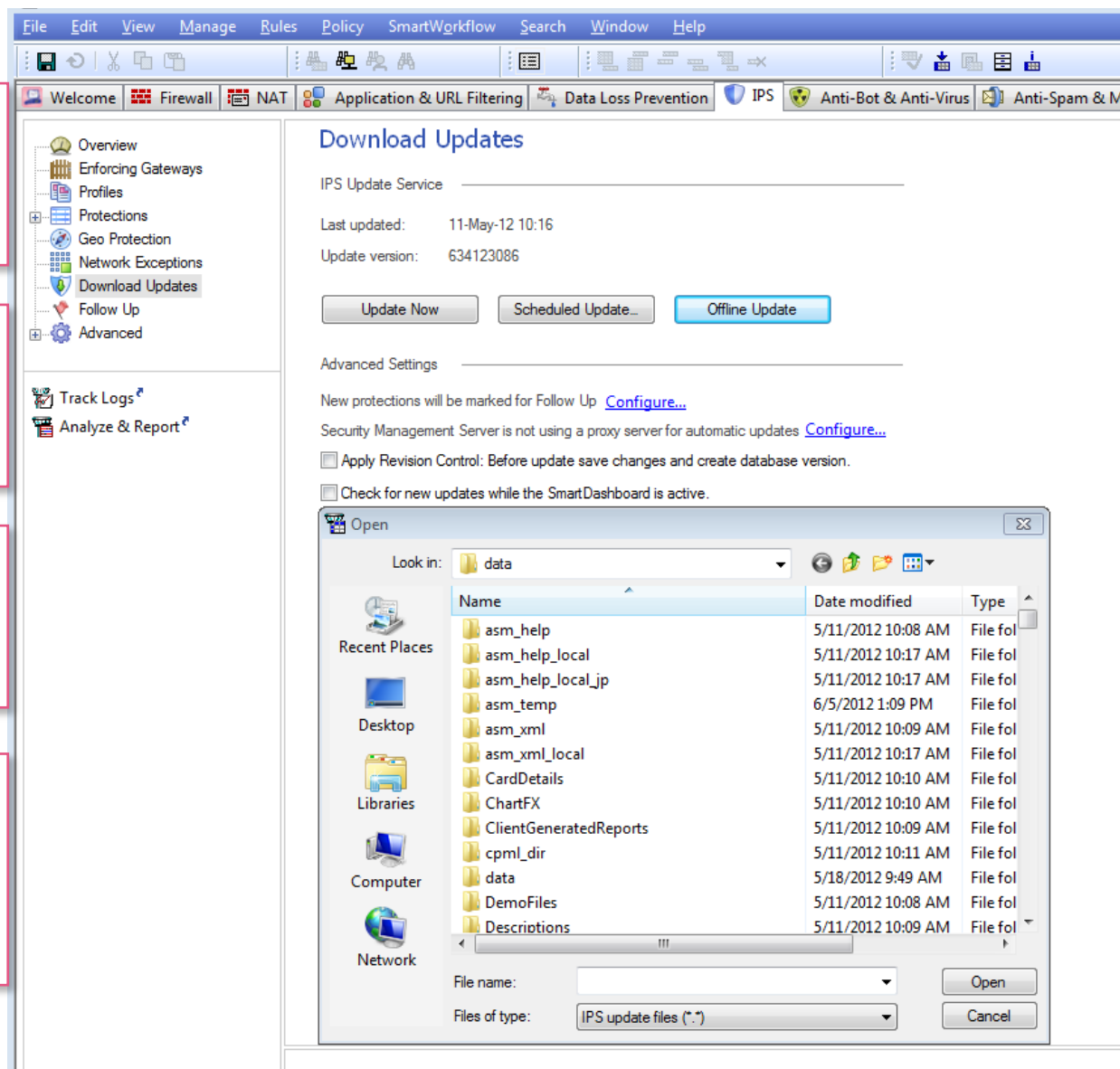
Check Point

Постоянное
совершенствование
сигнатур

Централизованное
обновление

Распространение в
режиме online и offline

Механизм Workflow для
аудита, отслеживания
изменения
конфигураций





Многоуровневая система противодействия современным угрозам



Предотвращает атаки на приложения

Борется с вирусами

Обезвреживает ботов



Check Point Anti-Bot Software Blade



ЭФФЕКТИВНАЯ БОРЬБА С БОТАМИ!

