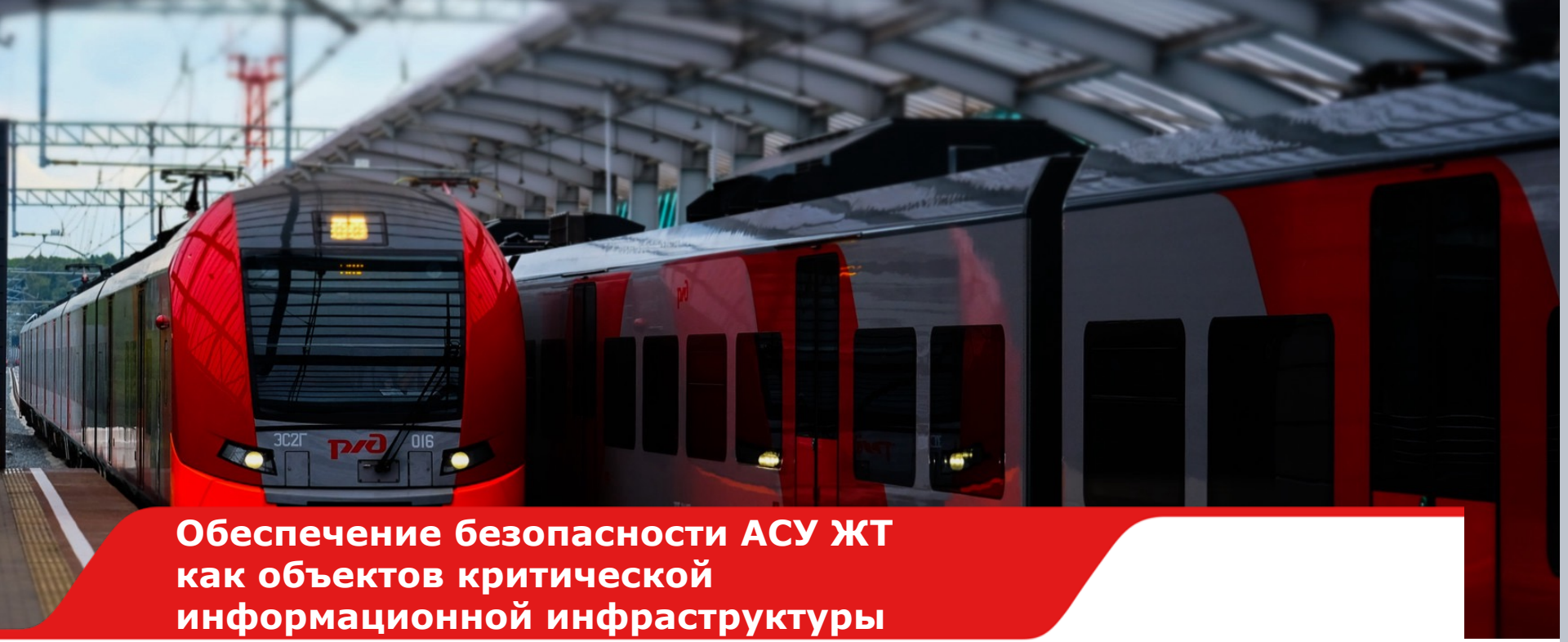


Обеспечение безопасности АСУ ЖТ как объектов критической информационной инфраструктуры

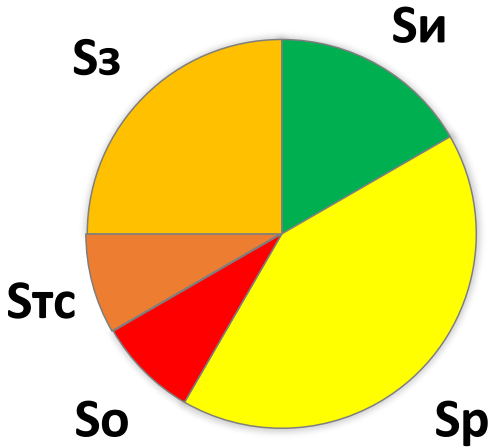
Безродный Борис Федорович
Заместитель начальника Центра кибербезопасности АО «НИИАС»
доктор технических наук, профессор

