



Особенности обеспечения безопасности информации в системах железнодорожной автоматики и телемеханики

Безродный Борис Федорович

Заместитель начальника Центра кибербезопасности АО «НИИАС»
доктор технических наук, профессор





Негативные последствия

🏠 > Объекты сфер деятельности

Система микропроцессорной централизации на железнодорожном транспорте



Система интервального регулирования на железнодорожном транспорте



Система диспетчерской централизации на железнодорожном транспорте



Система управления сортировочным процессом на железнодорожном транспорте



Система телемеханического управления объектами электроснабжения на железнодорожном транспорте



Микропроцессорные системы управления и диагностики на железнодорожном транспорте



Локомотивные устройства безопасности на железнодорожном транспорте



Угрозы безопасности информации



Угрозы

Банк данных угроз АСУ ТП

выберите категорию, чтобы быстро найти необходимую вам информацию

Поиск по разделу...

Угрозы

Типовые сценарии

Компоненты

Объекты воздействия

Нарушители

Способы реализации угроз

УТП:01 Угроза утечки информации

УТП:02 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УТП:03 Угроза удаленного несанкционированного подключения к компонентам АСУ ТП

УТП:04 Угроза несанкционированного доступа

УТП:05 Угроза несанкционированной модификации (искажения)

УТП:06 Угроза несанкционированной подмены

УТП:07 Угроза удаления информационных ресурсов

УТП:08 Угроза отказа в обслуживании

Негативные последствия от компьютерных атак

☰

Банк данных угроз АСУ ТП

Поиск...

Войти

Негативные последствия

🏠 > Объекты сфер деятельности

Система микропроцессорной централизации на железнодорожном транспорте

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Крушение железнодорожного подвижного состава
Социальный ущерб

Система интервального регулирования на железнодорожном транспорте

Крушение железнодорожного подвижного состава
Социальный ущерб

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Система диспетчерской централизации на железнодорожном транспорте

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Система управления сортировочным процессом на железнодорожном транспорте

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Крушение железнодорожного подвижного состава
Социальный ущерб

Система телемеханического управления объектами электроснабжения на железнодорожном транспорте

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Микропроцессорные системы управления и диагностики на железнодорожном транспорте

Снижение скорости или полная остановка движения железнодорожного подвижного состава
Социальный ущерб

Локомотивные устройства безопасности на железнодорожном транспорте

Крушение железнодорожного подвижного состава
Социальный ущерб

Сфера деятельности

Транспорт X

Объект сферы деятельности

Железнодорожный подвижной сост... X

Архитектура АСУ ТП

Вид негативного последствия

Поиск Сброс

Скачать список (.xlsx, .ods)

Безопасность систем ЖАТ – свойство непрерывно сохранять работоспособное или защитное состояние в течение установленного времени или наработки на отказ (ГОСТ Р 53431-2009).

Si – исправное состояние
(система работает в норме)

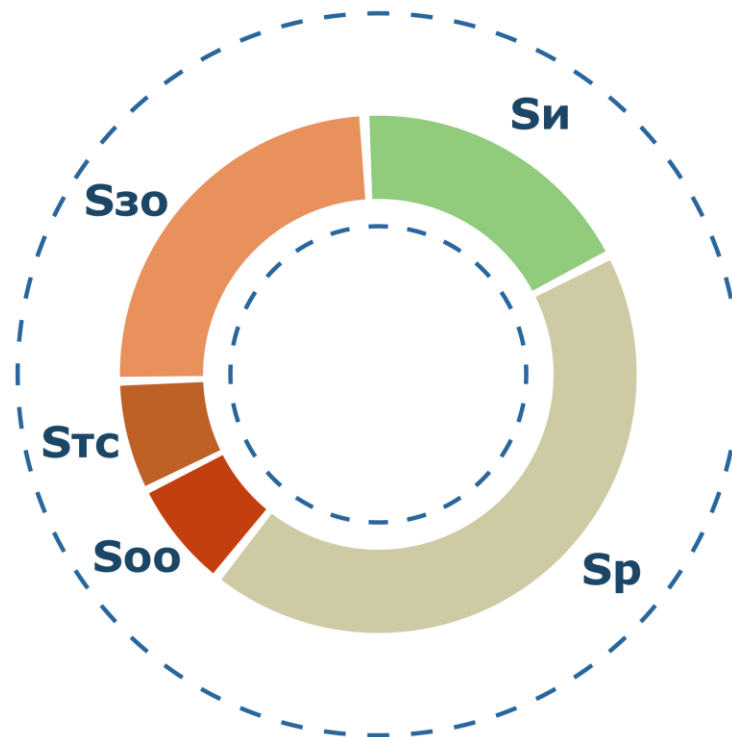
Sp – работоспособное состояние
(система выполняет свои функции при наличии некритичных неисправностей)