Check Point Anti-Bot Software Blade

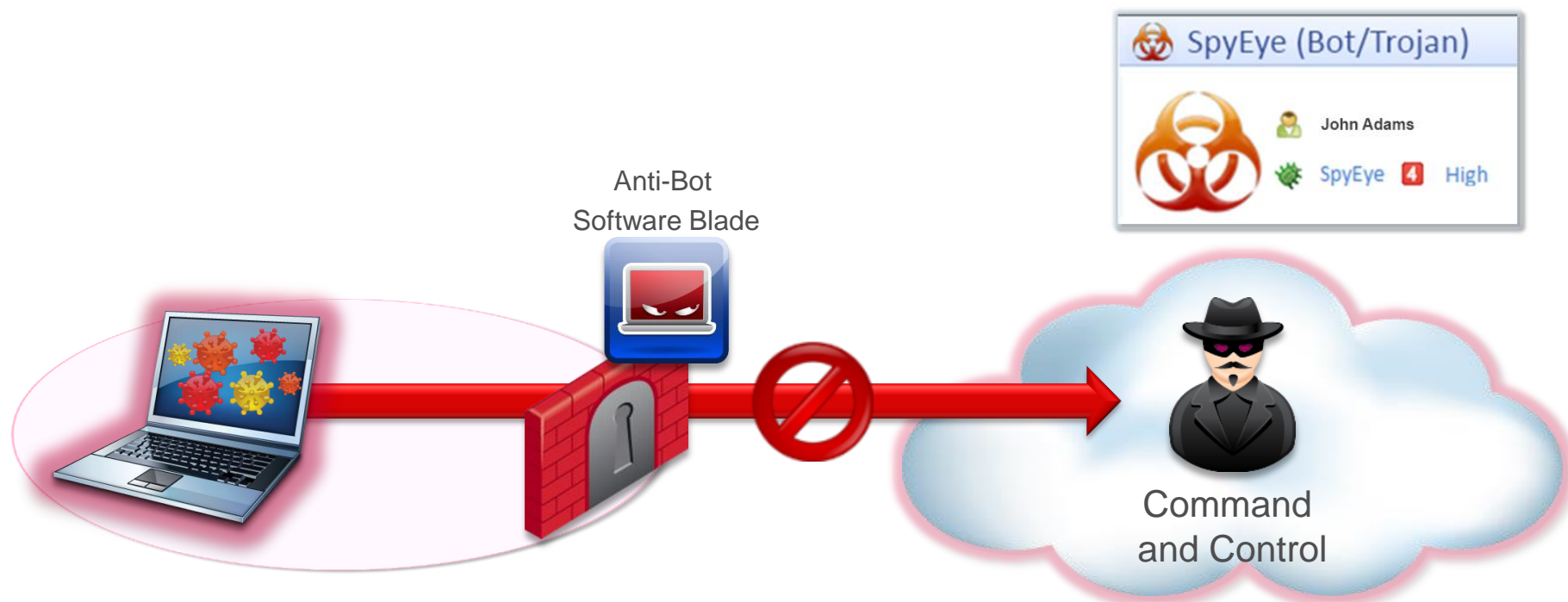


Check Point
SOFTWARE TECHNOLOGIES LTD.

Находит
зараженные
машины

Обезвреживает
зараженные
машины

Интегрированная
система



Защита от ботнетов и вредоносного ПО

Welcome Firewall NAT Application & URL Filtering Data Loss Prevention IPS Anti-Bot & Anti-Virus Anti-Spam & Mail Mobile Access IPSec

Overview

Threat Wiki

Policy

Exception Groups

Gateways

Protections

Type to Search		
Protection	Blade	Engine
File Types	Anti-Virus	File Type
Mail Activity	Anti-Bot	Suspicious Mail C
Malicious Activity	Anti-Bot	Signatures
Reputation Domains	Anti-Bot	Reputation
Reputation IPs	Anti-Bot	Reputation
Reputation URLs	Anti-Bot	Reputation
Unusual Activity	Anti-Bot	Behavioral Patter
URLs with Malware	Anti-Virus	Reputation
Viruses	Anti-Virus	Signatures

- Защита от нескольких векторов атак
- Обнаружение Ботов с помощью эвристических методов и контроля обращений к command and control центрам
- Обнаружение и предотвращение вредоносной активности за счет использования антивирусных сигнатур

Description

For Reputation IPs protections, the Reputation layer of the ThreatSpect engine prevents "call home" connections to Command and Control (C&C) servers. The ThreatCenter monitors the internet and pinpoint

Представляем:



Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Решения безопасности для АСУ ТП

CYBER DEFENSE

Специализир
ованная
защита от
SCADA угроз

Обзор и
детальный
контроль SCADA
трафика

Надежные
устройства для
агрессивной
среды

SCADA

Гранулярное логирование АСУ ТП трафика до уровня команд



Check Point
SOFTWARE TECHNOLOGIES LTD.

Может использоваться
для расследования
инцидентов

Подробно

Проанализировано
Check Point
SMARTLOG и
SMARTEVENT

Time	B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matched Ca
Today	10:45:35			gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33490	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33489	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33489	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33488	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33488	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33487	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33487	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33486	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33486	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33485	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33485	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33484	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33484	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33483	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33483	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33482	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33482	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33481	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33481	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33480	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot

Сгруппировано

Count	Source	Destination	Unit ID	Function Description	Transaction ID	Start Address
500	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Holding Registers		
100	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Input Registers		10
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register	19	50

Детальные отчеты по трафику АСУ ТП



Check Point
SOFTWARE TECHNOLOGIES LTD.

Allowed application Modbus_all

Log Info

SCADA Детализация

Modbus	
Unit ID	1
Transaction ID	2667
Function Code	6
Function Description	Write Single Register
Range Start Address	41
Range End Address	41
Quantity	1
Value	0001

Application Properties	
Application Risk	Unknown
Application Name	Modbus_all

Modbus	
Unit ID	1
Transaction ID	2667
Function Code	6
Function Description	Write Single Register
Range Start Address	41
Range End Address	41
Quantity	1
Value	0001

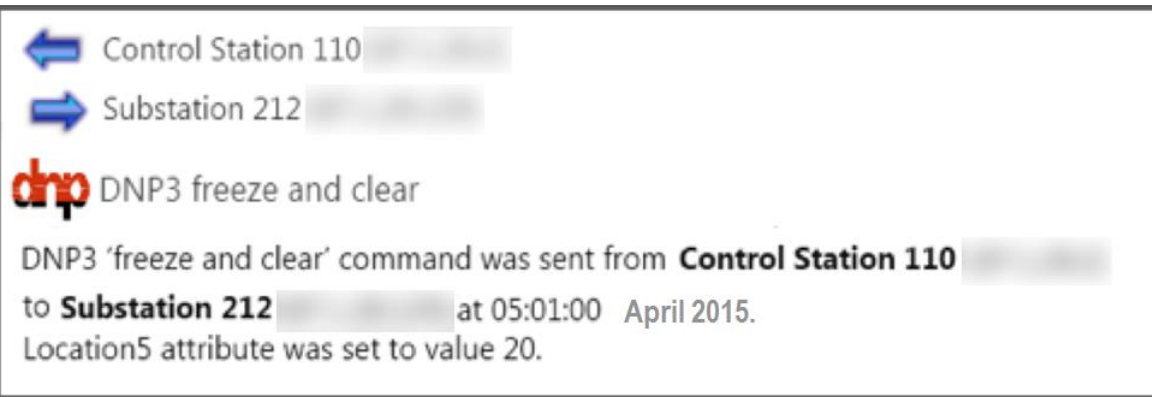
More	
Application ID	20000002
Application Rule ID	(DBD03A47-AA8C-44DB-997
Application Rule Na...	Learning Rule
Application Signatur...	20000002:1
Primary Category	SCADA Protocols
Proxy Source IP	HMI (10.1.1.5)

Protocol	TCP (6)
Destination Port	502
Source Port	49159
Service Name	Modbus

Мгновенный анализ подозрительного трафика между контроллерами



Check Point
SOFTWARE TECHNOLOGIES LTD.



