Ш. С. Фахми[1,2], Ю. М. Соколов[1], Е. В. Костикова[3]

Безопасность в интеллектуальных транспортных системах

[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина);

[2]Институт проблем транспорта им. Н.С. Соломенко Российской академии наук;

[3]Государственный университет морского и речного флота им. адмирала С.О. Макарова г. Санкт-Петербург, Россия

Аннотация. *На современном этапе развития образования и науки технологии проектирования с использованием ПЛИС широко используются в интеллектуальных транспортных системах. Интеллектуальные транспортные системы, даже если они облегчают сбор, обработку и обмен информацией, сами по себе не являются гарантами и возникают вопросы безопасности, требующие особого внимания: каковы основные меры безопасности, которые следует принять для устранения риска кибератак в своих коммуникациях? Чтобы разработать полную архитектуру безопасности с механизмами, адаптированными к коммуникациям, авторами предлагается использовать метод анализа рисков для предотвращения различных атак и предлагать контрмеры в соответствии с выявленными уровнями угрозы.*

Ключевые слова: интеллектуальные транспортные системы; ПЛИС; анализ рисков; цели безопасности; технологии связи

Интеллектуальные транспортные системы (ИТС) – это решение множественных проблем обеспечения безопасности на транспорте, таких как заторы, аварии и т.д., например, одной из важнейших проблем транспорта в рамках ИТС – это уведомление водителей об опасностях на дороге впереди, прежде чем они станут видны, и принять соответсвующие решения для того, чтобы транспортные средства находились на безопасном расстоянии друг от друга, предлагая водителям оптимальную скорость, на основе вычисленных значений параметров, связанных с дорожными условиями [1].

Развивающиеся мобильные технологии существенно меняют окружающую среду, проникая во все отрасли, в том числе автомобильную промышленность. В автоиндустрии эта концепция называется «Connected Car».

Connected Car – это «подключенный» инновационный автомобиль с сетевыми возможностями. Они оснащены средствами навигации и ориентации, связью с Интернетом и т.д. Стандарт пятого поколения технологии 5G только усилит тенденцию внедрения Connected Car.

«Умный» автомобиль через сеть взаимодействует с окружающей средой и объектами, поэтому в нем выделяют несколько систем: автомобиль-автомобиль (vehicle-to-vehicle, V2V), автомобиль – инфраструктура (vehicle-to-infrastructure, V2X) и автомобиль-пешеход (vehicle-to-pedestrian, V2P), а также автомобиль – электросеть (vehicle-to-grid, V2G) и автомобиль – устройство (vehicle-to-device, V2D) [2].

Эти средства и технологии связи обеспечивают компонентам системы возможности взаимодействия путем обмена информацией об услугах общественного транспорта в режиме реального времени, информацией о поездках и дорожном движении в режиме реального времени, а также интеллектуальными и бесшовными решениями для продажи билетов. Как и любая подключенная система, интеллектуальные транспортные системы, особенно системы автомобильной специальной сети, подвергают транспортных операторов повышенным рискам с точки зрения кибербезопасности. Действительно, эти системы часто являются совместными и взаимодействуют друг с другом, с оборудованием или с разнородными информационными системами и обеспечивают доступ к различным сетям, таким как Интернет.

Взаимосвязь этих сетей увеличивает уязвимость к атакам и может создать возможность стать объектом вторжений и кибератак. Ущерб от этих атак может быть значительным.

Защита этих систем требует глубокого анализа рисков (качественного и количественного) и внедрения эффективных методов, адаптированных к критическим средам.

Поскольку ИТС предлагают критически важные приложения для обеспечения безопасности дорожного движения, которые могут повлиять на людей, безопасность ИТС является важной и актуальной проблемой. Эти системы основаны на автомобильной связи, которая наследует традиционные проблемы, связанные с беспроводными сетями.

Интеллектуальные транспортные системы, даже если они облегчают сбор, обработку и обмен информацией, сами по себе не являются гарантами и возникают вопросы безопасности, требующие особого внимания: каковы основные меры безопасности, которые следует принять для устранения риска кибератак в своих коммуникациях? Чтобы разработать полную архитектуру безопасности с механизмами, адаптированными к коммуникациям, авторами предлагается использовать метод анализа рисков для предотвращения различных атак и предлагать контрмеры в соответствии с выявленными уровнями угрозы.

Анализ рисков в основном используется для выявления потенциальных уязвимостей и угроз, связанных с ИТС, ее интерфейсами и окружающей средой, с целью их оценки и предложения решений безопасности для их устранения, уменьшения или контроля. В литературе существует множество методов анализа рисков, таких как оценка потребностей и определение целей безопасности, анализ уязвимостей, угроз и рисков и т.д.

В данной работе рассматривается анализ, основанный на методологии определения триады: уязвимости, угроз и рисков, чтобы принять решение о соответствующих мерах и средствах контроля для управления ими [3].

В заключение следует отметить, что качественный и эффективный анализ рисков различных угроз должны быть сосредоточены на коммуникационной архитектуре ИТС с использованием методики определения выше указанной триады [4]. При этом, в качестве будущей работы и в целях повышения безопасности ИТС авторами предлагается использовать методы машинного обучения, позволяющий проводить глубокий прогностический анализ киберрисков, а правильное применение машинного обучения может предоставить контекстуальную информацию для снижения потенциальных рисков и затрат, связанных с нарушением безопасности.

Список литературы:

1. Фахми Ш.С., Костикова Е.В. Шаталова Н.В. Спектральная обработка изображений в транспортных системах наблюдения: Монография. - СПб.: Издательско- полиграфическая ассоциация ВУЗ, 2022. С. 322.

2. Al-Qizwini, M., Barjasteh, I., Al-Qassab, H., & Radha, H. (2017). Deep learning algorithm for autonomous driving using googlenet. In 2017 IEEE intelligent vehicles symposium (IV) (pp. 89–96).

3. Ahmad, Farhan, Asma Adnane, and Virginia N. L. Franqueira. 2016. A systematic approach for cyber security in vehicular networks. Journal of Computational Chemistry 4: 38–62.

4. Иванов А.В., Фахми Ш.С. Обработка видеоинформации в транспортных видеосистемах реального времени: Монография. – СПб.: Издательско-полиграфическая ассоциация ВУЗ, 2021. С. 222.

Sh. S. Fahmi[1,2], Y. M. Sokolov[1], E. V. Kostikova[3]

Security in intelligent transport systems

[1]Saint Petersburg Electrotechnical University;

[2]Institute of transport problems N.S. Solomenko of the Russian Academy of Sciences;

[3]Admiral Makarov State University of Maritime and Inland Shipping, Russia

Abstract. *Self-driving Intelligent transport systems, even if they facilitate the collection, processing and exchange of information, are not guarantors in themselves, and security issues arise that require special attention: what are the main security measures that should be taken to eliminate the risk of cyber-attacks in their communications? In order to develop a complete security architecture with mechanisms adapted to communications, the authors propose to use the risk analysis method to prevent various attacks and propose countermeasures in accordance with the identified threat levels.*

Keywords: Intelligent transport systems; risk analysis; security objectives; communication technologies