Введение

Обеспечение безопасности движения поездов является одной из важнейших задач, стоящих перед железнодорожным транспортом. Системы железнодорожной автоматики и телемеханики (ЖАТ) во многом определяют пропускную и провозную способность, обеспечивают безопасность движения. В настоящее время для управления процессом перевозок широко применяются системы микропроцессорной и диспетчерской централизации (МПЦ и ДЦ), локомотивные устройства безопасности (АЛСН, САУТ, КЛУБ), тестируются системы автоведения. Системы микропроцессорной горочной автоматической централизации дают возможность оптимизировать процесс формирования составов и пересмотреть перечень запрещенных к роспуску вагонов, что дает колоссальные резервы в переработке. Микропроцессорные системы также внедряются в локомотивном хозяйстве для решения задач управления электропередачей локомотивов, в хозяйстве ЭЧ, в системах релейной защиты.

Применение подобных систем выдвигает новые требования к инфраструктуре связи, что влечет за собой массовое внедрение цифровых систем проводной и радиосвязи, поддерживающих протокол TCP/IP.

Внедрение микропроцессорных систем управления дает широкие возможности по оптимизации процесса перевозок, масштабированию управления и автоматизации контроля и диагностики. Однако, с другой стороны, использование стандартного системного и прикладного программного обеспечения, сетевых протоколов, распространённых технологий АСУ ТП, в сочетании с широким применением механизмов удаленного управления, диспетчерской централизации и диспетчерского контроля, приводит к наследованию проблем кибербезопасности типовых компонентов.

Немаловажными факторами являются большая интеграция с СПД, широкое использование беспроводных технологий, внедрение интерактивных информационных сервисов, что приводит к увеличению поверхности атак, расширению числа потенциальных источников негативного информационного воздействия и компьютерных атак.

Исследования в области информационной безопасности АСУ ТП и ряд инцидентов продемонстрировали возможность использо-

вания методов и подходов, традиционно использовавшихся при нарушении информационной и компьютерной безопасности, для реализации угроз функциональной безопасности, надежности и безопасности технологического процесса.

Определенным толчком в пересмотре отношения к устойчивости МПСУ к компьютерным атакам стала серия инцидентов, связанных с масштабными компьютерными атаками на АСУ ТП различных предприятий. Выявленный в 2010 году компьютерный червь Stuxnet [1], используя традиционные для программ подобного класса методы распространения, взаимодействия со злоумышленником и противодействия обнаружению, конечной целью имел деструктивное воздействие на технологический процесс.

Используя уязвимости операционных систем семейства Microsoft Windows и особенности АСУ ТП на основе SCADA Siemens SIMATIC WinCC и PLC S7-400, вредоносное ПО изменяло режим работы электродвигателей центрифуг урановой обогатительной фабрики в Натанзе (Ирак), что приводило к возникновению биений, вызвавших ускоренный износ [2]. Ряд источников указывает, что в результате атаки было выведено из строя 1368 из 5000 центрифуг, установленных на обогатительном предприятии

Эти атаки продемонстрировали возможность влияния методов и подходов, традиционно использовавшихся для нарушения информационной и компьютерной безопасности, функциональной безопасности, надежности и безопасности технологического процесса.

Немаловажным фактором в современном мире является геополитика. В задачи железнодорожного транспорта, как стратегической отрасли народного хозяйства, входит обеспечение живучести в случае негативных воздействий со стороны других государств, обеспечение воинских перевозок. В то же время ведущие государства мира осуществляют развитие военных подразделений, ориентированных на действия в киберпространстве.

В качестве примера можно привести Кибернетическое командование США, созданное в 2010 году и направленное на подготовку и осуществление полного спектра военных операций в киберпространстве, в том числе и наступательных. Данное подразделение насчитывало в 2019 году около 6200 сотрудников [3]. Таким образом, ситуация в мире требует иметь возможность противостоять угрозам критической инфраструктуре, к которой относится в том числе и железнодорожный транспорт.

