НАУЧНАЯ СТАТЬЯ
УДК 658.7:004
DOI: https://doi.org/10.30932/1992-3252-2023-21-6-12

Мир транспорта. 2023. Т. 21. № 6 (109). С. 103–109

Транспортная кибербезопасность

Евгений НЕСТЕРОВ

Виктор ЦВЕТКОВ

Евгений Александрович Нестеров [1]***,***
Виктор Яковлевич Цветков [2]

[1,2] Российский университет транспорта, Москва, Россия.
[1] ORCID 0009-0009-9100-3410; Web of Science Researcher ID: JUF-4957-2023; Scopus ID: 58707809100; РИНЦ SPIN-код: 9008-0780; РИНЦ Author ID: 1119794.
[2]ORCID 0000-0003-1359-9799; Web of Science Researcher ID J-5446-2013; Scopus ID: 000313599799; РИНЦ Author ID: 1399061.
✉ *[2] cvj2@mail.ru.*

АННОТАЦИЯ

Одной из особенностей цифровой трансформации транспортной отрасли является тенденция повышения числа кибератак, которые входят в число информационных угроз. Транспортная кибербезопасность является более широким явлением по сравнению с кибератакой и информационной безопасностью. Она включает организационную безопасность и другие виды безопасности, которые в таком виде в информационной области не встречаются.

Актуальность транспортной кибербезопасности дополнительно обусловлена широким применением информационно-вычислительных сетей и информационных пространств. Киберпространство в транспортной сфере можно трактовать как совокупность сетей, информационных пространств, коммуникационного и реального пространства. Включение реального пространства является отличительной особенностью транспортного киберпространства.

При этом рост информационных угроз происходит независимо от развития транспортного киберпространства. Он обусловлен цифровизацией общества, включая сферу транспорта. Киберпространство создаёт предпосылки для киберугроз нового качества, и для новых киберугроз прежние методы информационной безопасности становятся неэффективными. Возникновение информационных угроз продиктовано не столько цифровизацией, сколько большей открытостью информационных и коммуникационных технологий. Мультимодальные перевозки как отношения между многими организациями также способствуют росту киберугроз и снижению информационной безопасности.

Статья предлагает построенный на обзоре тематических публикаций анализ состояния и подходов, применяемых в транспортной кибербезопасности. Приведена систематика угроз и рисков транспортной кибербезопасности. Введены понятия «железнодорожная информация», «транспортная информация». Описаны уязвимости транспортного киберпространства.

Ключевые слова: транспорт, транспортное киберпространство, транспортная кибербезопасность,киберфизические системы, сетевые системы, цифровые риски, киберфизические угрозы.

Для цитирования: Нестеров Е. А., Цветков В. Я. Транспортная кибербезопасность // Мир транспорта. 2023. Т. 21. № 6 (109). С. 103–109. DOI: https://doi.org/10.30932/1992-3252-2023-21-6-12.

Полный текст статьи на английском языке публикуется во второй части данного выпуска.
The full text of the article in English is published in the second part of the issue.

ВВЕДЕНИЕ

Цифровизация трансформирует железные дороги во всем мире. Одной из особенностей цифровой трансформации любой отрасли, включая железную дорогу, является повышенная подверженность кибератакам [1–3]. Железнодорожная отрасль уязвима для таких атак, поскольку количество цифровых элементов, а также количество интерфейсов между цифровыми и физическими компонентами в железнодорожных системах продолжает расти. Увеличение количества элементов и интерфейсов требует новых структур, концепций и архитектур для обеспечения устойчивости железнодорожной системы к проблемам кибербезопасности, таким как отсутствие проактивности, отсутствие целостного подхода и старение систем безопасности, подверженных будущим киберугрозам.

Железнодорожный транспорт является важной производственной отраслью. В настоящее время в сфере транспорта существует киберпространство как промышленный кластер, включающий интеграцию информационных систем, интеллектуальных транспортных систем, технологии Интернета вещей, транспортные кибер-физические системы, телекоммуникационные сети, цифровую железную дорогу [4] и прочее. Нарушение транспортной кибербезопасности может создать множество критических ситуаций. Современные транспортные системы не работают изолированно, а используют разные сети для улучшения бизнес-процессов. Следствием этого развития является повышенная подверженность киберугрозам.

