Белорусский государственный университет транспорта
Гомель, Республика Беларусь

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ НОРМАТИВНЫХ ДОКУМЕНТОВ

БОЧКОВ К.А. д.т.н., профессор
ХАРЛАП С.Н. к.т.н., доцент
БУЙ П.М. к.т.н., доцент

Научно-исследовательская лаборатория
«БЕЗОПАСНОСТЬ И ЭМС ТЕХНИЧЕСКИХ СРЕДСТВ»

Кибератака

Кибертерроризм

Информационная инфраструктура

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов

- **Информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки (ГОСТ Р 53113.1-2008)

Функциональная безопасность (functional safety) системы управления – это часть общей безопасности системы, работающей правильно в ответ на входные воздействия и обеспечивающей отсутствие неприемлемого риска здоровью людей, их собственности или окружающей среде со своей стороны

Автоматизированные системы управления ответственными технологическими процессами

Системы железнодорожной автоматики и телемеханики

в первую очередь должны выполнять требования функциональной безопасности, заключающиеся в обеспечении безопасности движения поездов

во вторую очередь все остальные требования, включая требования информационной безопасности

Приказ №31 ФСТЭК России
от 14.0-3.2014

Приказ №239 ФСТЭК России
от 25.12.2017

Порядок подтверждения соответствия

Процедуры по подтверждению соответствия требованиям функциональной безопасности

(испытания, верификация ПО и т.д.) и экспертиза «Доказательство безопасности» в соответствующей лаборатории, аккредитованной в области функциональной безопасности

Процедуры подтверждения соответствия требованиям информационной безопасности

с участием лаборатории, аккредитованной в области информационной безопасности

дополнительные средства защиты, внешние
по отношению к средствам обеспечения
функциональной безопасности

Приказ №239 ФСТЭК России от 25.12.2017

… если меры функциональной безопасности являются достаточными для нейтрализации актуальных угроз информационной безопасности, то дополнительные меры защиты можно не применять …

эти рекомендации на практике не выполняются

Основание: различия в перечне угроз и объектов защиты

Интегрировать же дополнительные средства защиты в комплекс мер функциональной безопасности невозможно, т.к. это потребует повторной процедуры подтверждения соответствия требованиям функциональной безопасности

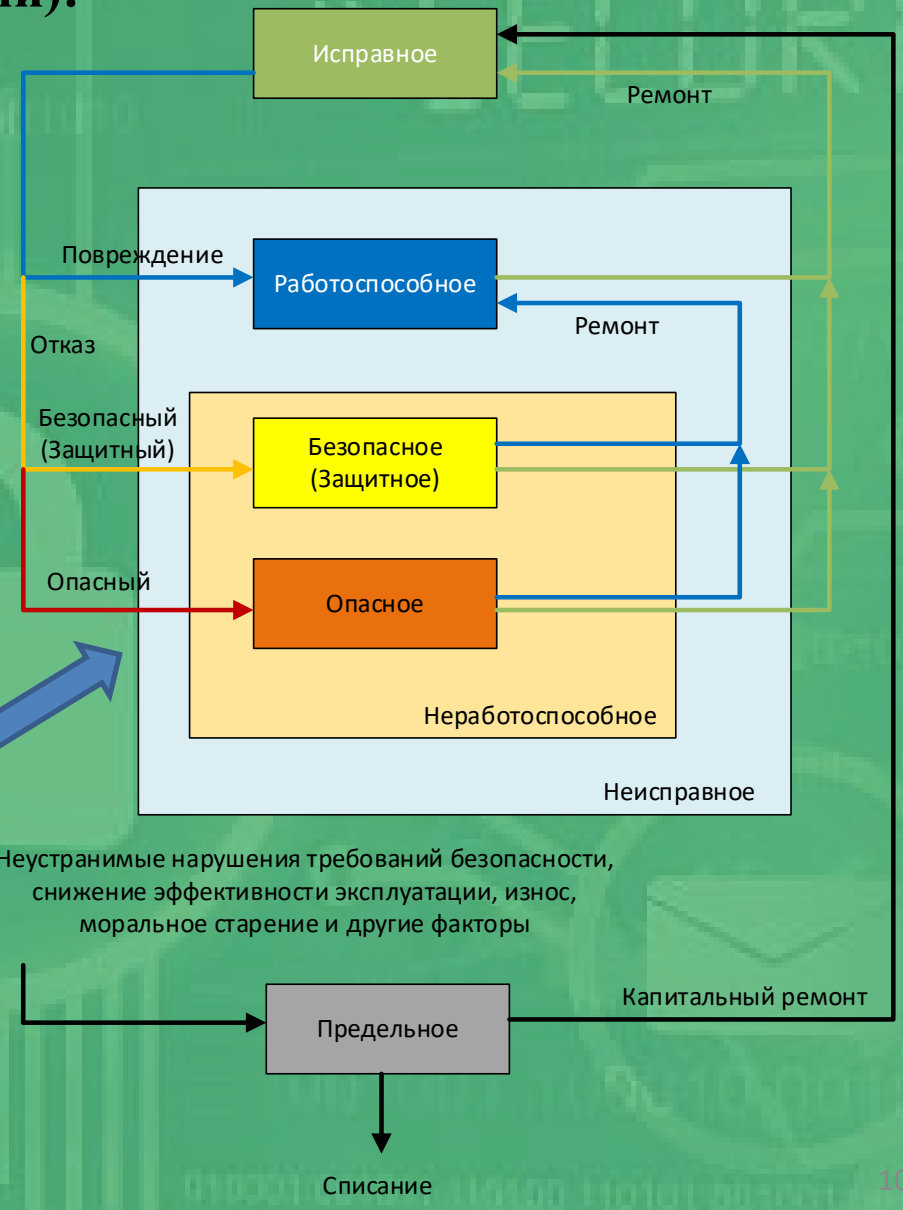
Для обеспечения функциональной безопасности используются несколько подходов (стратегий):

