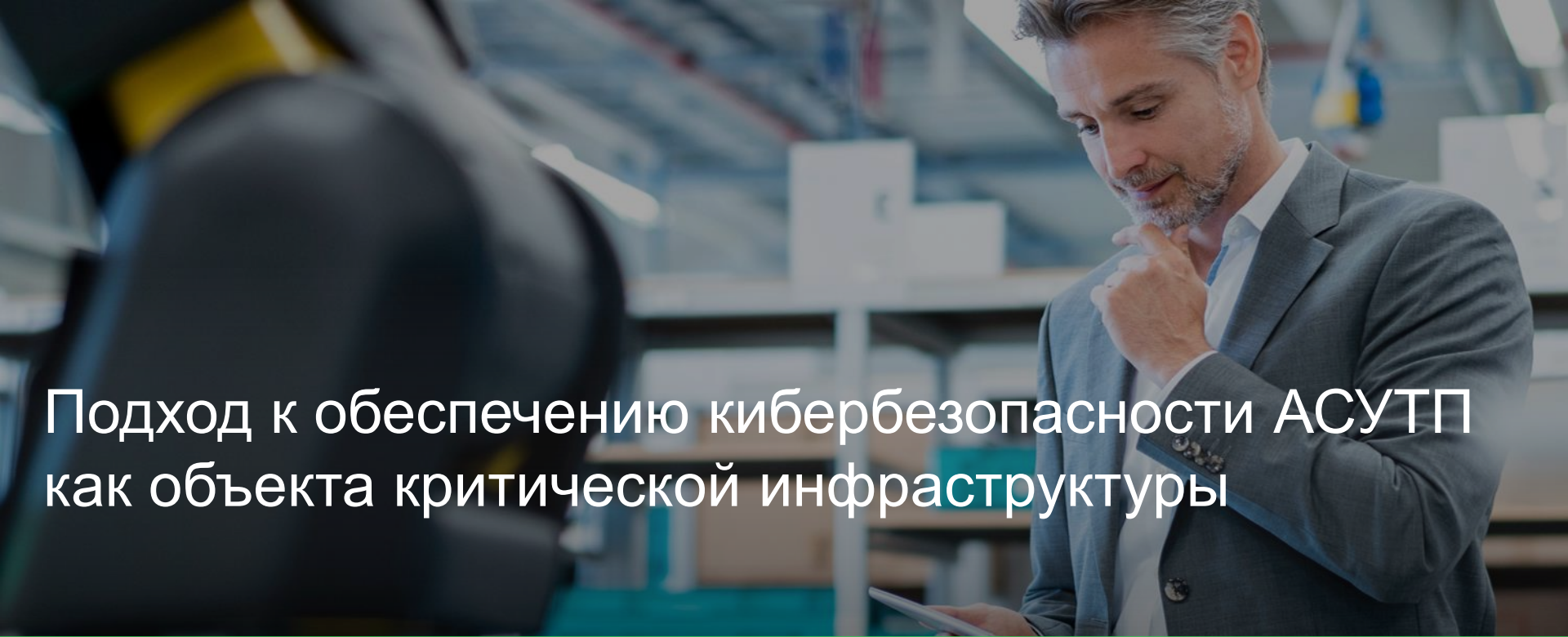


Подход к обеспечению кибербезопасности АСУТП как объекта критической инфраструктуры

Андрей Иванов, технический консультант

Докладчик

Андрей Иванов

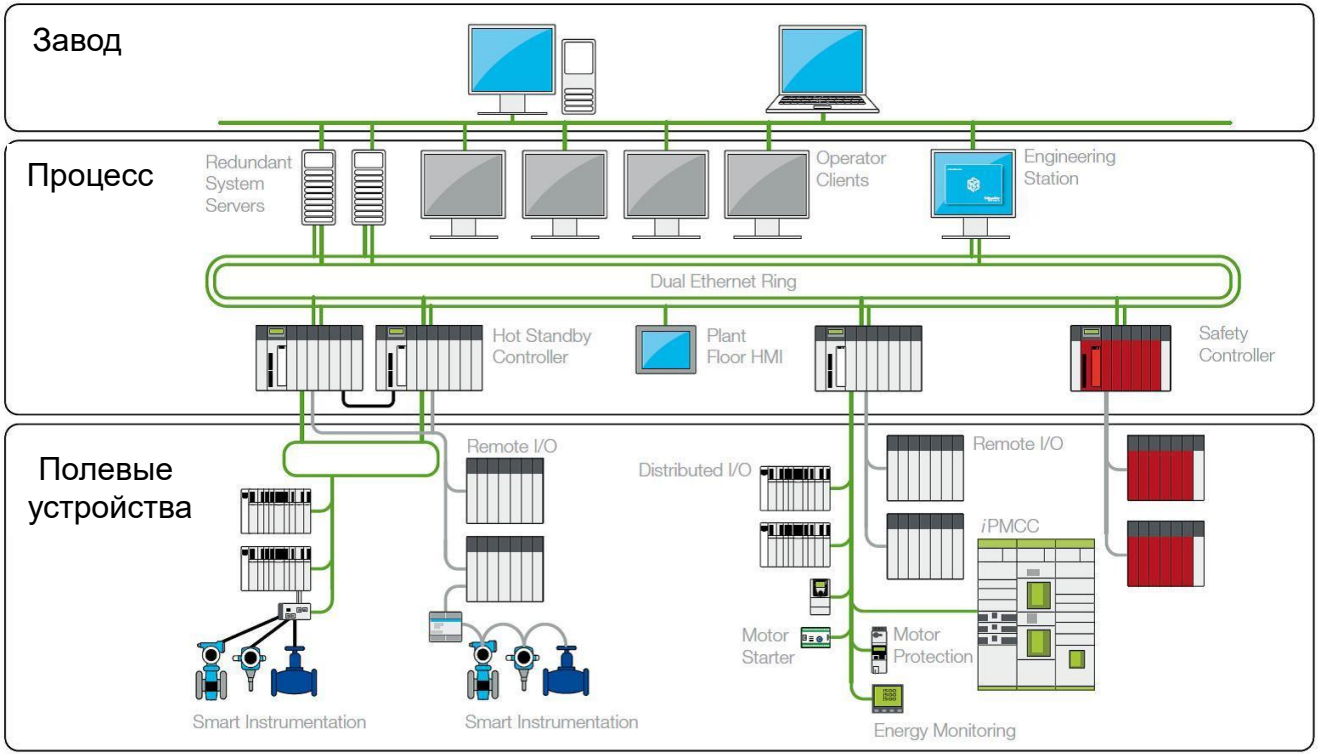
Технический консультант
по кибербезопасности
Schneider Electric

