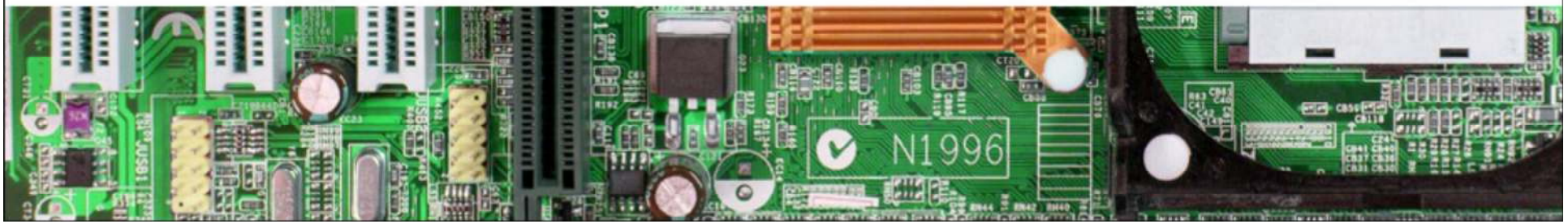
Обеспечение безопасности критически важных информационных систем в вопросах и ответах

Андрей Рыбин

Руководитель комплексных проектов

Global Trust Solutions

Продукты и услуги в области информационной безопасности



Какие информационные системы относятся к критически важным?

Признаки критически важных информационных систем:

- **Управляющие потенциально опасными производствами или технологическими процессами**
- **Обеспечивающие функционирование опасных объектов, осуществляющих управление (или информационное обеспечение управления) чувствительными (важными) для государства процессами**

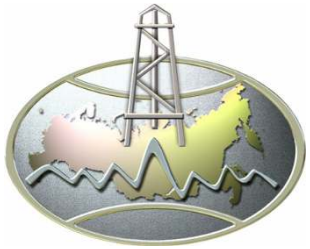
Виды критически важных информационных систем:

- **Множество различных классов информационных, автоматизированных систем и информационно-телекоммуникационных сетей (системы предупреждения и ликвидации чрезвычайных ситуаций, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и другие системы и сети)**
- **Автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды**

