УДК 004.738.5

Д-р техн. наук, проф. С. Е. АДАДУРОВ, канд. техн. наук С. В. ДИАСАМИДЗЕ, д-р техн. наук, проф. А. А. КОРНИЕНКО, канд. техн. наук А. А. СИДАК

Международная кибербезопасность на железнодорожном транспорте: методологические подходы и нормативная методическая база

Аннотация. Представлены методологические подходы и практические направления международного сотрудничества в области информационной безопасности и кибербезопасности на железных дорогах, одобренные созданной в рамках программы COLPOFER рабочей группой «Кибербезопасность на железнодорожном транспорте».

Проанализированы основные факторы и предпосылки необходимости защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак. Рассмотрен понятийный аппарат кибербезопасности. Изложены основные положения нормативных методических документов, разрабатываемых международной рабочей группой «Кибербезопасность на железнодорожном транспорте».

Охарактеризованы объекты информационной инфраструктуры железнодорожного транспорта с точки зрения подверженности их компьютерным атакам и выделены наиболее уязвимые элементы. Приведена классификация типов компьютерных атак и способы их реализации.

Рассмотрены основные организационные и технические меры защиты объектов информационной инфраструктуры железнодорожного транспорта от компьютерных атак.

Ключевые слова: кибербезопасность; информационная безопасность; компьютерная атака; защита информационной инфраструктуры

Факторы и предпосылки необходимости обеспечения защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак. Информационная сфера (информация, информационная инфраструктура, информационно-коммуникационные технологии), информационная безопасность и кибербезопасность начинают играть одну из ключевых ролей в обеспечении важных, прежде всего экономических, интересов транспортного комплекса России, в управлении отраслью и железнодорожным транспортом, в решении проблем безопасности движения, пассажирских и грузовых перевозок. Факторы информационной безопасности и кибербезопасности будут решающими при организации высокоскоростного движения и построении интеллектуальных центров и систем ситуационного управления, особенно с учетом исходящих из киберпространства угроз и потенциальной подверженности информационной инфраструктуры компьютерным атакам [1].

К основным общим факторам информационной безопасности и кибербезопасности можно отнести [2–6]:

1. Двойственную эволюцию такого явления в киберпространстве, как хактивизм: развитие его как социального протестного движения и в то же время постепенное превращение ряда хакеров и хакерских групп в киберпреступные сообщества.

2. Усиление информационного терроризма, принятие доктрин кибервойны и создание кибервойск США, Китаем, НАТО. Информация все чаще выступает инструментом мягкой силы и становится оружием массового поражения.

3. Рост числа прицельных (целенаправленных) компьютерных атак (Stuxnet, Flame, Duqu, Gauss, Red October, NetTraveler) на системы управления технологическими процессами критически важных объектов (вывод из строя энергосистем, объектов ядерной промышленности, других объектов жизнеобеспечения, кражи банковских активов и т. п.) и др.

Основными предпосылками обеспечения информационной безопасности и кибербезопасности железнодорожного транспорта (ЖТ) с акцентированием внимания на защите его информационной инфраструктуры (ИИ) от компьютерных атак являются следующие:

1. Интеграция в единые комплексы автоматизированных систем, связанных с управлением движением поездов, и других автоматизированных информационных и телекоммуникационных систем (АИТС) железнодорожного транспорта.

2. Постоянное усложнение программного обеспечения и оборудования, используемых в АИТС железнодорожного транспорта.

3. Практика осуществления разработчиками АИТС и поставщиками оборудования мониторинга, технического обслуживания и удаленной настройки АИТС в целом или их составных частей, а также серверного и телекоммуникационного оборудования, входящего в состав элементов информационной инфраструктуры железнодорожного транспорта.

4. Интенсивное совершенствование потенциальными нарушителями средств и методов использования информационных и телекоммуникационных технологий, методов социальной инженерии для нанесения ущерба, а также участившиеся попытки их применения в противоправных целях и конкурентной борьбе.

5. Риск сокрытия попыток или фактов нарушения штатного функционирования АИТС железнодорожного транспорта со стороны эксплуатирующих подразделений.

6. Временное вынужденное привлечение при создании АИТС, в том числе автоматизированных систем управления технологическими процессами (АСУ ТП), связанных с организацией и управлением движением поездов, представителей неконтролируемых фирм — производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации и применение неконтролируемых программно-аппаратных решений.

