Khalyapin I.V., 2nd year master's student, Naberezhnye Chelny Institute, Kazan Federal University

IMPROVING THE PROCESS OF REPAIR OF TECHNOLOGICAL TRANSPORT OF THE SEAPORT

Abstract: The article considers the problem of ensuring failure prediction of technological transport of port terminals. The fleet of technological transport of the port terminal is considered. The analysis of the existing system of organizing technical maintenance and repair of equipment is carried out. The statistics of sudden failures of technological transport is considered. An algorithm for organizing repairs in case of failures of technological equipment of the port terminal is developed.

Keywords: technological transport, technological transport service, port terminal.

УДК 004.056

Мухитов А.А., студент, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

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

ЦИФРОВЫЕ РИСКИ АВТОПРОМА: УЯЗВИМОСТИ, УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Аннотация: Цифровая трансформация автомобильной промышленности, характеризующаяся интеграцией взаимосвязанных цифровых систем в производственный процесс, привела к экспоненциальному росту уязвимостей в области кибербезопасности. В данной статье анализируется специфика киберугроз, нацеленных на автомобилестроительные заводы, и предлагается систематизированный обзор стратегий защиты, ориентированных на обеспечение целостности производственных процессов, сохранности интеллектуальной собственности и безопасности конечного продукта.

Ключевые слова: кибербезопасность, автомобилестроение, уязвимости, угрозы, стратегии защиты, искусственный интеллект, блокчейн.

Введение

Автомобильная промышленность, находящаяся на переднем крае технологического прогресса, все больше опирается на интегрированные

цифровые системы для повышения эффективности, оптимизации производственных процессов и внедрения инноваций. Концепция индустрии 4.0, характеризующаяся широким применением роботизации, автоматизации, интернета вещей (IoT) и аналитики больших данных, привела к радикальным изменениям в производственной среде автомобилестроительных заводов. Однако, эта трансформация неразрывно связана с существенным увеличением поверхности атаки и потенциальных векторов проникновения злоумышленников в критически важные системы. Недостаточная защита цифровой инфраструктуры может привести к катастрофическим последствиям, включая остановку производства, кражу интеллектуальной собственности, нарушение логистических цепочек, компрометацию данных и даже небезопасную эксплуатацию выпускаемых автомобилей. Целью данной статьи является систематический анализ существующих и потенциальных киберугроз, нацеленных на автомобилестроительные заводы, и разработка комплексного подхода к обеспечению кибербезопасности производственных мощностей.

Киберугрозы и методы борьбы с ними

Исследователи Upstream проанализировали критические риски и уязвимости в сфере автомобильной и интеллектуальной мобильности:

- 60% всех инцидентов в 2024 году имели значительные или масштабные последствия;
- 92% инцидентов были выполнены удалённо, из которых 84% были на большом расстоянии [1].

Автомобилестроительные заводы представляют собой сложные и многоуровневые системы, включающие в себя широкий спектр цифровых компонентов, таких как системы автоматизированного проектирования, системы управления производством, системы управления запасами, роботизированные сборочные линии и подключенное оборудование. Каждая из этих систем может являться потенциальной целью для кибератак.

Тип угрозы	Описание	Последствия
Программы-вымогатели (Ransomware)	Шифрование критически важных данных с последующим требованием выкупа.	Остановка производства, потеря данных, финансовые потери, нарушение конфиденциальности.
Целенаправленные атаки (APT)	Сложные многоступенчатые атаки, направленные на долгосрочное присутствие в сети и кражу данных.	Кража интеллектуальной собственности, нарушение конкурентного преимущества, компрометация критически важных систем, нанесение репутационного ущерба.
Фишинговые атаки	Использование социальной инженерии для получения доступа к системам через обман сотрудников.	Компрометация учетных данных, заражение вредоносным ПО, несанкционированный доступ к системам.
Эксплуатация уязвимостей ПО	Использование известных или новых уязвимостей в программном обеспечении и оборудовании для проникновения в сеть.	Несанкционированный доступ, заражение вредоносным ПО, отказ в обслуживании, компрометация данных.
Инсайдерские угрозы	Действия сотрудников, как намеренные, так и по неосторожности, приводящие к нарушению безопасности.	Утечка данных, саботаж, нарушение целостности систем, финансовые потери.
Атаки на цепочку поставок	Использование уязвимостей в системах поставщиков для получения доступа к сети автопроизводителя.	Компрометация данных, нарушение производственных процессов, распространение вредоносного ПО, нарушение конфиденциальности.
DDoS-атаки	Перегрузка сети трафиком, приводящая к отказу в обслуживании критически важных систем.	Остановка производства, нарушение логистических цепочек, невозможность доступа к критически важным ресурсам.