АСУТП - состав

Автоматизированная система управления технологическим процессом (АСУ ТП) — группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. Может иметь связь с более общей автоматизированной системой управления предприятием (АСУП).

https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%BC_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D0%BC

АСУТП - состав



АСУТП - состав

EcoStruxure™ Innovation At Every Level

Plant

Пищевая промышленность | **Водоснабжение** | **Металлургия и добыча полезных ископаемых и минералов** | **Нефть и газ**

Аналитические сервисы

EcoStruxure – промышленное ПО

Process Engineering
Planning & Scheduling
Operations Management

Enterprise Asset Performance Management
Information Management
Operations Control

EcoStruxure Asset Advisor

EcoStruxure Profit Advisor

EcoStruxure Control Advisor

EcoStruxure Resource Advisor

Управление в реальном времени

EcoStruxure – промышленная автоматизация
SCADA, Modicon, PES, Foxboro, Triconex, Telemetry

EcoStruxure Power Monitoring Expert

Подключенные продукты

Кибербезопасность

Облачные или локальные хранилища

Magelis

Foxboro

TeSys

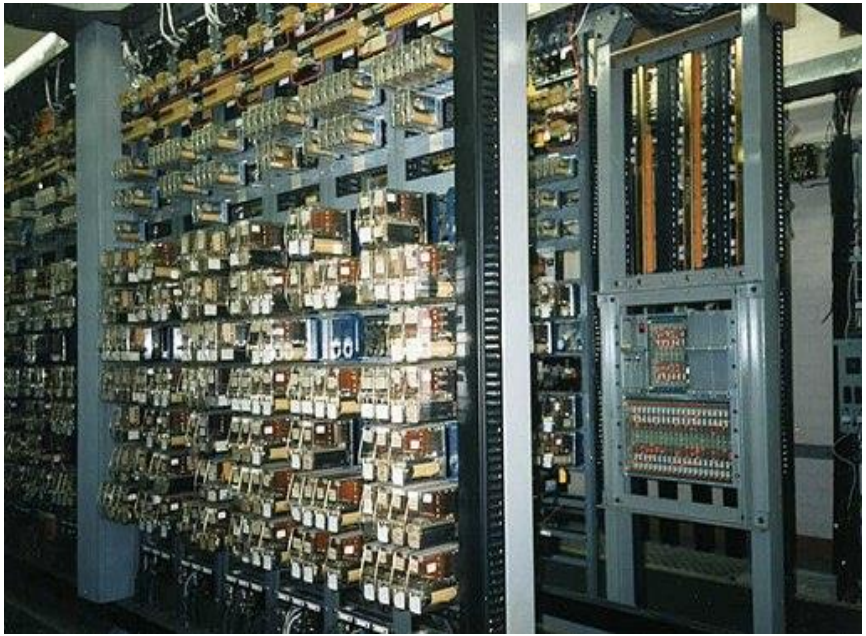
Sensors & RFID

Altivar

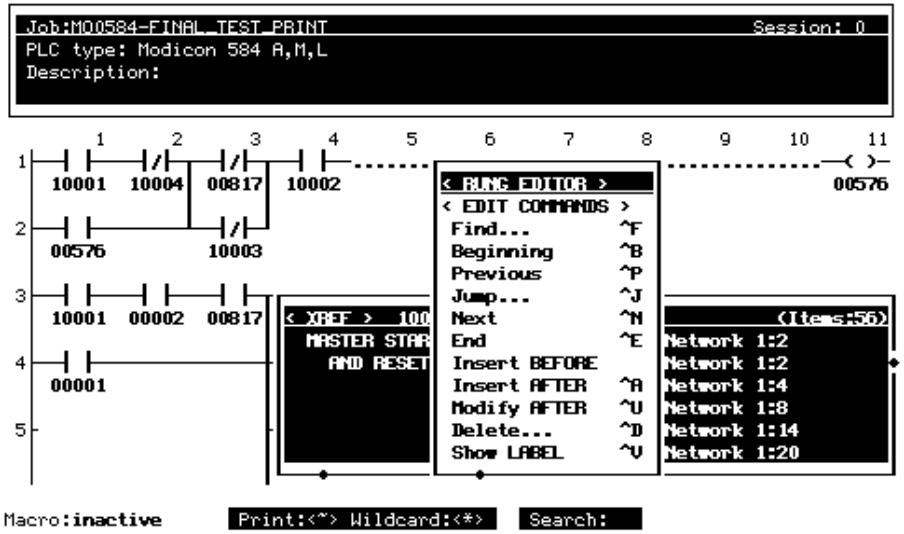
Intelligent Power & Motor Control Center