Целью исследования, описанного в статье, являлись анализ состояния транспортной кибербезопасности и используемых подходов, описанных в научной литературе, систематики угроз и рисков транспортной кибербезопасности, уязвимостей транспортного киберпространства.

РЕЗУЛЬТАТЫ

Причины киберугроз

Киберпространство железной дороги включает линии связи и точки доступа, а также точки управления транспортом. На железнодорожном транспорте широко практикуют корпоративный бизнес. Это особенно заметно в мультимодальных перевозках. В этом бизнесе участвует большое количество организаций и лиц. Большое количество участников корпоративного бизнеса создает большое количество связей, в которых существует много точек доступа. Связи растут в кубической прогрессии. Связи и точки доступа создают посторонним лицам возможность доступа в киберпространство, то есть создают киберугрозы. Эти угрозы следует отнести к внешним угрозам.

В киберпространстве дополнительно функционирует большое количество разнообразных программ, которые не всегда должным образом согласованы. Рассогласование программного обеспечения создает дополнительные угрозы, пропорциональные объему сети в киберпространстве. Специфика коммуникаций на транспорте требует введения понятия «транспортная информация». В сфере железнодорожного транспорта транспортная информация (ТИ) становится железнодорожной информацией (ЖИ). Эта информация делится на управляющую и дескриптивную. Несанкционированный доступ к любой из этих информаций представляет угрозу.

Дополнительным источником киберугроз являются организационные или нормативные угрозы. Большое количество нормативных документов разных отраслей и организаций не согласованы полностью. Рассогласование нормативной документации служит источником внутренних угроз функционированию транспортной системы. Особенностью ТИ и ЖИ является то, что они организованы в блоки, которые обладают свойством целостности и системности. Возможное нарушение целостности информации также представляет собой причину угрозы. Таким образом, нормативы, линии коммуникации, точки доступа, информационные блоки создают внешние и внутренние киберугрозы.

Железнодорожная инфраструктура все больше переходит к интеллектуальным и киберфизическим системам, что создает новые риски и возможности для киберпреступлений.

Существуют проблемы в работе транспортной инфраструктуры, проблемы, связанные с большими данными [5], имеющие свою специфику для железных дорог [6], отсутствует законодательство о транспортной кибербезопасности.

Меры противодействия кибератакам на железнодорожном транспорте находятся в состоянии разработки. Пока идет процесс систематизации рисков и их последствий, которых следует избегать. Например, эти риски систематизированы в работе [7]. С позиций категориального анализа можно ввести понятие категории риска или рисковых категорий. К числу рисковых категорий относят: задержки движения; антропоэнтропию; столкновения; повреждение путей; террористические акты; человеческие жертвы; техногенные факторы; потерю конкурентоспособности; утечку ценной информации.

На объектах транспортной инфраструктуры периодически возникают аномальные или нештатные ситуации, ряд из которых описан в [1]. Эти случаи обусловлены развитием ИТ технологий и возможностью умышленного или неумышленного доступа к каналам связи и вмешательства в каналы управления транспортом.

При этом доступ к конфиденциальной информации может быть не только прямым, но и косвенным. Например, информация, передаваемая по электронной почте, является открытой не менее чем в семи точках на разных узлах передачи. Здесь следует отметить такую угрозу как передача служебной информации или информации о служебной информации в личных почтовых сообщениях. Для предотвращения этой угрозы, например, в Великобритании запрещено использовать служебную электронную почту для передачи личной информации или в частные адреса лиц.

Инициатива Shift2Rail.

В исследовании [8] рассмотрено несколько европейских проектов, посвященных кибербезопасности, в контексте Shift2Rail.

В рамках пяти этапов проекта Shift2Rail был реализован ряд рабочих пакетов (IP2 Technical Demonstrators. Advanced Traffic Management and Control Systems[1]), пятый этап завершился в октябре 2023 года.

