УДК 004.056

Ягудина Г.Р., студент, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

Фатихова Л.Э., кандидат экономических наук, доцент, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

КИБЕРБЕЗОПАСНОСТЬ В ЛОГИСТИКЕ: РИСКИ ВЗЛОМА АВТОНОМНЫХ СИСТЕМ И ЗАЩИТА ДАННЫХ

Аннотация: статья посвящена исследованию проблем кибербезопасности в современной логистической отрасли, которая характеризуется активным внедрением цифровых технологий, включая автономные системы и Интернет вещей (IoT). Рассматриваются риски, связанные с уязвимостью автономных транспортных средств, а также угрозы утечки конфиденциальных данных, включая персональные данные клиентов и коммерческие секреты. Анализируются различные векторы атак и предлагаются комплексные меры защиты, охватывающие все аспекты логистических операций. Подчеркивается необходимость разработки строгих политик и процедур кибербезопасности, проведения регулярных аудитов, использования шифрования, многофакторной аутентификации и мониторинга сетевой активности.

Ключевые слова: кибербезопасность, логистика, автономные системы, Интернет вещей (IoT), защита данных, логистические системы, цепочка поставок, транспортная безопасность, управление рисками, инциденты кибербезопасности.

Введение. Глобальная логистическая отрасль быстро меняется благодаря внедрению технологий: Интернета вещей (IoT), искусственного интеллекта (ИИ), облачных вычислений и автономных систем. Это повышает эффективность, снижает затраты и улучшает работу цепочек поставок. Вместе с тем, рост цифровизации увеличивает риски кибербезопасности: расширение сети подключенных устройств и обработка больших объемов данных делают логистику уязвимой к кибератакам, что грозит финансовыми потерями и сбоями в работе.

Проблемы современной логистики. В первом квартале 2025 года российские компании столкнулись с 801 миллионом кибератак — вдвое больше,

чем за тот же период 2024 года. Основные цели — онлайн-платформы логистики, госструктуры и финансы [1].

Автономные системы — транспортные средства, роботизированные склады и автоматизация запасов — повышают эффективность и снижают влияние человека. Но их сложность и взаимосвязанность делают их мишенью для хакеров. Уязвимости в ПО и архитектуре безопасности могут привести к взлому: изменение маршрутов, кража грузов, саботаж операций или аварии. На складах взлом может нарушить комплектацию, повредить товары или остановить работу.

Для систематизированного понимания спектра угроз, связанных с автономными системами в логистике, рассмотрим таблицу, в которой представлены наиболее распространенные векторы атак и потенциальные меры защиты:

Вектор атаки	Описание	Потенциальные последствия	Меры защиты
Взлом программного обеспечения	Использование уязвимостей в программном обеспечении для получения несанкционированного доступа к системе.	Контроль над ATV, изменение маршрута, кража груза, авария; нарушение работы склада, повреждение товаров.	Регулярные обновления ПО, тестирование на проникновение, статическое и динамическое анализ кода, безопасные практики разработки.
Атаки на сенсоры и датчики	Подмена или блокировка данных, поступающих от сенсоров, используемых для навигации, обнаружения препятствий и мониторинга состояния груза.	Некорректная работа ATV, авария, повреждение груза; принятие неверных решений на основе искаженных данных.	Шифрование данных сенсоров, криптографическая аутентификация сенсоров, мониторинг аномалий, использование надежных сенсоров с защитой от подмены.
Физический доступ и саботаж	Получение физического доступа к ATV или другим автономным системам для установки вредоносного ПО, изменения настроек или физического повреждения оборудования.	Контроль над системой, кража данных, саботаж, вывод системы из строя.	Физическая охрана, контроль доступа, мониторинг активности, использование защищенных корпусов и систем защиты от несанкционированного вмешательства.
Атаки на беспроводные сети	Использование уязвимостей в беспроводных сетях (Wi-Fi, Bluetooth, сотовая связь) для получения несанкционированного доступа к системе.	Контроль над ATV, изменение маршрута, кража груза, утечка данных; нарушение работы беспроводных датчиков и сенсоров.	Использование защищенных беспроводных сетей (WPA3), многофакторная аутентификация, мониторинг трафика, сегментация сети, регулярное тестирование на проникновение.

Рис. 6. Векторы атак на автономные системы в логистике

Защита данных — ключевой аспект кибербезопасности в логистике. Логистические операции генерируют большие объемы конфиденциальной информации о клиентах, поставщиках, товарах и маршрутах, которая является привлекательной целью для киберпреступников. Утечка таких данных грозит финансовыми потерями, ущербом репутации и юридическими проблемами.

Особое внимание нужно уделять безопасности облачных платформ, где хранятся и обрабатываются данные. Слабые пароли, отсутствие многофакторной аутентификации, неправильные настройки доступа и отсутствие шифрования делают данные уязвимыми к взлому. Атаки на облако могут вызвать массовые утечки и сбои в работе систем.

Также важно защищать оконечные устройства сотрудников — смартфоны и планшеты, которые подвержены фишингу и вредоносному ПО, что может привести к компрометации учетных данных и утечке информации.

Говоря кратко, кибератаки в сфере логистики могут иметь серьезные последствия:

- Остановка работ из-за отказа систем.
- Потеря продукции из-за перебоев в холодильном хранении или маршрутах доставки.
- Задержки и потери при обслуживании клиента.
- Потеря доверия и ущерб репутации.

