ИНТЕГРАЦИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКАЗАТЕЛЬСТВО ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

БОЧКОВ
Константин Афанасьевич

д.т.н., профессор
научный руководитель -
заведующий НИЛ

ХАРЛАП
Сергей Николаевич

к.т.н., доцент, заведующий
кафедрой «ИУСиТ» БелГУТа,
ведущий научный сотрудник НИЛ

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Основные тенденции развития систем железнодорожной автоматики и риски нарушения требований информационной безопасности

Цифровизация железнодорожных систем

Расширение возможностей подключения к существующим цифровым системам

Переход от заказных автономных систем к стандартизированному оборудованию с открытой платформой, созданному с использованием готовых коммерческих компонентов (COTS)

Широкое использование сетевых систем управления и автоматизации, доступ к которым возможен удаленно через общедоступные и частные сети

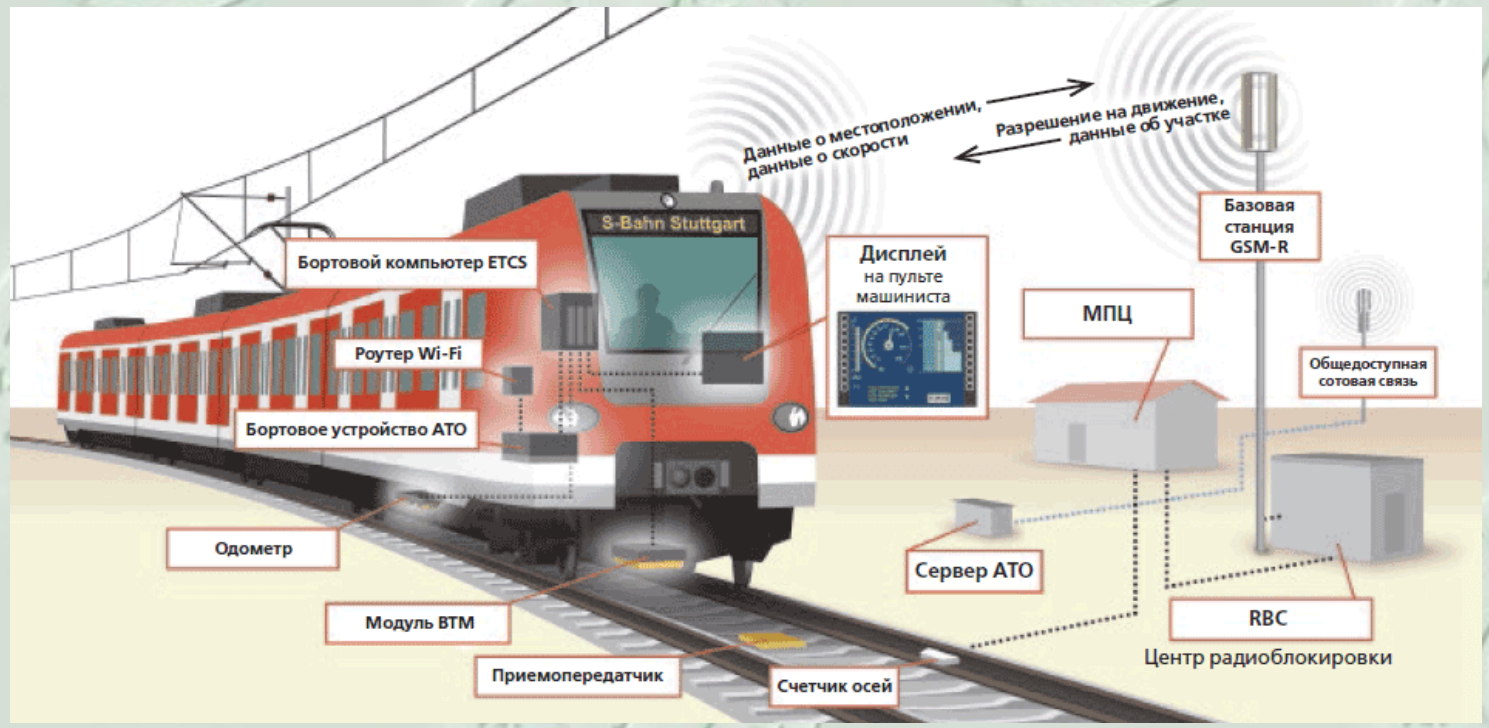
34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Тенденции развития систем железнодорожной автоматики и риски нарушения требований информационной безопасности

Применение открытых сетей передачи данных (в том числе радиоканала) для передачи ответственной информации

Искажение критической информации, вызывающие нарушения требований функциональной безопасности

Несанкционированное вмешательство в работу систем ЖАТ (ложные команды управления)



34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Тенденции развития систем железнодорожной автоматики и риски нарушения требований информационной безопасности

Применение систем искусственного интеллекта для принятия ответственных решений по управлению железнодорожным транспортом (системы беспилотного вождения)