7. Рост в мире и стране количества противоправных действий с использованием информационных и телекоммуникационных технологий, в том числе компьютерных атак на железнодорожном транспорте.

Цели функционирования международной рабочей группы «Кибербезопасность на железнодорожном транспорте» и понятийный аппарат. Для совместного решения проблем информационной безопасности и кибербезопасности на железных дорогах России и Европы в рамках международной организации COLPOFER, объединяющей службы безопасности европейских железных дорог и подразделения полиции на железнодорожном транспорте, в 2013 г. под председательством ОАО «РЖД» была создана рабочая группа «Кибербезопасность на железнодорожном транспорте».

Были обозначены следующие цели функционирования этой рабочей группы:

• организация обмена опытом и информацией в области обеспечения кибербезопасности информационной инфраструктуры;

• разработка рекомендаций по защите информационной инфраструктуры;

• оказание методической и, при необходимости, иной поддержки на всех этапах организации защиты инфраструктуры от кибератак.

На заседаниях рабочей группы «Кибербезопасность на железнодорожном транспорте» российская сторона, опираясь на собственный опыт по созданию систем обеспечения и управления информационной безопасностью холдинга ОАО «РЖД», предложила к обсуждению как первоочередные следующие вопросы:

• формирование однозначно трактуемого понятийного аппарата и терминологии, разработка нормативных методических документов в области информационной безопасности и кибербезопасности на железнодорожном транспорте;

• разработка методологических подходов к защите от кибератак (компьютерных атак) в комплексе с минимизацией других угроз и обеспечением приемлемых рисков информационной безопасности;

• определение принципов организации работы в условиях полной или частичной невозможности использования устройств железнодорожной автоматики, связи, сигнализации и автоблокировки, средств вычислительной техники и автоматизированных систем управления и другие вопросы.

Существует ряд международных нормативных документов, вводящих понятия и регламентирующих процессы обеспечения кибербезопасности [7]. Разработан стандарт ISO 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности», в котором рассматриваются преимущественно вопросы безопасной работы в Интернете [8]. Также в качестве примеров можно привести определения и понятия, данные некоторыми национальными и международными организациями.

Кибербезопасность — комплекс мероприятий, направленных на защиту компьютеров, цифровых данных и сетей их передачи от несанкционированного доступа и других действий, связанных с манипулированием или кражей, блокированием, порчей (искажением), разрушением и уничтожением как умышленного, так и случайного характера (Минобороны США, [9]).

Кибербезопасность — набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, информационных ресурсов организации и пользователя (Международный союз электросвязи, [10]).

В Российской Федерации нормативными правовыми документами введены понятия «информационная безопасность» и «защита информации», понятие «кибербезопасность» не определено. В то же время ряд специалистов связывают кибербезопасность с обеспечением безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ и с защитой критической информационной инфраструктуры [11 – 15].

В разрабатываемом Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации», в частности, вводится понятие компьютерной атаки. Компьютерная атака — целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах.

Рассмотрим цели, источники угроз и особенности реализации направленных компьютерных атак на информационную инфраструктуру критически важных объектов (КВО) и автоматизированные системы управления производственными и технологическими процессами [16].

Цель кибератаки (направленной компьютерной атаки) — дезорганизация и перехват управления КВО и АСУ ТП, в частности системами управления движением и перевозками.

Объект кибератаки: КВО (транспортные, промышленные, энергетические и другие критически важные объекты) и их АСУ ТП, например системы управления и обеспечения безопасности движения поездов, и АСУ более высокого уровня — АСУ КВО.

Источники угроз: высокопрофессиональные организованные сообщества — сообщества киберпреступников, кибертеррористов и т. п.

Особенности реализации кибератаки на АСУ ТП:

1. Тщательное (возможно, долговременное) изучение объекта и его АСУ ТП, использование инсайдерской информации, методов социальной инженерии, уникальных средств для проведения кибератаки;

2. Кибератака ориентирована не столько на компрометацию данных, сколько на нарушение целостности и доступности технологической и управленческой информации, а также на информационную инфраструктуру и исполнительные устройства АСУ ТП;

3. Скоротечность кибератаки (реальный масштаб времени, учитывая малое время жизни информации).