Szo – защитное состояние
(состояние защитного отказа системы)

Stc – случайные отказы технических средств
(случайный отказ системы, вызывающий задержки поездов)

Soo – опасный отказ системы
(опасное состояние системы)

Диаграмма состояний
систем ЖАТ



Обеспечение функциональной безопасности. Опасные и защитные отказы



Состояния, вызывающие ущерб

Критическая информационная инфраструктура

Функциональная
безопасность

S₀₀

Информационная
безопасность

S₃₀

S_{ТС}

S00 — опасный
отказ;

S30 — защитный
отказ;

ТС — отказ
технических средств.

$$C_{\text{(ожидаемый ущерб)}} = \overbrace{C(S_{00}) \times P(S_{00})}^{\text{Функциональная безопасность}} + \overbrace{C(S_{30}) \times P(S_{30})}^{\text{Информационная безопасность}} + \underbrace{C(S_{TC}) \times P(S_{TC})}_{\text{Критическая информационная инфраструктура}}$$

$C(S_{00})$ – средний ущерб от крушения (опасного отказа);

$P(S_{00})$ – вероятность наступления опасного отказа;

$C(S_{30})$ – средний ущерб от задержки поездов по причине защитного отказа, с учетом затрат на восстановление работоспособности;

$P(S_{30})$ – вероятность наступления защитного отказа;

$C(S_{TC})$ – средний ущерб от задержки поездов по причине случайного отказа технических средств с учетом затрат на восстановление работоспособности;

$P(S_{TC})$ – вероятность наступления отказа технических средств.

Технический регламент таможенного союза

«О безопасности инфраструктуры железнодорожного транспорта» (ТР ТС 003/2011)



Оценка соответствия (обязательная)		Требования	Документы устанавливающие требования
Сертификация	Декларации о соответствии		
Стр. 220 Приложение 3 1.Автоматизированные системы оперативного управления технологическими процессами, связанными с обеспечением безопасности движения и информационной безопасностью	Стр. 222 Приложение 4 11.Программные средства железнодорожного транспорта для автоматизированных систем оперативного управления технологическими процессами, связанными с обеспечением безопасности движения и информационной безопасностью	Стр. 183 29. К железнодорожной автоматике и телемеханике, составным частям железнодорожной автоматики и телемеханики и элементам составных частей железнодорожной автоматики и телемеханики предъявляются следующие требования: программные средства, функционирующие в составе железнодорожной автоматики и телемеханики , как встраиваемые, так и поставляемые на материальных носителях, должны обеспечивать: защищенность от компьютерных вирусов, несанкционированного доступа , последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, от возможности случайных изменений информации (отсутствие НСД) ; соответствие свойствам и характеристикам, описанным в программных документах , а также в документации, поставляемой с оборудованием и содержащей информацию для сборки, установки и эксплуатации данного оборудования (отсутствие НДВ) .	ГОСТ 33895-2016 - СТАНДАРТ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ПЕРЕГОНАХ ЖЕЛЕЗНОДОРОЖНЫХ ЛИНИЙ п 4.4.6; ГОСТ 33894-2016 - СТАНДАРТ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ЖЕЛЕЗНОДОРОЖНЫХ СТАНЦИЯХ п 4.7.6 ; ГОСТ 33893-2016 - СТАНДАРТ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ЖЕЛЕЗНОДОРОЖНЫХ ПЕРЕЕЗДАХ п 4.3.6; ГОСТ 33892-2016 - СТАНДАРТ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА СОРТИРОВОЧНЫХ СТАНЦИЯХ п 4.4.6, п 4.4.7.



Спасибо за внимание!