Нарушение целостности выполняемой программы

Например, переполнение буфера или целочисленное переполнение

Принятие неверного решения под воздействием кибератаки

Воздействия через входные данные – состязательные атаки (возможно обмануть модель ИИ и заставить ее выдавать абсолютно разные результаты путем небольших возмущений на входе, которые создаются с помощью процесса оптимизации)

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Функциональная безопасность и системы искусственного интеллекта

Technical Report

ISO/IEC TR 5469

Artificial intelligence — Functional safety and AI systems

Intelligence artificielle — Sécurité fonctionnelle et systèmes d'intelligence artificielle

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC TR 5469:2024

First edition
2024-01

Reference number
ISO/IEC TR 5469:2024(en)

© ISO/IEC 2024

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 836— 2023 (ISO/IEC DTR 5469)

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Функциональная безопасность и системы искусственного интеллекта

(ISO/IEC DTR 5469, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

TECHNICAL REPORT

ISO/IEC TR 24027

First edition
2021-11

Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making

Technologie de l'information — Intelligence artificielle (IA) — Tendance dans les systèmes de l'IA et dans la prise de décision assistée par l'IA

Reference number
ISO/IEC TR 24027:2021(E)

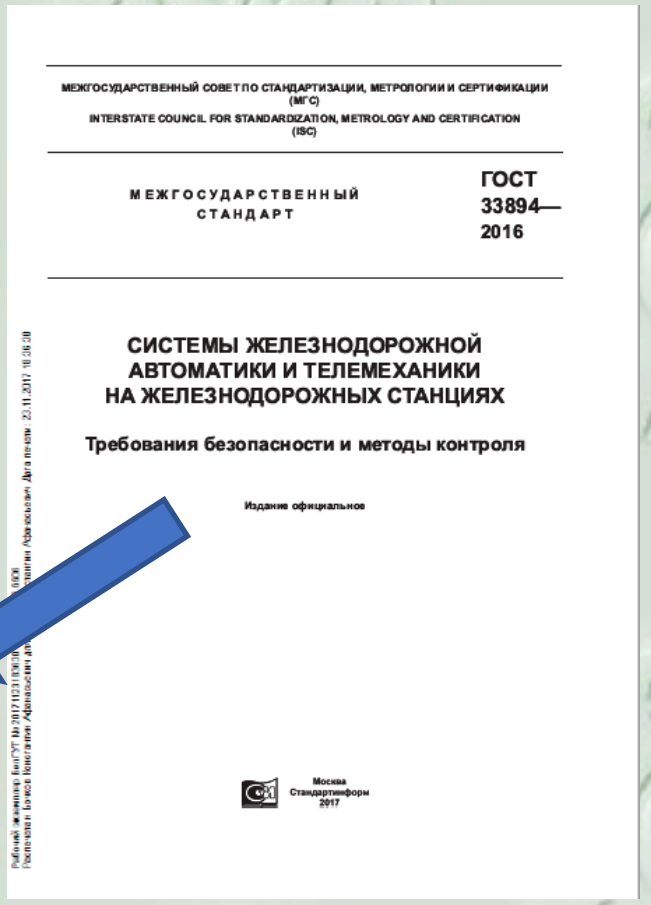
© ISO/IEC 2021

34, Kirov str., 246653 Gomel, Belarus, Laboratory "Safety & EMC of hardware"
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Сближение требований информационной и функциональной безопасности в нормативных документах

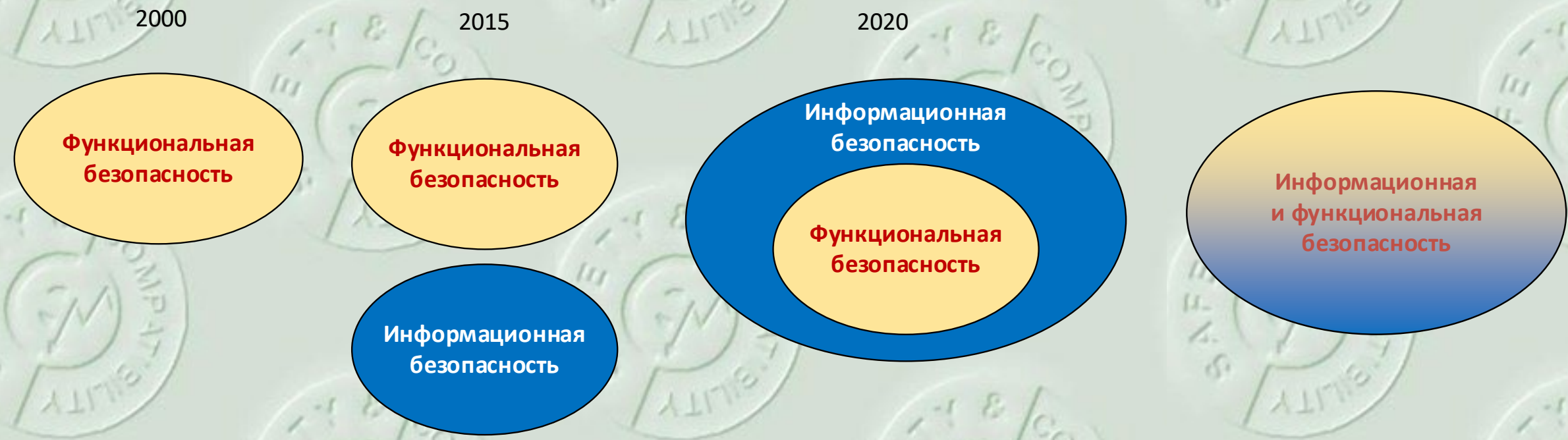
«Автоматизированные системы оперативного управления технологическими процессами, связанными с **обеспечением безопасности движения** и **информационной** безопасности»