Нормативная методическая база защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак. Международная рабочая группа COLPOFER приняла решение использовать понятие «кибербезопасность на железнодорожном транспорте», отражающее ее название, методологические подходы и опыт ОАО «РЖД» по защите информационной инфраструктуры железнодорожного транспорта от компьютерных атак. Российской стороной в инициативном порядке были разработаны и представлены на рассмотрение два проекта нормативных методических документов (НМД):

НМД-1: «Основные положения защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак» («Guidelines for protection of railway transport information infrastructure against cyber attacks»);

НМД-2: «Основные положения порядка использования сил и средств предупреждения и обнаружения компьютерных атак на информационную инфраструктуру железных дорог» («Guidelines for using forces and tools to prevent and detect computer attacks against rail information infrastructure»).

По результатам дискуссии и изучения НМД рабочая группа «Кибербезопасность на железнодорожном транспорте» утвердила первый документ в качестве памятки для членов COLPOFER.

В условиях глобальной конкуренции важным условием устойчивой деятельности железнодорожного транспорта является обеспечение безопасности его информационной инфраструктуры от компьютерных атак. Целесообразно сосредоточить внимание на данном этапе на создании комплексной системы защиты информационной инфраструктуры железнодорожного транспорта (ИИ ЖТ) от компьютерных атак и ее основного компонента — системы обнаружения и предупреждения компьютерных атак. В то же время в последующем необходимо предусмотреть детальную проработку вопросов защиты уровня АСУ ТП.

Предлагается рассматривать компьютерные атаки на ИИ ЖТ как инциденты информационной безопасности и выполнять построение системы обнаружения и предупреждения компьютерных атак как важного элемента системы управления инцидентами и в более общем плане — системы управления информационной безопасностью и кибербезопасностью железных дорог.

Необходимо использовать смешанный подход при создании системы защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак, сочетающий верификационно-факторную и риск-ориентированную модели, а также основываться на методах ситуационного управления и интеллектуальных систем при построении системы управления информационной безопасностью и кибербезопасностью железных дорог.

НМД-1 является базовым рекомендательным документом, определяющим направления работ по созданию системы защиты ИИ ЖТ от компьютерных атак и общие меры по предупреждению, обнаружению, анализу и ликвидации компьютерных атак. В документе представлены исходные данные и основные направления решения указанных задач:

- дана общая характеристика ИИ ЖТ, идентифицированы основные элементы ИИ ЖТ, подверженные компьютерным атакам, проведена типизация возможных компьютерных атак на элементы ИИ ЖТ;
- определены основные принципы защиты ИИ ЖТ от компьютерных атак;
- представлен облик системы защиты ИИ ЖТ от компьютерных атак;
- определены этапы создания системы защиты ИИ ЖТ от компьютерных атак и определены мероприятия по поддержке защиты ИИ ЖТ от компьютерных атак.

Отметим, что под информационной инфраструктурой понимается совокупность центров обработки данных, информационно-телекоммуникационных сетей, центров управления, программно-технических комплексов и технологий обеспечения сбора, обработки и передачи информации. Территориально распределенный характер ИИ, использование различных, в

том числе беспроводных, каналов связи, подключение к сети Интернет, наличие корпоративных и внешних связей усиливают возможности по реализации компьютерных атак на ИИ железнодорожного транспорта со стороны как внутренних, так и внешних нарушителей.

Архитектура ИИ ЖТ предполагает размещение технических средств ИИ ЖТ на территориально удаленных друг от друга объектах.

Перечень объектов размещения наиболее важных элементов ИИ ЖТ включает:

- объекты связи и информатизации;
- объекты энергохозяйства (системы и линии дистанционного управления и телеуправления устройствами электроснабжения);
- здания, строения, сооружения и помещения станций и вокзальных комплексов (с линейным и станционным оборудованием сетей связи и систем автоматической коммутации, обеспечивающих технологические процессы на железнодорожном транспорте и потребность в связи);
- пункты управления и информационные комплексы управления движением на железнодорожном транспорте и системы управления перевозками, в том числе стационарные пункты управления владельца объектов инфраструктуры железнодорожного транспорта и железнодорожного подвижного состава;
- объекты сигнализации, централизации и блокировки, используемые при ремонте и эксплуатации устройств и линий сигнализации, централизации и блокировки;
- инженерные системы и системы жизнеобеспечения информационно-вычислительных и диспетчерских центров;
- железнодорожные переезды;
- объекты вагонного хозяйства;
- объекты локомотивного хозяйства;
- подвижной состав.

