# ИБ Решения для АСУ ТП

Дата обновления: 10 ноября 2015

**Обзор основных продуктов и решений**

Алексей Комаров
ZLONOV.ru
@zlonov

# Содержание 1/3

- **Комплексные решения**
  - DATAPK
  - InfoWatch ASAP
  - Kaspersky Industrial CyberSecurity
    - Kaspersky TMS
    - KasperskyOS
  - АПК «ЩИТ»
  - Industrial Control System Defender*
- **Сканеры защищённости**
  - MaxPatrol
  - SCADA-аудитор
- **Однонаправленные диоды**
  - Fox DataDiode
  - InfoDiode
  - Waterfall Security Solutions

# Содержание 2/3

- **Промышленные межсетевые экраны**
  - Основные отличия
  - Check Point 1200R
  - Check Point UTM-1 Edge N Industrial Appliance
  - Cisco ASA 5506H-X
  - Cisco CGR 2000
  - Cisco CGS 2500
  - Cisco IE-3000-8TC
  - Cisco ISA 3000
  - Symanitron Secure
    - Symanitron SEWM-DF-S200
    - Symanitron SEWM-DF-S300
    - Symanitron SEWM-DF-S500
  - Symanitron ViPNet 100
  - ViPNet Coordinator IG10
  - Другие производители

# Содержание 3/3

- **Другие решения**
  - Honeywell Industrial Cyber Security Risk Manager
  - ViPNet ICM
  - АПК «Свиток»
  - «СТРАЖ-ЧПУ»
- **Дополнительная информация**

# Комплексные решения

# DATAPK

- Комплекс DATAPK обеспечивает оперативный мониторинг и контроль состояния защищённости автоматизированных систем управления технологическими процессами (АСУ ТП).

- Разработчик: УЦСБ

- Запланирована сертификация ФСТЭК и Газпромсерт.

http://zlonov.ru/catalog/datapk/

# InfoWatch ASAP

- Предназначен для защиты информации, обрабатываемой в автоматизированных системах управления (АСУ), от компьютерных атак, неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий.

- Разработчики: ИнфоВотч/ Инжиниринговый центр НИЯУ МИФИ.

- Запланирована сертификация ФСТЭК.

http://zlonov.ru/catalog/infowatch-asap

# Kaspersky Industrial CyberSecurity

- Специализированное решение для защиты АСУ ТП.

- Разработчик: Лаборатория Касперского.

http://zlonov.ru/catalog/kics/

# Kaspersky TMS

- Компонент Kaspersky Industrial CyberSecurity
- Комплексное решение для делегирования аномальной активности в индустриальной сети, своевременного обнаружения и расследования инцидентов ИБ.
- Разработчик: Лаборатория Касперского


http://zlonov.ru/catalog/kaspersky-tms/

# KasperskyOS

- Используется в Kaspersky Industrial CyberSecurity

- Защищённая ОС, предназначенная, главным образом, для использования в индустриальных системах.

- Разработчик: Лаборатория Касперского.

```
#ifndef __X86_IRQ_H
#define __X86_IRQ_H

#include <KRT/Types.h>

#ifdef __cplusplus
namespace x86_irq {
extern "C" {
#endif

typedef int (__cdecl *t_IrqHandler)( dword_t Irq, void* Context );
typedef void (__cdecl *t_DsrHandler)( void* Context );
typedef void (__cdecl *t_AsrHandler)( void* Context );

/** Attach interrupt handler to IRQ handling chain
\param      Irq             -       Irq number
\param      Handler         -       interrupt handler callback
\param      Context         -       context passed to interrupt handler
\return     0               -       unsuccessful, low resources
NonZero                     -       interrupt handler installed
*/
bool_t __cdecl AttachInterrupt( dword_t Irq, t_IrqHandler Handler, void* Context );
/** Detaches interrupt handler from the IRQ handling chain
\param      Irq             -       Irq number
\param      Handler         -       interrupt handler callback
\return     0               -       unsuccessful, handler not found
NonZero                     -       interrupt handler detached
*/
bool_t __cdecl DetachInterrupt( dword_t Irq, t_IrqHandler Handler );
//////////////////////////////////////////////////////////////////////
/** Queue DSR to DSR handling chain
\param    Handler               -       DSR handler callback
\param    Context               -       context passed to DSR handler
\return   0                     -       unsuccessful, low resources
NonZero                         -       DSR handler installed
*/
bool_t __cdecl QueueDSR( t_DsrHandler Handler, void* Context);
/** Queue ASR to ASR handling chain
\param    Handler               -       ASR handler callback
\param    Context               -       context passed to ASR handler
\return   0                     -       unsuccessful, low resources
NonZero                         -       ASR handler installed
*/
bool_t __cdecl QueueASR( t_AsrHandler Handler, void* Context);
/** Queue usermode ASR to usermode ASR handling chain
\param    Handler               -       ASR handler callback
\param    Context               -       context passed to ASR handler
\return   0                     -       unsuccessful, low resources
NonZero                         -       usermode ASR handler installed
*/
bool_t __cdecl QueueUserASR( t_AsrHandler Handler, void* Context);

/** Set irq line sensitivity (edge/level)
\param    Irq           -       irq line number
```