В связи с этим при проектировании, разработке и внедрении систем железнодорожной автоматики и телемеханики, основанных

на микропроцессорных системах управления, требуется учет возможности целенаправленного дистанционного антропогенного воздействия с использованием информационных технологий, негативно влияющего на безопасность движения, заданного уровня пропускной и провозной способности железных дорог и надежности оборудования.

Целью данной работы является разработка методического обеспечения повышения устойчивости МПСУ ЖАТ к компьютерным атакам и определение перспективных направлений развития кибербезопасности МПСУ ЖАТ с учетом требований информационной и функциональной безопасности и безопасности движения. Для достижения поставленной цели решались следующие основные задачи:

- определение задач повышения устойчивости к компьютерным атакам применительно МПСУ ЖАТ, влияния атак на функциональную безопасность, экономическую эффективность процесса перевозок и безопасность движения;
- определение подходов к построению процессов обеспечения устойчивости МПСУ ЖАТ к компьютерным атакам, учитывающих современные угрозы, состояние нормативной базы и требования безопасности движения;
- разработка и апробация методик анализа защищенности МПСУ ЖАТ, учитывающих влияние уязвимостей и дефектов на устойчивость МПСУ ЖАТ к компьютерным атакам, безопасность движения и надежность;
- разработка требований к специализированным средствам защиты МПСУ ЖАТ.

На основе этого подхода сформулированы ключевые этапы процессов обеспечения устойчивости к компьютерным атакам. Предложены и апробированы методика разработки модели угроз МПСУ ЖАТ, методика анализа защищенности ПТК МПСУ и технические характеристики перспективных средств защиты МПСУ.

Большая часть работы основывается на практическом опыте автора и возглавляемого им коллектива. По результатам более чем десятков проектов по анализу устойчивости АСУ ТП к компьютерным атакам для различных отраслей, включая специфичные для ЖТ системы, был использован индуктивный подход для разработки методик анализа защищенности, разработки требований по кибербезопасности и частных моделей угроз (МПЦ, СИМ и т. д.), требования к перспективным системам защиты. Требования к перспективным системам защиты основаны на теории автоматов и подходах имитационного моделирования.

1 Проблема устойчивости МПСУ ЖАТ к компьютерным атакам

1.1. Современное состояние киберзащищенности АСУ ТП

Практический анализ защищенности ряда широко используемых МПСУ ЖАТ показал наличие дефектов и уязвимостей, использование которых злоумышленником позволяет не только снижать ключевые показатели надежности и обходить механизмы функциональной безопасности, но и реализовывать атаки, напрямую влияющие на безопасность движения. При этом с точки зрения информационной и функциональной безопасности данные системы соответствуют всем выдвигаемым требованиям, имеют все необходимые международные, отраслевые и государственные сертификаты.

Основным отличием кибернетических негативных воздействий на СЖАТ от привычных «несанкционированных перемычек» является возможность проведения атак удаленно (при отсутствии непосредственного физического доступа), а также простота сокрытия доказательств, позволяющих восстановить причину инцидента (так называемая «безуликовость»).

В настоящее время вопрос влияния информационной безопасности на современные автоматизированные системы управления технологическим процессом (АСУ ТП) широко обсуждаются в научных и инженерных кругах в России и за рубежом.

Основным направлением развития здесь являются попытки адаптации опыта, наработанного в области информационной безопасности, к кибербезопасности АСУ ТП по трем направлениям:

- анализ и оценка защищенности кибербезопасности АСУ ТП;
- разработка нормативного и методического обеспечения;
- разработка специализированных методов и средств обеспечения кибербезопасности.