Проанализировано
Check Point
SMART EVENT

Анализ рисков с помощью
специализированных отчетов по угрозам

Отслеживание попыток отправки
подозрительного количества команд

Отслеживание попыток разведки сети

SmartView Monitor



Check Point
SOFTWARE TECHNOLOGIES LTD.

*local - Check Point SmartView Monitor

SmartConsole

All Gateways

All Gateways

Gateway Name	IP Address	Status	Average CPU	Active Virtual Memory	Disk Free %	Version
Corporate-Cluster-2-member-A	192.168.80.1	OK	13%	77 MB	10	R75.40
Corporate-Cluster-2-member-B	192.168.80.2	OK	52%	228 MB	99	R75.40
Corporate-WA-proxy-server	172.16.2.3	OK	15%	223 MB	84	R75.40
Corporate-gw	192.168.75.1	OK	9%	138 MB	24	R77
Endpoint-1	10.14.1.132	OK	4%	384 MB	90	R75.40
Management	10.29.47.78	OK	2%	174 MB	84	R71
Management-b	172.16.1.201	OK	1%	471 MB	45	R75.40
Mobile_Access_London	Waiting...	Waiting...	Waiting...	Waiting...	Waiting...	Waiting...
Remote-1-gw	198.51.100.1	OK	2%	233 MB	92	NGX (R70)
Remote-1-web-server	192.168.2.2	OK	11%	369 MB	67	NGX (R70)
Remote-2-gw	205.50.200.1	Disconn...	6%	64 MB	45	R77
Remote-2-windows-domain-cont...	10.0.2.10	OK	36%	56 MB	23	R77
Remote-3-gw	100.75.25.1	Problem	4%	983 MB		R77
Remote-4-gw	10.125.100.1	OK	50%	77 MB	76	R75.40
Remote-5-gw	155.150.25.1	Attention	12%	143 MB	77	R75.20
Remote_branch_gw	198.85.100.120	OK	0%	138 MB	24	R75.40
VSX-gw	192.168.0.2	OK	9%	138 MB	24	R75.40VS

Monиторинг
состояния устройств
в реальном времени

Corporate-Cluster-2-member-A

IP Address: 192.168.80.1
Version: R75.40
OS: SecurePlatform
[System Information](#), [Network Activity](#), [Licenses](#)

Firewall Security Policy: Standard
Installed On: 01.08.04 [More...](#)

ClusterXL Working mode: High Availability
Member state: Up [More...](#)

IPSec VPN [More...](#)

Ready NUM

SmartView Tracker



Check Point
SOFTWARE TECHNOLOGIES LTD.

The image displays the SmartView Tracker interface with a detailed record for a threat emulation event. A pink callout bubble highlights the text: "Детальный отчет по каждому событию" (Detailed report for each event).

Record Details

Threat Emulation: Detect

Malicious file received from UnEmployment_Assitance@detma.org.

Log Info	
Time	Feb 12, 2013 at 14:58:52
Number	12
Type	Log
Origin	cn=cp_mgmt,o=gw-3296c0..iejtwy

Traffic	
Source	247.80.13.192
Proxied Source IP	---
Sender	UnEmployment_Assitance@detma.org
Destination	247.80.13.179
Recipients	HR_Jobs@AOL.com
Protocol	TCP tcp
Interface	---

Policy	
Action	Detect
Rule Name	Threat Emulation Detect Threat

Threat Emulation	
Email Subject	Action Required - Please check the Attached CV
Malware Activity	Malicious Filesystem activity Malicious Registr... >>
Vulnerable Operating Systems	Summary Report Microsoft Windows XP SP3 unpatched Microsoft Windows 7 fully patched
Analyzed On	Check Point Gateway
Severity	High
Confidence Level	High

Emulated File	
File Name	John Smith CV
File Type	Pdf
File Size	556.1 KB
File MD5	cbf76a32de0738f ea7073b3d4b3f1d60
File SHA-1	a7081468673e804 fb889507721f914438ab4e5fc

More	
Source User Name	Ella Eyelash
Product Family	Network
Verdict	malicious
Packet Capture ID	{0000007E-00C8-0042-9CE1-753ED8BA6322} 7e6fe36... >>