http://zlonov.ru/catalog/kasperskyos/

# АПК «ЩИТ»

- Многофункциональное устройство для обнаружения и предотвращения несанкционированных вторжений (Intrusion Prevention System — IPS) в информационные инфраструктуры систем автоматического управления различными технологическими процессами.


- Разработчик: Инжиниринговый центр НИЯУ МИФИ.

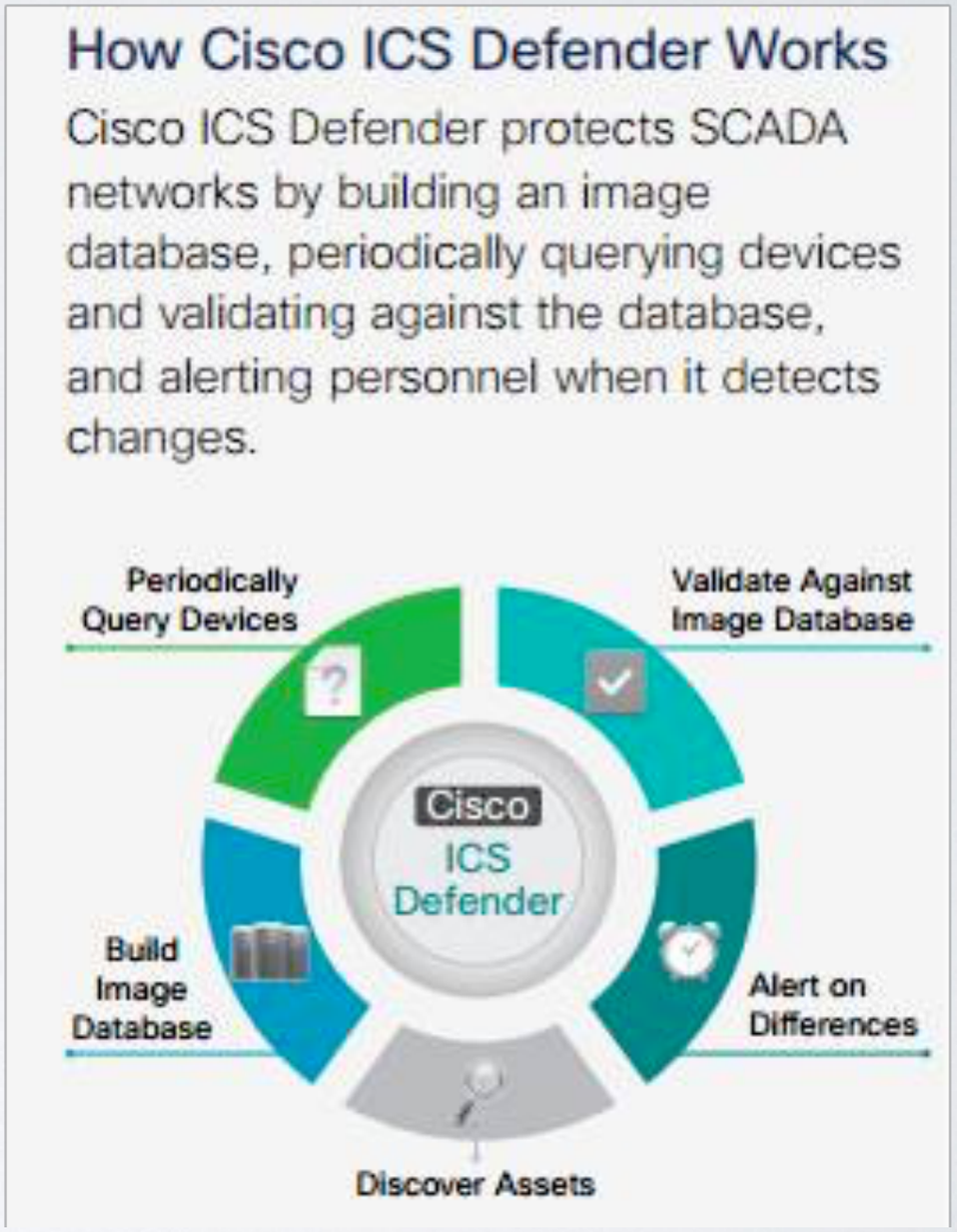
- Запланирована сертификация ФСТЭК.

