КИБЕРБЕЗОПАСНОСТЬ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ: ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ КИБЕРАТАК И УТЕЧКИ ДАННЫХ

Д.Д. Садовщиков, студент 1 курса, группа ПМ-241п
Руководитель: М.А. Халдарова, преподаватель
Государственное профессиональное образовательное учреждение
«Топкинский технический техникум»
Кемеровская область-Кузбасс, пгт. Промышленная

С развитием технологий и переходом к цифровому формату работы железнодорожные компании столкнулись с новыми угрозами в виде кибератак и утечек данных. Защита информационных систем на железнодорожном транспорте становится все более актуальной задачей.

Цель научно-исследовательской работы - исследовать современные методы защиты информационных систем на железнодорожном транспорте от кибератак и утечек данных, а также разработать рекомендации по максимально эффективной защите.

Задачи исследования включают в себя анализ текущего состояния кибербезопасности на железнодорожном транспорте, выявление основных уязвимостей и угроз, изучение принципов работы современных кибератак, анализ методов защиты информационных систем, разработку рекомендаций по улучшению кибербезопасности на железнодорожном транспорте, а также проведение практических тестов пригодности предложенных защитных механизмов.

Исследование позволит не только выявить уязвимости и угрозы, но и предложить конкретные меры по улучшению кибербезопасности на железнодорожном транспорте, что способствует безопасной и непрерывной работе транспортной системы.

Основные угрозы и риски для информационных систем на железной дороге

Данная работа ставит перед собой целью исследовать основные угрозы и риски, с которыми сталкиваются информационные системы на железной дороге, а также разработать методы и инструменты для их защиты.

На современных железнодорожных путях информационные системы стали ключевым звеном, обеспечивающим безопасное и эффективное движение поездов. Однако с ростом цифровизации и подключения к интернету уровень уязвимости систем значительно возрастает. Основными угрозами для информационных систем на железной дороге являются кибератаки, в том числе DDoS-атаки, вирусы, фишинг и другие формы злоумышленничества, направленные на нарушение работы и безопасности систем.

Риски возникновения кибератак на информационные системы на железной дороге включают в себя потенциальные последствия для безопасности пассажиров и грузов, а также возможные финансовые потери для компаний-провайдеров железнодорожных услуг. Утечка данных также представляет серьезную угрозу, поскольку конфиденциальная информация о расписании поездов, пассажирах,

грузах и других аспектах может быть использована злоумышленниками для незаконных действий.

Для решения поставленных задач необходимо провести комплексное исследование уязвимостей информационных систем на железной дороге, а также разработать механизмы защиты, включающие в себя современные технологии шифрования, системы мониторинга и обнаружения аномалий, а также регулярное обновление программного обеспечения и обучение персонала по вопросам кибербезопасности.

Способы защиты от кибератак и утечки данных в железнодорожной отрасли

Для обеспечения кибербезопасности на железнодорожном транспорте необходимо эффективно защищать информационные системы от кибератак и утечки данных. Задачи исследования включают в себя анализ существующих угроз, идентификацию уязвимостей информационных систем, и поиск оптимальных методов для защиты от кибератак.

Рассматриваемые способы защиты от кибератак и утечки данных в железнодорожной отрасли включают в себя ряд мер и рекомендаций. Важным аспектом является использование многоуровневой системы защиты, которая включает в себя фаерволы, системы обнаружения вторжений, антивирусные программы, шифрование данных и другие технологии. Также следует обеспечить регулярное обновление программного обеспечения и прошивок, а также обучение персонала по вопросам кибербезопасности.

Дополнительно, для защиты информационных систем на железнодорожном транспорте рекомендуется установка систем аутентификации и авторизации пользователей, а также контроль доступа к данным. Важно также обеспечить физическую безопасность серверов и компьютеров, например, путем установки специальных замков и систем видеонаблюдения. Все эти меры позволят эффективно защищать информационные системы железнодорожной отрасли от киберугроз и предотвращать утечку конфиденциальных данных.

Практические примеры успешной реализации мер по кибербезопасности

Практические примеры успешной реализации мер по кибербезопасности могут включать в себя использование многофакторной аутентификации для доступа к железнодорожным информационным системам, построение защищенных виртуальных частных сетей для передачи данных, внедрение систем мониторинга и реагирования на потенциальные кибератаки.

На практике важно проводить регулярное обновление программного обеспечения, обучение сотрудников правилам кибербезопасности, а также осуществлять мониторинг и аудит защитных мероприятий. Только комплексный подход к обеспечению кибербезопасности на железнодорожном транспорте позволит минимизировать риски кибератак и утечки конфиденциальных данных, обеспечивая стабильную работу информационных систем и безопасность пассажиров.

Перспективы развития систем защиты информации на железнодорожном транспорте

В современном мире сфера железнодорожного транспорта столкнулась с необходимостью эффективной защиты информационных систем от киберугроз и утечек данных. Научные исследования в области кибербезопасности на железнодорожном транспорте направлены на разработку и совершенствование систем защиты информации для обеспечения безопасности важных транспортных систем и данных пассажиров.

Список источников:

1. Киселева Е.М. ЖЕЛЕЗНАЯ ДОРОГА КАК ОБЪЕКТ КИБЕРЗАЩИТЫ // Международный студенческий научный вестник. – 2018. – № 5.; – Текст : непосредственный.
2. Информационная безопасность в логистике и на транспорте [Электронный ресурс] // tadviser.– URL: https://www.tadviser.ru/index.php/ (дата обращения 5.10.2024).
3. Информационная безопасность на транспортных предприятиях [Электронный ресурс] // securenews.– URL: https://securenews.ru/information_security_on_transport/ (дата обращения 5.10.2024).
4. Кибербезопасная логистика [Электронный ресурс] // news.– URL: https://news.microsoft.com/ru-ru/features/logistic-cybersecurity/ (дата обращения 5.10.2024).
5. Кибербезопасность в транспортной отрасли [Электронный ресурс] // cybersecurityguide. – URL: https://cybersecurityguide.org/industries/transportation/ (дата обращения 5.10.2024).