Информзащита
Системный интегратор

ПРИМЕНЕНИЕ НОВЫХ ТРЕБОВАНИЙ К БЕЗОПАСНОСТИ АСУ НА ТРАНСПОРТЕ

Андрей Тимошенко
Начальник отдела консалтинга, CRISC

Информзащита
Системный интегратор

Цели и направления развития ОАО «РЖД»

- ✓ увеличение масштаба транспортного бизнеса
- ✓ повышение производственно-экономической эффективности
- ✓ повышение качества работы и безопасности перевозок
- ✓ развитие высокоскоростного движения

Информзащита
Системный интегратор

Последствия реализации угроз ИБ АСУ

- Снижение репутации
- Выход из строя транспортной инфраструктуры
- Ущерб экологии страны
- Ущерб экономике страны
- Гибель людей

Информзащита
Системный интегратор

Зарубежный опыт

ISA (Комитет ISA99), Международное общество автоматизации (Комитет по разработке стандартов безопасности АСУ ТП)

IEC, Международная электротехническая комиссия

NIST, Национальный институт стандартов и технологий США

- ✓ 13 документов серии ISA/IEC 62443;
- ✓ NIST SP800-82 «Guide to Industrial Control Systems (ICS) Security», June 2011

Информзащита
Системный интегратор

ФЗ «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Информзащита
Системный интегратор

Субъекты КИИ РФ должны создавать на своих объектах системы безопасности

Информзащита
Системный интегратор

Критерии отнесения к КИИ

критерий экономической значимости

критерий экологической значимости

критерий значимости для обеспечения обороноспособности

критерий значимости для национальной безопасности

критерий социальной значимости

Информзащита
Системный интегратор

Категории опасности КИИ

объекты КИИ РФ высокой категории опасности

объекты КИИ РФ средней категории опасности

объекты КИИ РФ низкой категории опасности

Объекты КИИ подлежат включению в реестры объектов КИИ

Информзащита
Системный интегратор

Требования к безопасности КИИ

организационные вопросы безопасности

требования к персоналу

требования к защите от вредоносного ПО и от компьютерных атак

требования безопасности при взаимодействии с сетями связи общего пользования

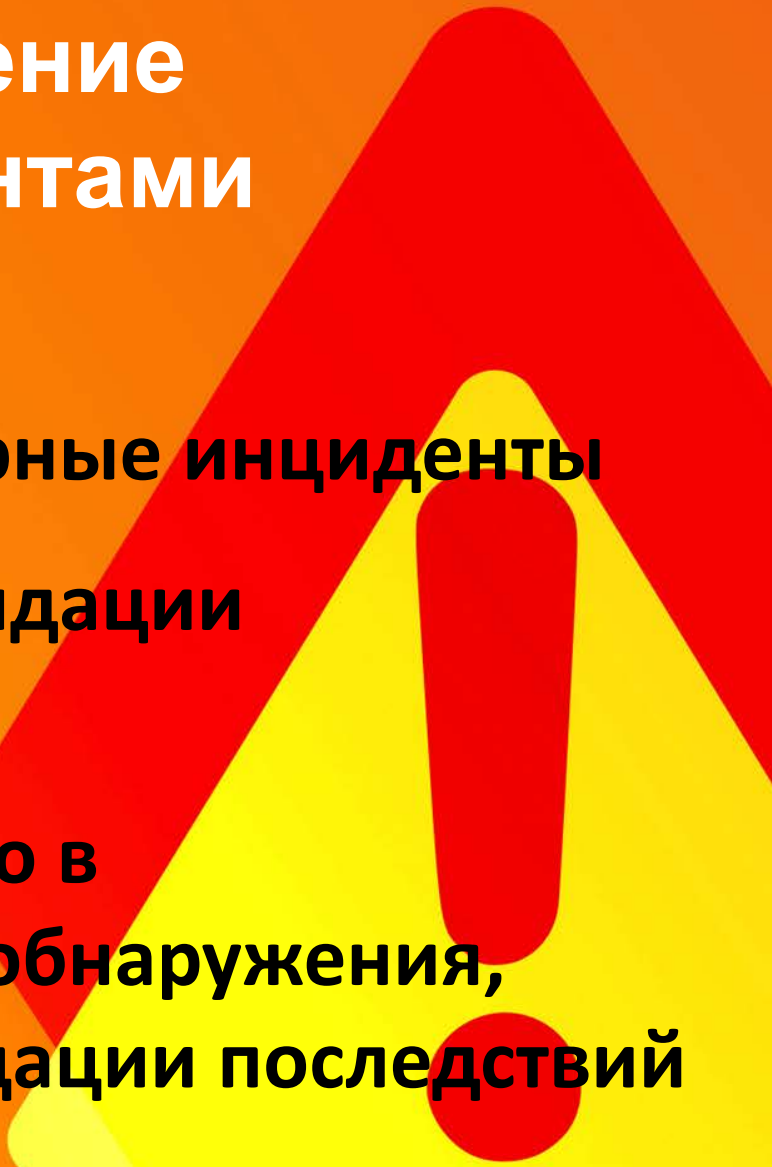
требования к обеспечению безопасности ИТ в ходе эксплуатации информационно-телекоммуникационных систем