Для повышения безопасности киберпространства применяют в том числе методы стандартизации и стандарты ISO. Метод стандартизации и стандарты подразделяют на четыре группы: международные, национальные, отраслевые и в рамках конкретного предприятия.

Доминанты в обеспечении безопасности

Среди множества технологий безопасности в киберпространстве транспортной инфраструктуры на основе анализа и обобщения были выявлены доминирующие или наиболее важные для транспортной отрасли технологии [10]. Эти технологии называют доминантами безопасности. Среди них следует выделить стандартные – такие как контроль доступа, и специальные – типа редукции точек входа. Кроме того, можно отметить когнитивно-информационные технологии типа технология «рукопожатия», технология унифицированного центра безопасности и т. д. [11].

Безопасность контроля доступа

Безопасность контроля доступа является основным вопросом для обеспечения безопасности любой системы управления или технической системы. Типичный подход к реализации доступа заключается в использовании списка (матрицы) управления доступом (ACL), управление доступом на основе ролей (RBAC) [12], управление доступом на основе задач (TBAC) [13]. Технологии контроля доступа делят на четыре категории: командный (TMAC), пространственный [14], когнитивный (CAC), контекстный (CBAC) [15]. Пространственный контроль связан с действиями в реальном пространстве и требует организации физической защиты. TMAC требует коммуникационной, информационной и криптографической защиты. Когнитивный контроль доступа требует анализа когнитивных моделей и использования когнитивной логики. Контекстный контроль доступа требует применения семантического анализа и латентного анализа передаваемой ТИ и ЖИ. Дополнительно ко всему в целях безопасности применяют аутентификацию личности клиента, методологию единого входа и т. д. В [16] обобщены требования к контролю доступа.

Одним из методов является использование списка безопасных данных. Некорректный список безопасных данных создает некорректный контроль доступа. Это может привести к опасным сценариям, когда некорректные данные могут быть использованы для ослабления безопасности инфраструктуры.

Безопасность передачи информации

Важным фактором киберпространства является безопасность передачи информации. Технология Enterprise Service Bus (ESB) используется для понимания нескольких систем, совместно использующих данные и услуги на железнодорожной платформе обмена информацией.

Безопасность хранения информации и ресурсов

Обеспечение надежного хранения информации, моделей и ресурсов является важной задачей безопасности ЖИ и ТИ. Базы данных являются слабым звеном в этой проблеме, поскольку широко используют типовые методы запросов и поиска, а главное – типовые и простые структуры данных, так как базы данных ориентированы на простоту и доступность, в то время как технологии безопасности требуют ограничения доступа и уникальности форм хранимой информации. Облачная обработка и облачное хранение частично решают

[1] [Электронный ресурс]: https://projects.shift2rail.org/s2r_ip_TD_r.aspx?ip=2&td=1bccaf76–7915–4283–8b52–36afdb1bdf42.

данную проблему. Однако применение облачных и туманных технологий вычислений усложняет структуру управления информацией. Это влечет рост угроз кибербезопасности в технологиях управления информацией. Простая технология управления несет меньшие риски. Сложная технология управления информацией несет б*о*льшие риски и большее число нештатных ситуаций. Эту проблему отчасти решает технология специализированных хранилищ данных.

Центр управления безопасностью **[11]**

Эти функции выполняют ситуационные центры. Централизация управления безопасностью является эффективной организационной мерой, исключающей мелкие и случайные проникновения в доступ к конфиденциальной информации. Ситуационные центры создают единую систему защиты и легко управляемую систему безопасности. Они позволяют накапливать опыт возникавших угроз и попыток проникновения. На этой основе с привлечением интеллектуальных систем, таких как искусственные нейронные сети, создают уникальные системы защиты для каждого объекта транспортной инфраструктуры. Централизованная система защиты создает внутреннюю систему безопасности киберпространства как самоорганизующуюся систему. Это очень важно на фоне постоянно растущих и меняющихся внешних угроз.