безотказность

отказоустойчивость

общее повышение надежности (безотказности)

безопасное поведение при отказах



Иерархия уровней защиты от опасных отказов

принцип «Защита в глубину» (Defense-in-Depth)

Уровни защиты	Средства защиты атомного энергоблока	Средства защиты системы переездной автоматики
Уровень аварийного реагирования	Группы по ликвидации последствий аварии	Инструкция по эксплуатации железнодорожных переездов
Уровень пассивной защиты	Корпус реактора	Устройства заграждения переезда
Уровень активной защиты	Активация системы аварийного охлаждения	Включение заградительной сигнализации
Уровень защитного отключения	Аварийный останов реактора	Переход на ручное управление переездом
Уровень контроля безопасности технологического процесса (останов процесса)	Локальные технологические защиты и блокировки	Контроль целостности нитей ламп переездных светофоров
Уровень управления технологическим процессом (нормальное состояние процесса)	Система управления технологическим процессом	Система управления технологическим процессом

Поставленные цели

Информационная безопасность

обеспечение доступности и целостности обрабатываемой в АСУ ТП информации

(Приказ №31 ФСТЭК России от 14.03.2014)

защита информации с целью недопущения ее искажения (в том числе недоступности актуальной информации)

Функциональная безопасность

отсутствии неприемлемого риска здоровью людей, их собственности или окружающей среде со стороны АСУ ТП при нарушении ее правильного функционирования

обеспечить выполнение всех функций, связанных с безопасностью

учитываются не только возможные искажения информации, но и отказы аппаратных средств, ошибки в программном обеспечении и др.

Критерии значимости объектов

Информационная безопасность

если инцидент на объекте КИИ приведет к гибели от одного до пятидесяти человек, то такой объект относят к низшей третьей категории

Перечень показателей критериев значимости объектов критической информационной инфраструктуры, утвержденный Постановлением Правительства РФ от 8 февраля 2018 № 127

Функциональная безопасность

если аварийная ситуация на объекте приведет к гибели одного или более людей, то последствия относят к наивысшему, катастрофическому уровню, а систему управления – к высшему уровню полноты безопасности УПБ4

ГОСТ 33433-2015 «Безопасность функциональная. Управление рисками на железнодорожном транспорте»

Объекты защиты в АСУ ТП

Информационная безопасность

Функциональная безопасность

источники возможного искажения информации

доступность и целостность

невыполнение функций, связанных с безопасностью

Угрозы безопасности в АСУ ТП

Информационная безопасность

1) Внешние угрозы:
   – несанкционированный доступ;
   – саботаж сторонних лиц;
   – вредоносное ПО (вирусы);
   – целевые атаки.
2) Внутренние угрозы:
   – ошибки конфигурации;
   – саботаж сотрудников;
   – уязвимости в индустриальном ПО.

Преднамеренные действия злоумышленников

Функциональная безопасность

1) Внешние угрозы:
   – случайные искажения информации;
   – отказы внешней инфраструктуры.

2) Внутренние угрозы:
   – отказы оборудования;
   – случайные искажения информации;
   – ошибки персонала;
   – ошибки в программном обеспечении.

Случайные события

Обеспечение доступности информации методами функциональной безопасности

Доступность – это обеспечение своевременного и надежного доступа к информации и информационным сервисам.

Парирование последствий нарушения доступности информации

1) сохранение доступности информации (резервирование);

2) сохранение безопасного состояния системы при отсутствии доступа к критической информации.