Анализ и оценка кибербезопасности систем АСУ ТП не носит систематического характера. Подобные работы часто проводятся в рамках корпоративного заказа, и в данном случае результаты исследований не публикуются. Однако в некоторых случаях информация

об уязвимостях открыто обсуждается на научно-практических конференциях. В 2013 году на конференции SCADA Security Scientific Symposium был представлен доклад об анализе уязвимостей платформы Siemens SIMATIC [4], элементы которой используются в системе железнодорожной автоматизации Siemens Sibas PN [5].

Одной из проблем является отсутствие скоординированной активности в данной области. Частично проблему пытаются решить государственные и отраслевые команды реагирования на инциденты компьютерной безопасности (Computer emergency response teams, CERT). Наиболее авторитетной организацией в данном отношении представляется подразделение Министерства Внутренней Безопасности США (US Department of Homeland Security) ICS-CERT [6]. Эта организация отслеживает информацию о публикуемых уязвимостях промышленных систем и координирует взаимодействие производителей и исследователей. В Европе эти задачи выполняет ENISA, рассматривающая ЖД транспорт как одну из подсистем общественного транспорта «умных городов» [7].

Кроме открытой части существует ряд организаций, специализирующихся на выявлении и перепродаже информации о выявленных уязвимостях и методов проведения атак. Примерами подобных организацией является компании ZDI, Zerodium, Exodus Intelligence.

Основной тенденцией здесь является рост числа выявляемых уязвимостей и методов атак. Если в 2012 году число выявленных известных дефектов не превышало 100 единиц [8], то к началу 2015 года это значение превысило 800 [9]. Согласно исследованиям команды SCADA StrangeLove, представленным на Chaos Communication Congress в Германии [10, 11], большая часть уязвимостей выявлена в продуктах крупных производителей: Siemens, Honeywell, Schneider Electric, причем соотношение устраненных и выявленных уязвимостей составляет около 65%, т. е. около 35% известных уязвимостей не имеют решения.

В части нормативного обеспечения кибербезопасности наиболее ярким представителем является семейство стандартов ANSI/ISA-62443, адаптированное в качестве ГОСТ Р МЭК 62443. Ряд требований к безопасности АСУ ТП изложен в документе «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [12], принятом в Приказе №31 ФСТЭК России от 14 марта 2014 г.

Отраслевые документы в области безопасности АСУ ТП наиболее хорошо развиты в энергетической отрасли. В большинстве случаев основой для них являются стандарты защиты критической инфраструктуры NERC CIP [13]. На железнодорожном транспорте требования по кибербезопасности изложены в технических регламентах Таможенного Союза «О безопасности железнодорожного подвижного состава» (ТР ТС 001/2011) [14], «О безопасности высокоскоростного железнодорожного транспорта» (ТР ТС 002/2011) [15], «О безопасности инфраструктуры железнодорожного транспорта» (ТР ТС 003/2011) [16]. Однако данные документы выдвигают достаточно поверхностные требования, сводящиеся к обеспечению «защищенности от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных изменений информации». Как видим, в данном случае речь опять идет в основном о «случайных воздействиях», не учитывающих целенаправленную атаку. Однако в документе присутствует упоминание «несанкционированного доступа», что косвенно вводит антропогенный фактор.

Стандарт ГОСТ Р 52980-2008 [17] устанавливает требования к программному обеспечению (ПО) устройств и систем, связанных с безопасностью на железнодорожном транспорте, в том числе используемому для разработки систем, связанных с безопасностью. Требования к безопасности программного обеспечения являются основополагающими для обеспечения кибербезопасности.

Стандарт СТО РЖД 02.049-2014 [18] рассматривает автоматизированные системы управления технологическими процессами на железнодорожном транспорте. Документ устанавливает порядок проведения оценки соответствия ПО АСУ ТП требованиям функциональной безопасности и информационной безопасности, а также оценки киберзащищенности ПО АСУ ТП. В соответствии со стандартом, «оценку соответствия ПО АСУ ТП требованиям ИБ проводят с целью проверки обеспечения защиты информации, обработку которой осуществляет АСУ ТП, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования АСУ ТП».