Life Is On Schneider Electric

Реле и программируемые логические контроллеры



Первый программируемый логический контроллер (ПЛК)



- 1968 - представлен первый ПЛК
- 1975 - представлен первый микропроцессорный ПЛК
- 1978 - представлена спецификация протокола ModBus

Информационные технологии

- Термин «информационные технологии» в его современном смысле впервые появился в статье 1958 года, опубликованной в Harvard Business Review; авторы Гарольд Дж. Ливитт и Томас Л. Уислер прокомментировали, что
- «The new technology does not yet have a single established name. We shall call it information technology.»

Информационная безопасность

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

About this paper

Manuscript received October 11, 1974; revised April 17. 1975.

Fourth ACM Symposium on Operating System Principles (October 1973).
Revised version in *Communications of the ACM* 17, 7 (July 1974).

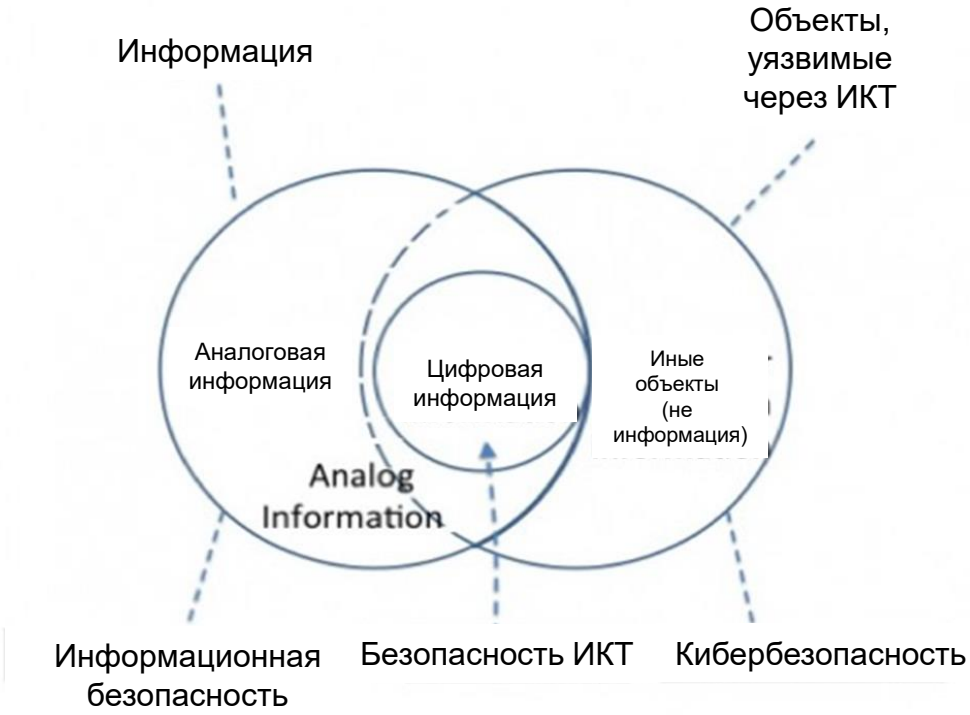
Original web version created by Norman Hardy.

Invited Paper

Abstract

This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection architectures and the relation between capability systems and access control list systems, and ends with a brief analysis of protected subsystems and protected objects. The reader who is dismayed by either the prerequisites or the level of detail in the second section may wish to skip to Section III, which reviews the state of the art and current research projects and provides suggestions for further reading.

Терминология



В России термин «кибербезопасность» не определен, поэтому может подразумеваться как информационная безопасность, так и безопасность ИКТ, и кибербезопасность (Cybersecurity)

ИКТ – Информационно-коммуникационные технологии

Кибер....

«Кибер» - это слово-приставка, означающая «связанный с компьютерами и интернетом». В английский язык слово «cyber» пришло из греческого, где «кибернетикой» называют науку об управлении и передаче информации среди людей и машин.

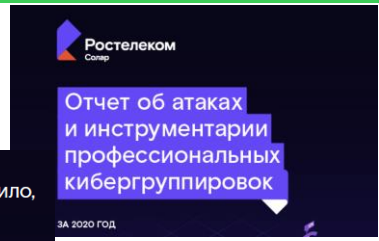
Примеры:
«Кибератака» - это попытка взломать или парализовать компьютерную сеть.
«Киберспорт» - это соревнования по компьютерным играм, имитирующим реальные спортивные состязания.
«Киберпространство» - это виртуальные просторы всемирной паутины, из которой не всегда бывает легко выбраться, даже если очень надо по нужде или спать.

http://www.helptofind.xyz/cyber.html#:~:text=%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%20(%D1%83%D0%B4%D0%B0%D1%80%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BD%D0%B0%20%C2%AB%D0%B8%C2%BB,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D1%81%D1%80%D0%B5%D0%B4%D0%B8%20%D0%BB%D1%8E%D0%B4%D0%B5%D0%B9%20%D0%B8%20%D0%BC%D0%B0%D1%88%D0%B8%D0%BD.

