ЗАСЕДАНИЕ № 6
ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 621.38

ГАРМОНИЗАЦИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РАЗЛИЧНЫХ ОБЪЕКТОВ ЗАЩИТЫ

К.А. БОЧКОВ, П.М. БУЙ, Д.В. КОМНАТНЫЙ
Учреждение образования «Белорусский государственный университет транспорта», г. Гомель, Республика Беларусь

Введение. В последнее время наблюдается активное внедрение информационных технологий во все отрасли народного хозяйства. Практически любая сфера жизнедеятельности человека связана с использованием современных инфокоммуникационных систем. Этот процесс как никогда актуализировал вопросы обеспечения информационной безопасности. В соответствии с Концепцией информационной безопасности Республики Беларусь информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. Чаще всего интересами отдельных граждан Республики Беларусь, организаций, общества в целом и, конечно же, государства в информационной сфере является защита информации. Но методы, обеспечивающие информационную безопасность, не в состоянии охватить весь спектр угроз, которые могут быть реализованы против инфокоммуникационных систем в современном мире с его уровнем технологического прогресса. До появления информационных технологий вопросы обеспечения безопасности систем управления стоял не менее остро, но, актуальные для того времени угрозы, смещали вопросы обеспечения их безопасности с информационной в функциональную сферу, которая и стала в последствии источником некоторых методов и подходов, используемых в настоящее время для обеспечения информационной безопасности. Однако все еще открытым остается вопрос о том, насколько в современном мире остаются актуальными вопросы функциональной безопасности и какова их роль в процессе обеспечения безопасности современных инфокоммуникационных систем.

1. Особенности обеспечения информационной и функциональной безопасности. Общие вопросы требований по информационной безопасности сформулированы в СТБ 34.101.1-2014 (IEC 15408-1:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» [2]. Предметом защиты в этом направлении является сама информаций, а точнее такие ее основные свойства, как конфиденциальность, целостность и доступность. В соответствии с [3], безопасность информации – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Функциональная безопасность – это совокупность таких условий функционирования инфокоммуникационной системы, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного ее функционирования. Принципы и методы обеспечения функциональной безопасности описаны в базовом ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» [4].

Для подавляющего большинства современных объектов информационных технологий актуальными являются исключительно вопросы информационной безопасности, т. к. задачами этих объектов является хранение, обработка и/или предоставление информации. К таким

объектам можно отнести персональные компьютеры, мобильные устройства пользователей, Internet of Things (IoT) и т. п.

Концепция информационной безопасности Республики Беларусь 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 предметом информационной защиты. Методы и средства обеспечивающие исключительно 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 выполнятся мероприятия по обеспечению информационной безопасности. Но в таких системах не информация должна являться главным объектом защиты, а в случае железнодорожного транспорта это в первую очередь обеспечение безопасности движения поездов. Атака на инфокоммуникационные системы 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. Это будет нарушением критериев опасного отказа. В таком случае преобладающими становятся вопросы функциональной безопасности.

Функциональная безопасность – свойство объекта железнодорожного транспорта, связанного с безопасностью, выполнять требуемые функции безопасности при всех предусмотренных условиях в течение заданного периода времени [5].

Для инфокоммуникационных систем железнодорожного транспорта, как, впрочем, и для многих подобных систем других отраслей необходимо обеспечивать как информационную, так и функциональную безопасность. Зачастую, классические методы, обеспечивающие функциональную безопасность и современные методы, обеспечивающие информационную безопасность, частично перекрывают зоны своей ответственности, которая, касается, например, обеспечения доступности и целостности информации и реализуется организационными мероприятиями.

Известный специалист в области функциональной безопасности профессор Скляр В.В. для того, чтобы избежать дублирования требований для таких инфокоммуникационных систем, рекомендует гармонизировать требования по информационной и функциональной безопасности, сформировать общий жизненный цикл, а также увязать процессы управления безопасностью и условия безопасности объекта защиты. Также, по аналогии с функциональной безопасностью, для которой определены уровни полноты безопасности (SIL), определяются пять (от 0 до 4) уровней информационной безопасности (SL) [6]. На рисунке 1 представлена гармонизированная структура требований к информационной и функциональной безопасности объекта защиты [6]. При такой гармонизации требований процессы обеспечения информационной и функциональной безопасности будут происходить параллельно. Причем, исходя из назначения и характеристик объекта защиты в общем жизненном цикле обеспечения информационной и функциональной безопасности определяется приоритет.