СТО РЖД 02.049-2014 может быть применен для оценки соответствия объектов ЖТ, использующих МПСУ, требованиям

ФСТЭК России к информационной безопасности этих объектов, рассматриваемых как автоматизированные системы управления. Тем не менее эффективному обеспечению кибербезопасности на объектах ЖТ препятствует отсутствие политики предотвращения инцидентов, связанных с отказом технических средств вследствие кибератак, и недостаточно определенная методическая база для поддержки процесса этого обеспечения.

В открытом доступе отсутствует информация о стандартах ОАО РЖД определяющих порядок описания модели угроз безопасности МПСУ ЖАТ и выбора (на основе этой модели угроз) мер безопасности, перечисленных Приказом № 31 ФСТЭК России. А именно эти мероприятия являются ключевыми как в обеспечении соответствия требованиям ФСТЭК, так и в построении эффективной системы защиты от атак. Применение стандарта для оценки киберзащищенности в таких условиях (и с учетом скудного опыта большинства оценивающих организаций по проведению экспертизы с учетом специфики объектов ЖТ) сильно затруднено. Во главу угла поставлено не потенциальное влияние направленного человеческого фактора на функционирование МПСУ, а определение несанкционированного доступа к информации. Приведенные стандарты в целом не определяют требования к безопасности ПО с учетом целенаправленных компьютерных атак.

Учитывая, что основной задачей кибербезопасности применительно к железнодорожному транспорту является обеспечение безопасности перевозок, важным является учет научного и практического опыта в области функциональной безопасности МПСУ ЖАТ. Анализ тематических научных публикаций показывает, что до недавнего времени основным направлением исследований и разработок было обеспечение достаточного уровня надежности и функциональной безопасности МПСУ [19–21].

В большинстве работ антропогенные угрозы сводились к ошибкам оператора и обслуживающего персонала. Такой подход был достаточен при отсутствии возможности широкомасштабных удаленных воздействий. Однако, в настоящий момент использование распределенных системы связи, беспроводных технологий, систем ДЦ и ДК требует пересмотра данной концепции. Такое ограничение не позволяет учитывать актуальные угрозы, связанные с возможностью удаленного воздействия на МПСУ, и, как следствие, не дает возможности сформировать объективную картину безопасности движения при использовании МПСУ.

Таким образом, нормативные, организационные и технические

вопросы кибербезопасности и устойчивости к кибератакам современных систем МПСУ на железнодорожном транспорте проработаны достаточно слабо и существует разрыв между подходами и методами обеспечения информационной безопасности и практикой решения задач безопасности движения.

1.2. Определение кибербезопасности

Для определения направлений совершенствования методического обеспечения кибербезопасности и устойчивости МПСУ ЖАТ к компьютерным атакам с учетом требований информационной и функциональной безопасности и безопасности движения необходимо определить предмет и задачи кибербезопасности МПСУ ЖАТ.

Кибербезопасность и устойчивость систем ЖАТ к компьютерным атакам — процесс обеспечения функционирования МПСУ ЖАТ, при котором отсутствуют опасные отказы и недопустимый ущерб, обеспечивается заданный уровень функциональной безопасности и надежности с учетом вероятности целенаправленного негативного антропогенного информационного воздействия на компоненты МПСУ.

В рамках развития этой концепции предлагается рассмотреть вопрос кибербезопасности МПСУ ЖАТ, используя методический аппарат трех дисциплин: безопасности движения, функциональной безопасности и информационной безопасности [22] (рис. 1).

