Список литературы

1 ГОСТ Р МЭК 61508-4–2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 4. Термины и определения. – Введ. 2013-08-01. – М. : Стандартинформ, 2014. – 36 с.

2 ГОСТ 33477–2015. Система разработки и постановки продукции на производство. Технические средства железнодорожной инфраструктуры. Порядок разработки, постановки на производство и допуска к применению. – Введ. 2016-07-01. – М. : Стандартинформ, 2016. – 44 с.

3 ТР ТС 003/2011. О безопасности инфраструктуры железнодорожного транспорта» (в редакции 2023 года). – Введ. 2011-11-09. – М. : Госстандарт, 2012. – 39 с.

4 ГОСТ 33436.4-1–2015. Совместимость технических средств электромагнитная. Системы и оборудование железнодорожного транспорта. Ч. 4-1. Устройства и аппаратура железнодорожной автоматики и телемеханики. Требования и методы испытаний. – Введ. 2016-09-01. – М. : Стандартинформ, 2016. – 21 с.

УДК 621.38

ОЦЕНКА РИСКОВ УГРОЗ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

К. А. БОЧКОВ, С. Н. ХАРЛАП, К. Я. ШАБЛОВСКИЙ
Белорусский государственный университет транспорта, г. Гомель

С. Г. ХАЛАМОВ, С. В. МОЛОТ, А. М. АКСЁНОВ
Производственное объединение «Белоруснефть», г. Гомель

В современных условиях кибербезопасность – одна из ключевых проблем критически важных отраслей, таких как железнодорожный транспорт [1]. В связи с цифровизацией и необходимостью повышения производительности и ремонтопригодности ранее изолированные системы управления железнодорожным транспортом теперь подключены к глобальным сетям и все чаще используют стандартные протоколы и коммерческие компоненты. Цифровизация предполагает широкое использование сетевых систем управления и автоматизации, доступ к которым возможен удаленно через общедоступные и частные сети. На железнодорожном транспорте также применяются открытые сети передачи данных для передачи ответственной информации, что приводит к появлению дополнительных рисков нарушения требований функциональной безопасности при искажении критической информации. В случае применения систем искусственного интеллекта для принятия ответственных решений по управлению железнодорожным транспортом, перед системами железнодорожной автоматики и телемеханики (ЖАТ) возникают новые опасности и риски, связанные с принятием неверных решения под воздействием кибератак.

В силу особенностей систем ЖАТ для них актуальны только киберугрозы, которые связаны с вмешательством в нормальное функционирование системы. Поэтому для систем ЖАТ оправдано рассмотрение угроз кибербезопасности с точки зрения их влияния на безопасность движения поездов. В связи с этим возможные угрозы кибербезопасности для систем ЖАТ можно классифицировать следующим образом:

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

На сегодняшний день единственным способом оценить киберзащищенность системы является качественный анализ, основанный на анализе рисков [2]. Для этого возможно применение методов анализа риска, используемых в функциональной безопасности, в частности матрицы рисков [3] (таблица 1).

Таблица 1 – **Матрица рисков**

Уровень частоты события	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

Для составления матрицы рисков необходимо определить частоты и оценить последствия киберинцидента. Пример нормирования последствий киберинцидентов исходя из предложенной классификации угроз приведен в таблице 2. Классификация последствий выполнена по ГОСТ 33433–2015 [3]. Частота допустимого риска взята из нормативных документов по функциональной безопасности (ФБ).

Рассмотрим оценку последствий для наиболее часто встречающихся угроз в сетях автоматизированных систем управления технологическим процессом (АСУ ТП) на примере системы микропроцессорной централизации стрелок и сигналов (МПЦ) (рисунок 1), осуществляющей управление движением поездов на станции.

Таблица 2 – **Пример нормирования последствий**

Угрозы	Типовые последствия, ущерб
Вызывающие нарушение требований безопасности движения поездов	**Катастрофический:** гибель одного человека или более, тяжкий вред здоровью пяти человек и более, связанных с функционированием железнодорожного транспорта
Вызывающие снижение эффективности процесса перевозок	**Несущественный:** задержка движения поездов на несколько часов, повреждение объекта инфраструктуры, требующее проведения ремонта для восстановления его работоспособного состояния
Вызывающие ухудшение показателей надежности функционирования	**Незначительный:** отказы, элементов, модулей и подсистем, не нарушающих работоспособность объекта инфраструктуры, требующих регулярного технического обслуживания

