УДК 625.8

ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «INNOTECH NETWORK MONITOR» НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ТРАНСПОРТНЫХ СИСТЕМ

Е. Н. КИЛЬЧЕНКО
ООО «ИнноТех Солюшнс», г. Минск, Республика Беларусь

Ф. Е. САТЫРЕВ, А. А. ПОДДУБНЫЙ, П. А. ПОДДУБНЫЙ
Белорусский государственный университет транспорта, г. Гомель

В современном мире для удобства, экономии времени и финансовых средств в транспортные системы внедряются цифровые системы автоматики, телемеханики и связи. А что делать, если цифровое оборудование подвергнется взлому?

Массированные кибератаки становятся настоящим бичом XXI века, глобальным вызовом цивилизации, несущим отнюдь не виртуальные – вполне реальные риски. Вредоносные вмешательства в транспортные информационные системы замедляют транспортные потоки и останавливают работу электронных сервисов и услуг.

В связи с этим, 14 февраля 2023 года Президентом подписан Указ № 40 «О кибербезопасности», направленный на защиту информационных технологий и обеспечение защиты интересов государства [1].

Современные объекты транспортной информационной инфраструктуры состоят из различных информационно-коммуникационных технологий: это и платежные системы, и приложения, ответственные за автоматический сбор средств и управление финансовыми потоками, и централизованные системы контроля дорожного трафика, и системы связи и коммуникации, включающие системы передачи данных между транспортными средствами, между транспортными средствами и информационной инфраструктурой, между элементами инфраструктуры, а также сайтов, приложений и социальных сетей для размещения важной информации и объявлений.

Сетевые атаки представляют собой наибольшую угрозу для информационной инфраструктуры транспортных систем. Эти атаки направлены на дестабилизацию работы устройств и оборудования, утечку данных и кражу ценной информации. Киберпреступники часто используют вредоносное программное обеспечение, которое может полностью парализовать функционирование целых секторов инфраструктуры или предоставить им доступ к незащищенным элементам сети. Такие атаки могут привести к значительным потерям ресурсов, доходов и даже собственности. Вредоносное программное обеспечение (ПО), проникшее в систему, может нарушить работу критически важных компонентов, что приведет к серьезным последствиям, которые могут повлечь за собой причинение ущерба здоровью человека.

Беспроводные системы взаимодействия между транспортными средствами, между транспортными средствами и информационной инфраструктурой, между элементами инфраструктуры становятся ключевыми компонентами, обеспечивая обмен данными между элементами инфраструктуры в реальном времени. Однако их взлом вполне возможен, как неоднократно подтверждалось на практике.

Уязвимости в прошивках транспортных средств и их системах, а также использование сетей с открытым трафиком могут позволить злоумышленникам перехватывать управление. Слабые пароли, незащищенные сайты и уязвимости в приложениях предоставляют хакерам возможность получить доступ к учетным данным пользователей и, например, зашифровать сервера, базы данных и рабочие станции с целью замедлить и нарушить работу предприятия.

Для решения задач по выявлению действий нарушителей в сетевой инфраструктуре, сетевом и серверном оборудовании в основном используются средства защиты иностранной разработки. При всей их эффективности они не исключают ситуации, когда программные средства защиты могут содержать программные закладки. Анализ вероятных последствий применения программных закладок показывает, что в случае систем управления речь может идти о блокировании возможности применения системы защиты. В других случаях – о блокировании передачи, утечке или модифика-

ции (вплоть до уничтожения) информации в информационно-телекоммуникационных системах, утечке или модификации (уничтожении) информации. Фактически это означает, что транспортная отрасль может оказаться беззащитной к кибератакам и будет поставлена на грань катастрофы.

Учитывая тенденцию постоянного роста количества киберугроз, способных нарушить работу IT инфраструктуры и информационных систем предприятий, и дефицит высококвалифицированных специалистов, ООО «ИнноТех Солюшнс» разработан многофункциональный Программно-аппаратный комплекс «Innotech Network Monitor» (далее – ПАК).

В настоящее время ПАК «Innotech Network Monitor» сертифицирован Оперативно-аналитическим центром при Президенте Республики Беларусь на соответствие требованиям технического регламента ТР 2013/027/BY (регистрационный номер сертификата соответствия BY/112 02.02. ТР027 036.01 01834 от 12.02.2025) и может быть применим на различных объектах (предприятиях и организациях) как устройство для защиты информации [2].

ПАК включает в свой состав следующие модули:

1 Модуль «Сетевая активность» анализирует копию сетевого трафика (зеркалирование), что позволяет осуществлять сбор и анализ состояния информационного взаимодействия хостов (узлов) контролируемой сетевой инфраструктуры на предмет выявления аномалий и индикаторов компрометации (IoC).

2 Модуль «Монитор сети» обеспечивает функцию по периодическому сканированию контролируемой сетевой инфраструктуры с целью обнаружения новых устройств, открытых портов, используемых сетевых сервисов и их версий.

3 Модуль «Сканер уязвимостей» выполняет функции сканирования назначенных узлов контролируемой сетевой инфраструктуры с целью обнаружения потенциальных уязвимостей и мисконфигураций в установленных на узлах ОС, базах данных и других программных компонентах.

4 Модуль «Безопасность Wi-Fi» осуществляет функции мониторинга беспроводной сети Wi-Fi на предмет наличия аномалий, индикаторов компрометации, выявление атак на Wi-Fi.

5 Модуль «Целостность инфраструктуры» выполняет функции контроля целостности назначенных файловых ресурсов выбранных узлов контролируемой сетевой инфраструктуры.

6 Модуль «Эмулятор уязвимости» реализует функции преднамеренно сконфигурированного уязвимого сетевого узла (honeypot) для привлечения потенциальных нарушителей с высоким потенциалом атаки с целью затруднения продвижения нарушителя в контролируемой сетевой инфраструктуре и сбора информации об используемых инструментах и тактиках нарушителей.

ПАК поставляется с преднастроенным системным и прикладным программным обеспечением, что позволяет максимально сократить период внедрения ПАК в информационную инфраструктуру предприятия, обеспечить своевременное выявление и классификацию аномалий в контролируемых системах и сократить время реагирования на них со стороны профильных специалистов (рисунок 1).

Рисунок 1 – Общий вид ПАК

В настоящее время, несмотря на все страхи и недоверие, отечественные ИБ-решения получают хорошую репутацию среди потребителя и экспертов. Это связано с высоким уровнем технической экспертизы и контроля качества продукции, а также с усилиями регулятора по ужесточению процедур сертификации и вводу ограничений на использование зарубежных средств защиты.

Конечно, нельзя не сказать и о факторе санкционных ограничений извне, без которого мы могли бы и не увидеть столь стремительного развития. Разумеется, еще остается много векторов для развития и адаптации, ведь киберугрозы также не стоят на месте. Однако в целом отечественные ИБ-решения уже сегодня являются надежным и качественным выбором для киберзащиты любой современной организации.

Список литературы

1 О кибербезопасности : Указ Президента Респ. Беларусь, 14 февр. 2023 г., № 40 // Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2 Сертификат соответствия Комплекс программно-аппаратный «Innotech Network Monitor». Зарегистрирован в реестре № BY/112 02.02. ТР027 036.01 01834. – Дата регистрации 12.02.2025 г.