Требования **функциональной безопасности** и требования **информационной безопасности**: защита от несанкционированного доступа, контроль целостности программ и данных, отсутствие недекларированных возможностей



34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Тенденции по организации взаимодействия методов информационной и функциональной безопасности в АСУ ТП



34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Сближение требований информационной и функциональной безопасности

Угрозы информационной безопасности

События, связанные с нарушением:
- конфиденциальности
- целостности
- доступности

обрабатываемой в АСУ ТП информации

Угрозы функциональной безопасности

неприемлемый риск физического повреждения или ущерба:
- здоровью людей
- собственности
- окружающей среде

Угрозы информационной безопасности для систем ЖАТ

- угрозы, вызывающие нарушение требований безопасности движения поездов;
- угрозы, вызывающие снижение эффективности процесса перевозок;
- угрозы, вызывающие ухудшение показателей надежности функционирования устройств ЖАТ.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Угрозы, вызывающие нарушение требований безопасности движения поездов

Приводят к нарушениям функциональной безопасности (к столкновению поездов, крушениям и другим катастрофам)

Цели функциональной и информационной безопасности **полностью совпадают** и направлены либо на полное исключение таких угроз, либо на снижение вероятности таких событий до допустимого значения.

Для предотвращения угроз информационной безопасности, вызывающих нарушение требований безопасности движения поездов, **целесообразно применять методы функциональной безопасности**, так как классические методы информационной безопасности в этом случае мало эффективны.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Угрозы, вызывающие снижение эффективности процесса перевозок

Не могут нарушить функциональную безопасность систем ЖАТ, но могут привести к задержкам поездов, снижению допустимой скорости движения по участку

Причина: срабатывание защитных механизмов функциональной безопасности, направленных на парирование возможных опасных последствий нарушений в их работе (отказобезопасность).

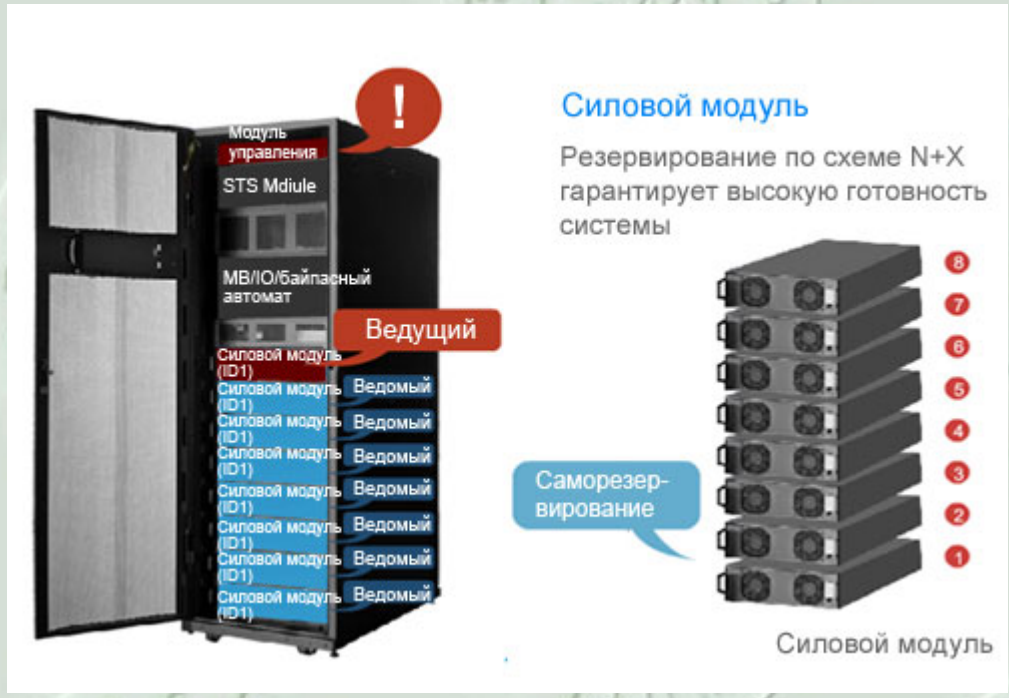
Функциональная безопасность рассматривает переход в защитное состояние как естественную реакцию на угрозу возникновения опасной поездной ситуации. Интенсивность защитных отказов нормируется через показатели надежности.