Предполагается, что элементы ИИ ЖТ данных объектов, в состав которых включены программно-технические средства обработки (передачи) информации, включая оборудование каналов связи, потенциально подвержены компьютерным атакам. Выделены основные элементы ИИ ЖТ, размещенные на перечисленных объектах и *потенциально* подверженные компьютерным атакам, следующих категорий:

- системы обработки и анализа информации (представлены различными АИТС в составе ИИ ЖТ);
- технические и программные средства обработки информации;
- оборудование каналов связи и телекоммуникаций, используемое службами и сервисами;
- системы и средства защиты информации;
- системы и средства поддержания (обеспечения) функционирования элементов ИИ.

В частности, к таким элементам ИИ ЖТ, как системы и средства защиты информации, относятся:

- подсистема антивирусной защиты;
- подсистема защиты от несанкционированного доступа (идентификации и аутентификации, управления доступом, регистрации событий безопасности, контроля целостности, ограничения программной среды, криптографической защиты информации, защиты межсетевого взаимодействия);
- подсистемы резервного копирования и восстановления, средства резервирования;
- системы мониторинга событий информационной безопасности;
- системы оценки защищенности и управления информационной безопасностью;
- система управления информационной безопасностью.

В документе составлен детальный перечень элементов ИИ ЖТ, подверженных компьютерным атакам.

В НМД-1 под компьютерной атакой понимается целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях.

В соответствии с опытом эксплуатации средств защиты информации ЖТ можно установить одиннадцать типов компьютерных атак, характерных для элементов ИИ ЖТ. Каждый тип компьютерной атаки направлен на выполнение определенной целевой функции, связанной с нанесением ущерба элементам ИИ ЖТ и называемой целевой функцией компьютерной атаки. Набор целевых функций компьютерных атак и перечень типов компьютерных атак, реализующих конкретную функцию, представлены в таблице.

В качестве основных мер обеспечения безопасности информационной инфраструктуры ОАО «РЖД» рассматриваются следующие:

- обеспечение физической безопасности элементов информационной инфраструктуры;
- учет активов (объекты, носители информации и пр.);
- идентификация и аутентификация субъектов доступа;
- управление доступом к информации;
- обеспечение целостности информации и средств защиты информации;
- регистрация действий пользователей и других событий в системе;
- использование криптографических механизмов защиты;
- резервное копирование и восстановление;
- межсетевое экранирование;
- контроль подключения к сети Интернет;
- обнаружение вторжений (компьютерных атак);

• анализ защищенности;
• защита информации при передаче по каналам связи;
• защита электронной почты;
• защита электронного документооборота;
• защита системы IP-телефонии;
• антивирусная защита;
• контроль беспроводных соединений;
• защита при виртуализации и облачных вычислениях;
• разделение средств разработки и тестирования;
• использование механизмов защиты прикладных систем;
• контроль и мониторинг действий пользователей в системе.

В НМД-2 «Основные положения порядка использования сил и средств предупреждения и обнаружения компьютерных атак на информационную инфраструктуру железных дорог» раскрываются:

• привлекаемые силы и средства, необходимые для защиты ИИ ЖТ от компьютерных атак, порядок и основные принципы их использования;
• способы обнаружения и предупреждения компьютерных атак, характерные для элементов ИИ ЖТ, с использованием таких компонентов, как ложные информационные системы и ресурсы, а также с использованием «традиционных» систем и средств защиты ИИ от компьютерных атак;
• порядок использования дополнительных компонентов для обнаружения и предупреждения компьютерных атак.

Использование сил и средств предупреждения и обнаружения компьютерных атак предусматривает выполнение комплекса организационно-технических мероприятий. В НМД-2 рассмотрены:

• перечень организационных мер по предупреждению и обнаружению компьютерных атак на ИИ железных дорог;
• перечень технических мероприятий по предупреждению и обнаружению компьютерных атак в процессе эксплуатации АИТС;
• последовательность действий сил предупреждения и обнаружения компьютерных атак, представленная общей схемой (порядком) использования сил и средств предупреждения и обнаружения компьютерных атак на элементы ИИ;
• перечень средств, применяемых для обнаружения и предупреждения компьютерных атак, и порядок их применения (использования), составляющий основу технических мероприятий по предупреждению и обнаружению компьютерных атак;
• рекомендации по поиску и выявлению уязвимостей элементов ИИ, используемые для определения области и способов применения средств контроля (анализа) защищенности.