Global Trust Solutions

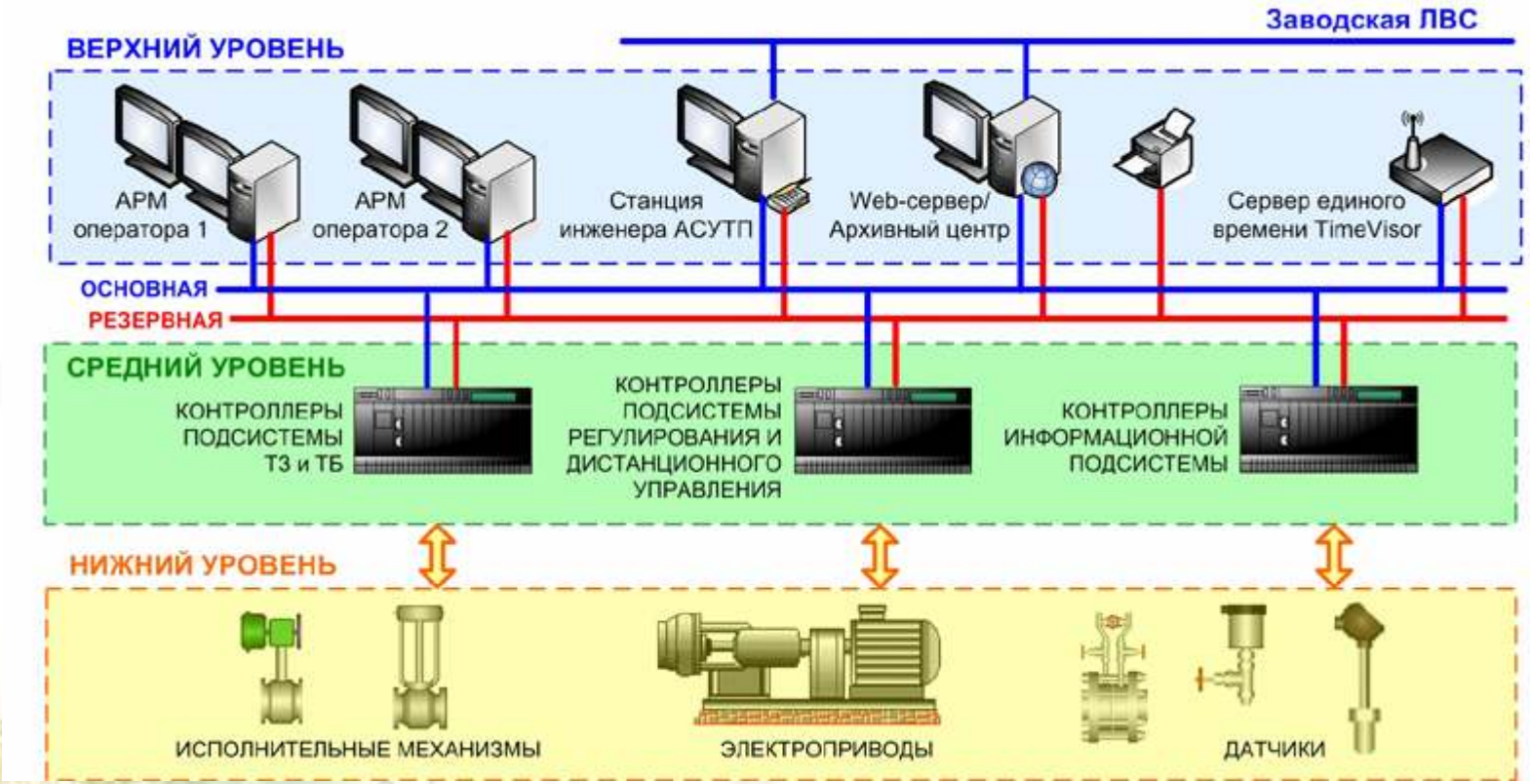
В каких отраслях присутствуют критически важные системы?

- Электроэнергетика
- Нефть и газ
- ЖКХ
- Транспорт
- Химическое производство
- Фармацевтика
- Целлюлозно-бумажное производство
- Пищевая промышленность
- Высокотехнологичное производство



Global Trust Solutions

Архтитектура промышленных систем



Global Trust Solutions

В чем особенность функционирования критически важных систем?

- **Круглосуточная бесперебойная работа в режиме реального времени.**
- **Недопустимость незапланированных прерываний работы системы.**
- **Детерминированность времени отклика системы.**
- **Критическая инфраструктура (пожаро- и взрывоопасные объекты, угроза жизни и здоровью людей, ущерб окружающей среде, оборудованию, системам жизнеобеспечения).**
- **Приоритеты обеспечения ИБ в порядке убывания: Доступность-Целостность-Конфиденциальность.**
- **Обеспечение ИБ центральных компонентов АСУТП также важно, как и обеспечение ИБ конечных устройств (распределенных компонентов).**

Global Trust Solutions

В чем особенность функционирования критически важных систем?

- **Применение ряда широко распространённых практик и продуктов в области обеспечения ИБ в АСУТП невозможно. Вместо этого должны использоваться компенсирующие механизмы контроля, включая физическое ограничение доступа к средствам автоматизации, видеонаблюдение с синхронной аудиозаписью, пассивный мониторинг действий пользователей.**
- **Техническая поддержка, обслуживание и эксплуатация осуществляется различными подрядными организациями, специализирующими в области промышленной автоматики и не всегда обладающими необходимой квалификацией в области обеспечения ИБ.**
- **Технологии, используемые в АСУТП, во многих случаях, разрабатываются для очень узкой и специфичной области, поэтому срок жизни таких технологий составляет, в среднем, от 15 до 20 лет. Отсюда наличие устаревшего ПО, оборудования и протоколов обмена данными, не поддерживающих функции по обеспечению ИБ.**

Global Trust Solutions

Какие существуют требования по информационной безопасности ключевых систем?

ФСТЭК России издан приказ от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах …».

