УДК 656.025.4

ВОПРОСЫ БЕЗОПАСНОСТИ «ФИЗИЧЕСКОГО ИНТЕРНЕТА» В ТРАНСПОРТНЫХ СИСТЕМАХ

Е. И. ЕЛИНА
Санкт-Петербургский политехнический университет Петра Великого, Российская Федерация
В. А. ГЛИНСКИЙ
Санкт-Петербургский государственный университет гражданской авиации, Российская Федерация

В современном мире происходят постоянные изменения в транспортной логистике и повышаются требования потребителей к качеству, скорости и прозрачности процессов перевозки. Новые рыночные модели и современные технологии доставки позволяют сократить ряд звеньев логистической цепи и изменить характер логистических процессов.

Физический Интернет (PI) – это новая концепция обеспечения глобальной мобильности физических объектов. Традиционно логистические сети являются закрытыми и независимыми. В соответствии с концепцией PI они превращаются в открытую логистическую сеть, обеспечивающую эффективный способ перемещения физических товаров в заданное место за короткий период.

В соответствии с парадигмой Физического интернета используется множество существующих городских логистических объектов в цепочках поставок, включая распределительные центры, склады и автопарки. Кроме того, товары инкапсулированы в легко блокируемые смарт-контейнеры модульного размера, называемые PI-контейнеры. Они состоят из трехуровневой иерархии управления: транспортный контейнер (T-контейнер), обрабатываемый контейнер (H-контейнер) и упаковочный контейнер (P-контейнер). Благодаря модульным размерам PI-контейнеры легко транспортируются PI-перевозчиками (поставщиками услуг доставки, включая краудсорсинговый парк доставки и сторонних курьеров), хранятся и обрабатываются PI-операторами (погрузочно-разгрузочное оборудование, конвейерные системы, подъемники).

Однако для практической реализации поставленной задачи необходима разработка и внедрение современных решений для безопасного взаимодействия всех участников перевозочного процесса в Физическом интернете. Далее рассмотрим отдельно основные уязвимости Физического интернета.

1 Радиочастотная идентификация.

Существует несколько преимуществ RFID-меток по сравнению со штрих-кодами – это более быстрое и точное сканирование продуктов и хранение большей информации о продукте. Однако RFID метки можно прикрепить к поддельному продукту, изъяв их у подлинника, что называется «захват бирки». Далее поддельные продукты внедряются в процесс цепочки поставок с использованием идентичности подлинного продукта. Как и штрих-коды, RFID-метки можно использовать в качестве среды для распространения вирусов и отключения целых систем. Кроме того, данные метки могут быть повреждены или изменены злоумышленником с помощью вредоносного модуля, что позволит проникнуть в незащищенное место сканирования, вставив вредоносный код в память.

2 Интернет вещей.

Интернет вещей (IoT) будет играть важную роль в слежении за жизненным циклом объекта. Интернет вещей в контексте цепочки поставок представляет сеть физических объектов со способностью подключаться, контролировать и взаимодействовать с объектами. Хоть устройства IoT и обладают более высокими вычислительными возможностями, чем метки RFID, их способность подключаться и дистанционно управлять объектами становится привлекательной для различных атак. Злоумышленники, имеющие доступ к IoT-устройству, смогут изменять данные датчиков, таких как температура, уровень влажности и местонахождение. Еще одна угроза – небезопасные действия пользователей, такие как использование ненадежных паролей и использование паролей по умолчанию для устройств Интернета вещей, открытых в интернете. Это привело к тому, что многие вредоносные программы были нацелены на потребительские устройства Интернета вещей. Недостаточные меры безопасности IoT приводят к подключению к цепи поставок неисправных устройств, тем самым делая систему цепочки поставок уязвимой.

3 Недостаточная прозрачность PI-контейнеров.

В современной логистике не хватает устройств, которые могут эффективно обеспечивать видимость информации по перевозке контейнерных грузов в режиме реального времени. Необходима реализация системы прослеживаемости достоверной информацией, которая эффективно гарантиро-

вала бы безопасность за счет сбора, передачи и обмена данными о производстве, обработке, складировании и распределении.