Угрозы кибербезопасности для железных дорог

Существует несколько угроз, связанных с кибербезопасностью железных дорог. Преобладающей операционной проблемой для железнодорожного сектора являются угрозы для систем идентификации, конфиденциальности и данных. Следует выделить наиболее важные [2].

Мотивированные риски и угрозы

Этот класс угроз направлен не на уничтожение, порчу или кражу информации, а на нанесение ущерба репутации: организации, корпорации, фирме-посреднику, правительству. Основная причина мотивированной атаки на систему – это конкурентная борьба, которая состоит в потере клиентуры и последующего ущерба.

Достаточно часто в этих угрозах применяют «агентный» подход, использующий индивидуальные и групповые алгоритмы. Агент как вирус может адаптироваться к среде и обладает полиформностью, то есть способностью изменения формы при его обнаружении. Этот тип угроз также называют «политическим».

Прагматические угрозы

Они состоят в использовании посредников и третьих лиц, способных иметь финансовую информацию, или информацию о финансовой информации, или информацию о лицах, имеющих доступ к финансовой информации.

Коммуникационные угрозы

Они связаны со слабостью коммуникаций и наличием в них слабых мест. Они включают не только кражу информации, но и порчу информации и даже ее подмену с целью нанести вред технологии и перевозкам.

Изъятие данных

Эта угроза включает использование атрибутов ИТ технологий для последующего незаконного использования уже важной информации. Эти данные могут быть предметом торга или шантажа.

Угрозы БД

База данных является информационной системой хранения данных и информационной системой обработки данных. Изначально базы данных создавались для широких слоев потребителей, и их концепцией была и остается простота использования. Существуют стандартные или типовые форматы баз данных, что существенно упрощает доступ к таким системам. Методом защиты может быть хранение данных в БД не в «чистом» виде, а в виде фрагментов конструкций или в закодированном виде.

Зеркалирование и резервирование

Эти технологии близки, но имеют различие. При зеркалировании практически осуществляется клонирование информации и информационных образов или кластеров. При резервировании (которое тоже основана на копировании) допускается исключение малосущественной информации с целью экономии физической памяти. Слабым местом обеих технологий является то, что «зеркала» и резервные копии не хранят с такой же тщательностью, как оригинал. Система безопасности для копий обычно много слабее, чем для оригинальной информации. Поэтому рекомендуется вести политику безопасности для копий, такую же, как и для оригиналов.

Серверные угрозы

Принято делить серверы на основные и серверы приложений. Принято защищать основные серверы с большей тщательностью, чем серверы приложений. Опасность состоит в том, что через

слабозащищенный сервер приложений появляется возможность доступа к основному серверу с ценной информацией.

Администраторные угрозы

Этот специфический вид угроз является антропогенным и строится на психологических особенностях любого человека, к числу которых относится системный администратор. В силу этого тип угроз имеет такое название. Угроза реализуется путем коммуникации злоумышленника с системным администратором в условиях информационной неопределенности. Злоумышленник выдает себя за другое лицо и в конце концов получает фрагмент или полностью необходимую информацию для входа в защищаемую систему. Такой механизм входа допустим по отношению к любому сотруднику системы безопасности. Но администраторы представляют наибольшую информационную ценность.

Близким к данной угрозе является «аварийный» вход. В случае сбоя или отключения питания информационной системы система безопасности отключается на секунды. Злоумышленникам этого достаточно для проникновения в систему и последующего входа после ликвидации сбоя.

Нарушение системности

Системность данных и алгоритмов обработки включает полноту, целостность, структурность, комплементарность. В первую очередь уделяют внимание конфиденциальности. Во вторую очередь проводят анализ целостности. Что касается модификации данных, то это третья по очередности задача. Одним из инструментов безопасности в этой части является журнализация. Но она фиксирует события, оставляя без внимание содержание событий. Можно отметить, что многие алгоритмы являются аналогом системы. Многие алгоритмы формируют по образцу прототипов алгоритмов. Знание прототипа алгоритма дает знание о модифицированном алгоритме и дает знание, позволяющее модифицировать текущий алгоритм.

