Особенности анализа кибербезопасности АСУ ТП на железнодорожном транспорте

Безродный Борис Федорович
Заместитель руководителя Центра кибербезопасности АО «НИИАС»
доктор технических наук, профессор

НИИАС

Возможные объекты кибератак на железнодорожном транспорте

Комплексные системы интервального регулирования движения поездов на основе использования радиосвязи

Возможно подавление радиоканала

Бортовые интеллектуальные системы безопасности локомотива

Возможно вмешательство в алгоритм работы

Комплексные системы контроля и управления движением, включающие бортовые системы локомотива

Возможно подавление радиоканала

Системы радиосвязи и радионавигации, обеспечивающие гарантированное перекрытие

Возможно подавление радиоканала

Микропроцессорные системы железнодорожной автоматики и телемеханики, электроснабжения

Искажение алгоритма

Системы автоматизации сортировочного процесса

Искажение алгоритма

Приказ ФСТЭК России N 31 от 14 марта 2014 г.

Технологические каналы связи и информационно-коммуникационные сети

Возможно подавление радиоканала, искажение алгоритма

Многообразие факторов обеспечения безопасности

Угрозы безопасности в системах управления движением поездов

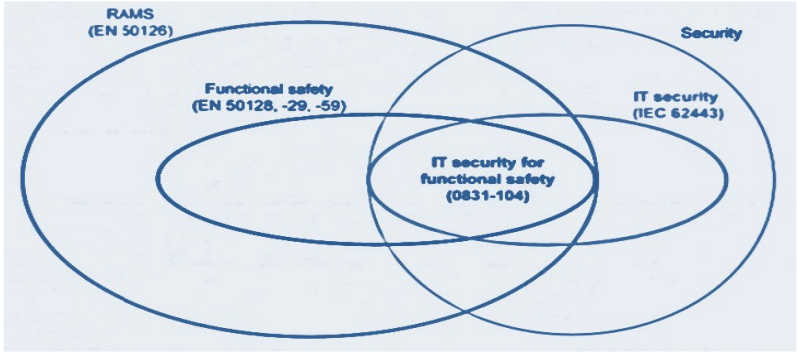
Киберзащищенность

Киберзащищенность – способность системы управления успешно выполнять предусмотренные задачи при сохранении безопасного состояния в условиях кибератак и функциональных отказов, направленных на нанесение ущерба критически важным (государственный уровень) или потенциально опасным (отраслевой уровень) объектам.

1. Не существует абсолютной киберзащищенности (отказоустойчивости, отказобезопасности) систем управления.
2. Чем более сложная система, чем больше задач она выполняет, тем ниже ее киберзащищенность.
3. Необходимым условием повышения киберзащищенности системы является введение избыточности в сочетании с организацией эффективного контроля.
4. Киберзащищенность системы управления должна обеспечиваться на всех этапах жизненного цикла.
5. Уровень киберзащищенности системы ограничен экономическими рисками заказчика и эксплуатирующей организации.

Кибербезопасность цифровой железной дороги

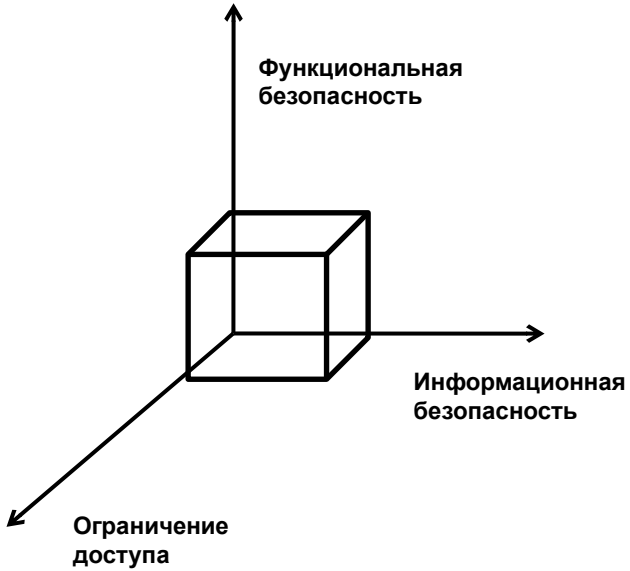
Подход, применяемый в ОАО «РЖД»