ФСТЭК России разработана и утверждена следующая система методических документов:

- **Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры**
- **Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры**
- **Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры**
- **Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры**
- **Положение о реестре ключевых систем информационной инфраструктуры**

Global Trust Solutions

Какие дополнительные меры безопасности вводятся в отношении КСИИ?

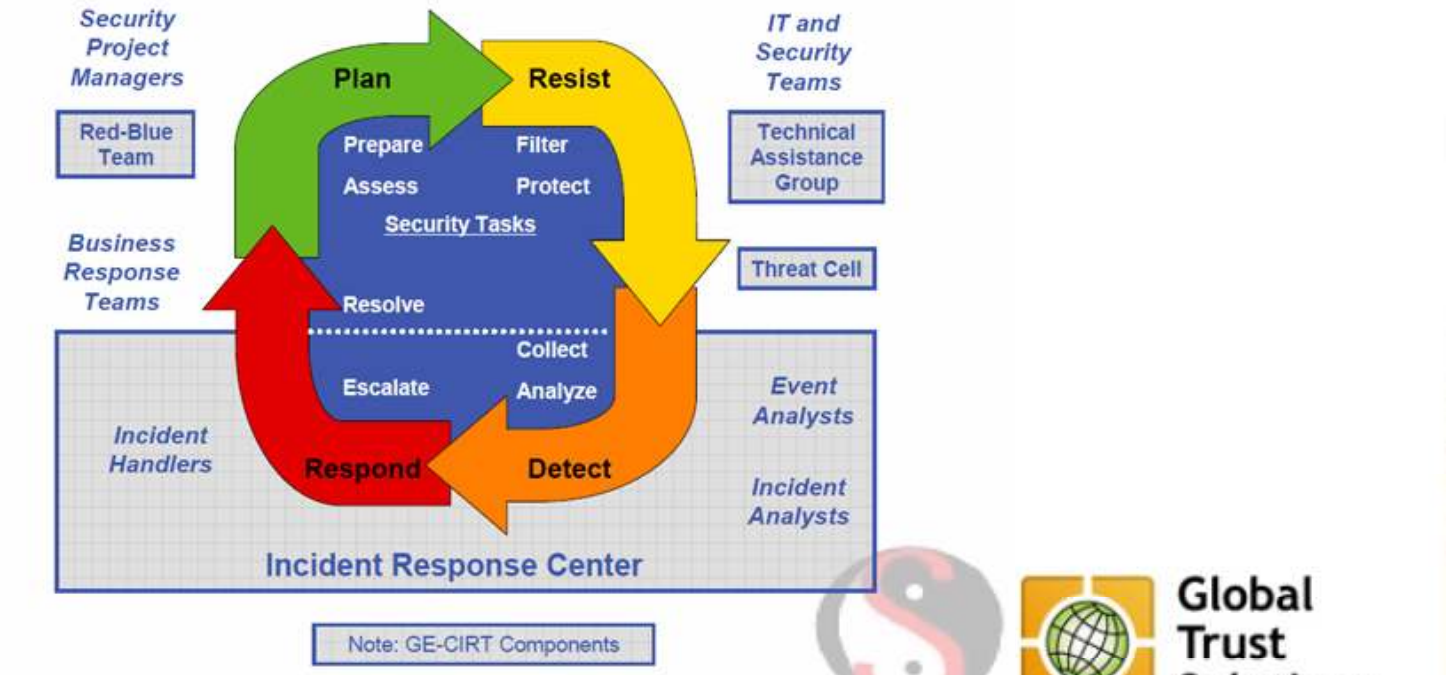
В дополнение к мерам безопасности, установленным в отношении Государственных информационных систем (Приказ ФСТЭК России №17) и информационных систем, обрабатывающих персональные данные (Приказ ФСТЭК России №21), вводятся следующие меры:

- **Обеспечение безопасной разработки прикладного (специального) программного обеспечения**
- **Управление обновлениями программного обеспечения**
- **Планирование мероприятий по обеспечению защиты информации**
- **Обеспечение действий в нештатных (непредвиденных) ситуациях**
- **Информирование и обучение пользователей**
- **Анализ угроз безопасности информации и рисков от их реализации**

Global Trust Solutions

Какие дополнительные меры безопасности вводятся в отношении критически важных информационных систем?