Для предотвращения угроз информационной безопасности, вызывающих снижение эффективности процесса перевозок, **целесообразно применять методы повышения надежности** (отказоустойчивость), так как классические методы информационной безопасности в этом случае также мало эффективны.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Угрозы, вызывающие ухудшение показателей надежности функционирования

Не могут нарушить работоспособность систем ЖАТ, однако приводят к срабатыванию механизмов, обеспечивающих отказоустойчивость систем, например переключение на резерв, реконфигурация оборудования.



Экономический ущерб при этом **минимальный**.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Количественная оценка рисков

Угрозы информационной безопасности

События, связанные с нарушением:
- конфиденциальности
- целостности
- доступности

обрабатываемой в АСУ ТП информации

Угрозы информационной безопасности для систем ЖАТ

- угрозы, вызывающие нарушение требований безопасности движения поездов;
- угрозы, вызывающие снижение эффективности процесса перевозок;
- угрозы, вызывающие ухудшение показателей надежности функционирования устройств ЖАТ.

Уровень риска определяют по величине риска, рассчитываемой по формуле:

$$R = F_R\{C, P\} = \sum_i \left[F_{R_i}(C_i, P_i)\right]$$

где R - величина риска;

F_R - функционал, связывающий вероятность P возникновения события и математическое ожидание последствия (ущерба) C от этого события;

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Количественная оценка рисков

Угрозы	Типовые последствия, ущерб	Частота допустимого риска
Угрозы, вызывающие нарушение требований безопасности движения поездов	**Катастрофический:** Гибель одного человека или более, тяжкий вред здоровью пяти человек и более, связанных с функционированием железнодорожного транспорта	Интенсивность опасных отказов установлена в ГОСТ и составляет для разных систем значения от 10^{-7} до 10^{-9} 1/ч.
Угрозы, вызывающие снижение эффективности процесса перевозок	**Несущественный:** Задержка движения поездов на несколько часов, повреждение объекта инфраструктуры, требующее проведения ремонта для восстановления его работоспособного состояния	Интенсивность отказов установлена в ГОСТ и составляет для разных систем значения от 10^{-4} до 10^{-5} 1/ч.
Угрозы, вызывающие ухудшение показателей надежности функционирования	**Незначительный:** Отказы, элементов, модулей и подсистем, не нарушающих работоспособность объекта инфраструктуры, требующие регулярного ТО.	Интенсивность отказов определяется надежностью элементов, их количеством и составляет для разных систем значения от 10^{-2} до 10^{-3} 1/ч.

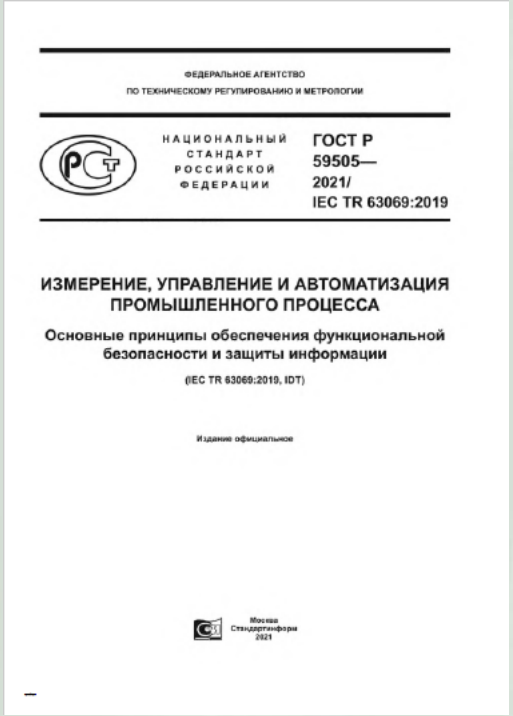
34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Идентификация рисков информационной безопасности МПЦ

Направления возможных кибератак на объекты МПЦ

Принятый подход к обеспечению информационной безопасности СЖАТ

Недостаток:
избыточность, так как методы защиты частично могут дублировать друг друга



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59505— 2021/ IEC TR 63069:2019