Если почитать отчеты...

За 2020 год центр мониторинга и реагирования на кибератаки Solar JSOC зафиксировал более 200 хакерских атак со стороны профессиональных кибергруппировок, включая массовые попытки воздействия на целые отрасли и сектора экономики.

Примерно в 30 случаях за атаками стояли злоумышленники наиболее высокого уровня подготовки и квалификации – кибернаемники и кибергруппировки, преследующие интересы иностранных государств. В числе наиболее частых целей – объекты критической информационной инфраструктуры России.



Кибернаемники и проправительственные группировки в своих атаках, как правило, были нацелены на получение доступа к следующим узлам инфраструктуры:

80% АРМ ИТ-администраторов с высоким уровнем привилегий

75% Системы ИТ-управления инфраструктурой (серверы инвентаризации, обновления, управления конфигурацией и т. д.) для возможности получения наиболее полной информации об инфраструктуре

65% Прикладные системы, обеспечивающие документооборот для более типизированной монетизации за счет платежной информации или вирусов-шифровальщиков

50% Системы ИБ-управления инфраструктурой (антивирусное ПО, системы защиты от несанкционированного доступа, сканеры уязвимостей) для получения возможности централизованного управления парком серверов и рабочих станций с высоким уровнем привилегий

40% Серверы и технологические рабочие станции управления технологическими процессами

Если почитать отчеты...

Оглавление

Life Is On Schneider Electric

Состав комплексного решения

Доступ

- Авторизация, аутентификация и аккаунтинг
- Многофакторная аутентификация
- Сегментировани е сети
- Безопасный удаленный доступ
- Физическая безопасность

Защита

- Защита конечных узлов (Anti Virus, Anti Malware)
- DLP, HIPS, белые списки
- Управление устройствами
- Доверенная загрузка/управление процессами
- Patch Management

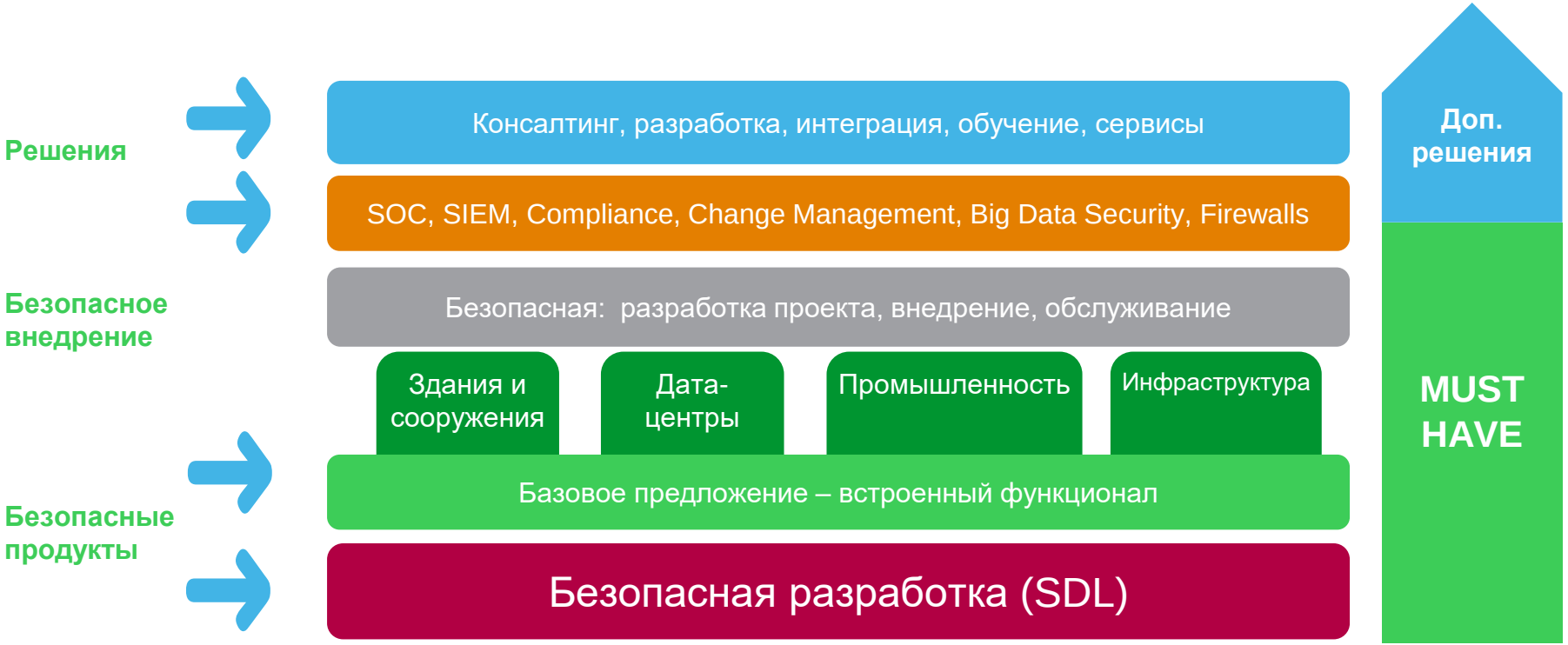
Обнаружение

- Security Information & Event Management (SIEM)
- Системы мониторинга сети
- Обнаружение аномалий
- СОВ/СПВ (NIDS/NIPS)
- SOC (центры управления)