247.83.93.144 Check Point Threat Emulation Cloud Sales promo... 9ea44121c104e7d5c979fabe6d518842e0437d8a D...

Total records in file: 111
Local Mode NUM



✓ Обзор
состояния
безопасности

✓ Анализ и
корреляция в
реальном
времени

✓ Анализ
тенденций

Контроль за событиями



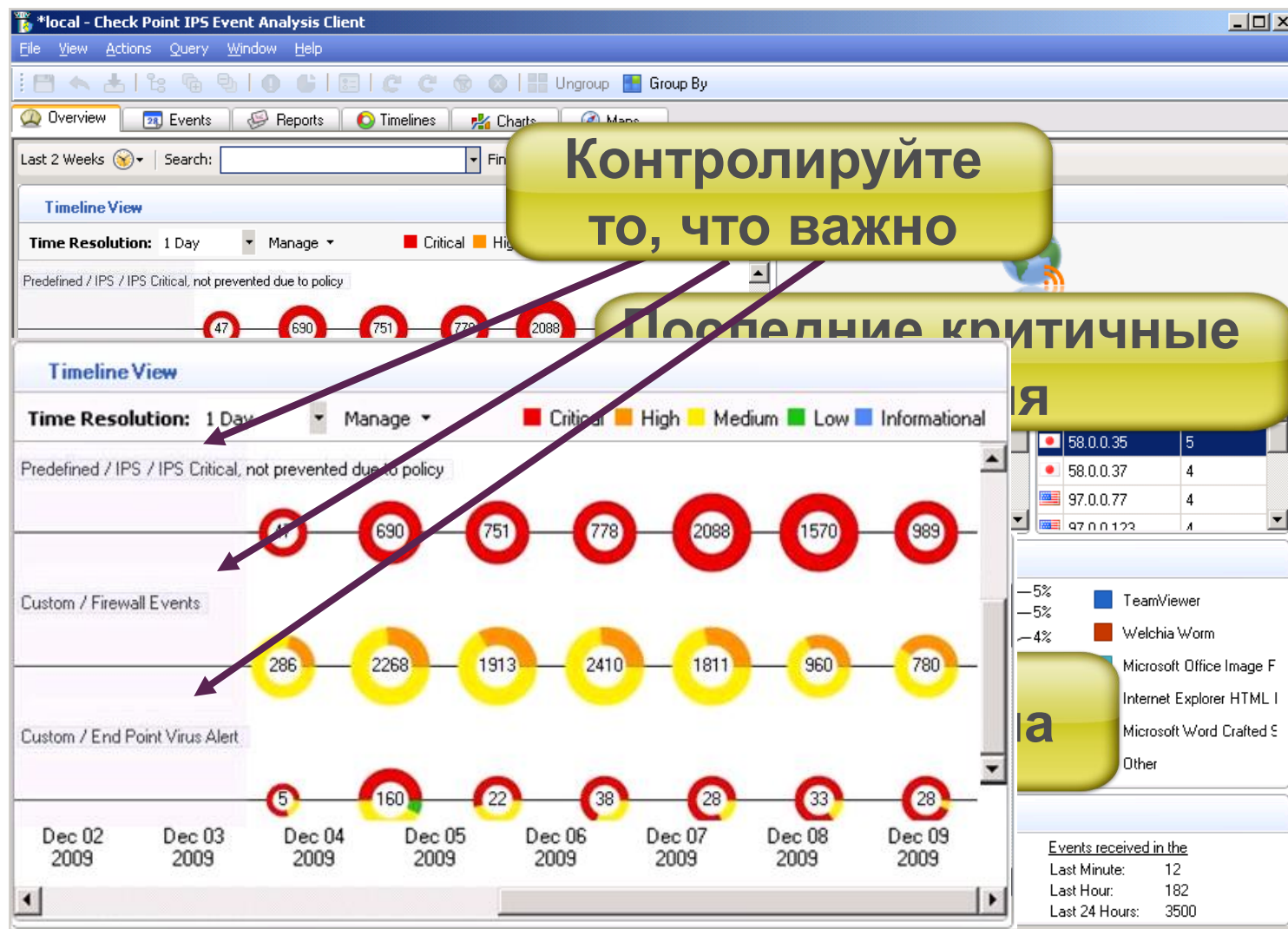
Check Point
SOFTWARE TECHNOLOGIES LTD.

Временная шкала

- Количество и важность атак
- Просто кликните мышкой для дальнейшего анализа
- Кастомизация – добавление своих временных шкал

Последние критичные события

- Обзор последних критичных событий
- Просто кликните мышкой для дальнейшего анализа



Мониторинг соответствия специализированным стандартам и правилам



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point SmartDashboard R77.30 - Compliance

Settings

Active Regulations

Regulation / Standard: Russia Data Protection (17)

Regulation Full Name: Russia Data Protection (17) Regulation Short Name: RU Data - 17

Regulation Description: Идентификация и аутентификация пользователей, являющихся работниками оператора. источник: Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

Regulation / Standard Requirements

Requirement ID	Requirement Name
01.01 (ИАФ.1)	Идентификация и аутентификация пользователей, являющихся работниками оператора. источник: Идентификация и аутентификация субъектов доступа и объектов доступа...
01.02 (ИАФ.2)	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных. источник: Идентификация и аутентификация субъектов доступа и об...
01.03 (ИАФ.3)	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. источник: Идентификация и аутентификация субъектов доступа и об...
01.04 (ИАФ.4)	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) ко...
01.05 (ИАФ.5)	Защита обратной связи при вводе аутентификационной информации. источник: Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
01.06 (ИАФ.6)	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей). источник: Идентификация и аутентификация субъек...
01.07 (ИАФ.7)	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых...
02.01 (УПД.1)	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. источник: Управление доступо...
02.02 (УПД.2)	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступ...
02.03 (УПД.3)	Управление (фильтрация, маршрутизация, контроль соединений, односторонняя передача и иные способы управления) информационными потоками между устройствам...
02.04 (УПД.4)	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы. источник: Управление доступом су...
02.05 (УПД.5)	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. источни...
02.06 (УПД.6)	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе). источник: Управление доступом субъектов доступа к объектам ...
02.07 (УПД.7)	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости ...

Save Cancel

Available Best Practices (301):

Best Practice ID	Best Practice Name
AB102	Check the 'KB of Email Messages' setting on each Anti-Bot Profile
AB104	Check that each Gateway's Anti-Bot configuration is activated according to the po
AB105	Check that the Malware Database is automatically updated
AB106	Check the frequency of scheduled Malware Updates in the Anti-Bot blade
AB107	Check that HTTPS Inspection is enabled on Gateways with Anti-Bot installed
AB108	Check the 'High Confidence' setting in the Anti-Bot blade
AB109	Check the 'Medium Confidence' setting in the Anti-Bot blade
AB110	Check the 'Low Confidence' setting in the Anti-Bot blade
APP101	Check that each Application Control rule has a name defined
APP102	Check that Application Control policy is blocking File storage and sharing applica
APP103	Check that Application Control policy is blocking Share files applications and sites
APP104	Check that Application Control policy is blocking Supports file transfer applications
APP105	Check that the Application Control blade has a defined Instant Messaging policy
APP106	Check that the Application Control blade has a defined web based instant messag
APP107	Check that the Application Control blade has a defined instant chat policy
APP108	Check that the Application Control blade has a defined instant messenger dating c...