ИЗМЕРЕНИЕ, УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОЦЕССА

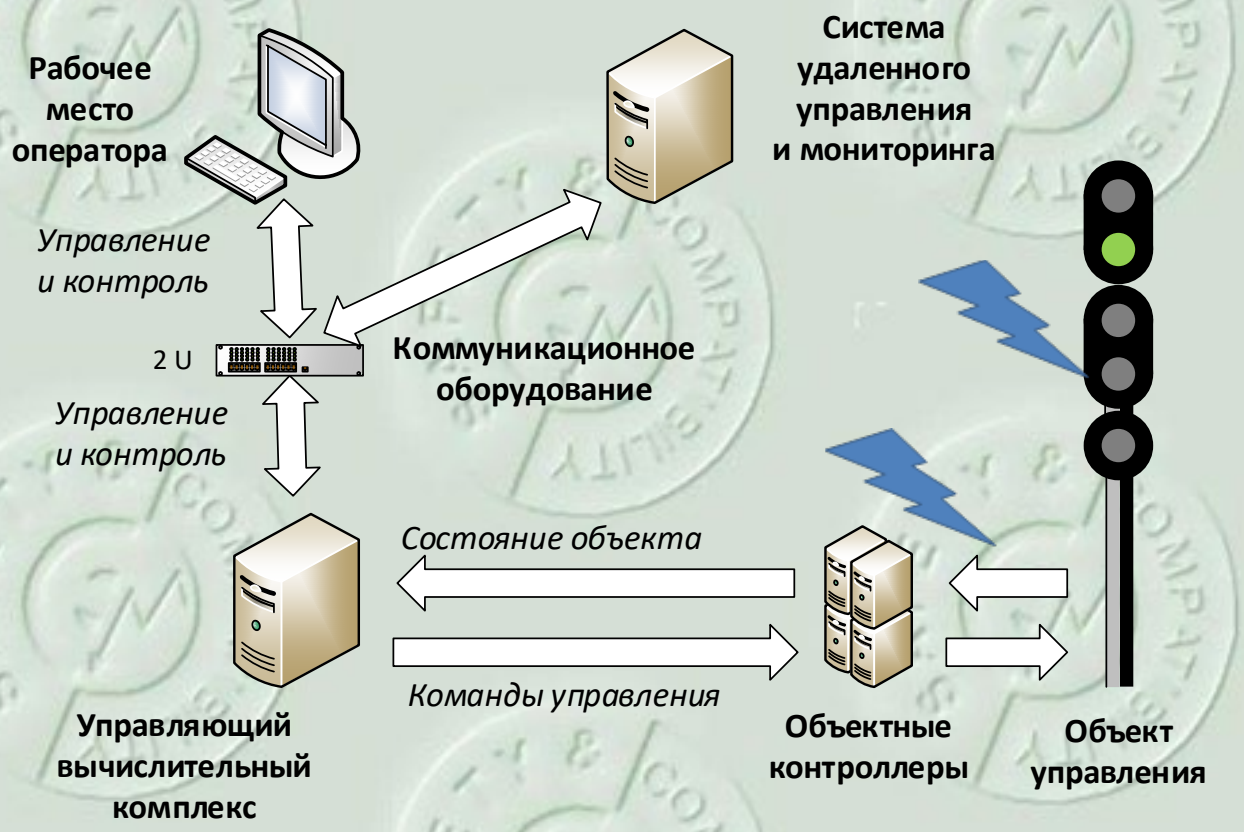
Основные принципы обеспечения функциональной безопасности и защиты информации

(IEC TR 63069:2019, IDT)

Издание официальное

Москва
Стандартинформ
2021

Направления возможных кибератак на объекты нижнего уровня



– непосредственное воздействие на объекты (стрелки и сигналы) или на интерфейсные линии между объектным контроллером и объектом управления.

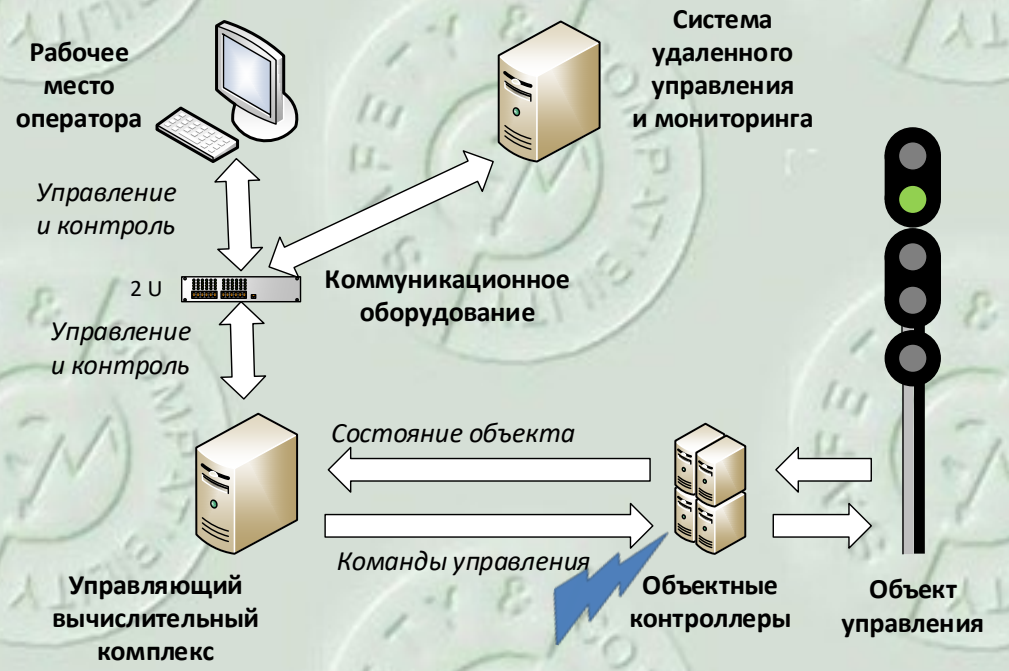
Данные объекты используют прямопроводное управление и не обладают развитым интерфейсом, кабельные сети размещены в зоне круглосуточного контроля.