Примером подхода, учитывающего вопросы обеспечения как информационной, так и функциональной безопасности, является СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия» [7]. Опыт использования такого совместного подхода описан в статье [8].

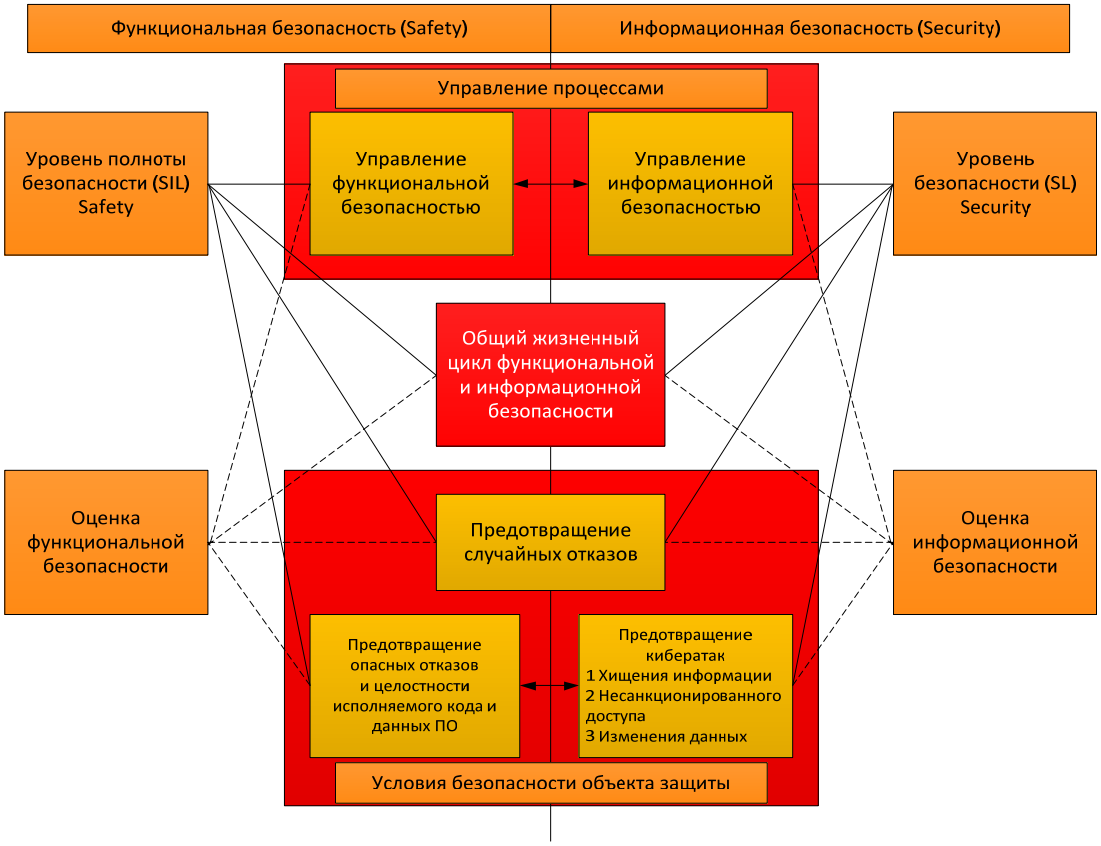

Рис. 1. Гармонизированная структура требований к информационной и функциональной безопасности объекта защиты

2. Безопасность АСУ ОТП железнодорожного транспорта. Уже около десяти лет в Республике Беларусь была выделена особая категория объектов информатизации – критически важные объекты информатизации (КВОИ). Впервые КВОИ упоминается в Указе Президента Республики Беларусь от 9 ноября 2010 г., № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [9], а в Указе Президента Республики Беларусь от 25.10.2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», было определено, какие объекты информатизации являются критически важными.

В соответствии с Указом Президента Республики от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации» КВОИ – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации [10]. В этом же указе утверждено положение о порядке отнесения объектов информатизации к КВОИ и представлен перечень соответствующих критериев.

