Кожанов Евгений Николаевич,
магистрант, кафедра " Менеджмент высоких технологий и бизнеса" Московский автомобильно-дорожный государственный технический университет (МАДИ)

КИБЕРБЕЗОПАСНОСТЬ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ СИСТЕМ: МОДЕЛЬ УГРОЗ И МЕРЫ ЗАЩИТЫ

Аннотация: В статье рассмотрены транспортно-логистические системы как сложные киберфизические комплексы, в которых цифровая инфраструктура непосредственно определяет устойчивость физических процессов перевозки и распределения. Обоснована модель угроз кибербезопасности, учитывающая архитектурную распределённость, межорганизационный характер логистических цепочек и интеграцию информационных технологий с системами управления транспортом. Выявлены ключевые уязвимости информационного и организационного характера, а также показано, что киберинциденты в данной сфере обладают потенциалом каскадного распространения и трансформации в технологические сбои. Сформулированы системные меры защиты, ориентированные на архитектурную изоляцию критических компонентов, мониторинг аномалий и обеспечение устойчивости транспортно-логистических процессов.

Ключевые слова: кибербезопасность, транспортно-логистические системы, модель угроз, киберфизические системы, критическая инфраструктура, информационная безопасность, управление транспортом, цифровая логистика, каскадные риски, устойчивость систем, сетевые уязвимости, мониторинг безопасности

Abstract: The article examines transport and logistics systems as complex cyber-physical infrastructures where digital components directly affect the stability of physical transport processes. A structured cybersecurity threat model is proposed, taking into account distributed architectures, inter-organizational interactions and the integration of information technologies with transport control systems. The study

identifies key vulnerabilities and substantiates protection measures aimed at risk containment, anomaly detection and operational resilience.

Keywords: cybersecurity, transport and logistics systems, threat model, cyber-physical systems, critical infrastructure, information security, transport management, digital logistics, system resilience, network vulnerabilities

Интенсивная цифровизация транспортно-логистических процессов является одним из ключевых факторов трансформации современной экономики, определяющим повышение эффективности управления потоками грузов и пассажиров, оптимизацию маршрутов и сокращение транзакционных издержек. В условиях внедрения автоматизированных систем управления, интеллектуальных транспортных решений, платформ электронного взаимодействия и распределённых информационных сервисов транспортно-логистические системы приобретают характер сложных киберфизических комплексов, в которых цифровая среда неразрывно связана с функционированием материальной инфраструктуры. Это обстоятельство принципиально изменяет характер рисков, возникающих при нарушении информационной безопасности, поскольку последствия киберинцидентов выходят за рамки информационного ущерба и затрагивают устойчивость физических процессов.

Современные транспортно-логистические системы включают в себя большое количество взаимосвязанных компонентов, функционирующих в режиме реального времени и опирающихся на постоянный обмен данными между участниками логистических цепочек. В такой среде даже локальные нарушения целостности или доступности информации способны вызывать масштабные сбои, распространяющиеся по принципу каскадных эффектов. Кибербезопасность в данном контексте перестаёт рассматриваться как вспомогательная функция и становится одним из базовых условий устойчивого развития транспортной отрасли.

Актуальность исследования кибербезопасности транспортно-логистических систем обусловлена ростом зависимости отрасли от цифровых технологий, расширением поверхностей атак и увеличением числа инцидентов, направленных на критически важную инфраструктуру. Особую значимость приобретает задача формализации угроз, поскольку отсутствие целостной модели киберрисков затрудняет выработку адекватных мер защиты и приводит к фрагментарному характеру принимаемых решений. Целью настоящей статьи является разработка аналитически выверенной модели угроз кибербезопасности транспортно-логистических систем и системное рассмотрение мер защиты, обеспечивающих устойчивость их функционирования.