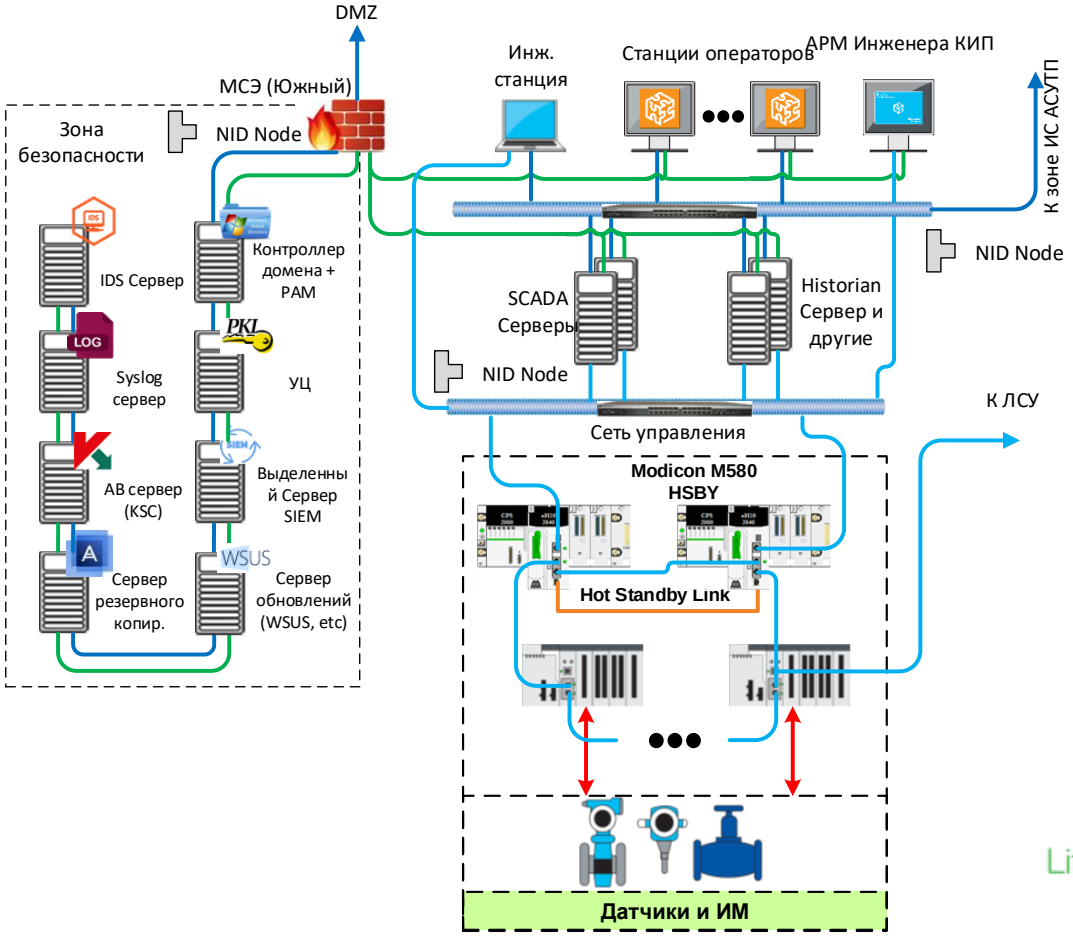
Реагирование

- Резервное копирование и восстановление
- Forensics (расследование киберпреступлений)
- Системы реагирования на инциденты

Комплексный подход



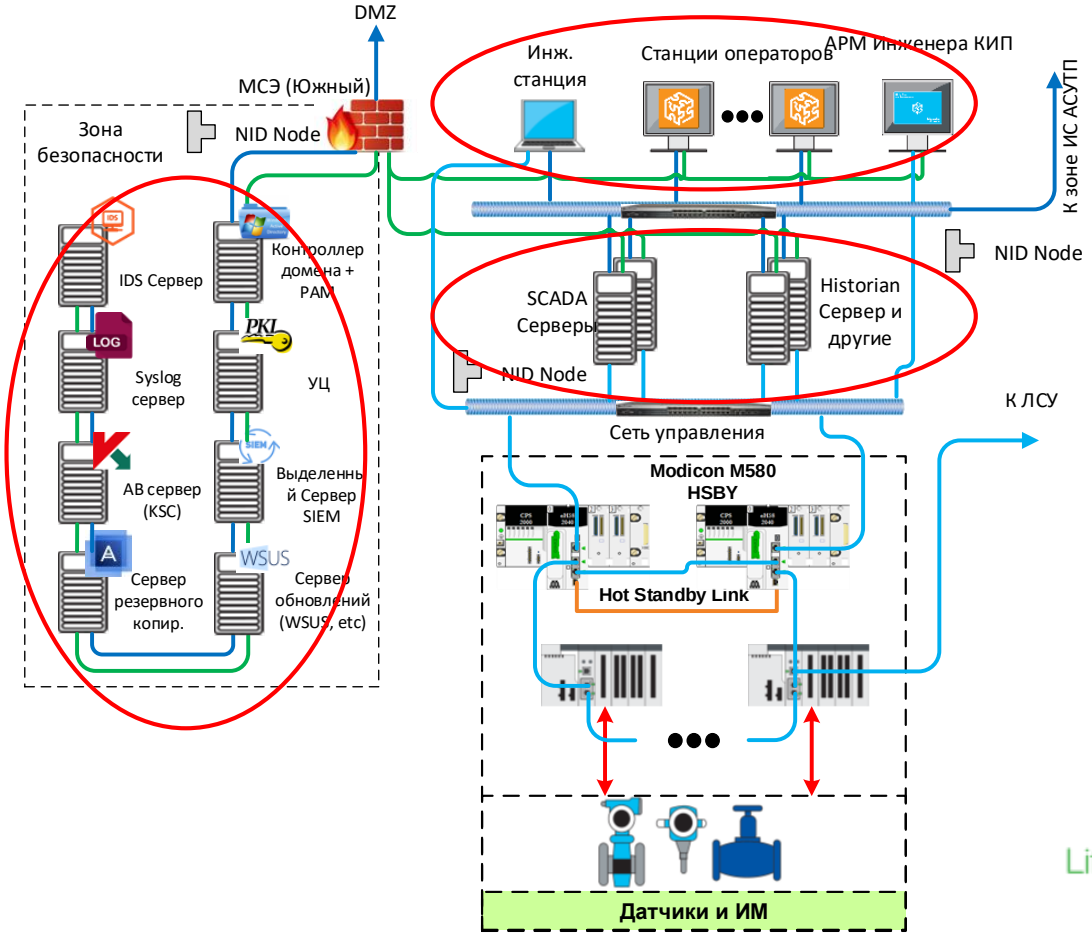
Как защитить АСУТП?