Для реализации большего обеспечения безопасности элементов Физического интернета необходимо придерживаться следующих принципов.

1 Современные системы защиты. Необходимо внедрение организациями новейших механизмов защиты, таких как безопасность конечных точек, система обнаружения вторжений, автоматизированное и непрерывное тестирование на уязвимости и проникновения. Программное обеспечение должно регулярно обновляться для обнаружения любых потенциальных кибератак.

2 Разумное использование современных технологий. Сегодняшние компании сильно зависят от искусственного интеллекта и машинного обучения. Это необходимо для анализа большого количества данных. Однако такие технологии открывают совершенно новый вектор киберугроз, которые представляют большую опасность.

3 Управление безопасностью устройств IoT и систем CPS. Автоматизированные цепочки поставок в значительной степени зависят от устройств IoT и системы CPS, поэтому важно, чтобы организации имели эффективные стратегии по управлению и установлению политик безопасности. Поскольку традиционные инструменты безопасности могут быть реализованы не на всех устройствах, важно использовать специальные, подходящие под эти системы.

4 Защита данных. Требуется постоянная шифровка данных независимо от их состояния (покой или передача). Также рекомендуется использование безопасных многосторонних вычислений (MPC) для защиты данных между несколькими торговыми партнерами.

5 Децентрализация. Методы децентрализованного обмена данными, такие как блокчейны, обеспечивают безопасную сеть для обмена данными с дополнительной устойчивостью к криптографическим атакам. Применение таких технологий может позволить партнерам по цепочке поставок обмениваться данными с определенной прослеживаемостью.

6 Безопасное хранение данных. Хранить данные важно в безопасных местах с надлежащей защитой (аутентификацией и доступом-контролем). Также рекомендуется уничтожение любых неиспользуемых данных.

Основной целью безопасности Физического интернета является не только защита данных, грузов и предотвращение вторжений, которые сосредоточены на угрозах, но и обеспечение того, чтобы важные функции, предоставляемые системами, сохранялись в условиях сбоев (как преднамеренных, так и непреднамеренных), что требует более стратегического и системного подхода.

Список литературы

1 Traceability in supply chains: A Cyber security analysis / N. F. Syed [et al.] // Computers & Security. – 2022. – Vol. 112. – 102536.

2 **Малюченко, В. К.** Оценка рисков проекта внедрения физического Интернета в логистическую сеть России / В. К. Малюченко, В. А. Глинский // Актуальные проблемы авиации и космонавтики : сб. материалов VII Междунар. науч.-практ. конф., посвящ. Дню космонавтики. В 3 т., Красноярск, 12–16 апреля 2021 года. – Красноярск : СибГУ им. М. Ф. Решетнева, 2021. – С. 402–404.

3 Логистика : учеб. пособие / В. И. Маргунова [и др.] ; под общ. ред. В. И. Маргуновой. – 2-е изд., испр. – Минск : Выш. шк., 2013 – 508 с.

4 **Puskas, E.** Physical Internet – a Novel Application Area for Industry 4.0 / E. Puskas, G. Bohacs // International Journal of Engineering and Management Scieces (IJEMS). – 2019. – Vol. 4, no. 1.

5 **Montreuil, B.** Toward a Physical Internet: meeting the global logistics sustainability grand challenge / B. Montreuil // Logistics Research. – 2011. – Vol. 3. – P. 71–87.

УДК 656.222/3

ОЦЕНКА ВЛИЯНИЯ ВНЕДРЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ НА НАДЕЖНОСТЬ СИСТЕМЫ УПРАВЛЕНИЯ ПЕРЕВОЗОЧНЫМ ПРОЦЕССОМ

А. А. ЕРОФЕЕВ

Белорусский государственный университет транспорта, г. Гомель

Использование информационных и интеллектуальных технологий в системе управления перевозочным процессом (СУПП), с одной стороны, позволяет снизить затраты на организацию и реа-