

ВНЕДРЕНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ТРАНСПОРТА

Сотникова И.С., студентка 4 курса

Устинова А.С., студентка 4 курса

Пономаренко П.Г., преподаватель

УО «Белорусский государственный университет транспорта»,

г. Гомель, Беларусь

Введение. В статье исследуются пути обеспечения кибербезопасности на транспорте, дается оценка уровня осведомленности пассажиров о киберрисках и угрозах в связи с использованием компьютерных систем управления транспортными средствами, обосновываются наиболее уязвимые места в интеллектуальных системах управления транспортом, используемые злоумышленниками для осуществления кибератак, анализируется степень доверия людей к существующим системам безопасности и защиты информации в транспортной инфраструктуре.

Актуальность исследования обусловлена тем, что с развитием цифровых технологий в транспортной отрасли появились новые возможности для киберпреступников. С внедрением технологий искусственного интеллекта в транспортной отрасли, таких как автономные автомобили и умные поезда, возрастает актуальность проблемы обеспечения кибербезопасности на транспорте. Рост числа кибератак на транспортные средства в последние годы обусловлен резким увеличением количества транспортных средств на дорогах, подключенных к системе искусственного интеллекта. Объектами атак становятся: каршеринги, общественный транспорт, электромобили и другие подключённые «умные» автомобили [1].

Цифровые технологии послужили отправной точкой для развития «умных» систем. Они контролируют железные дороги и автомобильные трассы, используя платформы мониторинга, собирают информацию о дорожных пробках на основе навигаторов, следят за безопасностью пассажиров, грузов и транспортных средств. Для целей контроля за транспортными средствами используются дистанционные датчики и контроллеры. Опыт эксплуатации машин с искусственным интеллектом показал, что чем больше средств контроля, позволяющих поддерживать связь с внешним миром, тем уязвимее становится транспортное средство для киберпреступлений.

Меры по обеспечению кибербезопасности транспорта направлены на защиту транспортных средств, систем управления и данных от киберугроз, таких как распространение компьютерных вирусов, внедрение вредоносного программного обеспечения, проведение хакерских атак и другие виды действий. Действия кибермошенников могут привести к негативным последствиям, включая сбои в работе транспорта, кражи данных и груза, утечку конфиденциальной информации. Они также создают угрозу безопасности перевозки пассажиров и грузов. Поэтому кибербезопасность транспорта имеет важное значение для обеспечения безопасности и надежности транспортных систем.

Научная новизна. Для обеспечения кибербезопасности транспортной отрасли нами предложены возможные варианты защиты систем управления транспортом и транспортных средств от кибератак. Они предусматривают установку антивирусного программного обеспечения, обновление прошивок и программного обеспечения на транспортных средствах и системах управления, а также обучение персонала правилам кибербезопасности.

Авторами рекомендовано использовать современные технологии контроля доступа к базам данных и шифрования их, которые позволят предотвратить несанкционированный доступ к системам управления транспортом. Важно проводить регулярное тестирование программного обеспечения на наличие

уязвимых мест и обучать персонал правилам кибербезопасности, чтобы они могли быстро и правильно реагировать на возможные кибератаки.

Материалы и методы исследования/приборы и материалы. Для оценки степени общественной осведомленности в необходимости соблюдения правил кибербезопасности при использовании транспорта был проведен опрос пассажиров и иных граждан, в котором приняли участие 150 человек. Его цель – изучить отношение опрошенных к системам сбора данных, а также к соблюдению конфиденциальности в отношении личной информации.

Опрос содержал 11 вопросов, при этом перечень вопросов был следующий:

1. Пользуетесь ли вы каким-либо каршерингом, системой «Оплати» или «БЧ мой поезд»?
2. Считаете ли вы перечисленные системы безопасными?
3. Считаете ли вы систему надёжной, если скачали её из официального магазина?
4. Доверяете ли вы системе, если слышали о ней от знакомых?
5. Используете ли вы разные пароли для приложений?
6. Сталкивались ли вы с утечкой информации?
7. Что, по вашему мнению, относится к персональным данным?
8. Позволяете ли вы сайту обрабатывать личные данные, если без этого воспользоваться сервисом невозможно?
9. Как часто вы меняете пароль?
10. Считаете ли вы, что сбор личных данных производится для персонализации (например, для выдачи билетов)?
11. Считаете ли вы, что сбор личных данных производится для статистики?

Результаты и их обсуждение. Результаты проведенного нами опроса показали, что большинство опрошенных пользуются электронными системами сбора данных, такими, как «Оплати», «БЧ мой поезд», «YouDrive» и другие. Это объясняется удобством и направленностью данных приложений, так как они позволяют удаленно провести оплату поездки, израсходовав на эти цели не

больше 5 минут времени. Из числа опрошенных 84% (126 человек) регулярно используют данные приложения в повседневной жизни.