Среди критериев отнесения объектов информатизации к КВОИ, указанных в [10], АСУ ОТП железнодорожного транспорта напрямую соответствуют критерию экономической значимости и косвенно могут соответствовать критериям социальной (железнодорожный транспорт является самым дешевым в Республике Беларусь) и экологической (железнодорожный транспорт осуществляет транспортировку опасных грузов, которые могут нанести вред окружающей среде при нарушении безопасности движения поездов) значимости. Однако, насколько известно авторам, ни одна АСУ ОТП железнодорожного транспорта в настоящее время не включена в Государственный реестр КВОИ. В Российской Федерации аналогом КВОИ являются критические системы информационной инфраструктуры (КСИИ) и все СЖАТ, входящие в состав АСУ ОТП, к ним отнесены.

Совокупность угроз информационной и функциональной безопасности потенциально реализуются через кибератаки. Кибератака, в соответствии с [1], – 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. В контексте термина «кибератака» обеспечение информационной и функциональной безопасности можно обозначить термином «кибербезопасность». При таком подходе можно говорить о двухмерной модели кибербезопасности, включающей как информационную, так и функциональную составляющую (рис. 2) [11].

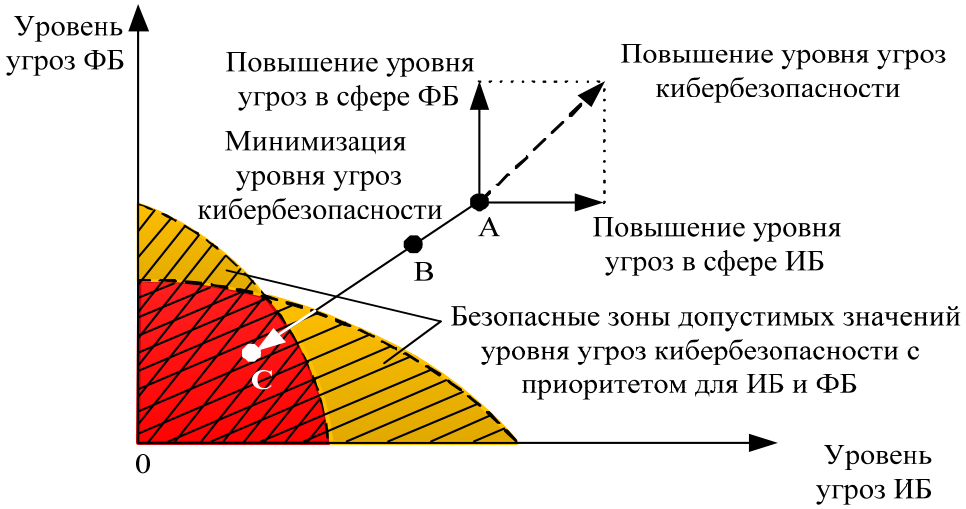

Рис. 2. Двухмерная модель кибербезопасности АСУ ОТП железнодорожного транспорта

Безопасная зона допустимых значений уровня угроз функциональной безопасности дискретно характеризуется уровнем полноты безопасности. Чем выше уровень SIL, тем меньше допускается угроз функциональной безопасности. Аналогичным образом необходимо привязать уровни информационной безопасности к допустимому уровню соответствующих угроз. Точка А, представленная на графике (рис. 2), описывает киберугрозу, при которой нарушается как информационная, так и функциональная безопасность. При необходимости обеспечить требуемые уровни SIL и SL необходимо реализовать такие условия функционирования и использовать средства защиты информации, при которых уровень угроз кибербехопасности будет находится в безопасной зане как по информационно, так и по функциональной безопасности учитывая приоритеты их обеспечения для конкретного объекта защиты (точка С).

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.

3. Опасность электромагнитных влияний и терроризма. Одним из новых видов киберугроз АСУ ОТП является «электромагнитный терроризм», суть которого заключается в преднамеренном воздействии на такие системы сверхширокополосными импульсами высокой энергии – электромагнитными импульсами преднамеренного воздействия (ЭИПВ). В связи с этим для обеспечения кибербезопасности АСУ ОТП и, в частности, СЖАТ в современных условиях особое значение приобретает помехоустойчивость. Элементная база таких систем в значительной степени подвержена влиянию электромагнитных помех, а сами СЖАТ работают в сложной электромагнитной обстановке. Не менее актуальной является проблема помехоустойчивости аппаратуры СЖАТ к электростатическому разряду (ЭСР), так как ЭСР обладают сравнимой с ЭИПВ шириной спектра, совпадающего по диапазону с тактовыми частотами ап-

паратуры современных АСУ ОТП. При этом ЭПИВ обладают большей энергией и достаточно трудно локализуемы. Воздействие ЭИПВ или ЭСР может одновременно привести к нарушению как информационной, так и функциональной безопасности.