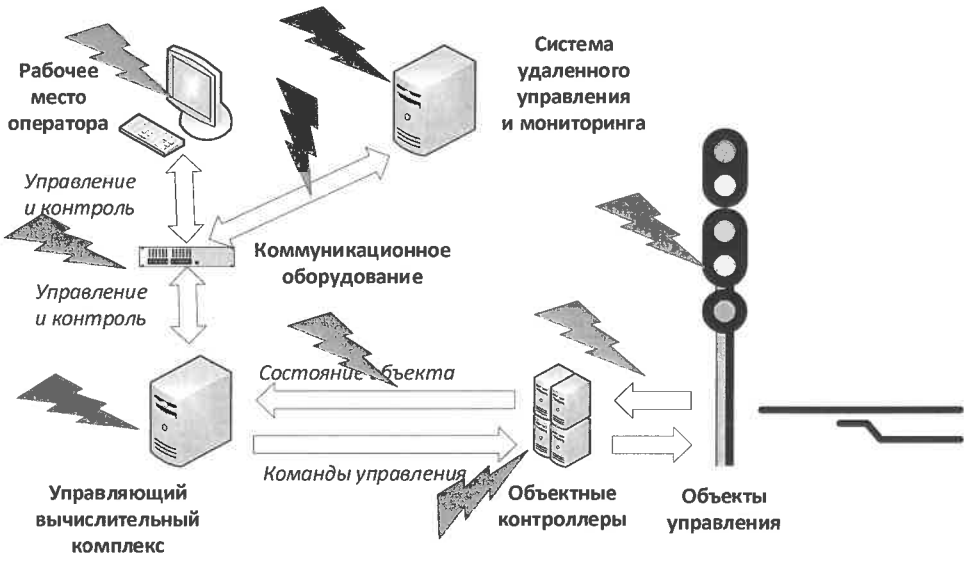

Рисунок 1 – Направления возможных кибератак системы МПЦ

Система МПЦ имеет три основных уровня иерархии (снизу вверх): объектные контроллеры (ОК), управляющий вычислительный комплекс (УВК) и рабочее место человека-оператора (АРМ).

Анализ направления возможных кибератак на объекты нижнего и среднего уровня (см. рисунок 1) позволяет выделить следующие угрозы:

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

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

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

– непосредственное воздействие на УВК с целью исказить алгоритм функционирования.

Очевидно, что вмешательство в работу объектов нижнего и среднего уровня МПЦ может вызвать крушение, гибель людей, т. е. приводит к катастрофическим последствиям (см. таблицу 2).

Аналогично для верхнего уровня можно выделить следующие угрозы возможных кибератак:

– воздействие на коммуникационное оборудование с целью исказить или подменить команды управления или статусы;

– воздействие на АРМ и канал связи между УВК и АРМ;

– воздействие на систему удаленного управления и мониторинга, а также канал связи между УВК и системой удаленного управления и мониторинга.

Пример более детального анализа опасных последствий кибератак на систему удаленного управления и мониторинга приведен в таблице 3.

Таблица 3 – **Пример анализа последствий**

ID опасности		Описание опасности	Причина	Последствия	Уровень тяжести последствий
О1		Шифрование файлов, хранящихся на заражённой машине, в том числе исполняемых файлов программ	Проникновение трояновшифровальщиков	Невозможность выполнять необходимую работу на данной машине. Финансовые издержки, связанные с восстановлением зашифрованных данных	Несущественный
О2		Получение несанкционированного доступа к системе	Проникновение троянских программ, нацеленных на получение доступа к управлению системой, закреплению там, горизонтальное и вертикальное распространение	Выход из строя оборудования, ложное формирование ответственных команд, что может привести к угрозам жизни и здоровья людей	Катастрофический
О3	О3.1	Установка майнеров	Проникновение программ *keygen*	«Забивание трафика», сети предприятия	Несущественный
	О3.2	Шпионского ПО		Создание *backdoor*	

Таким образом, последствия вмешательства в работу объектов верхнего уровня МПЦ (за исключением ответственных команд, которые передаются по специальному протоколу) в самом худшем случае могут привести к снижению эффективности процесса перевозок или вызвать ухудшение показателей надежности функционирования устройств ЖАТ. Возможность реализации угроз, вызывающих нарушение требований безопасности движения поездов, будет блокироваться УВК или объектными контроллерами. Таким образом, в целом можно классифицировать данные последствия как несущественные (см. таблицу 2).

При оценке рисков функциональной безопасности в качестве частот опасных событий принимается интенсивность опасных отказов системы, которая может быть получена расчетными методами при выполнении *FMECA*-анализа. К сожалению, для определения частот опасных событий, связанных с кибератаками, нет тривиального решения. На данный момент существуют три основных метода:

– экспертная оценка;

– проведение пентеста до установки защитного ПО и после его установки с последующим сравнением времени, необходимого для наступления опасного события;

– сбор и анализ статистических данных.