Непосредственное воздействие на них в результате кибератак является **маловероятным** (по ГОСТ 33433-2015 - вероятность возникновения крайне маловероятна. Можно предположить, что опасное событие не возникнет).

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Направления возможных кибератак на объекты нижнего уровня

– непосредственное воздействие на ОК с целью исказить команды управления или статусы.



Организационные меры ФБ:
- размещение в запираемой помещении поста МПЦ;
- конфигурация объектных контроллеров определена проектом, постоянна и не изменяется во время эксплуатации;
- доступ к ОК только через интерфейс ОК-УВК. Беспроводный интерфейс не применяется.

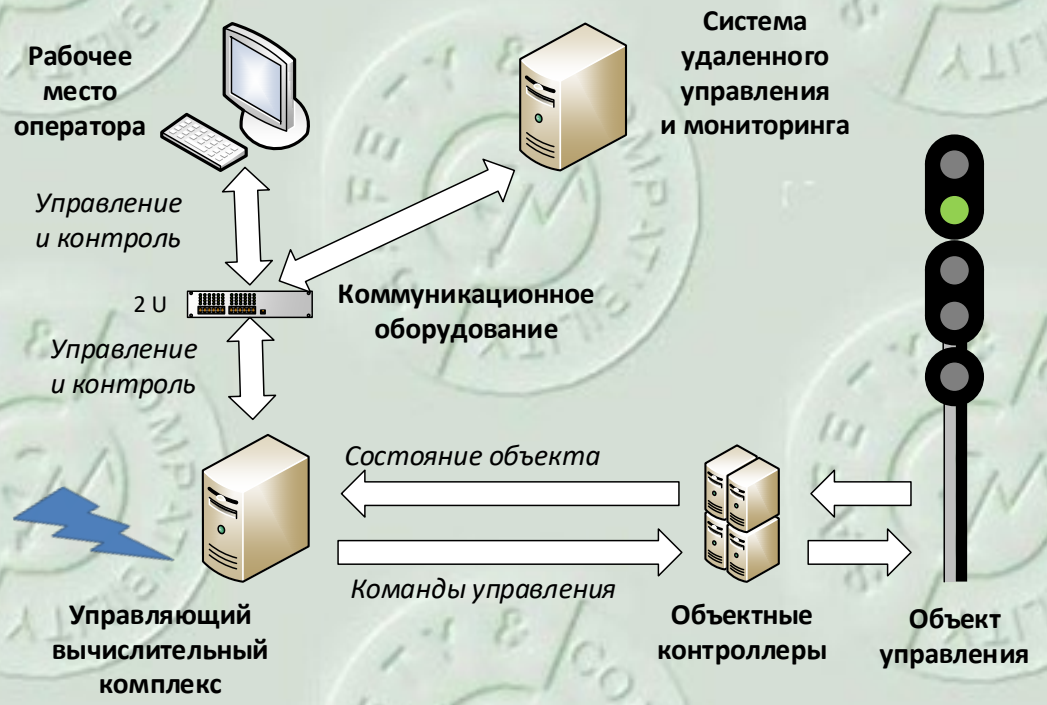
Программно-технические меры ФБ:
- двухканальная архитектура ОК, каждая команда для успешной реализации должна быть независимо принята обоими каналами, пройти процедуру кросс-сравнения;
- применение различных форматов команд и алгоритмов вычисления контрольных сумм для разных каналов (диверситет).

Непосредственное воздействие на ОК в результате кибератак является **крайне редким** (вероятность возникновения маловероятна, но возможна. Можно предположить, что опасное событие может возникнуть в исключительном случае)

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Направления возможных кибератак на объекты среднего уровня

– непосредственное воздействие на УВК с целью исказить алгоритм функционирования.



Организационные меры ФБ:
- размещение в запираемой помещении поста МПЦ;
- конфигурация системы определена проектом, постоянна и не изменяется во время эксплуатации;
- доступ к УВК только через интерфейс ОК-УВК или проводной интерфейс локальной сети. Беспроводный интерфейс не применяется.