Анализ последствий такого вида воздействия на АПК СЖАТ осуществляется как для устройств, реализующих алгоритмы безопасности, так и для устройств хранения и передачи информации. Приоритет анализа устанавливается соотношением угроз для информационной и функциональной безопасности АСУ ОТП.

Уровень устойчивости СЖАТ к ЭПИВ и ЭСР, а также их уровень защищенности оцениваются путем расчета и анализа помеховых электромагнитных полей. При этом отличие задачи оценки защищенности СЖАТ от задач электромагнитной совместимости радиоэлектронных средств состоит в том, что ЭПИВ проникают внутрь корпуса-экрана через паразитные (неоднородности корпуса), а не через штатные антенны, как это происходит с узлами радиоэлектронного оборудования. В связи с этим необходимо рассматривать распространение помех внутри корпуса аппаратуры, а не только их прохождение через экран.

Для расчетов электромагнитного поля ЭПИВ могут использоваться численные и аналитические методы. Численные методы основаны на решении интегрального уравнения в частотной области для распределения токов в структуре рецептора [12, 13]:

$$j\omega\frac{\mu}{4\pi}\int\limits_S \vec{J}(r)\frac{\exp(-jkR)}{R}dS - \frac{1}{j4\pi\omega\varepsilon}\int\limits_S \vec{J}(r)\frac{\exp(-jkR)}{R}dS = \vec{E}_t - Z_S\vec{J}(r), \qquad (1)$$

где ω – круговая частота, рад/с;

μ – магнитная проницаемость, Гн/м;

J – плотность тока, А/м^2;

r – радиус-вектор элементарной площадки, м;

k – волновой вектор, рад/м;

R – расстояние между элементарными площадками, м;

S – площадь элементарной площадки, м^2;

ε – диэлектрическая проницаемость среды, Ф/м;

E_t – тангенциальная составляющая помехового электрического поля в пределах элементарной площадки, В/м;

Z_s – полное сопротивление элементарной площадки, Ом.

Аналитические методы позволяют получить пессимистическую, то есть перекрывающую все резонансы в корпусе, оценку помехового поля внутри корпуса рецептора. Они основаны на замкнутых выражениях для электрической составляющей электромагнитного излучения простых излучателей [14–16]. Такая оценка зачастую достаточна для решения задачи оценки уровня защищенности.

Для прямоугольного отверстия в неоднородности корпуса оборудования электрические составляющие поля в сферической системе координат имеют следующий вид:

$$\begin{aligned} E_\Theta &= \frac{jabE(j\omega)}{2\lambda}\frac{e^{-\lambda kR}}{R}(1+\cos\phi)\cos\phi\frac{\sin(0.5ka\sin\Theta\sin\phi)}{0.5ka\sin\Theta\sin\phi}\frac{\sin(0.5kb\sin\Theta\cos\phi)}{0.5kb\sin\Theta\cos\phi}, \\ E_\phi &= \frac{-jabE(j\omega)}{2\lambda}\frac{e^{-\lambda kR}}{R}(1+\cos\phi)\sin\phi\frac{\sin(0.5ka\sin\Theta\sin\phi)}{0.5ka\sin\Theta\sin\phi}\frac{\sin(0.5kb\sin\Theta\cos\phi)}{0.5kb\sin\Theta\cos\phi}, \end{aligned} \qquad (2)$$

где $E(j\omega)$ – напряженность электрической составляющей поля в раскрыве отверстия, В/м;

a, b – стороны отверстия, м;

λ – длина волны, м;

θ, φ – сферические координаты, рад.

Электрические составляющие излучения круглого отверстия в неоднородности корпуса оборудования в сферической системе координат описывается выражениями:

$$E_{\Theta} = \pi r_0^2 \frac{E(j\omega)}{2\lambda R} e^{-jkR}(1+\cos\Theta)\cos\phi,$$
$$E_{\phi} = \pi r_0^2 \frac{-jE(j\omega)}{2\lambda R} e^{-jkR}(1+\cos\Theta)\sin\phi, \quad (3)$$

где r_0 – радиус отверстия, м.

