ям визуальной картины изображения. В коды таких пикселей можно внедрить большое количество битов секретного сообщения. Были использованы исследования, которые описаны в работах [5–7]. В этих работах на основе конструирующей стеганографии биты секретного сообщения внедряются в младшие разряды кодов специально выделенных пикселей (шумовые пиксели, краевые пиксели, пиксели, определенные с помощью пороговой обработки).

В данной работе используется оператор Собеля для выделения краевых пикселей, в двоичные коды которых внедряются биты секретного сообщения [8]. Оператор Собеля использует фрагмент изображения в виде матрицы 3×3 и организует свертку по формулам:

$$G_x = (z_7 + 2z_8 + z_9) - (z_1 + 2z_2 + z_3),$$
$$G_y = (z_3 + 2z_6 + z_9) - (z_1 + 2z_4 + z_6).$$

Формулы описаны согласно кодировки, представленной на рисунке 1.

В коды выделенных пикселей внедряются биты зашифрованного изображения с помощью ГПСЧ. Используется ГПСЧ, построенный на клеточных автоматах с активными и неоднородными клетками [4]. Эти ГПСЧ показали высокое качество сформированных псевдослучайных битовых последовательностей. Также были исследованы различные типы окрестностей, которые были реализованы в клеточных автоматах. Анализировались локальные функции переходов и влияние дополнительных бит.

| | | |
|---|---|---|
| $z_1$ | $z_2$ | $z_3$ |
| $z_4$ | $z_5$ | $z_6$ |
| $z_7$ | $z_8$ | $z_9$ |

Рисунок 1 – Область матрицы изображения для реализации оператора Собеля

**Заключение.** В данной работе проведены исследования современных методов и средств стеганографического сокрытия информации. Разработана система стеганографической защиты информации с применением контейнеров, представленные файлами графического формата. Увеличен объем внедряемой информации за счет использования пикселей, выделенных как краевые пиксели с помощью оператора Собеля. Внедрены дополнительные меры защиты внедряемого сообщения за счет шифрования секретного сообщения с помощью ГПСЧ, реализованных на клеточных автоматах. Показано, что использование дополнительного бита, формирующего самим клеточным автоматом, дает возможность получить битовые последовательности большой длины.

**Список литературы**


1 **Грибунин, В. Г.** Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

2 **Рябко, Б. Я.** Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. – 2-е изд. – М. : Горячая линия – Телеком, 2013. – 232 с.

3 **Конахович, Г. Ф.** Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

4 **Bilan, S.** Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities / S. Bilan // IGI Global. – USA. – 2017. — P. 301.

5 **Albdour, N.** Selection Image Points Method for Steganography Protection of Information / N. Albdour // WSEAS transactions on signal processing. – 2008. – Vol. 14. – P. 151–159.

6 **Bilan, M.** Research of Methods of Steganographic Protection of Audio Information Based on Video Containers. Handbook of Research on Intelligent Data Processing and Information Security Systems / M. Bilan, A. Bilan ; ed. by S. M. Bilan & Al-Zoubi, S. I. Hershey. – USA : IGI Global. – 2019. – P. 79–94.

7 **Albdour, N.** A Novel Methods for Image Steganography by Effective Image Points Selection / N. Albdour // Journal of Electrical and Electronics Engineering. – 2019. – Vol. 14, is. 5. Ser. II. – P. 06–11.

8 Real-time volume graphics / K. Engel [et al]. – Wellesley. Massachusetts: A K Peters, Ltd., 2006. – P. 112–114.



УДК 656.2.08


## КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА


*К. А. БОЧКОВ, П. М. БУЙ*

*Белорусский государственный университет транспорта, г. Гомель*


В соответствии с Концепцией информационной безопасности Республики Беларусь, которая была утверждена Президентом Республики Беларусь 18 марта 2019 года, кибербезопасность – это

состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [1]. Информационная инфраструктура, согласно Концепции, – это совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации. При таком подходе понятие кибербезопасности включает в себя исключительно информационную безопасность, ограничивая рамки объекта защиты на информации и средствах, связанных с ней непосредственно.

Вместе с тем эта же Концепция указывает на то, 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]. Но безопасность людей, социальной и экологической сферы не является объектом информационной защиты. Очевидно, что методы и средства, обеспечивающие информационную безопасность, не в силах решить эти задачи. Особенно это актуально для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), которые широко применяются на железнодорожном транспорте. Основную роль в обеспечении безопасности движения поездов выполняют системы железнодорожной автоматики и телемеханики (СЖАТ). Такие системы в своем составе используют информационную инфраструктуру и на них должны выполняться мероприятия по обеспечению информационной безопасности. Но в таких системах не информация должна являться главным объектом защиты, а, в случае железнодорожного транспорта, безопасность движения поездов. Атака на информационную инфраструктуру и/или на информацию при обнаружении будет заблокирована, но если она не будет обнаружена (например, действия нарушителя будут признаны законными) или будет направлена исключительно на технологический процесс в обход информационной инфраструктуры (например, электромагнитный терроризм), то могут пострадать люди или может быть нанесен вред окружающей среде. В таком случае актуальными становятся вопросы функциональной безопасности. Здесь под функциональной безопасностью следует понимать совокупность таких условий функционирования АСУ ОТП, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных информационных воздействий, приводящих к появлению опасных отказов.

Концепция информационной безопасности Республики Беларусь делает шаг в сторону функциональной безопасности в понятии кибератаки. Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [1].

Однако для АСУ ОТП остается открытым вопрос о взаимодействии информационной и функциональной безопасности. Исследования, представленные в источнике [2], предлагают трехмерную модель, которая помимо информационной и функциональной безопасности в качестве третьей составляющей кибербезопасности учитывает физическую безопасность (системы разграничения доступа). Такой подход характерен для классического понимания информационной безопасности, предложенного Джерри Зальцером и Майклом Шредером в 1975 году и включающего только конфиденциальность, доступность и целостность информации (триада CIA или КДЦ). Однако использование других моделей информационной безопасности (например, гексады Паркера, в которой дополнительно вводятся понятия владения, аутентичности и полезности информации) позволяет включить системы разграничения доступа в область ответственности информационной безопасности. Для Республики Беларусь можно считать, что с 2019 года Концепцией информационной безопасности к понятиям конфиденциальности, доступности и целостности дополнительно вводятся подлинность и сохранность информации.

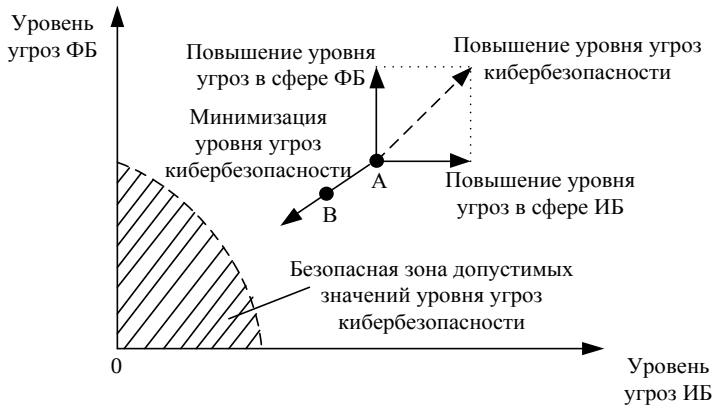


Рисунок 1 – Двухмерная модель кибербезопасности АСУ ОТП железнодорожного транспорта

При таком подходе можно говорить о двухмерной модели кибербезопасности (рисунок 1).

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-