В документах сформулированы принципы защиты ИИ ЖТ от компьютерных атак, обоснованы меры и средства защиты по предотвращению реализации целевых функций компьютерных атак на элементы ИИ ЖТ с описанием возможных действий нарушителя и способов их реализации.

Перечень целевых функций компьютерных атак и способов их достижения

№ п/п	Наименование целевой функции компьютерной атаки	Типы компьютерных атак, реализующих целевую функцию
1	Анализ сетевого трафика	1. Прослушивание сетевого трафика. 2. Сканирование сети. 3. Компьютерные атаки через посредника
2	Сканирование сети	1. Сканирование сети
3	Выявление паролей	1. Прослушивание сетевого трафика. 2. Компьютерные атаки, направленные на подбор пароля
4	Навязывание ложного маршрута сети	1. Компьютерные атаки, направленные на подмену сетевого адреса. 2. Компьютерные атаки, связанные со злоупотреблением доверием. 3. Компьютерные атаки, направленные на переадресацию портов
5	Подмена доверенного объекта	1. Компьютерные атаки через посредника. 2. Компьютерные атаки, направленные на переадресацию портов. 3. Компьютерные атаки, связанные со злоупотреблением доверием
6	Внедрение ложного объекта сети	1. Компьютерные атаки через посредника. 2. Компьютерные атаки, направленные на подмену сетевого адреса. 3. Компьютерные атаки, направленные на переадресацию портов. 4. Компьютерные атаки, связанные со злоупотреблением доверием
7	Отказ в обслуживании	1. Компьютерные атаки через посредника. 2. Компьютерные атаки типа «отказ в обслуживании». 3. Удаленное проникновение и блокирование ресурсов
8	Удаленный запуск приложений	1. Компьютерные атаки на уровне приложений. 2. Удаленное проникновение и блокирование ресурсов
9	Внедрение вредоносных программ	1. Компьютерные атаки на уровне приложений. 2. Вирусы и приложения типа «троянский конь»

НМД «Основные положения порядка использования сил и средств предупреждения и обнаружения компьютерных атак на информационную инфраструктуру железных дорог» носит типовой характер. Конкретные действия по предупреждению и обнаружению компьютерных атак, представленные в документе, могут уточняться с учетом особенностей организационной структуры организаций ЖТ, различных АИТС, а также для конкретных объектов размещения элементов ИИ.

Заключение. Рассмотрены основные предпосылки необходимости обеспечения информационной

безопасности и кибербезопасности на железнодорожном транспорте в условиях широкой информатизации и автоматизации транспортных процессов.

По результатам анализа статистических данных отмечена возрастающая подверженность информационной инфраструктуры железнодорожного транспорта и систем организации и управления движением поездов компьютерным атакам и особенно целенаправленным кибератакам. Это требует объединения усилий различных стран с учетом интеграции транспортных систем и создания железнодорожных коридоров по обеспечению международной информационной безопасности и кибербезопасности на железнодорожном транспорте.

Представлены методологические подходы и практические направления международного сотрудничества, понятийный аппарат в области кибербезопасности на железных дорогах, одобренные созданной в рамках программы COLPOFER рабочей группой «Кибербезопасность на железнодорожном транспорте».

Изложены основные положения разработанных рабочей группой нормативных методических документов по защите информационной инфраструктуры железнодорожного транспорта от компьютерных атак. Выделены элементы объектов информационной инфраструктуры железнодорожного транспорта, потенциально подверженные компьютерным атакам. Приведена классификация типов компьютерных атак и способы их реализации.

Рассмотрены принципы, организационные и технические меры обеспечения кибербезопасности, которые могут стать основой построения комплексной системы защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак.

СПИСОК ЛИТЕРАТУРЫ

1. Ададуров С.Е., Глухов А.П., Корниенко А.А. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 439 с.

2. NIST Computer Security Resource Clearinghouse. URL: http://csrc.nist.gov

3. P. Ludlow. What is a 'Hacktivist'? // The New York Times, January 13, 2013. URL: http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/

4. E. Mills. Report: Countries prepping for cyberwar // November 17, 2009. URL: http://www.cnet.com/news/report-countries-prepping-for-cyberwar/

5. Блехшмидт П. НАТО готовится к ведению компьютерных войн // Süddeutsche Zeitung, 2010. 5 октября. URL: http://inosmi.ru/europe/20101005/163386175-print.html

6. Singer, P. W. & Friedman, A. Cybersecurity and cyberwar: what everyone needs to know. New York, NY: Oxford University Press, 2014. viii, 306 p. ISBN 978-0-19-991811-9.