Life Is On Schneider Electric

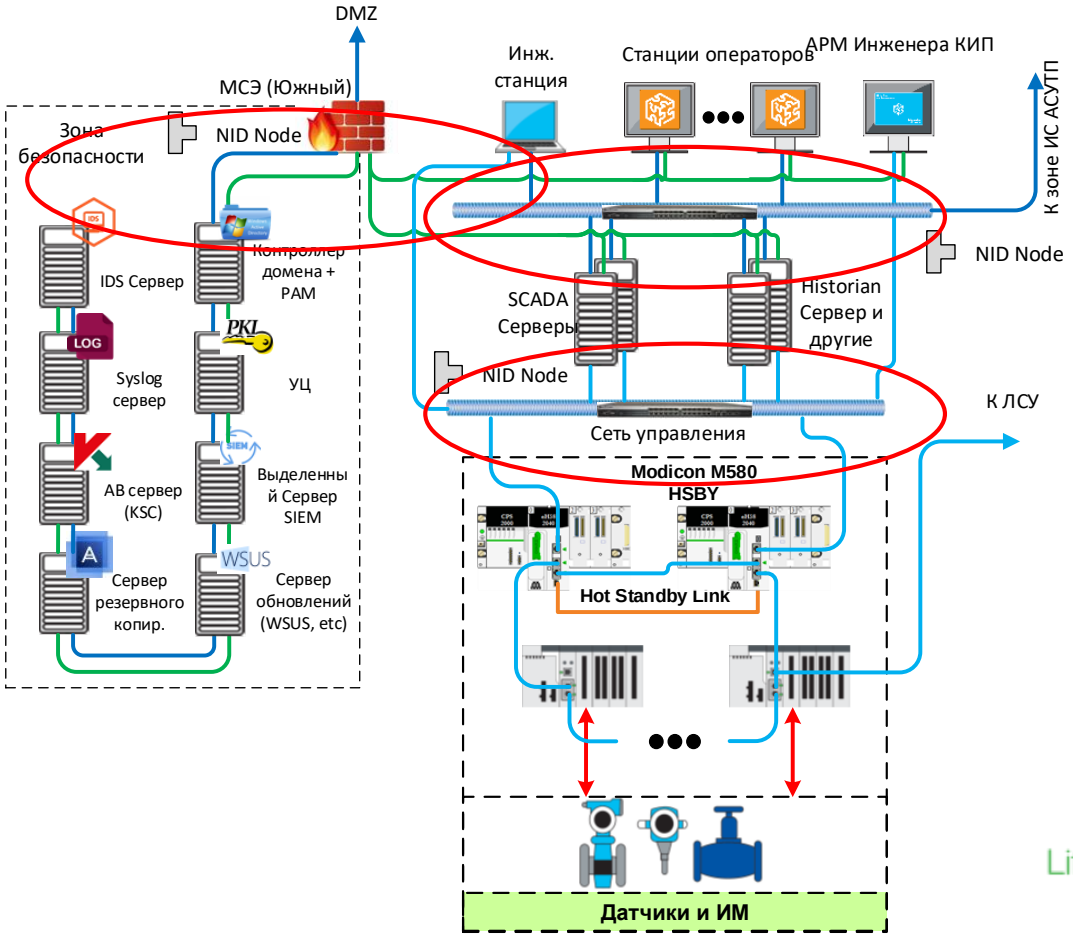
Архитектура защищенной АСУТП

Защита АРМ и серверов:
- Антивирусное ПО
- Контроль запуска и целостности приложений
- Контроль подключаемых устройств
- Авторизация и аутентификация
- Логирование событий безопасности
- Оптимальная настройка служб и сервисов
- Регулярные обновления АВ баз и ПО
- Другие меры