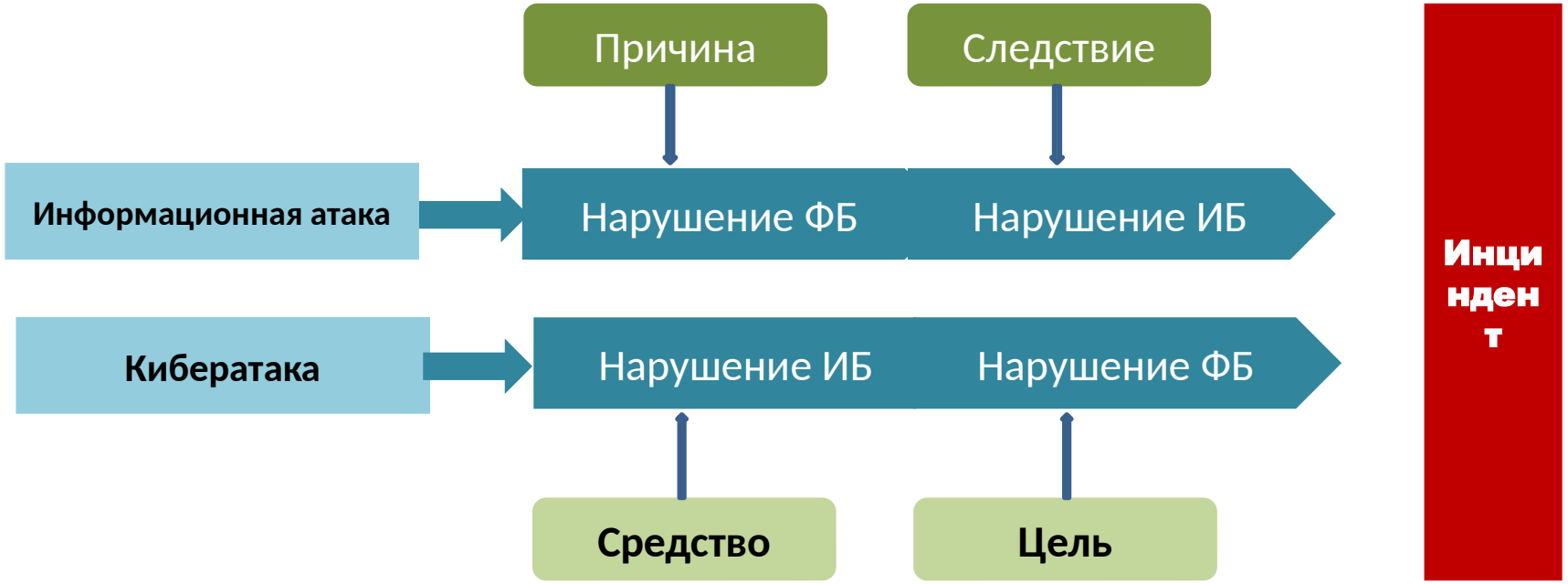
Европейский подход

Обеспечение кибербезопасности программно-аппаратных средств АСУ ТП на железнодорожном транспорте (СТО 02.049-2014)

Три основные методологические ошибки, допускаемые при рассмотрении вопросов кибербезопасности АСУ ТП



Отличие кибератаки от информационной атаки



ОЦЕНКА КИБЕРЗАЩИЩЕННОСТИ МПСУ ОАО «РЖД»

Нормативная база по кибербезопасности, применяемая в ОАО «РЖД»

СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия».
ГОСТ Р 54505-2011 «Безопасность функциональная. Политика, Программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта.
ГОСТ Р 54505-2011 «Безопасность функциональная. Управление рисками на железнодорожном транспорте». А так же
ГОСТ Р 56205-2014, ГОСТ Р 5498-2015,
ГОСТ Р МЭК 62443-2-1-2015 (части 1,2,3)
Приказ ФСТЭК РФ от 14.03.2014 № 31

Методические документы, разработанные Центром кибербезопасности АО«НИИАС»

- **Термины и определения** в области кибербезопасности микропроцессорных систем управления движением поездов, локомотивами и электроснабжением (утвержден 13.01.2016)
- **Регламент проведения аудита** состояния кибербезопасности микропроцессорных систем управления движением поездов, локомотивами и электроснабжением (утвержден 13.01.2016)
- **Требования по кибербезопасности** микропроцессорных систем управления локомотивами (утвержден 10.12.2016)
- **Правила анализа уязвимостей и угроз** кибербезопасности микропроцессорных систем управления движением поездов, локомотивами и электроснабжением и разработки базовых угроз на основании результатов анализа (утвержден 13.01.2016)
- **Требования по кибербезопасности** микропроцессорных систем управления движением поездов (утвержден 13.01.2016)
- **Правила классификации по требованиям кибербезопасности** систем управления движением поездов, локомотивами и электроснабжением (утвержден 13.01.2016)
- **Требования по кибербезопасности** микропроцессорных систем управления электроснабжением (утвержден 29.10.2015)
- **Регламент подтверждения соответствия требованиям** по кибербезопасности микропроцессорных систем управления движением поездов, локомотивами и электроснабжением (утвержден 24.12.2015)

Исследования на кибербезопасность микропроцессорных систем управления ОАО «РЖД»

За период с 2014г по 2018г в Центре кибербезопасности АО «НИИАС» проверены на киберзащищенность **26** МПСУ ОАО «РЖД», в том числе разработанные: ООО «Сименс», ООО «Бомбардье Транспортейшн (Сигнал)», ОАО «Радиоавионика», ОАО «Элтеза» и т.д.
Выявлено **233** уязвимости. В результате : **148** уязвимостей - устранены разработчиками; **25** уязвимостей – конструктивные недоработки, являющиеся причинами выявленных уязвимостей – устранены разработчиками;
60 уязвимостей – устраняются.

Спасибо за внимание!

Безродный Борис Федорович
Заместитель руководителя Центра кибербезопасности АО «НИИАС»
доктор технических наук, профессор

НИИАС