Безопасность и надежность АСУ ЖТ

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

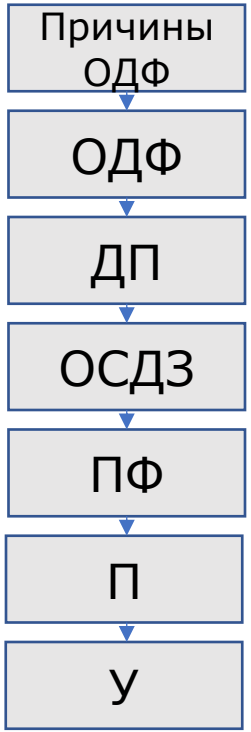
Sи – исправное состояние (система работает в норме)
Sр – работоспособное состояние (система выполняет свои функции при наличии некритичных неисправностей)
Sз – защитное состояние (состояние защитного отказа системы)
Sтс – случайные отказы технических средств (случайный отказ системы, вызывающий задержки поездов)
So – опасный отказ системы (опасное состояние системы)

ДИАГРАММА СОСТОЯНИЙ СИСТЕМ АСУ ЖТ



НИИАС

Возникновение потерь и ущербов от них



Причины опасных и дестабилизирующих факторов

Опасные и дестабилизирующие факторы

Движение поездов

Опасные состояния движения и задержки поездов

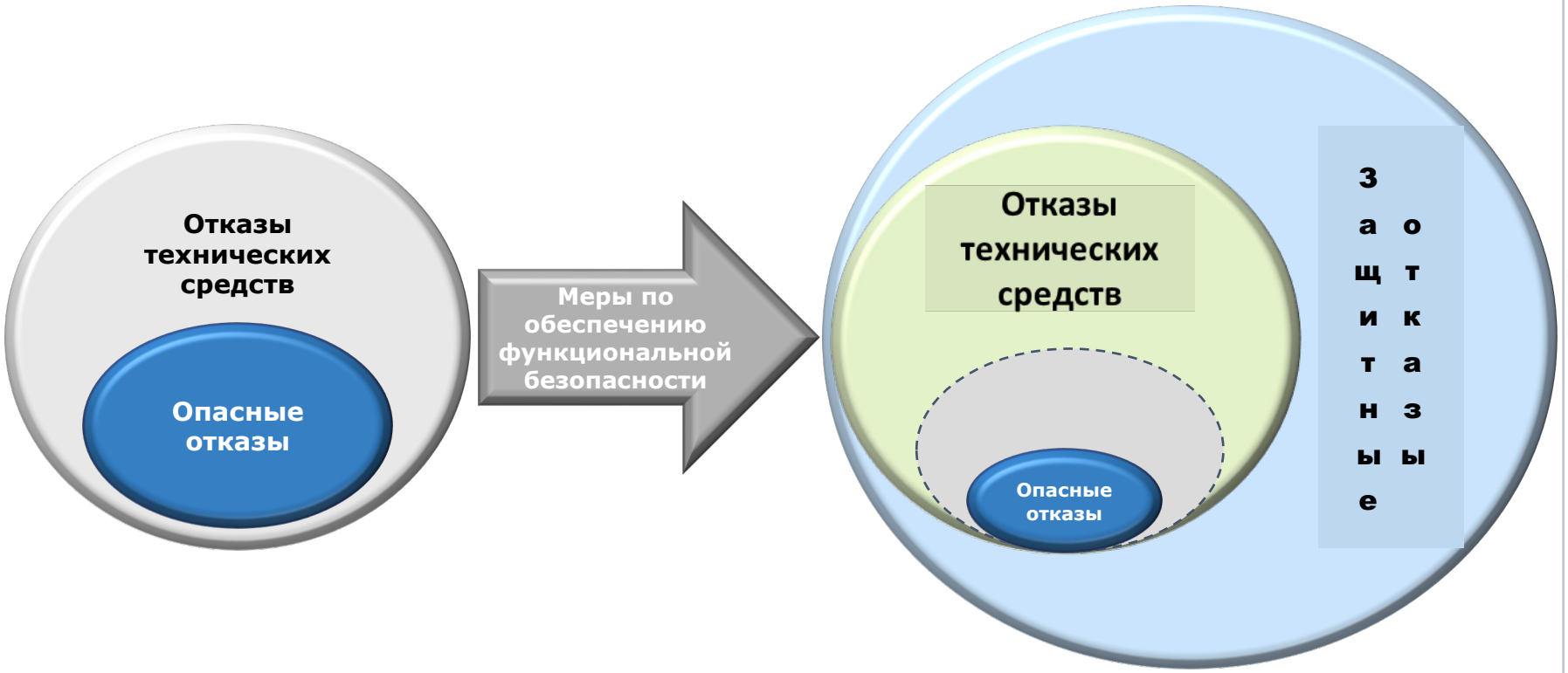
Поражающие факторы

Потери

Ущерб от потерь

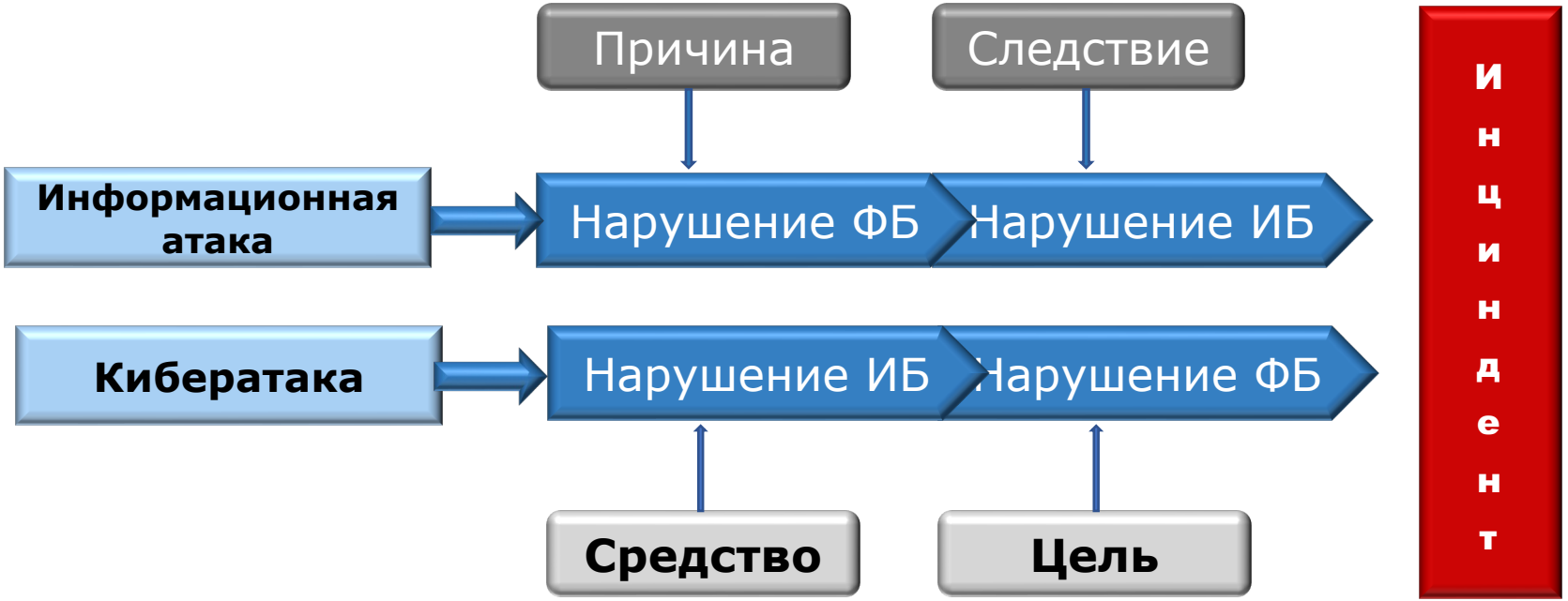
НИИАС

Обеспечение функциональной безопасности