Транспортно-логистические системы представляют собой многоуровневые комплексы, объединяющие физические объекты, средства управления и информационные ресурсы. Физический уровень включает транспортные средства, инфраструктурные элементы, складские комплексы и терминалы. Управляющий уровень формируется автоматизированными системами диспетчеризации, планирования перевозок, управления движением и мониторинга технического состояния. Информационный уровень представлен корпоративными сетями, облачными сервисами, платформами обмена данными и внешними навигационными и телекоммуникационными системами[1].

Характерной особенностью транспортно-логистических систем является их распределённость и межорганизационная природа. В рамках одной логистической цепочки взаимодействуют субъекты с различным уровнем цифровой зрелости, собственными стандартами информационной безопасности и неодинаковыми ресурсами для защиты инфраструктуры. Это приводит к формированию сложного контекста угроз, в котором безопасность всей системы определяется не столько наиболее защищёнными элементами, сколько наличием уязвимых узлов на периферии.

[1] Масленников С. Н., Синицын М. Г., Окружко О. В. Транспортная безопасность и транспортно-логистические процессы //Редакционная коллегия. – 2025. – С. 6.

Дополнительным фактором уязвимости выступает интеграция информационных технологий с системами оперативного управления транспортом. Использование специализированных промышленных протоколов, встраиваемых контроллеров и сенсорных устройств расширяет поверхность потенциальных атак и усложняет мониторинг состояния безопасности. В отличие от традиционных корпоративных систем, транспортно-логистическая инфраструктура характеризуется жёсткими требованиями к времени отклика и непрерывности работы, что ограничивает возможность применения стандартных мер защиты без адаптации к отраслевой специфике.

Модель угроз кибербезопасности транспортно-логистических систем должна учитывать как технические, так и организационные особенности их функционирования. В основе модели лежит идентификация источников угроз, уязвимых элементов и возможных сценариев воздействия. Источники угроз могут быть внешними, внутренними и смешанными, включая компрометацию цепочек поставок программного обеспечения и сервисов[2].

Внешние угрозы реализуются через сетевые интерфейсы, удалённые каналы управления и публичные сервисы обмена данными. Внутренние угрозы связаны с действиями пользователей и администраторов, обладающих легитимным доступом к системам, а также с ошибками конфигурации и эксплуатации. Смешанные угрозы формируются в результате взаимодействия этих факторов и характеризуются высокой сложностью выявления.

Уязвимости транспортно-логистических систем возникают вследствие архитектурной сложности, использования устаревших компонентов и недостаточной сегментации сетей. Отсутствие чёткого разграничения между корпоративными и технологическими сетями повышает риск распространения инцидентов от информационного уровня к физическому. Существенное значение имеют и уязвимости организационного характера, включая отсутствие

[2] Сизов В. А. и др. Разработка моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода //Development. – 2023. – Т. 18. – №. 4.

единых требований к безопасности для всех участников логистической цепочки и фрагментарность ответственности за защиту информации.

Сценарии реализации угроз в транспортно-логистической сфере характеризуются многоуровневым воздействием. Нарушение конфиденциальности данных о маршрутах, грузах и расписаниях способно привести к экономическим потерям и подрыву конкурентных позиций. Искажение данных управления и навигации создаёт риски принятия ошибочных решений и возникновения аварийных ситуаций. Нарушение доступности ключевых сервисов может вызвать остановку логистических процессов и дестабилизацию смежных отраслей[3].

Особое место в модели угроз занимают воздействия на системы управления транспортом и инфраструктурой, при которых киберинцидент приобретает свойства технологической аварии. В таких условиях граница между информационной и промышленной безопасностью становится условной, а последствия инцидентов приобретают системный характер.

Обеспечение кибербезопасности транспортно-логистических систем требует комплексного подхода, сочетающего технические и организационные решения. В основе такого подхода лежит многоуровневая защита: архитектура системы снижает «радиус поражения» при инциденте, технические средства обеспечивают выявление и сдерживание аномалий, а организационные правила формируют единые требования для всех участников логистической цепочки.