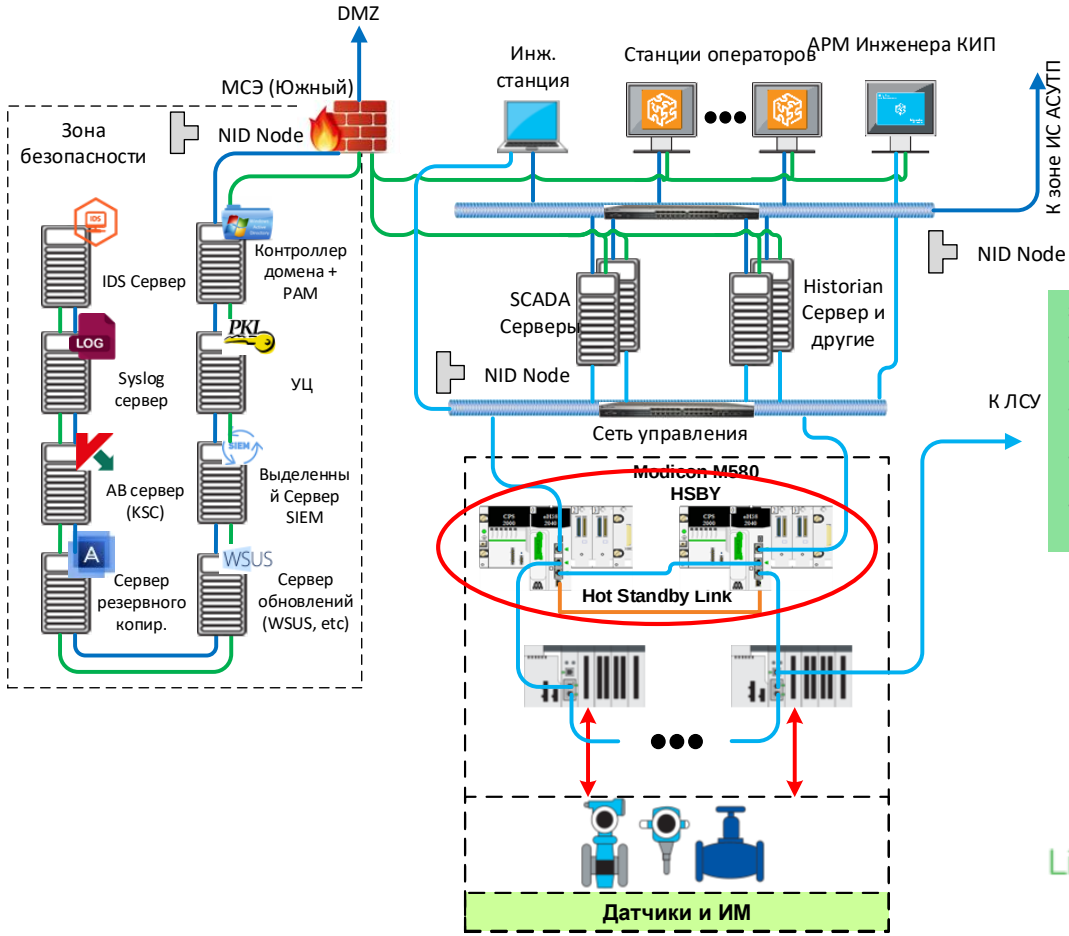
Life Is On Schneider Electric

Архитектура защищенной АСУТП



Защита сетей:
- Разделение сетей и их сегментирование
- Мониторинг и анализ трафика
- Конфигурация сетевого оборудования
- Авторизация и аутентификация
- Логирование событий безопасности
- Регулярные обновления прошивок
- Другие меры

Архитектура защищенной АСУТП



Защита ПЛК:
- Настройка списков подключений
- Логирование событий безопасности
- Отключение неиспользуемых сервисов (FTP/TFTP и т.д.)
- Установка сложных паролей и многоуровневого доступа
- Контроль целостности прошивки

Кибербезопасность в решениях

Решение предполагает централизованное обеспечение информационной защиты и включает в себя следующие основные элементы:

- Антивирусное сканирование и обновление файлов антивирусных данных,
- Обнаружение несанкционированного вторжения (HIDS),
- Централизованная платформа управления безопасностью,
- Система предотвращения потери данных (DLP) - опционально
- Сервис администрирования Windows - доменных сетей, Microsoft Active Directory (A/D),
- Процедура повышения «прочности» операционной системы (Hardening OS),
- Политика «белых» списков используемого программного обеспечения (Whitelisting),
- Инструментарий для оценки состояния станций Foxboro (SAT),
- Система резервного хранения и восстановления.

Типовые требования

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/Security-IRD/Security-IRD.html

Основные тезисы

- Стандарты и руководящие принципы являются важной основой, но они не описывают, как обеспечить безопасность конкретных систем. Они должны быть использованы в качестве основы и адаптированы специально для нужд бизнеса.
- Наилучшая стратегия снижения риска - это использование системы, где все компоненты спроектированы, протестированы, проверены и сертифицированы, где это возможно, принимая во внимание сквозную кибер и физическую безопасность.
- Безопасность - это непрерывный процесс, а не единичное, изолированное усилие. Каждый этап проектирования должен включать в себя набор шагов безопасности, которые необходимо выполнить, интегрируя безопасность непосредственно в решение на протяжении его жизненного цикла. Чтобы быть наиболее эффективным, безопасность должна быть включена в проект жизненного цикла с самого начала.
- **Инциденты безопасности неизбежно произойдут.** Наличие хорошо документированного набора процессов и процедур реагирования на инциденты имеет важное значение. Это не только скорость, с которой обнаруживается угроза, но и скорость, с которой угрозы безопасности смягчаются и устраняются, что контролирует потенциальные риски и возникающие расходы.