Это же относится и к данным. Их форматы и структура строятся на основе прототипов. Знание структуры прототипа дает знание о текущей структуре данных, а модификация алгоритма и модификация формата данных влекут деструктивные последствия.

В отношении систем безопасности и защищаемых ими систем существует большое количество типов атак, которые делят на распределенные, когнитивные и целевые (векторные). Соразмерно этому стоят системы отражения атак.

Выделяют группы стохастических угроз. Они чаще всего связаны с воздействием внешней среды и стохастичностью среды функционирования системы управления или управляемой транспортной системы.

Внутренние угрозы аналогичны злонамеренным действиям, но исходят от сотрудников организации.

Кибербезопасность транспортных киберфизических систем

Из числа кибер-физических систем выделяют транспортные кибер-физические системы (TCPS/ТКФС) [18]. Эти системы приходят на смену интеллектуальным транспортным системам (ИТС) и служат основой управления цифровым транспортом. Рост применения ТКФС для соединения различных компонентов железнодорожной отрасли, расширение возможностей подключения с помощью коммуникационных технологий также привело к рискам киберугроз ТКФС. Реализации ТКФС требуют упреждающей идентификации рисков, четкого определения и обеспечения их безопасности. Для повышения эксплуатационной безопасности и эффективности все большее число физических компонентов железных дорог соединяется с помощью различных ТКФС посредством коммуникаций, создавая новую парадигму «железнодорожного Интернета вещей». Тенденция к интеграции ТКФС также привела к постоянно растущей зависимости железнодорожной отрасли от кибертехнологий и технологий IoT, что повышает опасности киберугроз. Железнодорожная отрасль подвержена киберрискам, присущим развертываниям ТКФС. К сожалению, компоненты ТКФС обеспечивают не только желаемое подключение, но и возможности для злоумышленников при достижении злонамеренных целей. В таблице 1 [19] дана систематика угроз для ТКФС.

Общие кибертехнологии [19] часто используются в разных отраслях, поэтому их основные схемы безопасности хорошо изучены в ходе технических модернизаций и исследований в области ИТ.

ЗАКЛЮЧЕНИЕ

Киберпространство трактуют в узком и широком смысле. В узком смысле – это информационное пространство цифровых двойников и киберфизических систем, информационное пространство беспилотного транспорта, а также технологии интернета вещей. В широком

Таблица 1

Систематика угроз ТКФС

Субъекты железнодорожной киберфизической системы	Возможные угрозы
Системы управления поездом нового поколения (например, зарубежные ERTMS, ETCS, PTC, CBTC)	Множественные атаки, включая электромагнитные помехи, глушение, отказ в обслуживании (DoS), модификацию сообщений и несанкционированный доступ и т. д.
	Атаки полным перебором, несанкционированный доступ к сети и модификация сообщений
	Пассивное подслушивание, активный отказ от контроля и принятие контроля
Традиционные системы железнодорожной сигнализации	Несанкционированный доступ к сети, отказ в обслуживании и модификация сообщений
	Электромагнитная интерференция
Балисная передача данных	Нарушение доступности или целостности данных балис [евробалис], глушение, электромагнитные помехи
Службы тяги железных дорог, системы электроснабжения	Атаки с внедрением ложных данных, модификация сообщений и несанкционированный доступ к сети
Человеко-машинный интерфейс	Множественные атаки, включая отказ в обслуживании, модификацию сообщений, несанкционированный доступ и т. д.
Системы громкой связи или системы отображения информации для пользователей	Несанкционированные вторжения
Железнодорожная путевая инфраструктура	Как физическое, так и кибервторжение

смысле киберпространство включает открытые сети и все средства коммуникации, связанные с управлением транспортными, информационными и интеллектуальными системами. Для всех видов этих пространств существуют киберугрозы или угрозы в киберпространстве.

Рост киберугроз имеет несколько причин. Первая причина состоит в росте открытых сетей и систем.

Вторая причина заключается в глобализации, которая повышает доступ общества к технологиям и системам.