На архитектурном уровне защита предполагает проектирование систем с учётом изоляции критически важных компонентов, разграничения сетевых сегментов и сокращения точек удалённого доступа. Это уменьшает вероятность каскадного распространения инцидентов и позволяет локализовать последствия атак в пределах ограниченных контуров[4].

---

[3] Дмитриев А. В. Нейтрализация угроз внедрения цифровых инструментов в транспортно-логистических системах //Вестник Астраханского государственного технического университета. Серия: Экономика. – 2024. – №. 2. – С. 96-103.

[4] Малёшина Л. М., Шатская И. И. Транспортно-логистическая отрасль: основные вызовы и тенденции цифрового развития //Транспортное право и безопасность. – 2022. – №. 4. – С. 44.

Технические меры ориентированы на непрерывный контроль состояния систем и своевременное выявление отклонений от штатного режима. В транспортно-логистической сфере особенно важно, чтобы мониторинг учитывал специфику технологических процессов и временные характеристики управления, поскольку задержки и несогласованность сигналов могут напрямую влиять на устойчивость операций. Дополнительную роль играет контроль целостности программного обеспечения и конфигураций оборудования: он снижает риск незаметного вмешательства и упрощает обнаружение несанкционированных изменений.

Организационные меры связаны с выстраиванием согласованной политики безопасности для всех участников цепочки поставок. Она включает требования к управлению доступом, порядок реагирования на инциденты и регламент обмена информацией о киберугрозах. Существенным элементом остаётся подготовка персонала: обучение и регулярные практики повышают дисциплину работы с доступами и данными, уменьшая вероятность ошибок и нарушений, связанных с человеческим фактором[5].

Неотъемлемой частью системы кибербезопасности является обеспечение устойчивости и способности к восстановлению. Планирование непрерывности деятельности, резервирование критических ресурсов и отработка сценариев реагирования позволяют минимизировать последствия инцидентов и обеспечить сохранение ключевых функций транспортно-логистических систем даже в условиях частичной утраты работоспособности.

Кибербезопасность транспортно-логистических систем представляет собой сложную междисциплинарную задачу, обусловленную интеграцией цифровых технологий с физической инфраструктурой и управленческими процессами. Сформированная модель угроз демонстрирует, что уязвимости в данной сфере имеют как техническую, так и организационную природу, а

[5] Журбина В. В. Эволюция роли безопасности логистических цепей поставок //Вестник Ростовского государственного экономического университета (РИНХ). – 2024. – Т. 31. – №. 1. – С. 30-36.

последствия реализации угроз способны выходить за рамки отдельных систем и затрагивать устойчивость отрасли в целом.

Эффективные меры защиты должны основываться на системном подходе, сочетающем архитектурные решения, специализированные технические средства и согласованные организационные механизмы. Только при условии целостного управления киберрисками возможно обеспечение надёжного функционирования транспортно-логистических систем в условиях возрастающей цифровой взаимозависимости и усложнения угрозовой среды.

Список использованной литературы и источников:

1. Дмитриев А. В. Нейтрализация угроз внедрения цифровых инструментов в транспортно-логистических системах //Вестник Астраханского государственного технического университета. Серия: Экономика. – 2024. – №. 2. – С. 96-103.
2. Журбина В. В. Эволюция роли безопасности логистических цепей поставок //Вестник Ростовского государственного экономического университета (РИНХ). – 2024. – Т. 31. – №. 1. – С. 30-36.
3. Малёшина Л. М., Шатская И. И. Транспортно-логистическая отрасль: основные вызовы и тенденции цифрового развития //Транспортное право и безопасность. – 2022. – №. 4. – С. 44.
4. Масленников С. Н., Синицын М. Г., Окружко О. В. Транспортная безопасность и транспортно-логистические процессы //Редакционная коллегия. – 2025. – С. 6.
5. Сизов В. А. и др. Разработка моделей для автоматизированного формирования компетентностей специалиста по кибербезопасности на основе сценарного подхода //Development. – 2023. – Т. 18. – №. 4.