http://zlonov.ru/catalog/апк-щит/

# Industrial Control System Defender*

- Cisco ICS Defender осуществляет мониторинг работы программируемых логических контроллеров и интеллектуальных удаленных терминалов.

- * - Решение было анонсировано в русскоязычном сегменте Интернета в октябре 2015 года, но в том же месяце на запрос участника Facebook-группы Кибербезопасность АСУ ТП представитель Cisco сообщил: "I'm sorry, but the product is no longer available."




http://zlonov.ru/catalog/ics-defender/

# Сканеры защищённости

# MaxPatrol

- Возможности MaxPatrol для АСУ ТП: поиск уязвимостей PLC/SCADA/MES, встроенные (безопасные) профили для SCADA, проверки HMI Kiosk mode и доступа в интернет, черные/белые списки, антивирусы/HIPS проверки, анализ конфигурации АСУ ТП

- Разработчик: Позитив Текнолоджиз.

- Сертификат ФСТЭК №2922 от 08.07.13 (до 08.07.16) на Систему контроля защищенности и соответствия стандартам «MaxPatrol» — по 4 уровню контроля отсутствия НДВ и ТУ.


http://zlonov.ru/catalog/maxpatrol/

# SCADA-аудитор

- Программное средство анализа защищенности информационных систем «Сканер SCADA-аудитор» предназначен для анализа защищённости автоматизированных систем управления технологических процессов (АСУ ТП), реализованных на базе систем SCADA (Supervisory Control and Data Acquisition, Диспетчерское управление и сбор данных).


- Разработчик: Станкоинформзащита.

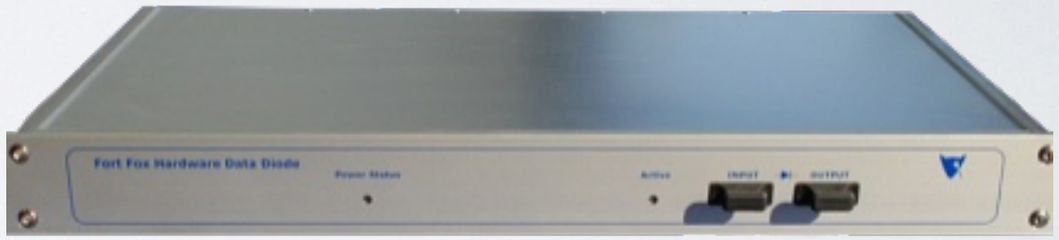
- Сертификат ФСТЭК №3165 от 28.05.14 (до 21.05.17) на Программный комплекс сканера «SCADA-аудитор» — по 4 уровню РД НДВ и ТУ.

http://zlonov.ru/catalog/scada-аудитор/

# Однонаправленные диоды

# Fox DataDiode

- Устройство Fox DataDiode автоматизирует и ускоряет процесс добавления информации к конфиденциальным сетям, не ухудшая безопасности. Обеспечивает гарантированное однонаправленное подключение, для безопасной и бесперебойной передачи информации в режиме реального времени 24 часа в сутки.




http://zlonov.ru/catalog/fox-datadiode/

# InfoDiode

- Аппаратно-программный комплекс однонаправленной передачи данных InfoDiode предназначен для обеспечения защиты данных в локально-вычислительных сетях посредством изоляции критичных сегментов сети с сохранением возможности межсетевого взаимодействия.