Selected Best Practices (3):

Best Practice ID	Best Practice Name
MOB144	Check the Authentication Method defined in the Mobile Access blade
MOB145	Check the Two Factor Authentication with DynamicID in the Mobile Access b
MOB146	Check that Two-factor Authentication in the Mobile Access blade allows Dym

Save Cancel

Представляем:



Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Решения безопасности для АСУ ТП

CYBER DEFENSE

Специализир
ованная
защита от
SCADA угроз

Обзор и
детальный
контроль SCADA
трафика

Надежные
устройства для
агрессивной
среды

SCADA



Спецификация устройств

Индустриальные решения Check Point



Check Point
SOFTWARE TECHNOLOGIES LTD.

Универсальность



Функциональность



- 1200R
- IAS U1
- 3200 (2016 Appliances + SSD + DC)
- Integrated Security Module for Siemens / RuggedCom 1500 Switch

Защита АСУ ТП с помощью Check Point



Check Point
SOFTWARE TECHNOLOGIES LTD.

Линейка устройств в промышленном исполнении

- Работа в широком диапазоне температур, влажности
- Отсутствие движущихся частей
- Соответствие международным стандартам IEC 61850-3 и IEEE 1613



IAS U1



IAS T1



RuggedCom/Siemens



1200R

Монтаж на Din-рейку

**Средняя
производительность
Монтаж в стойку**

**Высокая
производительность
Монтаж в стойку**

Линейка устройств Check Point

Для защиты предприятий
любых масштабов

41000 и 61000
23000 линейка
(3 модели)



15000 Appliances
(2 модели)



Крупный офис

Защита ЦОД
Защита сервис
провайдеров

5000 Appliances
(4 модели)



Средний офис

3200 Appliance
1400 Appliances
(4 модели)



Малый офис

CHECK POINT 1200R



Check Point
SOFTWARE TECHNOLOGIES LTD.

Специализированное решение для
применения в промышленных и SCADA сетях



CHECK POINT 1200R



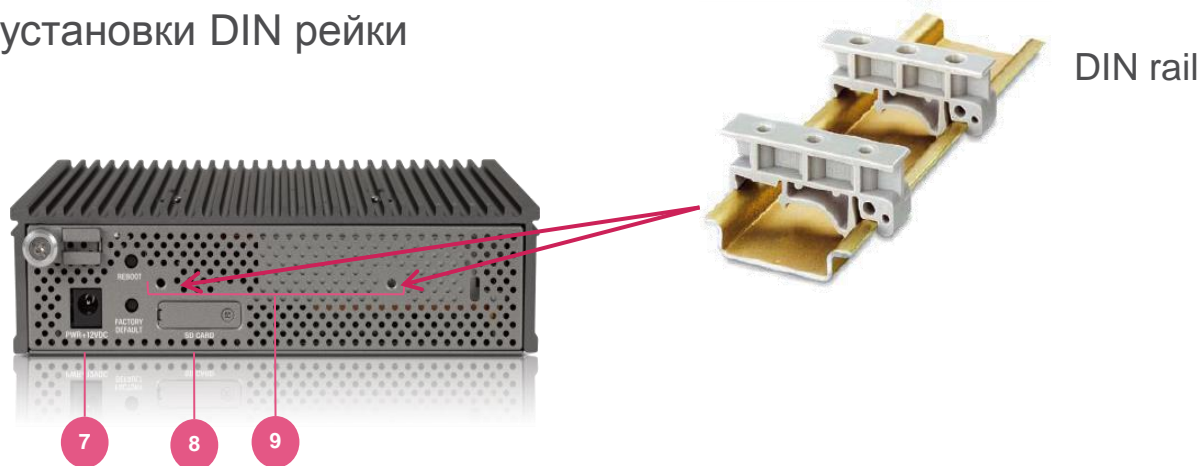
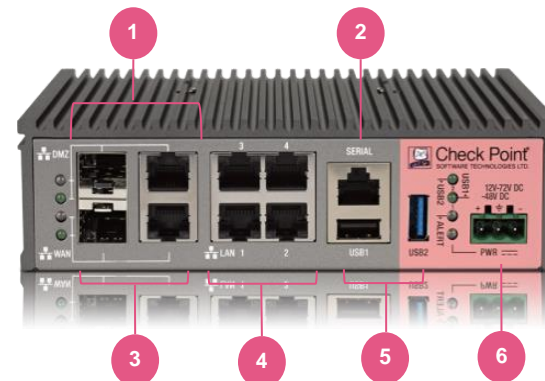
Check Point
SOFTWARE TECHNOLOGIES LTD.



- **Надежное решение**
 - Специализированное решение
 - Прочная конструкция – высокий уровень MTBF около 300,000 часов
 - Различные варианты монтажа и питания AC/DC
- **Функциональность**
 - Firewall,
 - IPS,
 - Application Control & URL Filtering,
 - Antivirus & AntiBot
 - IPSec VPN
- **Различные варианты управления**
 - SMART архитектура
 - Локальное управление
 - Out-of-the-box развертывание
- **Промышленное применение**
 - SCADA + Modbus, BACNet, DNP3, MMS, Profinet, S7 (Siemens) и прочие
 - IPS

Check Point 1200R

- 1 DMZ порт (медный или оптический)
- 2 Консольный порт RJ-45
- 3 WAN-порт (медный или оптический)
- 4 LAN-порты (4 x 10/100/1000BaseT)
- 5 USB-порты (2.0/3.0)
- 6 DC питание
- 7 [AC](#) питание
- 8 [SD](#) card слот (для хранения логов)
- 9 Крепления для установки DIN рейки



Check Point 1200R- Спецификация



Check Point
SOFTWARE TECHNOLOGIES LTD.



