ЛИТЕРАТУРА

1. Протокол заседания Президиума Совета Министров Республики Беларусь от 4 февраля 2020 г. № 3 «Национальная стратегия устойчивого развития Республики Беларусь на период до 2035 года».

2. Капский, Д. В., Семченков, С. С. / Транспортная экология. Лабораторный практикум для студентов специальностей 1-44 01 01 «Организация перевозок и управление на автомобильном и городском транспорте», 1-44 01 02 «Организация дорожного движения» и 1-44 01 06 «Эксплуатация интеллектуальных транспортных систем на автомобильном и городском транспорте» / Д. В. Капский, С. С. Семченков // Минск : БНТУ, 2017.

УДК 656.1

ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Студ. гр. 10117122 **Афонин И. Д., Шуппо А. В., Калитин М. С.**
Научный руководитель – ст. преп. ***Алисеенко Д. С.***

Несмотря на то, что интеллектуальные транспортные системы (далее – ИТС) могут существенно отличаться друг от друга в зависимости от основных целей своего функционирования и способов технической реализации, одна из основных их проблем при эксплуатации заключается в обеспечении низкого уровня безопасности цифровой среды.

Представим основные компоненты предлагаемой системы безопасности цифровой среды ИТС.

1. Определение ключевых элементов безопасности:

– конфиденциальность (защита от несанкционированного доступа к информации);

– целостность (обеспечение невозможности несанкционированного изменения данных);

– доступность (гарантия доступа к информации и ресурсам для уполномоченных пользователей).

2. Моделирование угроз (использование методов моделирования для описания потенциальных угроз и атак).

3. Разработка критериев безопасности (создание количественных и качественных показателей для оценки уровня безопасности).

4. Принципы построения защищенной архитектуры (разработка модульной структуры системы, позволяющей легко адаптироваться к изменяющимся угрозам).

5. Стратегии реагирования на инциденты (определение процедур и действий при обнаружении угрозы или инцидента).

6. Правовые и нормативные аспекты (учет законодательных актов и стандартов в области безопасности ИТС).

7. Обучение (разработка программ обучения для пользователей и специалистов по эксплуатации и безопасности ИТС).

8. Интеграция с другими системами (обеспечение совместимости и безопасного взаимодействия с другими цифровыми системами).

9. Использование искусственного интеллекта (применение алгоритмов машинного обучения для прогнозирования и предотвращения угроз).

10. Непрерывное тестирование и контроль (регулярное проведение тестов на выявление угроз).

Предлагаемая система может быть дополнена и адаптирована в зависимости от специфики ИТС и изменений в цифровой среде. Важно также учитывать развитие технологий и перманентно меняющуюся природу угроз. Создание предлагаемой системы – это многоуровневая задача, требующая интеграции усилий и сотрудничества специалистов в области безопасности и эксплуатации ИТС, разработчиков программного обеспечения, экспертов в области транспортных систем.

Для решения прикладных задач цифровой безопасности ИТС следует применять комплексный подход, включающий аналитическое исследование и моделирование различных угроз, разработку стратегий защиты и непрерывное тестирование.

Под угрозой понимается вмешательство в работу ИТС со стороны злоумышленника:

– неавторизованный доступ (хакеры могут получить доступ к управляющим системам транспортных средств);

– внедрение вредоносного программного обеспечения (распространение вредоносного программного обеспечения через системы обновления);

– сбой процесса обслуживания – DoS-атаки (атаки, направленные на перезагрузку сетевой инфраструктуры);

– манипуляция данными (изменение или подделка данных о движении транспортных средств с целью создания хаоса на улично-дорожной сети);

– фишинг (сбор конфиденциальной информации через поддельные сайты).

Актуальным примером подобных угроз является умышленное внедрение вредоносного программного обеспечения в систему поезда, производимого польской компанией Newag, с целью недопущения ее фирменных поездов к обслуживанию в других сервисах.

Выделим основные пути решения проблемы безопасности цифровой среды ИТС.

Многоуровневая аутентификация. Усиление процедур аутентификации для доступа к наиболее важным системам означает, что при запуске какого-либо программного продукта в процессе авторизации должен соблюдаться ряд правил. Они касаются ограничения количества активных сессий пользователей в текущий момент времени, доверенности к определенному кругу лиц, допускаемых к работе с ИТС.

Шифрование данных. Современная криптография активно развивается в направлении использования передовых методов шифрования для защиты данных при передаче и хранении. Модификация методов криптографии входящего/исходящего трафика направлена на дезориентацию злоумышленника.

Обучение персонала. Работники транспортных организаций должны быть постоянно осведомлены о новых угрозах подобного рода, а также методах фишинга и повышения безопасности ИТС.

Регулярное обновление ПО. Следует постоянно дорабатывать и обновлять программное обеспечение для устранения его уязвимостей.

Тестирование на проникновение. Необходимо регулярно проводить тесты на предмет проникновения угроз для выявления потенциальных уязвимостей ИТС.

Резервное копирование и восстановление. Следует автоматически создавать резервные копии информационных данных и разрабатывать стратегии их восстановления после сбоев системы.

Системы обнаружения и предотвращения вторжений (IDS/IPS). Подобные системы обнаружения основаны на принципе постоянного контроля за работой сети с целью мониторинга сетевого трафика и блокировки подозрительных несанкционированных действий.

Предлагаемые пути решения проблемы безопасности цифровой среды ИТС должны быть интегрированы в единую систему управления безопасностью, которая будет постоянно адаптироваться к новым угрозам и изменениям в технологической сфере. При этом ключевым аспектом является сотрудничество с государственными органами и другими заинтересованными лицами с целью обмена информацией о новых угрозах и передовых практиках защиты.

ЛИТЕРАТУРА

1. Превышая скорость: риски и уязвимости в сфере интеллектуальных транспортных систем. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/trendmicro/articles/492018/. – Дата обращения: 17.05.2024.

2. Кибербезопасность в автомобильной промышленности: новые обязательные правила [Электронный ресурс]. – Режим доступа: https://www.dqsglobal.com/ru-by/izuchajte2/blog/kiberbezopasnost%27-v-avtomobil%27noj-promyshlennosti-novye-obyazatel%27nye-pravila. – Дата доступа: 17.05.2024.

3. Кибератаки на автомобили. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D0%B8. – Дата доступа: 17.05.2024.

4. Основные виды атаки на инфраструктуры. – [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B

8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D0%B8. – Дата доступа: 17.05.2024.

5. Безопасность интеллектуального городского транспорта: два исследования [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/intellectual-transport/3543/. Дата доступа: 17.05.2024.

УДК 656.1

ПЕРСПЕКТИВЫ РАЗВИТИЯ ВОДОРОБУСОВ В СТРАНАХ СНГ,

Студ. гр. 10114122 **Салаш А. Д.**
Научный руководитель – ст. преп. ***Алисеенко Д. С.***

Водоро́бус – это электробус, использующий водородный топливный элемент в качестве источника энергии для электродвигателя, иногда дополненный гибридным способом батареей или суперконденсатором.

Его принцип работы основан на том, что в двигателе, в состав которого входит электрохимический генератор, происходит реакция водорода с кислородом, в результате чего получается электроэнергия, которая может быть задействована для обогрева салона и конденсата.

Анализ источников по проблеме исследования позволил выделить ряд достоинств и недостатков водоробуса. Обозначим его основные преимущества.

Водоробус является более экологически безопасным видом транспорта по сравнению с электробусом:

– водоробус не использует литий-ионные батареи, которые загрязняют природу при производстве и утилизации;