Необходимость синтеза различных научных направлений обусловлена, с одной стороны, возможностью применения наработанных научных и методических инструментариев, а с другой стороны — рядом ограничений, не позволяющих применять каждую из дисциплин самостоятельно для решения поставленных задач. Так, функциональная безопасность связана с непреднамеренно вызванными от-

Рис. 1. Дисциплины, связанные с кибербезопасностью

Таблица 1

Определение кибербезопасности МСУ ЖАТ через смежные дисциплины

Дисциплина	Используемые методики
Безопасность движения	Требования к уровню безопасности Функциональные требования к МПСУ
Функциональная безопасность и теория надежности	Методический аппарат анализа рисков Методы доказательства безопасности Оценка эффективности средств защиты
Информационная безопасность	Методический аппарат моделирования угроз Методики анализа защищенности Процессы, средства и механизмы защиты Оценка эффективности средств защиты

казами в выполнении отдельных функций системы и не учитывает целенаправленных угроз, а информационная безопасность направлена на обеспечение целостности, доступности и конфиденциальности информации, что напрямую не связанно с задачами безопасности движения.

Основным преимуществом данного подхода является возможность интеграции предмета кибербезопасности и задач обеспечения устойчивости систем ЖАТ к компьютерным атакам в существующие процессы проектирования, разработки и внедрения систем МПСУ ЖАТ, используя зарекомендовавшие себя наработки (табл. 1).

Определение предмета кибербезопасности через дисциплины безопасности движения, функциональной безопасности и информационной безопасности позволяет перейти к учету отраслевой специфики и оценивать влияние негативных воздействий в терминах опасных отказов и теории надежности, что позволяет встроить процессы кибербезопасности в существующие процессы обеспечения безопасности движения и экономической эффективности перевозок.

Воспользуемся понятийным аппаратом информационной безопасности для более полного понимания круга задач кибербезопасности применительно к железнодорожному транспорту.

1.3. Классы угроз

Основой обеспечения кибербезопасности и устойчивости систем ЖАТ к компьютерным атакам является корректное определение угроз. Можно выделить три основных класса угроз МПСУ ЖАТ, используя для группировки потенциальный ущерб, связанный с реализацией атаки.

1. Нарушение безопасности движения: реализация угроз непосредственно влияет на безопасность движения.

2. Снижение эффективности процесса перевозок: реализация угроз явно снижает пропускную или проездную способность или другие количественные экономические показатели процесса перевозки.

3. Другие нарушения функциональной безопасности и надежности: реализация угроз непосредственно не влияет на безопасность движения, но оказывает косвенное влияние на качественные или количественные показатели эффективности процесса перевозок, надежности и безопасности (SIL, наработка на отказ и т. д.).

Наиболее опасны угрозы, связанные с возможностью нарушения правил безопасности движения, установленных в ПТЭ, Инструкциях по сигнализации, Инструкциях по безопасности движения поездов и других основополагающих документах. Превышение максимальной допустимой скорости в кривых, задание враждебных маршрутов, изменение состояния сигналов на станции и перегонах — все эти действия потенциально можно выполнять в обход заложенных зависимостей.

Поскольку информационно-управляющие системы широко используются для оптимизации процесса перевозок, нарушение штатного функционирования микропроцессорных систем могут негативно влиять на эффективность. Так, системы интервального регулирования движения высокоскоростных поездов активно используют радиоканал для обмена информацией между локомотивом и диспетчерским центром и передачи информации об оптимальной скорости движения и состоянии сигналов и блок-участков по ходу движения. Однако в случае негативного воздействия на радиоканал, например, с использованием средств подавления диапазона ISM или GSM, использование радиоканала для определения скорости движения становится невозможным, что требует перехода на движение по сигналам трехзначной автоблокировки, т. е. ограничения максимальной скорости до 120 км/ч, что негативно сказывается на пропускной способности участка. В ряде европейских стран скорость движения при нарушении работоспособности радиоканала ограничена 40 км/ч.

Кибератаки могут приводить к ухудшению ключевых показателей функциональной безопасности и надежности. Так, при отсутствии адекватных средств защиты даже неспециализированные компьютерные вирусы могут негативно влиять на элементы МПЦ, например снижать производительность, блокировать или выводить из строя АРМ ДСП, использующий стандартную операционную систему семейства Windows. Это приводит к снижению значения нара-