- Сертификат ФСТЭК №3434 от 17.08.15 (до 17.08.18) на Аппаратно-программный комплекс «InfoDiode» — на соответствие РД НДВ по 4 уровню и ТУ

- Разработчик: АМТ-ГРУП.

http://zlonov.ru/catalog/infodiode/

# Waterfall Security Solutions

- Waterfall's® Unidirectional Security Gateways — семейство продуктов на базе единого технологического ядра, аппаратно реализующих функционал однонаправленных сетевых шлюзов (диодов), с поддержкой широкого числа сетевых приложений и протоколов, в том числе, специфичных для промышленных сетей.


http://zlonov.ru/catalog/waterfall-security-solutions/

# Промышленные межсетевые экраны

# Основные отличия

| **Некоторые указываемые производителями отличия специализированных промышленных межсетевых экранов от офисных решений** | |
|---|---|
| **Конструктивные особенности** | • пыле/влагозащищённость<br>• безвентиляторное исполнение<br>• работа в условиях повышенной влажности<br>• расширенный температурный диапазон<br>• устойчивость к электромагнитным наводкам<br>• питание от постоянного тока (9В..48В)<br>• специализированное крепление (DIN-рейка)<br>• наличие специализированных разъёмов (RS232/485) |
| **Конструктивно-функциональные особенности** | • быстрое восстановление конфигураций с физических носителей (карты памяти или USB)<br>• физическая кнопка отключения/изменения режимов работы |
| **Функциональные особенности** | • упрощённый интерфейс управления<br>• длительное время безобслуживаемой работы<br>• корректная работа со специфическим трафиком (значительное число пакетов в секунду при небольшом их размере)<br>• глубокая поддержка промышленных протоколов |

# Check Point 1200R

- Check Point 1200R — это специально разработанный шлюз безопасности повышенной прочности, рассчитанный на использование в тяжелых условиях и на удаленных площадках, таких как производственные цеха, электрические подстанции и объекты электроэнергетики. Поддерживает системы ICS/SCADA и обеспечивает высокий уровень защиты для самых ценных активов государства.


http://zlonov.ru/catalog/check-point-1200r/

# Check Point UTM-1 Edge N Industrial Appliance

- Спецверсия UTM-1 Edge N, отличающаяся защищённым корпусом – защита от ударов, влажности и экстремальных температур. Программное обеспечение на всех шлюзах Check Point одинаково и зависит от используемых лицензий и программных модулей.


http://zlonov.ru/catalog/utm-1-edge-n-industrial-appliance/

# Cisco ASA 5506H-X

- Cisco ASA 5506H-X включает в себя межсетевой экран, VPN-решение, систему обнаружения вторжений и систему защиты от вредоносного кода, помещенные в специализированный корпус, предназначенный для работы в агрессивной окружающей среде.


http://zlonov.ru/catalog/cisco-asa-5506h-x/

# Cisco CGR 2000

- Сертификат ФСТЭК №2638 от 14.05.12 (до 14.05.15)

- Маршрутизатор серии «Cisco CGR 2000» (модель Cisco CGR 2010) с установленным программным обеспечением Cisco IOS версии 15.1(4)M2 — на соответствие РД МЭ по 4 классу


http://zlonov.ru/catalog/cisco-cgr-2000/

# Cisco CGS 2500

- Сертификат ФСТЭК №2692 от 22.08.12 (до 22.08.15)
- Коммутатор серии «Cisco CGS 2500» (модель Cisco CGS-2520-24TC, модель Cisco CGS-2520-16S-8PC) с установленным программным обеспечением Cisco IOS Software версии 12.2(58)EY2 — на соответствие РД МЭ по 4 классу защищенности