Критическая инфраструктура в РФ

- 187 ФЗ - вступил в действие 1 января 2018 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

187-ФЗ. Статья 2. Основные понятия.

Объекты и субъекты

7) объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в …

187-ФЗ. Статья 2. Основные понятия.

К КИИ относятся системы, функционирующие в сферах:

Здравоохранение

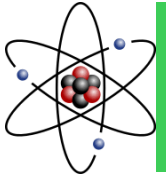
Наука

Транспорт

Связь

Банковская и иные сферы финансового рынка

Топливно-энергетический комплекс



Атомная энергия

Оборонная промышленность

Ракетно-космическая промышленность

Горнодобывающая промышленность

Металлургическая промышленность

Химическая промышленность

Требования к организационным и техническим мерам

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" марта 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований
по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) П Р И К А З Ы В А Ю:

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

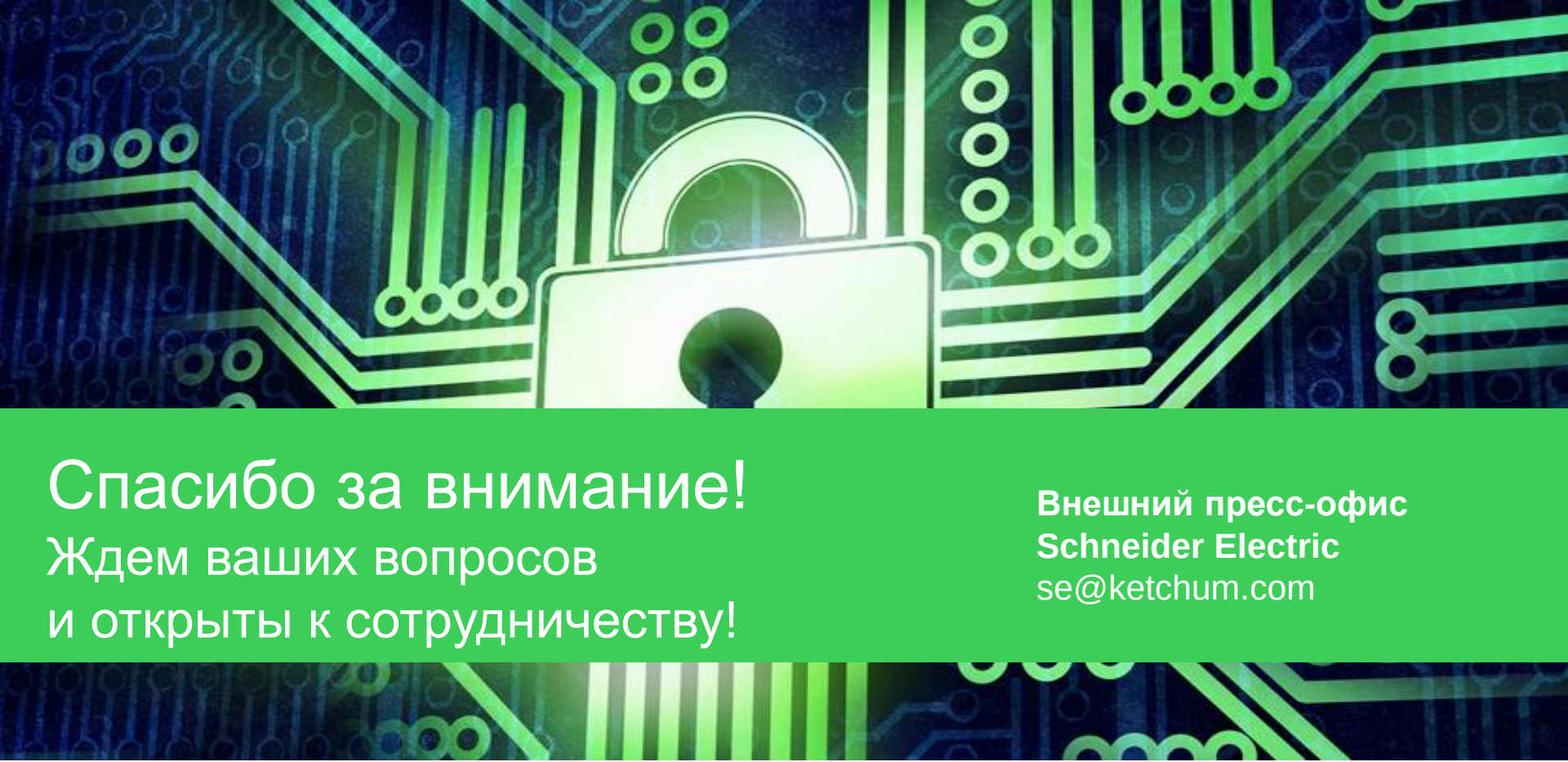
Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение:
Состав мер по обеспечению безопасности для значимых объектов соответствующей категории

Пример требований

VI. Антивирусная защита (АВЗ)				
АВЗ.0	Разработка политики антивирусной защиты	+	+	+
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
АВЗ.5	Использование средств антивирусной защиты различных производителей			+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+



Спасибо за внимание!

Ждем ваших вопросов
и открыты к сотрудничеству!

Внешний пресс-офис
Schneider Electric
se@ketchum.com

Life Is On | Schneider Electric