- ограничение времени жизни критической информации
- программный и аппаратный контроль тайм-аутов
- ограничение времени жизни команд
- контроль последовательности и времени выполнения процедур

Обеспечение целостности информации методами функциональной безопасности

Целостность – это отсутствие неправомочных искажений, добавлений или уничтожения информации

Нарушение целостности данных

случайное (непреднамеренное) искажение информации

преднамеренное искажение информации посредством внешних систем передачи информации

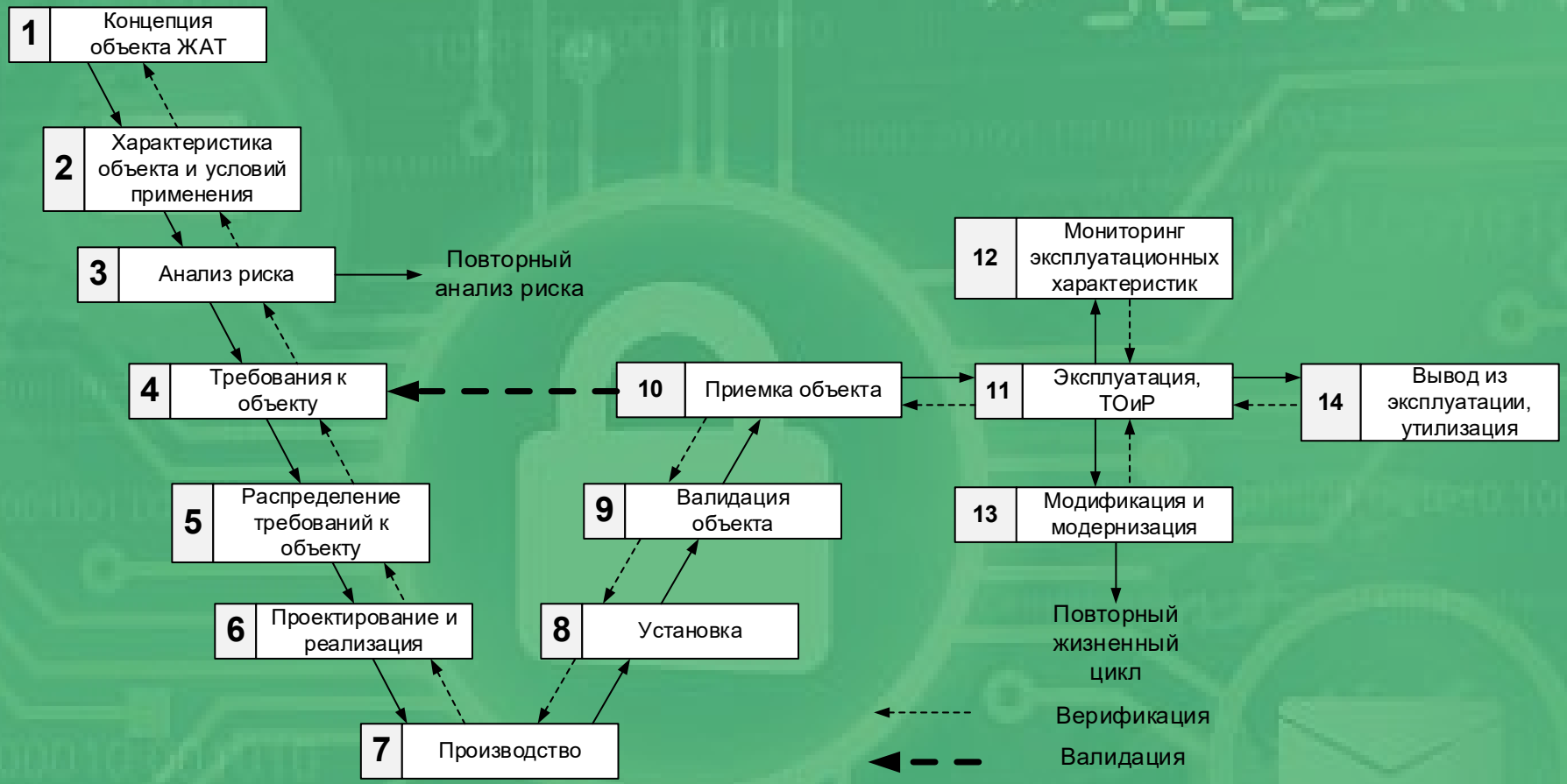
преднамеренное искажение информации посредством использования уязвимостей в ПО

Стандартные методы ФБ
избыточное кодирование,
дублирование,
диверсификация и т.д.

ГОСТ Р МЭК 62280 «Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации»

ГОСТ Р МЭК 62279 «Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах»

Этапы жизненного цикла, связанные с функциональной и информационной безопасностью



Выводы

Использование методов функциональной безопасности позволяет в полном объеме решить задачи информационной безопасности для АСУ ТП

Для всех угроз информационной безопасности существуют эффективные методы защиты, базирующиеся на стандартах по функциональной безопасности.

Для эффективного использования методов функциональной безопасности в целях обеспечения информационной безопасности необходимо выполнять эту работу на ранних стадиях разработки АСУ ТП.

Для исключения дублирования работ подтверждение соответствия требованиям функциональной и информационной безопасности желательно проводить в одной организации, аккредитованной в этих областях.

Спасибо за внимание!