Производительность:

- 49 SecurityPower¹ Units
- Пропускная способность МСЭ 2 Гбит/с, 1518 байт UDP
- 700 Мбит/с МСЭ, смешанный трафик
- 60 Мбит/с МСЭ и IPS, смешанный трафик
- Пропускная способность VPN 450 Мбит/с
- 400,000 одновременных соединений

Соответствие требованиям:

- IEEE 1613 , IEC 61850-3
- CE, EN 55024, EN 55022
- EN 61000-3, EN 61000-4
- CB, IEC 60950, UL 60950

- Температура и влажность:
 - от -40 до 75°C,
 - 20%-90%
- Соответствует промышленным стандартам по температуре, вибрациям, влажности и ЭМИ
- Отсутствие движущихся частей
- Гибкие варианты монтажа устройства
- Различные опции по питанию:
 - AC: 100-240V, 50 – 60 Hz
 - DC: 12V-72V, -48V DC



Специализированное устройство Check Point для защиты критичных систем (Smart Grid)



IAS U1

IEC 61850-3 and IEEE 1613
compliant Designed for critical
network security



- Богатый функционал Software Blades – R7X/R77
- Централизованное управление Smart Center/Multi Domain
- Удовлетворяет требованиям Smart Grid
 - IEC-61850-3 и IEEE 1613
- Работает в экстремальных условиях
- Нет движущихся компонентов
- Возможны 48v DC блоки питания
- Высокая плотность портов – поддержка Fiber



IAS U1 - Спецификация



Check Point
SOFTWARE TECHNOLOGIES LTD.

- Software Blades – R7X/R75
- Based on Secure Platform
 - SSD/HDD
 - 2 G ram
 - Rear wiring & I/O LED status indicators
 - 2 - USB 2.0
- IEC-61850-3 and IEEE 1613
- System Design: Fan less
- Power – 48v DC
- Interfaces – 3 x expansion slots
 - 2 x 1000 Base T, 4 x 1/100 Base T
 - Optional - 4 Fiber – mm 100 base FX
 - Serial 2x DB6 RS232, 8 screw terminal RS232/422/485
- **Environmental**
 - Power Consumption 5V $\pm 5\%$ @
 - Operating Temperature $-20^{\circ} \sim 70^{\circ} \text{C}$
 - Operating humidity 20 ~ 95% RH non-condensing (refer to IEC 68-2-3)
 - Shock and vibration protection



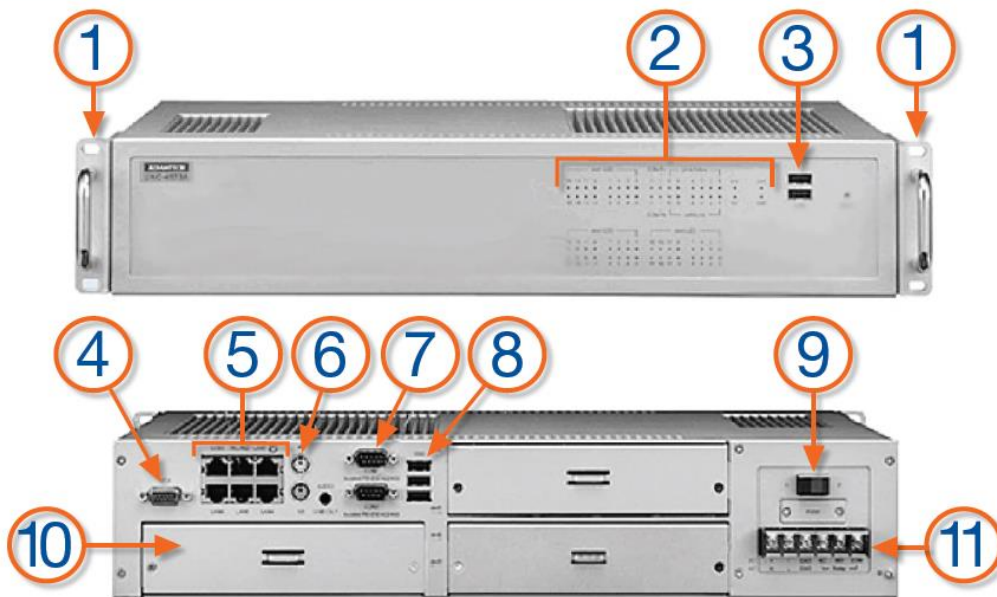
IAS U1 - Спецификация



Check Point
SOFTWARE TECHNOLOGIES LTD.

IAS U1

- ① Rack mount
- ② Network interface LEDs
- ③ Two USB ports
- ④ DB-15 VGA monitor connector
- ⑤ 2 x 10/100/1000 Base-T and 4 x 10/100 Base-T
- ⑥ PS-2 keyboard connector
- ⑦ DB-9 serial console connectors
- ⑧ Three USB ports
- ⑨ Power switch
- ⑩ Three I/O expansion slots
- ⑪ DC/AC power supply



- Производительность до 3 Гб/с в режиме межсетевого экрана
- Производительность до 2 Гб/с в режиме IPS (Default IPS profile)
- Соответствие требованиям IEC 61850-3 и IEEE 1613
- Температура и влажность: от -20 до 70° C, 20%-95%
- Отсутствие движущихся частей— безвентиляторный дизайн с использованием SSD накопителей и отсутствием внутренних кабельных соединений
- Различные опции по питанию

Integrated Security Module for Siemens / RuggedCom 1500 Switch



Check Point
SOFTWARE TECHNOLOGIES LTD.