Рис. 1. Классификация киберугроз для автомобилестроительных заводов

Успешная кибератака может вызвать серьёзные последствия для автопроизводителей и потребителей. Задержки из-за взлома поставщиков компонентов могут сорвать выпуск новых моделей и привести к финансовым потерям.

Экономические последствия включают затраты на реагирование, привлечение экспертов, восстановление систем и устранение уязвимостей. Компании сталкиваются с юридическими издержками, судебными разбирательствами и штрафами. Потеря репутации снижает доверие к бренду, что ведёт к падению продаж и рыночной стоимости. Инвестиции в кибербезопасность увеличивают расходы. Утечка конфиденциальных данных даёт конкурентам преимущество. Повторяющиеся атаки подрывают конкурентоспособность и долю рынка.

В 2023 году европейские автокомпании столкнулись с атаками: голландская Kendrion сообщила о взломе и возможной утечке данных, а немецкая SAF-HOLLAND SE потеряла около 40 млн евро из-за остановки производства. Такие инциденты серьёзно угрожают производству и финансам [3].

Исходя из этого, риски могут делиться на 2 типа:

Рис. 2. Типы рисков

Эффективная защита автозаводов от киберугроз требует комплексного подхода, включающего технические и организационные меры.

Ключевыми техническими элементами являются многоуровневая система безопасности с брандмауэрами, IDS/IPS, антивирусами и сегментация сети с помощью VLAN и межсетевых экранов для ограничения распространения атак. Важно контролировать доступ к критически важным системам, предоставляя минимально необходимые права, регулярно обновлять ПО и применять патчи. Шифрование данных защищает от несанкционированного доступа, а системы обнаружения аномалий на базе машинного обучения выявляют подозрительную активность. Контроль целостности файлов (FIM) помогает обнаружить несанкционированные изменения [4].

Организационные меры включают регулярные оценки рисков и разработку плана их снижения, создание политики кибербезопасности, обучение сотрудников распознаванию угроз и правильному использованию систем. Важно разрабатывать и тестировать планы реагирования на инциденты, проводить аудиты безопасности и сотрудничать с поставщиками и партнерами для обмена информацией об угрозах и соблюдения стандартов [5].

Категория мер	Описание
Технические меры	Использование брандмауэров, систем обнаружения вторжений, антивирусов, шифрования данных, контроля доступа, обновления программ и т.д.
Организационные меры	Разработка политики безопасности, обучение персонала, оценка рисков, планирование реагирования на инциденты, аудит безопасности и т.д.

Рис. 3. Меры защиты от киберугроз для автомобильных заводов

Растущая сложность автомобильных систем и увеличение количества подключенных автомобилей привели к необходимости разработки четких нормативных рамок и стандартов кибербезопасности. В частности, стандарт ISO/SAE 21434 играет ключевую роль, определяя требования к процессам и мероприятиям по обеспечению кибербезопасности на протяжении всего жизненного цикла автомобиля, от проектирования до вывода из эксплуатации. Этот стандарт охватывает широкий спектр аспектов, включая управление рисками, проектирование безопасной архитектуры, тестирование на проникновение и реагирование на инциденты [6].

В дополнение к традиционным мерам защиты, внедрение перспективных технологий может значительно повысить уровень киберустойчивости автомобилестроительных заводов:

1. ИИ может использоваться для автоматического обнаружения и предотвращения кибератак, анализа больших объемов данных о безопасности, выявления аномалий и прогнозирования будущих угроз. Обнаружение вредоносного ПО, анализ сетевого трафика и анализ поведения пользователей на основе машинного обучения способствуют выявлению и предотвращению различных киберугроз.