При воздействии как ЭПИВ, так и ЭСР, в раскрыве паразитной антенны создается напряженность поля. В первом случае источником является аппаратура террориста, во втором, – генератор ЭСР, подключенный к паразитной антенне. Сходство каналов проникновения и методов расчета позволяет разработать методику комплексной оценки защищенности СЖАТ от ЭИПВ. Такая методика основывается на сопоставлении воздействия от ЭИПВ и ЭСР на паразитные антенны, а также влияния этого воздействия на кибербезопасность СЖАТ. Методика позволяет косвенно судить о защищенности СЖАТ от ЭИПВ по результатам анализа и испытания защищенности СЖАТ от ЭСР. Такая оценка целесообразна, так как испытания на ЭСР являются обязательными, а оборудование для испытаний доступно и безопасно.

Заключение

1. В НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта отработаны технологии, позволяющие прогнозировать поведение АСУ ОТП и, в частности, СЖАТ при воздействии на них ЭПИВ. Испытания проводятся путем принципа эквивалентности с применением стандартных программ тестирования на устойчивость к электростатическим разрядам.

2. Разработана методика оценки соответствия объекта защиты требованиям функциональной и информационной безопасности в соответствии с требованиями с СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия».

3. Проведенные исследования позволяют минимизировать последствия воздействия кибератак за счет дополнения СЖАТ системой поддержки принятия решений (СППР) в нештатных ситуациях.

Список литературы

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

2. СТБ 34.101.1-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. – Взамен СТБ 34.101.1-2004 ; введ. 2014–09–01. – Мн. : БелГИСС, 2014. – 60 с.

3. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

4. ГОСТ Р МЭК 61508-3-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению.

5. ГОСТ 33432-2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта.

6. Скляр, В. В. Обеспечение безопасности АСУТП в соответствии с современными стандартами : метод. пособие / В. В. Скляр. – М. : Инфра-Инженерия, 2018. – 384 с.

7. СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия» от 30.12.2014.

8. Бочков, К. А. Особенности обеспечения функциональной и информационной безопасности микроэлектронных систем управления движением поездов на железнодорожном транспорте / К. А. Бочков, Д. В. Комнатный, С. Н. Харлап // Комплексная защита информации : мат-лы XXV Междунар. науч.-практ. конф., Москва, 15–17 сентября 2020 г. – М. : Медиа Групп «Авангард», 2020. – С. 88–95.

9. О совершенствовании государственного регулирования в области защиты информации : Указ Президента Респ. Беларусь от 09.12.2019 № 449 // Эталон Online [Электронный ресурс] / Нац. Центр правовой информации Респ. Беларусь. – Минск, 2020.

10. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 09 ноября 2010 года, № 575 с изм. и доп. от 24 января 2014 г. № 49 // Эталон Online [Электронный ресурс] / Национальный Центр правовой информации Республики Беларусь. – Минск, 2018.

11. Бочков, К. А. Кибербезопасность автоматизированных систем управления ответственными технологическими процессами железнодорожного транспорта / К. А. Бочков, П. М. Буй // Проблемы безопасности на транспорте : мат-лы X Междунар. науч.-практ. конф., Гомель, 26–27 ноября 2020 г. / Бел. гос. ун-т трансп.; редкол. : Ю. И. Кулаженко [и др.]. – Гомель : БелГУТ, 2020. – С. 7–9.

12. Михайлов, В. А. Разработка методов и моделей анализа и оценки устойчивости функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного воздействия сверхкоротких электромагнитных излучений : автореф. дис. … д-ра техн. наук / НИУ ВШЭ. – М., 2014. – 45 с.

13. Акбашев, Б. Б. Теоретические и экспериментальные методы оценки устойчивости терминалов к воздействию сверхширокополосных электромагнитных импульсов : дис. … канд. техн. наук: 05.12.13 / Б. Б. Акбашев. – М., 2005. – 156 с.

14. Иванов, В. А. Электромагнитная совместимость радиоэлектронных средств / В. А. Иванов, Л. Я. Ильницкий, М. И. Фузик. – Киев : Техника, 1983. – 189 с.

15. Модель дифракции высокочастотной электромагнитной волны на апертуре в проводящем экране / Д. А. Ционенко [и др.] // Доклады БГУИР. – 2015. – № 5. – С. 5–11.

16. Бочков, К. А. Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. – Гомель : БелГУТ, 2013. – 185 с.