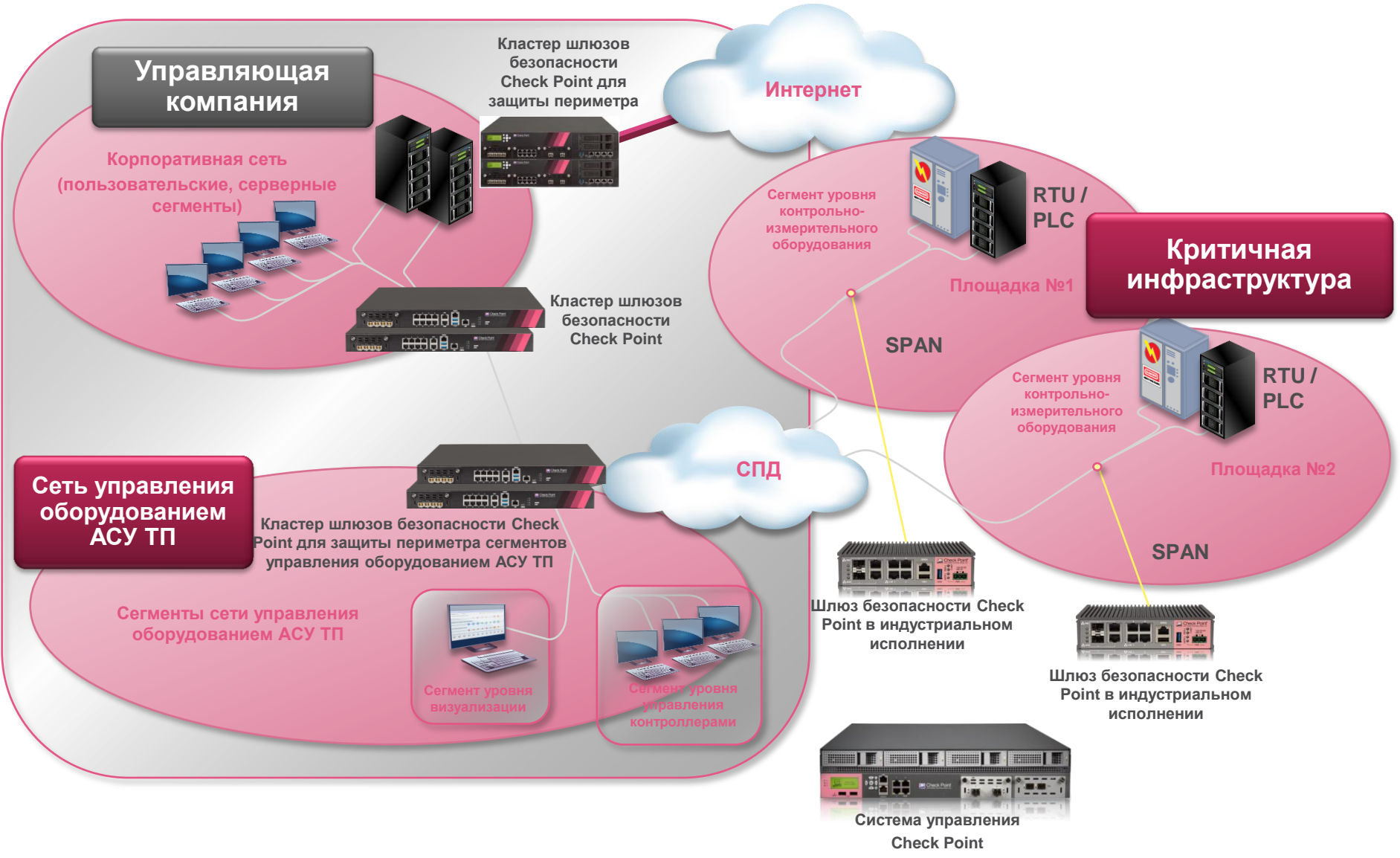


- ПО Check Point R77.10 интегрировано в модуль RuggedApe
- Прямой доступ к внутренней шине (не нужны лишние кабели)
- Соответствует требованиям IEC 61800-3 и IEC 61000-6-2
- Температура и влажность: от -40 до 70°C, 50%-95%
- Rack mount and DIN rail form factors
- 1x GigE и 2 x USB интерфейса на лицевой панели
- 1x GigE on backplane