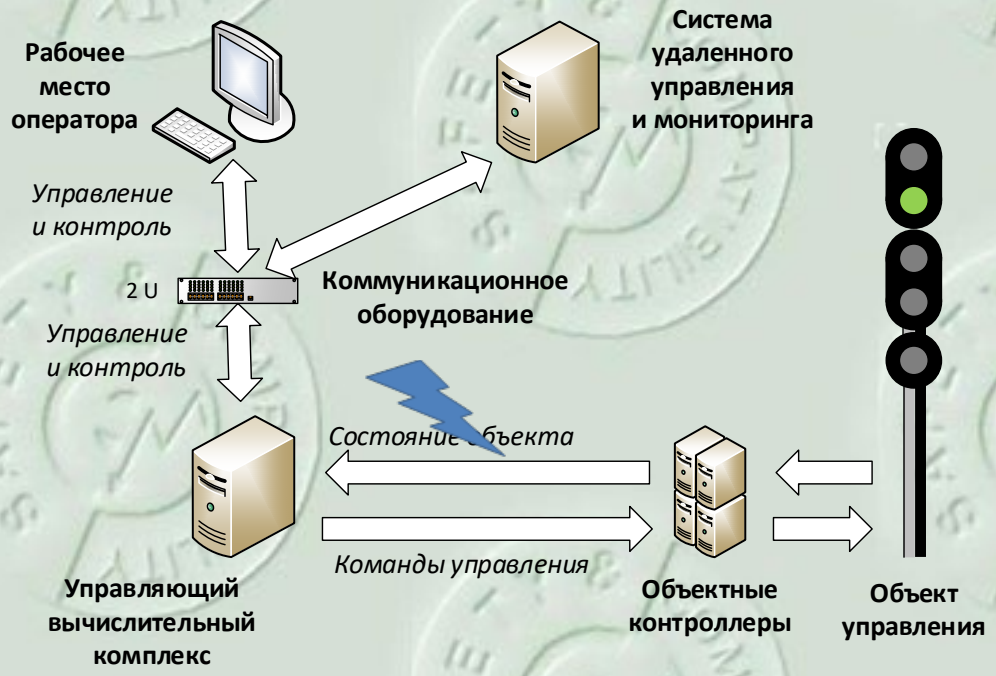
Программно-технические меры ФБ:
- двухканальная архитектура УВК, каждая команда для успешной реализации должна быть независимо принята обоими каналами, пройти процедуру кросс-сравнения;
- применение различных форматов команд и алгоритмов вычисления контрольных сумм для разных каналов (диверситет).

Непосредственное воздействие на УВК в результате кибератак является **крайне редким.**

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Направления возможных кибератак на объекты нижнего уровня

–воздействие на каналы связи между ОК и УВК с целью исказить или подменить команды управления или статусы.



Организационные меры ФБ:
- сеть передачи данных между ОК и УВК не выходит за пределы помещения запираемого поста МПЦ;
- конфигурация сети объектных контроллеров определена проектом, постоянна и не изменяется во время эксплуатации;
- доступ к ОК только через интерфейс ОК-УВК. Беспроводный интерфейс не применяется.

Программно-технические меры ФБ:
- двухканальная архитектура системы передачи данных;
- проверка принятых команд и статусов на соответствие временных меток, идентификаторов источника и пункта назначения, контрольных сумм и других средств защиты в соответствии с ГОСТ Р МЭК 62280
- применение различных форматов команд и алгоритмов вычисления контрольных сумм для разных каналов (диверситет).

В этом случае система передачи данных считается **закрытой**, несанкционированное подключение к каналам связи считается невозможным.

Непосредственное воздействие в результате кибератак является **крайне редким.**

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Направления возможных кибератак на объекты верхнего уровня

– воздействие на УВК через коммуникационное оборудование посредством стандартных интерфейсов.

Обычно реализована сеть второй категории, например, использование корпоративной сети передачи данных или сети с ограниченным доступом либо сеть третьей категории (открытая), при этом существует реальная возможность несанкционированного подключения и попыток получить доступ к коммуникационному оборудованию и каналам связи.

Непосредственное воздействие на УВК в результате кибератак является **редким** (есть вероятность того, что событие будет иногда возникать на протяжении жизненного цикла. Обоснованное ожидание возникновения опасного события)

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Направления возможных кибератак на объекты верхнего уровня

В настоящее время для защиты от угроз информационной безопасности по каналам удаленного управления применяется комплексный подход:

– со стороны функциональной безопасности: исключение передачи ответственной информации, искажение которой может привести к опасным последствиям. При этом в самом худшем случае могут быть реализованы **только угрозы, вызывающие снижение эффективности процесса перевозок или вызывающие ухудшение показателей надежности** функционирования устройств ЖАТ. Возможность реализации угроз, вызывающих нарушение требований безопасности движения поездов, будет блокироваться УВК или объектными контроллерами. Функциональная безопасность обеспечивается специальными протоколами обмена информацией на основе ГОСТ Р МЭК 62280 – 2017;

– со стороны информационной безопасности: классические решения по определению несанкционированных подключений, анализу трафика, криптозащиты, односторонней передаче информации и другие меры защиты.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Оценивание риска

Пример принимаемых решений по результатам оценивания риска по ГОСТ 33433-2015:

Уровень риска	Решение
Недопустимый	Риск должен исключаться. Обработка риска необходима.
Нежелательный	Риск должен быть снижен. Обработка риска необходима.
	Риск может быть принят при согласии руководства организации в случае, когда снижение риска невыполнимо или нецелесообразно. Обработка риска сводится к устранению последствий.
Допустимый	Риск принимается при соответствующем мониторинге и контроле и при согласии руководства организации. Обработка риска не требуется или сводится к устранению последствий.
Не принимаемый в расчет	Риск принимается без согласия руководства организации. Обработка риска не требуется.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Оценивание риска