http://zlonov.ru/catalog/cisco-cgs-2500/

# Cisco IE-3000-8TC

- Сертификат ФСТЭК №2911 от 26.06.13 (до 26.06.16)
- Коммутатор Cisco Cisco IE-3000-8TC с установленным программным обеспечением IES Software (IES-IPSERVISK9-M) версии 12.2(58)SE2 — на соответствие РД МЭ по 4 классу
- Сертификат ФСТЭК №2994 от 11.10.13 (до 11.10.16)
- Коммутатор Cisco IE-3000-8TC с установленным программным обеспечением IES Software Version 15.0 — на соответствие РД МЭ по 4 классу


http://zlonov.ru/catalog/cisco-ie-3000-8tc/

# Cisco ISA 3000

- Cisco Industrial Security Appliance 3000 включает в себя функционал межсетевого экрана, системы предотвращения вторжений, VPN и защиты от вредоносного кода.


http://zlonov.ru/catalog/cisco-isa-3000/

# Symanitron Secure

- Линейка промышленных межсетевых экранов с богатым функционалом защиты: Firewall, Deep Inspection (Modbus, IEC101/104, DNP3), защита от DoS-атак, включение/отключение портов, аутентификация пользователей, журнал активности пользователей, VPN.

- Разработчик: Симанитрон.

- Запланирована сертификация ФСТЭК.


http://zlonov.ru/catalog/tags/symanitron/

# Symanitron SEWM-DF-S200

- Промышленный шлюз с функциями брэндмауэра SEWM-DF-200 – это эксклюзивное предложение от компании Symanitron в области специальных устройств, предназначенных для тяжелых условий эксплуатации.


http://zlonov.ru/catalog/symanitron-sewm-df-s200/

# Symanitron SEWM-DF-S300

- Компактные Ethernet-коммутаторы Symanitron SEWM-DF-S300 имеют промышленное исполнение, усиленный корпус и обеспечивают функционал, который обычно требует применения отдельных видов оборудования.


http://zlonov.ru/catalog/symanitron-sewm-df-s300/

# Symanitron SEWM-DF-S500

- Модульные Ethernet-коммутаторы Symanitron SEWM-DF-S500 специально предназначены для обеспечения высоконадёжной сетевой инфраструктуры в промышленных условиях и обладают встроенным механизмом сетевой защиты с поддержкой приложений SCADA.


http://zlonov.ru/catalog/symanitron-sewm-df-s500/

# Symanitron ViPNet 100

- Российский промышленный шлюз безопасности, предназначенный для использования в производственных условиях (межсетевой экран, и VPN до 20 мбит/с)

- Разработчики: ИнфоТеКС и Симанитрон


http://zlonov.ru/catalog/symanitron-vipnet-100/

# ViPNet Coordinator IG10

- Межсетевой экран с VPN до 10 Мбит/с в промышленном исполнении с поддержкой Wi-Fi, 3G/LTE.
- Разработчик: ИнфоТеКС