- **Регламентация и контроль технического обслуживания**
- **Выявление инцидентов и реагирование на них**
- **Управление конфигурацией автоматизированной системы управления и ее системы защиты**



Source: Richard Bejtlich, *CIRT-Level Response to Advanced Persistent Threat*

Global Trust Solutions

В чем отличие в подходе к информационной безопасности критически важных систем?

Требование	Офисная ИС	Критически важная ИС
Производительность	Высокая	Средняя
Доступность	Средняя (допустима перезагрузка системы)	Высокая Обязателен резерв
Управление рисками	Риски определяет и управляет ими бизнес	Управляются бизнесом и государством (экология, жизнь людей и пр.)
Целостность	Определяется бизнесом	Высокая (не допускается разрушение или потеря данных)
Конфиденциальность	Определяется бизнесом	Высокая (охраняемая законом информация)

Global Trust Solutions

Какие возможны инциденты с критически важными системами?

- Вторжение в систему управления энергоснабжением

  26.09.2012 г. хакеры вторглись в систему управления энергоснабжением, осуществляющую мониторинг сетевых объектов в США, Канаде и Испании и получили полный контроль над ней

- Вторжение в систему управления зданием

  В январе 2012 г. хакеры проникли в систему управления зданием State Crime Lab Building и выложили видео об успешной атаке в YouTube

- Прерывание бизнеса US Power Utility

  В октябре 2012 г. компьютерная сеть US Power Utility была атакована вирусом Mariposa, который был занесен с flash-карты при установке новой версии программного обеспечения подрядчиком. Простой завода составил 3 недели

- Атака на внешние интернет-сервисы поставщика газа

  С 16.01.2013 г. и по 08.03.2013 г. продолжались попытки получить доступ из сети Интернет во внутреннюю сеть газораспределительной станции с помощью метода Brute Force

- Червь Stuxnet

  В июле 2010 года был обнаружен специально созданный компьютерный червь для Microsoft Windows, целью которого были критически важные системы

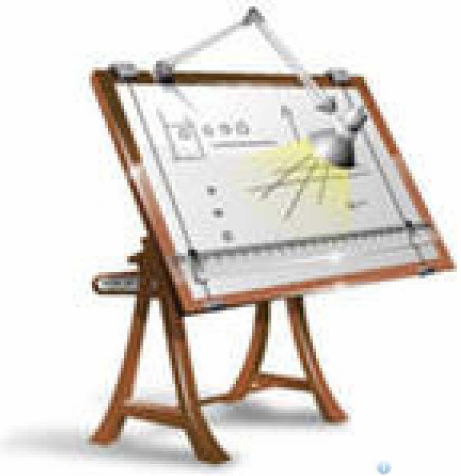
Global Trust Solutions

Как защитить свою ключевую систему?

Разработка Системы Обеспечения Информационной безопасности КСИИ осуществляется в соответствии с требованиями действующего законодательства, ГОСТов и нормативной базы РФ в области защиты информации.

Разработка СОБИ КСИИ включает в себя следующие этапы:

- **Предпроектный этап**
- **Проектирование СОБИ КСИИ**
- **Разработка организационно-распорядительных документов по ОБИ в КСИИ**
- **Ввод в действие**



Global Trust Solutions

Как защитить свою ключевую систему?

На предпроектном этапе:

- определяются конфигурация и топология КСИИ
- определяется (уточняется) уровень важности КСИИ
- определяется состав и содержание критически важной информации применительно к
- данной КСИИ
- определяются аппаратные и программные средства КСИИ
- определяется степень участия должностных лиц организации в обработке (обсуждении,
- передаче, хранении) критически важной информации, характер их взаимодействия между собой и со службой безопасности
- определяются (уточняются) угрозы безопасности информации, связанные с НСД к
- защищаемой критически важной информации и несанкционированными воздействиями на нее, формируется модель вероятного нарушителя применительно к конкретным условиям функционирования КСИИ
- определяются мероприятия по обеспечению конфиденциальности критически важной
- информации о КСИИ на этапе проектирования и создания СОБИ КСИИ

Global Trust Solutions

Как защитить свою ключевую систему?

