Точка, представленная на графике (см. рисунок 1), описывает киберугрозу, при которой нарушается как информационная, так и функциональная безопасность.

Исходя из этой двухмерной модели обеспечение кибербезопасности заключается в соотношении угроз в сферах информационной и функциональной безопасности. При этом, для систем обеспечения безопасности движения поездов, к которым относятся современные микроэлектронные СЖАТ на основе аппаратно-программных комплексов (АПК), преобладающим является обеспечение функциональной безопасности. Кроме того, необходимо учитывать целостность и подлинность технологической информации, циркулирующей в АПК СЖАТ, которая может быть недопустимо искажена при электромагнитных атаках или других видах кибератак.

Выполненные в НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта исследования позволяют минимизировать последствия воздействия кибератак за счет дополнения микропроцессорной централизации системой поддержки принятия решений (СППР) дежурным по станции в нештатных ситуациях. Разработаны методы анализа и прогнозирования устойчивости микроэлектронных СЖАТ от воздействия сверхширокополосных импульсов помех (преднамеренных электромагнитных атак). Это позволяет на стадии разработки определять зоны концентрации недопустимых уровней помех вблизи неоднородностей корпусов (экранов) устройств СЖАТ, где не рекомендуется размещать критичные к безопасности элементы систем.

Список литературы

1 О Концепции информационной безопасности Республики Беларусь: постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. [Электронный ресурс]. – Минск, 2019.

2 **Безродный, Б. Ф.** Отличительные особенности кибербезопасности АСУТП / Б. Ф. Безродный // Железнодорожный транспорт. – 2018. – № 5. – С. 52–54.

УДК 656.2.08

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

П. М. БУЙ

Белорусский государственный университет транспорта, г. Гомель

Отрасль железнодорожного транспорта в настоящее время находится на стадии активного внедрения инфокоммуникационных систем. Компьютерные сети, цифровые каналы связи, облачные технологии и сервисы, программное обеспечение осваиваются отраслью для оказания услуг пассажирам и выполнения технологических процессов. Все эти современные средства и технологии позволяют Белорусской железной дороге идти в ногу со временем и поступательно участвовать в информатизации отрасли, что дает возможность достигнуть ожидаемого синергетического эффекта от синхронной информатизации всех отраслей народного хозяйства Республики Беларусь.

Кибербезопасность – состояние защищенности инфокоммуникационной системы и содержащейся в ней информации от внешних и внутренних угроз. Состояние защищенности нарушается посредством кибератак. Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на инфокоммуникационную систему в целях нарушения и (или) прекращения ее функционирования и (или) создания угрозы безопасности обрабатываемой такой системой информации [1].

Таким образом, понятие кибербезопасности включает в себя защищенность информации, которая обрабатывается инфокоммуникационной системой (информационная безопасность), так и защищенность процесса функционирования самой инфокоммуникационной системы (функциональная безопасность). Причем для железнодорожного транспорта вторая составляющая кибербезопасности является более актуальной. Это связано с тем, что часть автоматизированных систем управления технологическими процессами (АСУ ТП) железнодорожного транспорта вообще могут не использовать информацию предоставление и (или) распространение которой ограничено, и при этом выполнять задачи, связанные с безопасностью грузо- и пассажироперевозок. Для таких систем мероприятия по обеспечению информационной безопасности фактически сводятся к функциям разграничения доступа и аудита выполняемых пользователем АСУ ТП операций.

В настоящее время неуклонно растет количество киберпреступлений, инфокоммуникационные системы становятся как предметом таких преступлений, так и средством их совершения. В даль-

нейшей перспективе намечается формирование тотальной зависимости отрасли железнодорожного транспорта от защищенности инфокоммуникационных систем.

В пункте 60 Концепции информационной безопасности Республики Беларусь сказано, что ни в глобальном, ни в региональном масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Вместе с тем, к сожалению, построить абсолютно адекватную систему защиты не представляется возможным. Особенно, если затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз.

Вместе с тем в Концепции информационной безопасности указано, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности [1].

К сожалению проанализировать статистику инцидентов в сфере кибербезопасности отрасли железнодорожного транспорта Республики Беларусь не представляется возможным в силу крайней редкости появления таких инцидентов (хочется верить) и ограниченности информации о таких событиях в открытых источниках из-за специфики отрасли. Однако есть объективная статистика таких инцидентов, которая предоставляется компаниями, занимающимися вопросами кибербезопасности. Одна из таких компаний – это АО «Лаборатория Касперского», программный продукт которой сертифицирован в Республике Беларусь и применяется в подразделениях Белорусской железной дороги для защиты инфокоммуникационных систем. За последние несколько лет Республика Беларусь достаточно часто была замечена в бюллетенях, которые эта компания ежегодно выпускает с анализом статистики инцидентов кибербезопасности [2–4].

Так, в 2017 и 2018 годах наша страна была на втором месте среди стран, в которых пользователи подвергались наибольшему риску заражения через сеть Интернет. В 2019 году по данному показателю она переместилась на 9-е место в мире. Среди стран, в которых компьютеры пользователей подвергались наибольшему риску локального заражения, Республика Беларусь в 2018 году занимала 17-е место. По сравнению с соседними странами пользователи электронных банковских систем Республики Беларусь чаще подвергались атакам в 2017 и 2019 году. В 2018 и 2019 годах компьютеры белорусских пользователей также чаще атаковались программами-майнерами.

Таким образом, в рамках информатизации, отрасль железнодорожного транспорта находится в серьезной опасности с точки зрения кибербезопасности. Для повышения уровня кибербезопасности отрасли необходимо решить следующие задачи:

1 Сформулировать цели и задачи в сфере кибербезопасности железнодорожного транспорта.

2 Проводить мониторинг инцидентов кибербезопасности отрасли. Оценивать уровень кибербезопасности Белорусской железной дороги. Обмениваться опытом обеспечения кибербезопасности с другими организациями Республики Беларусь.

3 Снизить зависимость Белорусской железной дороги от импортных инфокоммуникационных технологий и систем защиты информации. Устранить неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб кибербезопасности.

4 Готовить кадры для Белорусской железной дороги, которые будут знакомы с принципами обеспечения кибербезопасности и понимающими необходимость и значимость данных мероприятий, а также повышать квалификацию сотрудников Белорусской железной дороги в данной сфере.

Список литературы

1 О Концепции информационной безопасности Республики Беларусь : постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь: [Электронный ресурс]. – Минск, 2019.

2 Kaspersky Security Bulletin: Статистика 2017 [Электронный ресурс]. – Режим доступа: https://securelist.ru/ksb-overall-statistics-2017/88203/. – Дата доступа: 11.09.2020.

3 Kaspersky Security Bulletin 2018. Статистика [Электронный ресурс]. – Режим доступа: https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/. – Дата доступа: 11.09.2020.

4 Kaspersky Security Bulletin 2019. Статистика [Электронный ресурс]. – Режим доступа: https://securelist.ru/kaspersky-security-bulletin-2019-statistics/95264/?utm_source=securelist&utm_medium=blog&utm_campaign=ru_ksb-stats_ay0073&utm_content=banner&utm_term=ru_securelist__ay0073_banner_blog_ksb-stats. – Дата доступа: 11.09.2020.

5 **Курило, А.** Как нам реорганизовать ИБ / А. Курило // BIS Journal – Информационная безопасность банков. – 2020. – № 3 (38). – С. 14–21.