Данные методы имеют недостатки, которые приведены в таблице 4.

Таблица 4 – **Способы определения частот и их недостатки**

Название	Недостаток
Экспертная оценка	Эффективность зависит от квалификации эксперта
Проведение пентестов	Дорого. Позволяет обнаружить и закрыть обнаруженные уязвимости, но не гарантирует того, что взлом не будет осуществлен через необнаруженные уязвимости
Статистика кибератак	Данные быстро устаревают с появлением новых угроз

Для устранения указанных недостатков можно применять следующие мероприятия:

– для экспертных методов: вынесение решения несколькими экспертами;

– для пентестов: предоставлять инфраструктуру для проведения программы *bug bounty* [4], что позволит на постоянной основе оценивать уровень защищённости инфраструктуры с помощью финансово заинтересованных специалистов;

– для статистических методов: централизованный сбор информации и обмен статистическими данными между отделами кибербезопасности предприятий для более быстрого набора достаточного объема статистических данных.

В заключение следует отметить, что для эффективной оценки рисков кибератак достаточно обоснованным является использование методов анализа риска, получивших широкое применение при оценке функциональной безопасности. В частности, можно воспользоваться матрицей рисков, для составления которой необходимо предварительно выявить последствия и частоты наступления опасных событий. Для повышения эффективности оценки рисков необходимо совершенствовать способы оценки частот опасных событий.

Список литературы

1 PDCLC/TS 50701:2023 Railway applications. Cybersecurity. – BSI, 2023. – P. 164.

2 **Гордейчик, С. В.** Кибербезопасность микропроцессорных систем управления на железнодорожном транспорте / С. В. Гордейчик. – М. : Горячая линия – Телеком, 2021. – 120 с.

3 ГОСТ 33433–2015. Безопасность функциональная. Управление рисками на железнодорожном транспорте. – Введ. 2016-09-01. – М. : Стандартинформ, 2020. – 34 с.

4 Bug Bounty [Электронный ресурс] // Википедия. Свободная энциклопедия. – Режим доступа : https://ru.wikipedia.org/wiki/Bug_Bounty. – Дата доступа : 10.10.2024.

УДК 681.5.09

ПОДХОДЫ К ДОКАЗАТЕЛЬСТВУ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ, ТЕЛЕМЕХАНИКИ И СВЯЗИ

Н. А. БОЯРИНОВА, Н. Г. ПЕНЬКОВА, В. В. БАТРАЕВ, Е. С. РОДИМАНОВА
Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте (АО «НИИАС»), г. Москва, Российская Федерация

Стратегия и методология доказательства функциональной безопасности беспилотных систем управления движением на железнодорожном транспорте находится в начальной стадии развития как в России, так и за рубежом. Кроме того, информационных материалов по этой теме значительно меньше, чем в автомобильной отрасли.

Действующая в области железнодорожной автоматики нормативная база предполагает в качестве обязательного условия для допуска системы, отвечающей за безопасность движения, в опытную и постоянную эксплуатацию наличие положительного независимого экспертного заключения по документу «Доказательство безопасности». Назначение Доказательства безопасности, а также основные требования к порядку его разработки, структуре и содержанию определены в межгосударственном стандарте ГОСТ 33432–2015 «Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта». В соответствии с указанным стандартом обозначенный документ предназначен для аккумулирования всей совокупности материалов доказательного характера и отражения результатов работ по обеспечению требований безопасности на всех этапах жизненного цикла.

В процессе разработки системы управления движением поездов на Московском центральном кольце (МЦК) специалисты АО «НИИАС» столкнулись с отсутствием в действующих стандартах требований безопасности к некоторым новым функциям. Вопросы обеспечения функциональной безопасности хорошо развиты для традиционных систем микропроцессорной централизации, автоблокировки, локомотивной сигнализации. Для инновационных систем вопросы нормирования показателей безопасности и доказательства их выполнения проработаны не достаточно. Текущее исследование посвящено методам и подходам, которые могут быть использованы для доказательства безопасности систем, требования к которым не определены в нормативных документах отрасли.

В качестве примера рассматриваются системы интервального регулирования с использованием технического зрения, включая 4-й уровень автоматизации по ГОСТ Р 70059–2022 « Национальный стандарт Российской Федерации. Системы управления и контроля железнодорожного транспорта для перевозок пассажиров в пригородном сообщении. Принципы построения и основные функциональные требования».