Опасные и защитные отказы



НИИАС

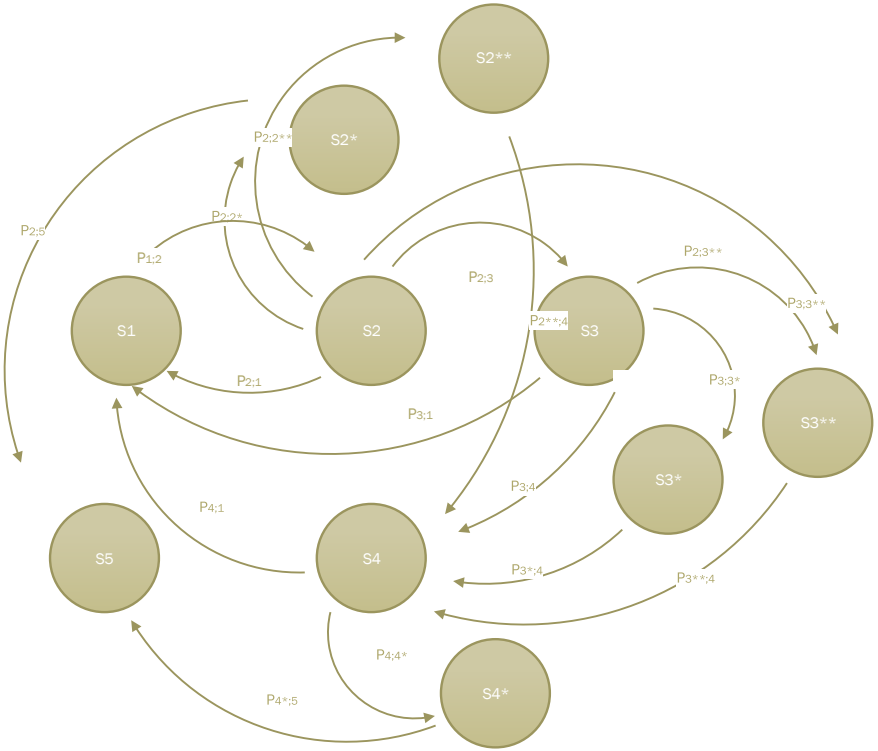
Отличие кибератаки от информационной атаки



НИИАС

Пример Марковской модели АСУ ЖТ

Граф Марковской модели



Обозначение	Описание
S1	исправное состояние (система работает в норме)
S2	работоспособное состояние (система выполняет свои функции при наличии некритичных неисправностей)
S3	работоспособное состояние (система выполняет свои функции при наличии некритичных неисправностей)
S4	работоспособное состояние (система выполняет свои функции при наличии некритичных неисправностей)
S5	отказ технических средств системы (отказ в обслуживании, вызывающий задержки поездов)
S2*	– опасный отказ системы (опасное состояние системы)
S3*	– опасный отказ системы (опасное состояние системы)
S4*	– опасный отказ системы (опасное состояние системы)
S2**	защитное состояние (состояние защитного отказа системы)
S3**	защитное состояние (состояние защитного отказа системы)

НИИАС

Выводы

1. Сложность моделей больших систем делает невозможным прямой 100% контроль функциональной безопасности

2. Анализ деревьев опасных событий для такой системы должен сводиться к построению марковских и полумарковских математических моделей с построением переходных систем уравнений и их решением

3. В условиях неполного контроля ключевыми подходами обеспечения безопасности становятся переход к работе с цифровыми двойниками (моделирования для пополнения недостаточной статистики) и различное резервирование элементов или подсистем

4. При выборе тех или иных средств защиты доступа, функционирования или информации в системах или подсистемах, обеспечивающих движение поездов и обслуживание пассажиров целесообразно комплексно оценивать их эффективность с учетом возможного снижения надежности и оперативности работы технических средств, а также их удорожания.

НИИАС

СПАСИБО ЗА ВНИМАНИЕ