На этапе проектирования:

- **осуществляется разработка проектных решений по СОБИ КСИИ и её частям**
- **создается технический (технорабочий) проект СОБИ КСИИ в соответствии с ГОСТом 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированную систему. Виды, комплектность и обозначение документов при создании автоматизированной системы»**
- **создается эксплуатационная документация, включающая в себя технический паспорт на СОБИ КСИИ, а также инструкции и руководства по эксплуатации технических и программных средств СОБИ для пользователей, администраторов системы и сотрудников службы безопасности**

На этапе разработки комплекса внутренних организационно-распорядительных документов:

- **разрабатываются и утверждаются такие документы, как положения, планы, методика**

Global Trust Solutions

Как защитить свою ключевую систему?

На этапе ввода СОБИ КСИИ в действие осуществляется :

- **поставка оборудования и программного обеспечения СОБИ КСИИ согласно закупочной спецификации**
- **монтаж оборудования**
- **установка и настройка ПО в соответствии с проектными решениями**
- **предварительные испытания и ввод СОБИ КСИИ в опытную эксплуатацию**
- **опытная эксплуатация СОБИ в комплексе с другими техническими и программными средствами КСИИ в целях проверки их работоспособности в составе объекта**
- **информатизации и отработки технологического процесса обработки (передачи) информации, прежде всего критически важной информации КСИИ. При необходимости, по результатам опытной эксплуатации СОБИ КСИИ осуществляется ее доработка;**
- **приемо-сдаточные испытания СОБИ КСИИ по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком**
- **аттестация КСИИ по требованиям безопасности информации.**

Global Trust Solutions

Какая ответственность существует за нарушение требований безопасности информации в ключевых системах?

УК РФ «Статья 217.1. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса

… лишение свободы на срок до 7 лет

КОАП РФ «Статья 20.30. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса

если не содержит уголовно-наказуемого деяния

… штраф на граждан 3000-5000 рублей,

должностные лица 30000-50000 рублей

Global Trust Solutions

Почему Global Trust ?

СЕРИЯ КИ 0073 НОМЕР 003609

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1414 от 25 марта 2011 г.

Федеральная служба по техническому и экспортному контролю разрешает осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации

Лицензия предоставлена Обществу с ограниченной ответственностью «ГлобалТраст Солюшнс» (ООО «ГлобалТраст»)

ОГРН 1037727011156, ИНН 7727241354

Адрес места нахождения:
117216, г. Москва, ул. Грина, д. 4, кв. 21

Адрес места осуществления лицензируемой деятельности:
123317, г. Москва, Пресненская набережная, д.10, офис № 444, кампус 1

Лицензия предоставлена на срок до 25 марта 2016 г.

на основании приказа ФСТЭК России от 25 марта 2011 г. № 166

Первый заместитель директора

В.Селин

Специализация GlobalTrust:

- **аудит и оценка рисков ИБ**
- **разработка систем управления информационной безопасностью**

Статусы GlobalTrust:

- **лицензиат ФСТЭК России**
- **официальный дистрибьютор и бизнес-партнер Британского Института Стандартов (BSI)**
- **разработчик русских редакций международных стандартов в области защиты информации и обеспечения непрерывности бизнеса**

Проекты GlobalTrust по защите промышленных систем:

- **Разработка технических стандартов ИБ АСУ ТП для критически важных объектов ТНК-ВР**
- **Разработка СОБИ КСИИ для предприятий Росатома.**

Global Trust Solutions

Контактная информация

РЫБИН АНДРЕЙ АЛЕКСАНДРОВИЧ

Руководитель комплексных проектов

123317, Россия, г.Москва,
Пресненская наб., блок С,
Бизнес-центр «Регус»
www.globaltrust.ru

Тел.: +7 (925) 203-95-11
Моб.: +7 (964) 627-02-67
Факс.: +7 (495) 967-76-00
rybin@globaltrust.ru

Global Trust Solutions