Чтобы свести эти риски к минимуму, необходимо иметь планы реагирования на инциденты, а также стратегии непрерывности работы и восстановления после сбоев, которые гарантируют, что в любой непредвиденной ситуации работа может быть быстро поддержана или возобновлена [2].

Категория защиты	**Рекомендации**
Данные клиентов	Минимизация сбора данных (сбор только необходимой информации), использование анонимизации и псевдонимизации данных, шифрование данных при хранении и передаче, соблюдение требований GDPR и других законов о защите персональных данных, прозрачная политика конфиденциальности.
Данные о поставщиках	Контроль доступа к данным (принцип наименьших привилегий), использование VPN и защищенных каналов связи для взаимодействия с поставщиками, регулярные аудиты безопасности поставщиков, включение требований к кибербезопасности в договоры с поставщиками.
Логистические данные (маршруты, грузы, запасы)	Шифрование данных, мониторинг активности, использование безопасных протоколов передачи данных (например, TLS/SSL), ограничение доступа к данным на основе ролей и обязанностей, внедрение систем контроля целостности данных.
Облачные платформы	Выбор надежных поставщиков облачных услуг с сертифицированными системами безопасности (например, ISO 27001, SOC 2), настройка прав доступа и разрешений, использование многофакторной аутентификации, регулярное резервное копирование данных в облаке, шифрование данных в облачном хранилище, мониторинг активности в облачной среде.

Рис. 7 Рекомендации по защите данных в умной логистике

Руководитель направления развития бизнеса Solar JSOC Евгения Хамракулова отмечает, что транспорт, здравоохранение и промышленность менее строго регулируются в части информационной безопасности, чем финансовый сектор. В этих отраслях часто есть неучтённые IT-активы, на которых злоумышленники могут запускать вредоносное ПО, например, для майнинга криптовалют или создания ботнетов [3].

В мае 2024 года один из крупнейших российских логистических операторов — СДЭК — подвергся масштабной кибератаке: сайт, мобильное приложение и call-центр не работали несколько дней. Хакерская группировка Head Mare заявила, что зашифровала базы данных и уничтожила резервные копии. Компания подтвердила использование вируса-шифровальщика [4].

В 2022 году Boxberry также столкнулась со сбоем внутренних сервисов, что затруднило оформление и доставку заказов. Для восстановления работы потребовалось двое суток [5].

Таким образом, кибербезопасность — критически важный фактор успеха в логистике. Уязвимости автономных систем и слабая защита данных могут привести к серьёзным последствиям. Комплексные меры безопасности, развитие технологий, обучение персонала и обмен информацией об угрозах необходимы для устойчивого развития отрасли в эпоху цифровой трансформации.

Список использованных источников

1. Российские компании столкнулись с 801 млн кибератак / [Электронный ресурс] // it.speaker : [сайт]. — URL: https://itspeaker.ru/news/rossiyskie-kompanii-stolknulis-s-801-mln-kiberatak/ (дата обращения: 03.05.2025).

2. Cybersecurity and its importance for operational continuity and the trust of the client / [Электронный ресурс] // emergent cold : [сайт]. — URL: https://emergentcoldlatam.com/en/trends/cybersecurity/ (дата обращения: 03.05.2025).

3. Хакеры в 2024 году чаще всего атаковали российскую транспортную отрасль / [Электронный ресурс] // РИА Новости: [сайт]. — URL: https://ria.ru/20250303/khakery-2002652303.html (дата обращения: 03.05.2025).

4. Взлом СДЭК: уроки для служб доставки на маркетплейсах / [Электронный ресурс] // cs cart : [сайт]. — URL: https://www.cs-cart.ru/blog/vzlom-cdek/ (дата обращения: 03.05.2025).

5. «Курьерки» атакуют по всем киберфронтам / [Электронный ресурс] // LOGIRUS: [сайт]. — URL: https://logirus.ru/news/e-commerce/kurerki-_atakuyut_po_vsem_kiberfrontam.html?sphrase_id=13635363 (дата обращения: 11.05.2025).

Yagudina G.R., student, Naberezhnye Chelny Institute of the Federal State Autonomous Educational Institution of Higher Professional Education "Kazan (Volga Region) Federal University"

Fatikhova L.E., PhD in Economics, Associate Professor, Naberezhnye Chelny Institute of the Federal State Autonomous Educational Institution of Higher Professional Education "Kazan (Volga Region) Federal University"

CYBERSECURITY IN LOGISTICS: RISKS OF HACKING AUTONOMOUS SYSTEMS AND DATA PROTECTION

Abstract: the article is devoted to the study of cybersecurity issues in the modern logistics industry, which is characterized by the active implementation of digital technologies, including autonomous systems and the Internet of Things (IoT). The risks associated with the vulnerability of autonomous vehicles, as well as threats of leakage of confidential data, including personal data of customers and trade secrets, are considered. Various attack vectors are analyzed and comprehensive security measures are proposed that cover all aspects of logistics operations. The need for strict cybersecurity policies and procedures, regular audits, encryption, multi-factor authentication and network activity monitoring is emphasized.

Keywords: cybersecurity, logistics, autonomous systems, Internet of Things (IoT), data protection, logistics systems, supply chain, transportation security, risk management, cybersecurity incidents.