Информзащита
Системный интегратор

Управление инцидентами

Субъект КИИ обязан

- ✓ **Реагировать на компьютерные инциденты**
- ✓ **Принимать меры по ликвидации последствий**
- ✓ **Представлять информацию в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак**
- ✓ **Оказывать содействие регулятору**



Информзащита
Системный интегратор

Информационный комплекс ОАО «РЖД»

- более 60 мейнфреймов
- более 300 корпоративных серверов
- около 4 000 информационных систем
- более 200 000 ПК

Информзащита
Системный интегратор

Наш опыт

Создание АС обработки и корреляции событий ИБ в ОАО «РЖД» Санкт-Петербургский ИВЦ

- интеграция с 13 ИС и системами защиты информации
- разработана логика и реализовано более 100 правил, отчетов и графических представлений для обнаружения инцидентов ИБ
- выполнено в кратчайшие сроки

Информзащита
Системный интегратор

Методические документы по защите АСУ ТП

Требования к обеспечению защиты информации в автоматизированных системах 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

Приказ ФСТЭК (проект)

Информзащита
Системный интегратор

Жизненный цикл системы защиты АСУ

- Формирование требований к защите информации
- Разработка системы защиты АСУ
- Внедрение и ввод ее в действие
- Обеспечение защиты информации в ходе эксплуатации АСУ
- Обеспечение защиты информации при выводе из эксплуатации АСУ

Информзащита
Системный интегратор

Требования к безопасности АСУ ТП

Источники требований

- Классификация АСУ
- Угрозы безопасности информации
- Меры защиты информации для каждого класса защищенности АСУ

Информзащита
Системный интегратор

Классификация АСУ

Высокая степень возможного ущерба

- **Возникновение ЧС федерального или межрегионального характера или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности**

Информзащита
Системный интегратор

Классификация АСУ

Средняя степень возможного ущерба

- **ЧС регионального или межмуниципального характера или иные умеренные негативные последствия**

Информзащита
Системный интегратор

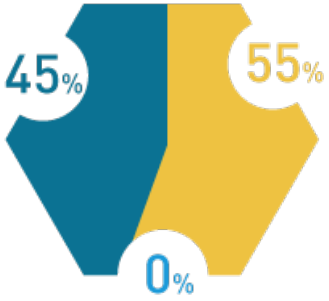
Классификация АСУ

Низкая степень возможного ущерба

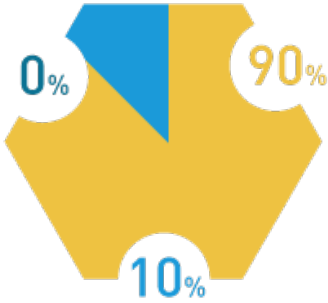
- **ЧС муниципального (локального) характера или возможны иные незначительные негативные последствия**

Информзащита
Системный интегратор

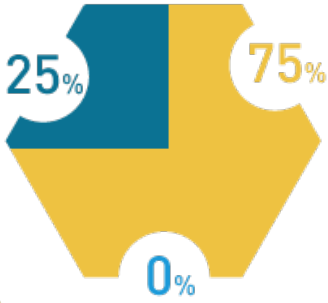
Статистика по выполнению требований ИБ в АСУ ТП



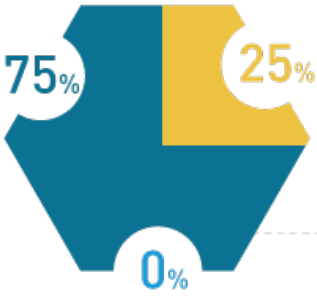
1. ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ В НЕПРЕДВИДЕННЫХ СИТУАЦИЯХ



3. ОЦЕНКА РИСКОВ



5. ИНФОРМИРОВАНИЕ И ОБУЧЕНИЕ ПО ВОПРОСАМ БЕЗОПАСНОСТИ



17. НАСТРОЙКИ ПРИМЕНЯЕМЫХ СРЕДСТВ ЗАЩИТЫ

2. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ АСУ ТП

НЕСООТВЕТСТВИЕ

УСЛОВНОЕ СООТВЕТСТВИЕ

СООТВЕТСТВИЕ

Информзащита
Системный интегратор

Типизация защищаемых объектов

Стандартизация требований по ИБ

Повышение осведомленности в ИБ

Проведение регулярных аудитов ИБ

Информзащита
Системный интегратор

БЛАГОДАРЮ ЗА ВНИМАНИЕ!