7. Лукацкий А. Безопасность критических инфраструктур. Международные аспекты. URL: http://lukatsky.blogspot.ru/2013/09/blog-post_26.html

8. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032: ed-1:v1:en

9. Высокие технологии в США: Опыт министерства обороны и других ведомств / Д.О. Рогозин [и др.]. М.: Издательство Московского университета, 2013. 384 с.

10. Recommendation ITU-T X.1205 (Международный Союз Электросвязи). URL: http://handle.itu.int/11.1002/1000/9136

11. ГОСТ Р ИСО/МЭК ТО 18044 – 2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. URL: http://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК_ТО_18044–2007

12. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации: утв. Президентом РФ 03.02.2012 № 803. URL: http://www.scrf.gov.ru/documents/6/113.html

13. Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15.01.2013 №31с. URL: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html

14. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17. URL: http://www.rg.ru/2013/06/26/gostajna-dok.html

15. Приказ ФСТЭК России «Об утверждении Требований 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» от 14.03.2014 № 31. URL: http://www.rg.ru/2014/08/06/fstek-dok.html

16. ISA/IEC 62443 Industrial Automation and Control Systems Security. URL: https://www.tofinosecurity.com/resources/topics/isaiec-62443

СВЕДЕНИЯ ОБ АВТОРАХ

АДАДУРОВ Сергей Евгеньевич,
советник генерального директора, АО «Росжелдорпроект».
129110, Москва, ул. Щепкина, д. 42, стр. 2 А.
Тел.: (495) 663-00-60, доб. 61467.
E-mail: czi_mpc@mail.ru

ДИАСАМИДЗЕ Светлана Владимировна,
доцент кафедры «Информатика и информационная безопасность», Петербургский государственный университет путей сообщения (ПГУПС).
190031, Санкт-Петербург, Московский пр., д. 9.
Тел.: (812) 570-76-68.
E-mail: sv.diass99@yandex.ru ✉

КОРНИЕНКО Анатолий Адамович,
заведующий кафедрой «Информатика и информационная безопасность», Петербургский государственный университет путей сообщения (ПГУПС).
190031, Санкт-Петербург, Московский пр., д. 9.
Тел.: (812) 570-76-68.
E-mail: kaa.pgups@yandex.ru

СИДАК Алексей Александрович,
заместитель председателя по безопасности ИТ,
ООО «Центр безопасности информации».
Московская область, г. Юбилейный, ул. Пионерская, д. 1/4.
Тел.: (495) 543-30-60.
E-mail: sidak@cbi-info.ru

International Cybersecurity on Railway Transport: Methodological Approaches and Normal Procedural Framework

Sergey E. Adadurov, Dr. of Technical Science, Professor, Advicer Director General, JSC "Roszheldorproekt". Building 2, 42, Schepkin str., 129110 Moscow, Russian Federation. Tel.: +7 (495) 663 0060, ext. 61467. E-mail: czi_mpc@mail.ru
Svetlana V. Diasamidze, Candidate of Technical Science, Assistant Professor, Chair of Information Technology and Information Security. Petersburg State Transport University (PGUPS). 9, Moskovsky av., 190031 St. Petersburg, Russian Federation. Tel.: +7 (812) 570 7668. E-mail: sv. diass99@yandex.ru ✉
Anatoly A. Kornienko, Dr. of Technical Science, Professor, Holder of Chair of Information Technology and Information Security. 9, Moskovsky av., 190031 St. Petersburg, Russian Federation. Tel.: +7 (812) 570 7668. E-mail: kaa.pgups@yandex.ru
Alexey A. Sidak, Deputy Chairman in charge of IT security, LLC "Information Security Center". 1/4, Pionerskaya str., 141090, Yubileiny, Moskovskaya Oblast', Russian Fedefation. Tel.: +7 (495) 543 3060. E-mail: sidak@cbi-info.ru

Abstract. The paper deals with methodological approaches and practical venues of international cooperation in the areas of information security and cybersecurity on railway transport. The approaches were adopted by the workshop "Cybersecurity on Railway Transport" established within the framework of the COLOPOFER program.