Матрица рисков по ГОСТ 33433-2015

Уровень частоты	Уровень тяжести последствий			
	Незначительный	Несущественный	Критический	Катастрофический
Частое	*Нежелательный*	*Недопустимый*	*Недопустимый*	*Недопустимый*
Вероятное	*Допустимый*	*Нежелательный*	*Недопустимый*	*Недопустимый*
Случайное	*Допустимый*	*Нежелательный*	*Нежелательный*	*Недопустимый*
Редкое	*Не принимается в расчет*	*Допустимый*	*Нежелательный*	*Нежелательный*
Крайне редкое	*Не принимается в расчет*	*Не принимается в расчет*	*Допустимый*	*Допустимый*
Маловероятное	*Не принимается в расчет*	*Не принимается в расчет*	*Не принимается в расчет*	*Не принимается в расчет*

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Оценивание риска

ID	Описание опасности	Последствия	Частота	Уровень риска
O1	непосредственное воздействие на объекты (стрелки и сигналы) или на интерфейсные линии между объектным контроллером и объектом управления	1) Катастрофические	1) Маловероятное	1) Не принимается в расчет
O2	непосредственное воздействие на ОК	2) Катастрофические	2) Крайне редкое	2) Допустимый
O3	воздействие на каналы связи между ОК и УВК	3) Катастрофические	3) Крайне редкое	3) Допустимый
O4	непосредственное воздействие на УВК	4) Катастрофические	4) Крайне редкое	4) Допустимый
O5	воздействие на УВК через коммуникационное оборудование посредством стандартных интерфейсов	5) Несущественные	5) Редкое	5) Допустимый

Методы функциональной безопасности достаточно эффективными. Применение дополнительных мер не требуется.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Требования информационной безопасности к системе МПЦ

По результатам оценки риска можно сформулировать основные требования информационной безопасности к системе МПЦ, при выполнении которых методы функциональной безопасности будут наиболее эффективны:

1 Должен быть исключен непосредственный физический доступ посторонних лиц к объектным контроллерам, УВК и сети передачи данных между ОК и УВК.

2 Сеть передачи данных между ОК и УВК должна быть организована как система передачи данных первой категории согласно ГОСТ Р МЭК 62280 – 2017.

3 На ОК и УВК должны быть предусмотрены средства контроля целостности программ и данных, которые должны исключать любое несанкционированное изменение программ и данных с помощью вредоносного ПО, в том числе компьютерных вирусов, через каналы удаленного управления и мониторинга. В случае нарушения целостности программ и данных должен быть обеспечен механизм перехода в защитное состояние, в котором должны быть исключены угрозы безопасности движения поездов.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Требования информационной безопасности к системе МПЦ

4 Через каналы удаленного управления и мониторинга по возможности должна быть исключена передача информации, связанной с обеспечением безопасности движения поездов. В случае необходимости передачи такой информации по открытым сетям (система передачи данных третьей категории) должны применяться дополнительные методы контроля несанкционированных подключений, анализа трафика, криптозащиты, односторонней передачи информации и другие меры защиты. Эффективность принятых мер должна подтверждаться в рамках процедур верификации и валидации и их результаты включаться в документ «Доказательство безопасности».

5 Локальные и удаленные автоматизированные рабочие места эксплуатационного персонала должны быть обеспечены средствами защиты от несанкционированного доступа, включающими средства разграничения доступа и средства учета (протоколирования) доступа.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Требования информационной безопасности к системе МПЦ

6 Программное обеспечение всех составных частей системы МПЦ должно проходить экспертизу исходного кода на отсутствие недекларированных возможностей.

7 Должны быть разработаны процедуры внесения изменений в существующее ПО и установки новых версий ПО, исключающие любое несанкционированное изменение программ и данных с помощью вредоносного ПО, в том числе компьютерных вирусов, с помощью инструментальных средств разработки и установки ПО.

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24

Выводы

Для эффективной реализации защиты от рассмотренных выше угроз, наиболее перспективной является интеграция требований информационной безопасности в требования функциональной безопасности на ранних стадиях жизненного цикла. Работы необходимо выполнять параллельно, все конфликты должны при этом разрешаться с приоритетом функциональной безопасности

В этом случае реализация требований информационной безопасности может быть выполнена в жизненном цикле функциональной безопасности

Применение предложенной в работе классификации угроз информационной безопасности через возможность обеспечивать безопасность движения поездов, позволит применять для оценки и подтверждения соответствия средств защиты опробованные методы функциональной безопасности, такие как анализ рисков, анализ видов, последствий и критичности отказов, а также методы защиты от систематических отказов, вызванных человеческими ошибками на этапах разработки и эксплуатации системы.

Результаты такой деятельности должны найти свое отражение в доказательстве безопасности систем ЖАТ

34, Kirov str., 246653 Gomel, Belarus, Laboratory “Safety & EMC of hardware”
E-mail: hsn2013@tut.by, bochkov1999@mail.ru Tel.: + 375 232 95 39 06, +375 232 20 22 24