Данные приложения являются безопасными в использовании с точки зрения утечки данных, так как сбор данных производится централизованно, при использовании политики конфиденциальности. В то же время результаты проведенного опроса показали, что большинство опрошенных никогда не задумывалось о безопасности подобных приложений. Из числа опрошенных 114 человек (76%) выбрали ответ «Не задумывался», 18 человек (или 12%) считают данные приложения безопасными, а ответ «Нет» не выбрал ни один человек. Также 135 человек (или 90% опрошенных) считают, что если приложение было установлено официальным представителем транспортной организации, то система является безопасной. Из общего количества опрошенных только 15 человек, то есть 10% на вопрос о безопасности приложения транспортной организации выбрали ответ «Нет». Можно сделать вывод, что пользователи электронных приложений транспортных организаций считают безопасными по причине их официальности.

Однако это не всегда предлагаемые приложения и представляемый ими бренды являются подлинными. Интернет-приложения следует скачивать с официальных сайтов, к тому же необходимо дополнительно удостовериться в их оригинальности. А вот приложения из неизвестных источников, не рекомендованных официальными органами, скачивать не стоит.

Немаловажным является то, что большинство опрошенных, а именно 87 человек (58%) используют одинаковый пароль для всех социальных сетей и онлайн-сервисов, а 126 человек (или 84%) из опрошенных меняют пароль реже одного раза в год, 21 человек (14%) меняют пароль каждые полгода, и только 3 человека из опрошенных (2%) меняет пароль каждый месяц.

Следует учитывать, что кибербезопасность важна и необходима как для пользователей систем, так и для владельца приложений. Так, в последние 6 лет участились кибератаки на системы оплаты. Ярким примером следует отметить взлом системы оплаты проездных документов в метро в 2016 году в Москве.

Трое граждан взломали систему оплаты и украли ключи шифрования и личные данные пользователей. Убыток от данной атаки составил 2 миллиона российских рублей [3]. Схожая ситуация произошла и в 2020 году, когда один из пользователей каршеринга «Делимобиль» воспользовался чужим аккаунтом, использовал автомобиль в течение 14 часов и попал в серьезную аварию [4].

Количество кибератак все больше увеличивается с каждым годом. Не следует забывать базовые правила пользователей для сохранности личных данных. Правила следующие:

- установка надежного антивирусного программного обеспечения;
- использование сложных вариантов паролей;
- защита при помощи брандмауэра (брандмауэр защищает как аппаратное, так и программное обеспечение, что делает его удобным для любой компании с физическими серверами) и др. [5].

Выводы. Кибербезопасность транспортной отрасли – это комплекс мер, направленных на защиту транспортных систем от кибератак и обеспечение безопасности пассажиров и грузов на транспорте.

Основными целями кибербезопасности транспортной отрасли являются:

- защита от несанкционированного доступа к транспортным системам и транспортным средствам;
- предотвращение кибератак на транспортные системы и транспортные средства;
- обеспечение безопасности перевозки пассажиров и грузов;
- минимизация киберрисков для транспортных компаний и их клиентов.

Для достижения этих целей необходимо применять следующие меры:

- ✓ установка антивирусного программного обеспечения и регулярное его обновление;
- ✓ установление четкого режима доступа к информационным базам и использование технологий шифрования данных для защиты транспортных систем и транспортных средств;

✓ обучение персонала правилам кибербезопасности и проведение регулярных тренингов по предотвращению кибератак;

✓ внедрение систем мониторинга и анализа данных для выявления уязвимых участков в информационных системах и транспортных средствах;

✓ разработка и внедрение новых технологий и методов для защиты транспортной отрасли от кибератак.

Для защиты от кибератак необходимо использовать современные технологии, такие как шифрование данных, двухфакторная аутентификация, системы обнаружения вторжений и другие меры безопасности. Кроме того, кибербезопасность транспорта также предполагает защиту от кибератак системы управления дорожным движением, так как вмешательство извне может привести к авариям и другим негативным последствиям. Для обеспечения безопасности дорожного движения необходимо использовать современные системы управления движением и контроля за трафиком, а также проводить обучение водителей и пассажиров мерам безопасности при использовании компьютерными системами и эксплуатации транспортных средств с искусственным интеллектом.

Кибербезопасность транспорта является ключевым аспектом системы обеспечения безопасности транспортных средств, данных и инфраструктуры. Ее надежность требует комплексного подхода к внедрению и использованию современных технологий и мер безопасности.

Список литературы

1. Информационная безопасность транспорта [Электронный ресурс]. – Режим доступа: <https://autovisor-vss.ru/transport-cybersecurity/>. – Дата доступа: 06.10.2023.

2. Кибербезопасность транспорта: как автомобиль могут угнать с компьютера [Электронный ресурс]. – Режим доступа: <https://trends.rbc.ru/trends/industry/614041579a79471ac5adba05>. – Дата доступа: 08.10.2023.

3. В Москве раскрыли хакерский взлом карты «Тройка» [Электронный ресурс]. – Режим доступа:

https://www.rbc.ru/technology_and_media/25/08/2017/599f0c6e9a7947641df10f03.

– Дата доступа: 07.10.2023.

4. Скандал с фейковым аккаунтом: разбили каршеринг под чужим именем [Электронный ресурс]. – Режим доступа: <https://kiozk.ru/article/skandal-s-fejkovym-akkauntom-razbili-karsering-pod-cuzim-imenem>. – Дата доступа: 08.10.2023.

5 Сетевое издание «РБК» [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology_and_media/25/08/2017/599f0c6e9a7947641df10f03 – Дата доступа: 08.10.2023.