There are analyzed main factors and prerequisites governing the necessity of hacking countermeasures on the part of railway IT infrastructure. Also discussed are cybersecurity related definitions. There are presented principal provisions of normative techniques being developed by the international workshop "Cybersecurity on Railway Transport".

Basic IT information infrastructure objects of railway transport are characterized with respect to their hacking susceptibility and their most vulnerable components are highlighted. There is presented classification of the types of computer attacks and their implementation me-dia.

Also discussed are organizational and routine hacking countermeasures to be taken in the railway IT infrastructure environment.

Keywords: cybersecurity; information security; computer attack; IT infrastructure protection

References

1. Adadurov S. E., Glukhov A. P., Kornienko A. A. *Informatsionnaya bezopasnost' i zashchita informatsii na zheleznodorozhnom transporte. Ch. 1: Metodologiya i sistema obespecheniya informatsionnoy bezopasnosti na zheleznodorozhnom transporte* [Information security and protection of information on railway transport. Pt. 1: The methodology and the system of information security in railway transport]. Moscow, Educational and Training Center in Railway Transport Publ., 2014. 439 p.

2. *NIST Computer Security Resource Clearinghouse*. Available at: http://csrc.nist.gov.

3. Ludlow P. *What is a "Hacktivist"?* The New York Times, January 13, 2013. Available at: http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/.

4. Mills E. *Report: Countries prepping for cyberwar*. CNET, November 17, 2009. Available at: http://www.cnet.com/news/report-countries-prepping-for-cyberwar/

5. Blechschmidt P. *NATO is preparing to conduct computer wars.* Süddeutsche Zeitung, October 5, 2010. Available at: http://inosmi.ru/europe/20101005/163386175-print. html. (in Russ.).

6. Singer P. W., Friedman A. *Cybersecurity and cyberwar: What everyone needs to know*. New York, OUP Publ., 2014. 306 p.

7. Lukatskiy A. Security of critical infrastructures: International experience. September 26, 2013. Available at: http://lukatsky.blogspot.ru/2013/09/blog-post_26. html. (in Russ.).

8. *ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity*. Available at: https://www.iso.org/obp/ui/#iso: std: iso-iec:27032: ed-1: v1: en.

9. Rogozin D. O., Sheremet I. A., Garbuk S. V., *Gubinskiy A. M. Vysokie tekhnologii v SShA: Opyt ministerstva oborony i drugikh vedomstv* [High-Tech in the USA: Experience of the Ministry of Defense and other agencies]. Moscow, MSU Publ., 2013. 384 p.

10. *Recommendation ITU-T X. 1205.* International Telecommunication Union. Available at: http://handle.itu.int/11.1002/1000/9136.

11. *GOST R ISO/MEK TO 18044 – 2007. Information technology. Methods and means of ensuring safety. Management of information security incidents*. Available at: http://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК_ТО_18044-2007. (in Russ.).

12. *The main directions of the state policy in the field of security of automated control systems of production and technological processes of critical infrastructure of the Russian Federation*. Approved by the President of the Russian Federation on February 03, 2012 № 803. Available at: http://www.scrf.gov.ru/documents/6/113. html. (in Russ.).

13. *Presidential Decree "On establishment of the state system of detection, prevention and elimination of consequences of cyber attacks on information resources of the Russian Federation"* dated January 15, 2013 № 31s. Rossiyskaya gazeta, January 18, 2013. Available at: http://www.rg.ru/2013/01/18/komp-ataki-site-dok. html. (in Russ.).

14. *Order of the Federal Service for Technical and Export Control of Russia "On approval of the Requirements for the protection of information of no state secret contained in the state information systems"* of February 11, 2013 № 17. Rossiyskaya gazeta, June 26, 2013, no. 6112. Available at: http://www.rg.ru/2013/06/26/gostajna-dok. html. (in Russ.).

15. *Order of the Federal Service for Technical and Export Control of Russia "On approval of requirements to ensure the protection of information in automated control systems of production and technological processes on critical facilities, potentially hazardous objects as well as objects representing the increased danger to life and health and to the environment"* of March 14, 2014. Rossiyskaya gazeta, August 6, 2014, no. 6447. Available at: http://www.rg.ru/2014/08/06/fstek-dok. html. (in Russ.).

16. *ISA/IEC 62443. Industrial automation and control systems security.* Available at: https://www.tofinosecurity.com/resources/topics/isaiec-62443