Третья причина состоит в конвергенции или универсализации. Выпускают универсальные пульты, которые управляют телевизором и транспортным средством. Выпускают смартфоны, которые могут не только осуществлять телефонную связь, но и управлять телевизором и создавать помехи или управлять транспортным средством.

Четвертая причина в росте объемов информации, который вызывает у человека противоположную реакцию в стремлении упростить информацию. Растущий объем информации не сопровождается ростом применения и усложнением паролей как средств защиты. Все легче взламывать пароли, используя стереотипы.

Пятая причина состоит в росте сложности технических и информационных систем. Этот рост также создает тенденцию к упрощению работы с такими системами. Упрощение работы влечет снижение информационной безопасности.

Шестая причина состоит в росте информационной асимметрии между требованиями технических и информационных систем и реальной способностью человека управлять этими системами. Имеет место опережение роста сложности систем по отношению к росту способностей и возможностей человека-управленца.

Седьмая причина состоит в росте цифрового неравенства[2]. Это неравенство в уровне ИТ-подготовки между странами и между людьми. Некоторые продвинутые в ИТ-технологиях специалисты противопоставляют себя обществу и совершают деструктивные действия для демонстрации превосходства. Цифровое неравенство растёт в системе «руководитель – исполнитель». Как правило, руководитель понимает в ИТ технологиях меньше, чем рядовой сотрудник, и тем более меньше, чем эксперт. Это непонимание выражается в торможении инновационных ИТ разработок. Такой руководитель отдаёт предпочтение простым, но более понятным для него системам безопасности, не обращая внимание на их слабую защищённость. Такой руководитель отвергает сложные и непонятные для него, но хорошо защищённые системы безопасности.

[2] См., напр.: DiMaggio, P., Hargittai, E. From the ‘Digital Divide’ to ‘Digital Inequality’: Studying Internet Use as Penetration Increases. Princeton University, Woodrow Wilson School of Public and International Affairs, Center for Arts and Cultural Policy Studies, Working Papers. 2001.

Восьмая причина состоит в появлении киберпространства как инструмента управления открытой системой.

Девятая причина роста киберугроз обусловлена использованием больших сетей, значительная часть из которых является открытой.

Наблюдается растущая тенденция к дифференциации исследования кибербезопасности, вместо написания общей теории. Актуальным остаётся необходимость разработки интегрированной основы для решения многих проблем кибербезопасности. Анализ [2] показывает, что большинство исследований кибербезопасности, проводимых на железных дорогах, пока носят концептуальный характер и отстают в применении безопасности на основе искусственного интеллекта (ИИ). Как и в других отраслях, очень важно, чтобы железные дороги также следовали новейшим технологиям безопасности.

СПИСОК ИСТОЧНИКОВ

1. Thaduri, A., Aljumaili, M., Kour, R., Karim, R. Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. International Journal of System Assurance Engineering and Management, 2019, Vol. 10, Iss. 6, pp. 149–159. DOI: 10.1007/s13198-019-00778-w.

2. Kour, R., Thaduri, A., Karim, R. A review on cybersecurity in railways. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 2023, Vol. 237, Iss. 1, pp. 3–20. DOI: 10.1177/09544097221089389.

3. Wang, Z., Liu, X. Cyber security of railway cyber-physical system (CPS) – A risk management methodology. Communications in Transportation Research, 2022, Vol. 2, Iss. 4, 100078. DOI: https://doi.org/10.1016/j.commtr.2022.100078.

4. Лёвин Б. А., Цветков В. Я. Цифровая железная дорога: принципы и технологии // Мир транспорта. – 2018. – Т. 16. – № 3 (76). – С. 50–61. DOI: https://doi.org/10.30932/1992-3252-2018-16-3-5.

5. Лёвин Б. А., Цветков В. Я. Информационные процессы в пространстве «больших данных» // Мир транспорта. – 2017. – Т. 15. – № 6 (73). – С. 20–30. DOI: https://doi.org/10.30932/1992-3252-2017-15-6-2.

6. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., Khan, S. U. The rise of «big data» on cloud computing: review and open research issues. Information Systems Journal, 2015, Vol. 47, pp. 98–115. DOI: 10.1016/J.IS.2014.07.006.

7. Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., Tonks, S. The Risk Assessment of ERTMS-based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: International Conference on Reliability, Safety and Security of Railway Systems. Springer, 2016, pp 3–19. DOI: 10.1007/978-3-319-33951-1_1.

8. Masson, É., Gransart, C. Cyber Security for Railways – A Huge Challenge – Shift2Rail Perspective. In: International workshop on communication technologies for vehicles. Springer, Cham, 2017, Vol. 10222, pp. 97–104. DOI: https://doi.org/10.1007/978-3-319-56880-5_10 [ограниченный доступ].

9. Álvarez, A., Ioannidis, S., Schlehuber, C., Rodríguez, F., Vallero, V. CIPSEC Project [Online], 2017. [Электронный ресурс]: DOI: https://upcommons.upc.edu/handle/2117/106378. Доступ 14.11.2023.

10. Cao, N., Wang, C., Li, M., Ren, K., Lou, W. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems, 2014, Vol. 25, Iss. 1, pp. 222–233. DOI: 10.1109/TPDS.2013.45.

11. Shi, H. Railway Information Sharing Platform Security Requirements Analysis. In: ICLEM 2014: System Planning, Supply Chain Management, and Safety, 2014, pp 1116–1121. DOI: https://doi.org/10.1061/9780784413753.169.

12. Edwards, W. K. Policies and Roles in Collaborative Applications. In: Proceedings of the 1996 ACM conference on Computer supported cooperative work 1996. ACM, pp 11–20. [Электронный ресурс]: DOI: https://faculty.cc.gatech.edu/~keith/pubs/policy.pdf. Доступ 14.11.2023.

13. Thomas, R. K., Sandhu, R. S. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. Database security XI. Springer, Berlin, 1998, pp 166–181. DOI: 10.1007/978-0-387-35285-5_10.

14. Bullock, A. SPACE: Spatial Access Control for collaborative virtual Environments. Doctoral dissertation, University of Nottingham, 1999, 183 p. [Электронный ресурс]: http://www.adrianbullock.com/documents/thesis.pdf. Доступ 14.11.2023.

15. Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M., Abowd, G. D. Securing Context-Aware Applications Using Environment Roles. In: Proceedings of the sixth ACM symposium on access control models and technologies 2001, ACM, pp 10–20. DOI: https://doi.org/10.1145/373256.373258 [ограниченный доступ].

16. Tolone, W., Ahn, G., Pai, T., Hong, S. Access Control in Collaborative Systems. ACM Computing Surveys (CSUR), 2005, Vol. 37, Iss. 1, pp. 29–41. DOI: 10.1145/1057977.1057979.

17. ENISA (2015) Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations, European Union Agency for Network and Information Security. [Электронный ресурс]: https://www.enisa.europa.eu/publications/good-practices-recommendations. Доступ 14.11.2023.

18. Цветков В. Я. Управление с применением киберфизических систем // Перспективы науки и образования. – 2017. – № 3 (27). – С. 55–60. [Электронный ресурс]: https://pnojournal.files.wordpress.com/2017/04/pdf_170310.pdf. Доступ 14.11.2023.

19. Knowles, W., Prince, D., Hutchison, D. [*et al*]. A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 2015, Vol. 9, pp. 52–80. DOI: 10.1016/j.ijcip.2015.02.002 [ограниченный доступ]. ●

Информация об авторах:

Нестеров Евгений Александрович *– кандидат юридических наук, доцент, директор Юридического института Российского университета транспорта, Москва, Россия, jnesterov@yandex.ru.*

Цветков Виктор Яковлевич *– доктор технических наук, профессор, заместитель директора Юридического института Российского университета транспорта, Москва, Россия, cvj2@mail.ru.*

Статья поступила в редакцию 22.09.2023, одобрена после рецензирования 19.12.2023, принята к публикации 23. 12.2023.