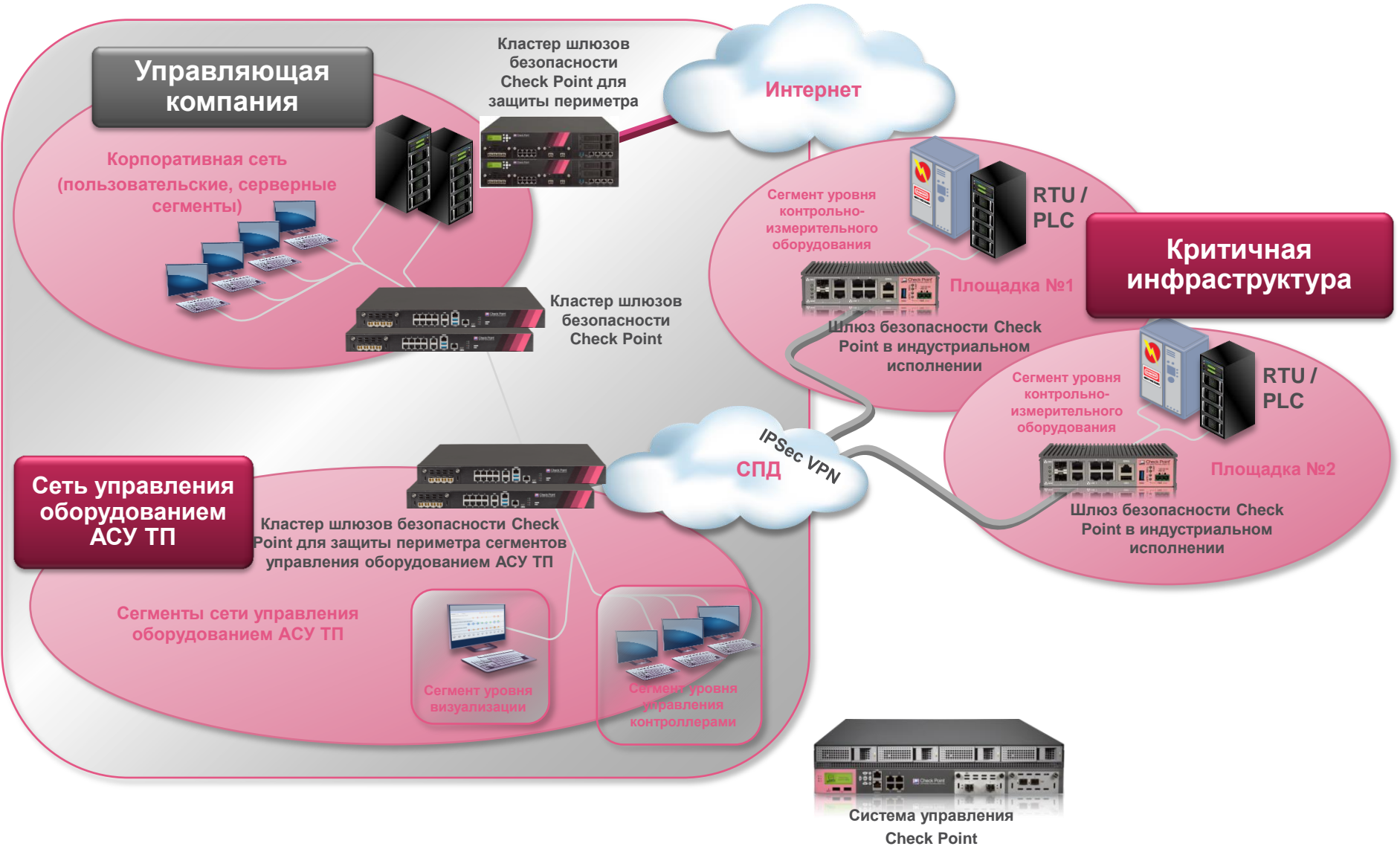


Варианты развертывания

Индустриальные сети



Индустриальные сети



Требования к сетевой безопасности



Check Point
SOFTWARE TECHNOLOGIES LTD.

Корпоративный периметр

- Application Control
- Firewall – Сегментация сети
 - в Internet
 - к индустриальной сети
- IPS
- Защищенный удаленный доступ
- Anti-Malware и Anti-Bot

Индустриальная сеть

- Firewall – контроль доступа
- IPS
- Защищенный удаленный доступ
- Неблагоприятное окружение
- Анализ протоколов SCADA
- Anti-Bot
- Управление
- Аудит

Консолидация и централизованное управление

Требования защиты информации в РФ



Защита информации при межсетевом взаимодействии



Check Point
SOFTWARE TECHNOLOGIES LTD.

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

МЭ не ниже 4 класса

5.7.4. Подключение ЛВС к сетям автоматизированной системы (локальной или вычислительной) осуществляется 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 R65, R71, R75, R77
сертифицированы
как МЭЗ

Сертифицированное СКЗИ

7.5. Для защиты конфиденциальной информации, передаваемой 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
сертифицированные ФСБ
КриптоПроCSP 3.6, 3.9

Сертификация Check Point во ФСТЭК



Check Point
SOFTWARE TECHNOLOGIES LTD.



Сертификация Check Point Security Gateway R75.30 на соответствие МЭЗ



СЕРТИФИЦИРОВАННЫЕ
ИНФОРМАЦИОННЫЕ
СИСТЕМЫ



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3018

Выдан 19 ноября 2013 г.
Действителен до 19 ноября 2016 г.

Настоящий сертификат удостоверяет, что шлюз безопасности «Check Point Security Gateway версии R75», разработанный компанией Check Point Software Technologies Ltd. и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5015-008-82487552-2012, функционирующий на аппаратных платформах с версиями программного обеспечения, указанными в формуляре 5015-008-82487552-2012 ФОР, 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 при выполнении ограничений по эксплуатации, приведенных в формуляре.

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R75» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

**Сертификация производства
Power-1,
UTM-1,
2012 series,
SG на универсальных платформах
Для АС до 1Г и ИСПДн до К2 включительно**

Сертификация Check Point во ФСТЭК



Check Point
SOFTWARE TECHNOLOGIES LTD.



Сертификация Check Point Security Gateway R75.40VS на соответствие МЭЗ



СЕРТИФИЦИРОВАННЫЕ
ИНФОРМАЦИОННЫЕ
СИСТЕМЫ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3297

Выдан 12 декабря 2014 г.
Действителен до 12 декабря 2017 г.

Настоящий сертификат удостоверяет, что **шлюз безопасности «Check Point Security Gateway версии R75.40VS»**, разработанный компанией Check Point Software Technologies Ltd. и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5015-009-82487552-2013, функционирующий на аппаратных и программных платформах, указанных в формуляре 501540-009-82487552-2013 01 30, 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 при выполнении ограничений по эксплуатации, указанных в

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R75.40VS» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

**Сертификация производства
Power-1, UTM-1,
2012 series,
61000,**

SG на универсальных платформах

Для АС до 1Г и ИСПДн до К2 включительно

Сертификация Check Point во ФСТЭК



Check Point
SOFTWARE TECHNOLOGIES LTD.



Сертификация Check Point Security Gateway R77.10 на соответствие МЭЗ+СОВ4+НДВ4



СЕРТИФИЦИРОВАННЫЕ
ИНФОРМАЦИОННЫЕ
СИСТЕМЫ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3457

Выдан 13 октября 2015 г.
Действителен до 13 октября 2018 г.

Настоящий сертификат удостоверяет, шлюз безопасности «Check Point Security Gateway версии R77.10», разработанный компанией «Check Point Software Technologies Ltd.» и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5015-003-82487552-14, функционирующий на аппаратных платформах Check Point: UTM-1, POWER-1, 2012 Models, 61K/41K System, Open Servers и в виртуальной инфраструктуре VMWare под управлением операционных систем, указанных в формуляре 501510-003-82487552-14 ФО, 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 техническим условиям при выполнении ограничений по эксплуатации, приведенных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 24.05.2006 № СЗН RU.304.507.022) – техническое заключение от 11.08.2015, и экспертного заключения органа по сертификации от 24.08.2015 ФАУ «Государственный

Сертификат ФСТЭК России на шлюз безопасности «Check Point Security Gateway версии R77.10» на соответствие требованиям РД Средства вычислительной техники. Межсетевые экраны. 3 класс защищенности.

**Сертификация производства
Power-1, UTM-1,
2012 series, 41000, 61000,
SG на универсальных платформах,
и в виртуальной инфраструктуре VMWare
Для АС до 1Г и ИСПДн до К2 включительно**



Анализ протоколов АСУ ТП
с точностью до команды

Предотвращение атак на АСУ ТП

Логирование всех команд АСУ ТП

Оповещение администраторов в
реальном времени

Итоги:

Решения Check Point для обеспечения безопасности АСУ ТП

Специализированные
аппаратные
платформы

Защита от
специфичных
угроз, за счет
анализа SCADA
протоколов

Централизованный
менеджмент



Check Point
SOFTWARE TECHNOLOGIES LTD.

СПАСИБО!