2. Блокчейн может использоваться для обеспечения безопасного и прозрачного обмена данными между участниками цепочки поставок, защиты интеллектуальной собственности и отслеживания про исхождения компонентов. Защита цепочки поставок с использованием блокчейна, защита интеллектуальной собственности с использованием блокчейна и безопасный

обмен данными с использованием блокчейна повышают прозрачность и безопасность в автомобилестроительной отрасли.

Кибербезопасность является критически важным аспектом для современных автомобилестроительных заводов в эпоху Индустрии 4.0. Сложность и взаимосвязанность цифровых систем, используемых в производственном процессе, создают широкий спектр уязвимостей и потенциальных векторов атаки. Успешное противодействие киберугрозам требует комплексного и многоуровневого подхода, охватывающего как технические, так и организационные меры защиты. Внедрение перспективных технологий, таких как искусственный интеллект, блокчейн, позволит значительно повысить уровень киберустойчивости производственных мощностей и обеспечить безопасность автомобильной промышленности в будущем. Дальнейшие исследования в области кибербезопасности автомобилестроения должны быть направлены на разработку новых методов обнаружения и предотвращения атак, адаптацию существующих технологий к специфике производственных систем и разработку стандартов кибербезопасности, учитывающих особенности автомобильной промышленности.

Список использованных источников

1. Upstream’s 2025 Global Automotive and Smart Mobility Cybersecurity Report / [Электронный ресурс] // Upstream: [сайт]. — URL: https://upstream.auto/reports/global-automotive-cybersecurity-report/ (дата обращения: 27.04.2025).

2. Upstream’s 2025 Global Automotive and Smart Mobility Cybersecurity Report / [Электронный ресурс] // Upstream: [сайт]. — URL: https://upstream.auto/reports/global-automotive-cybersecurity-report/ (дата обращения: 27.04.2025).

3. Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН / [Электронный ресурс] // Kaspersky: [сайт].

— URL: https://ics-cert.kaspersky.ru/publications/reports/2024/02/07/cybersecurity-in-the-automotive-industry-ensuring-compliance-with-unece-regulations/ (дата обращения: 27.04.2025).

4. Как обеспечить техническую защиту информации на предприятии / [Электронный ресурс] // Spectrum Data: [сайт]. — URL: https://spectrumdata.ru/blog/proverka-soiskatelya/kak-obespechit-tekhnicheskuyu-zashchitu-informatsii-na-predpriyatii/ (дата обращения: 27.04.2025).

5. Организационные меры по защите информации: состав и содержание документов и мероприятий / [Электронный ресурс] // TRINOSOFT.COM: [сайт]. — URL: https://trinosoft.com/index.php?page=/is/informaziya-organisazionnie-mery-zashiti (дата обращения: 27.04.2025).

6. Существующее международное регулирование в сфере автомобильной кибербезопасности / [Электронный ресурс] // ТБТ: [сайт]. — URL: https://autovisor-vss.ru/regulations/ (дата обращения: 27.04.2025).

Mukhitov A.A., student, Naberezhnye Chelny Institute of the Kazan (Volga Region) Federal University

Fatikhova L.E., Candidate of Economics, Associate Professor, Naberezhnye Chelny Institute of the Kazan (Volga Region) Federal University

CYBERSECURITY IN THE AUTOMOTIVE INDUSTRY: VULNERABILITIES, THREATS, AND STRATEGIES

Abstract: The digital transformation of the automotive industry, characterized by the integration of interconnected digital systems into the production process, has led to an exponential increase in cybersecurity vulnerabilities. This article analyzes the specifics of cyber threats aimed at automotive plants and provides a systematic overview of protection strategies aimed at ensuring the integrity of production processes, the preservation of intellectual property and the safety of the final product.

Keywords: cybersecurity, automotive industry, vulnerabilities, threats, protection strategies, artificial intelligence, blockchain.