http://zlonov.ru/catalog/vipnet-coordinator-ig10/

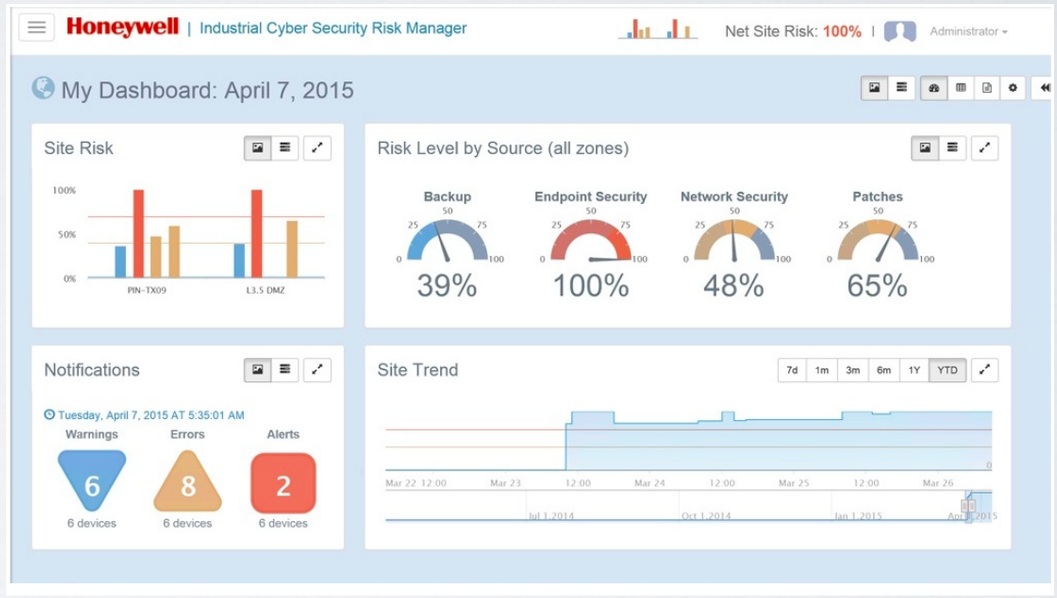
# Другие производители межсетевых экранов

- Fortinet - серия FortiGate Rugged
- Phoenix Contact mGuard - несколько моделей
- Tofino Xenon / EAGLE Tofino (Belden) - несколько моделей
- Zenwall (Secure Crossing) - несколько моделей

# Другие решения

# Honeywell Industrial Cyber Security Risk Manager

- Цифровая информационная панель, предназначенная для автоматического мониторинга, оценки и управления рисками возникновения киберугроз.




Решение интегрируется в системы управления нефтеперерабатывающих предприятий, электростанций и других автоматизированных производств и призвано помочь справляться с киберугрозами, число которых стремительно растет в последнее время.

http://zlonov.ru/catalog/honeywell-industrial-cyber-security-risk-manager/

# ViPNet ICM

- Индустриальный криптографический модуль – средство защиты данных для интеграции в автоматизированные системы управления (АСУ) и системы межмашинного взаимодействия (M2M)

- Разработчик: ИнфоТеКС

- Проходит сертификацию в ФСБ России на соответствие требованиям СКЗИ класса КС3

http://zlonov.ru/catalog/vipnet-icm/

# АПК «Свиток»

- Средство криптографической защиты информации, предназначенное для обеспечения защиты информации, передаваемой от удаленных IP-источников

- Разработчик: ГК МАСКОМ.

- АПК «Свиток» представлен на сертификацию как СКЗИ класса КС2.

http://zlonov.ru/catalog/апк-свиток/

# СТРАЖ-ЧПУ

- Программный комплекс «СТРАЖ-ЧПУ» предназначен для защиты геометри ческой и технологической информации, содержащейся в управляющий программе от возможных угроз НСД, а также преобразования отдельных параметров исходной управляющей программы таким образом, что ее несанкционированное использование, при дальнейшей установке и запуске на оборудовании с ЧПУ, становится невозможным.

- Разработчик: Станкоинформзащита.

- Сертификат ФСТЭК №2278 от 16.02.11 (до 16.02.14) на Программное обеспечение «СТРАЖ-ЧПУ» — по 3 уровню НДВ и ТУ.

http://zlonov.ru/catalog/страж-чпу/

# Продолжение следует...

Постоянная ссылка на актуальную версию данной презентации:
**http://bit.ly/zlonov-ics-security**

# Дополнительная информация

- Раздел ИБ АСУ ТП на ZLONOV.ru
  - http://zlonov.ru/ics-security/
- Инциденты ИБ АСУ ТП
  - http://zlonov.ru/category/incidents/
- Уязвимости ИБ АСУ ТП
  - http://zlonov.ru/category/vulnerabilities/
- Аналитика ИБ АСУ ТП
  - http://zlonov.ru/category/analytics/

# Спасибо!

Алексей Комаров
ZLONOV.ru
@zlonov

Узнать больше об услугах и решениях по безопасности промышленных систем автоматизации и управления

Уральский Центр Систем Безопасности
Тел.: +7 (343) 379-98-34
E-mail: info@ussc.ru
www.USSC.ru