

- 3 План реализации концепции развития аутсорсинга в холдинге «РЖД», утвержденный распоряжением ОАО «РЖД» № 1420 от 30 июня 2017 г.
- 4 Гражданский кодекс Российской Федерации (Ч. 1 от 30.11.1994 № 51-ФЗ; ред. от 03.08.2018, подгот. на осн. изм., внесенных Федеральным законом от 29.07.2017 № 217-ФЗ).
- 5 Гражданский кодекс Российской Федерации (Ч. 2 от 26.01.1996 № 14-ФЗ; ред. от 29.07.2018).
- 6 Изменения, которые вносятся в распоряжение ОАО «РЖД» от 4 сентября 2013 г. № 1899р «О принятии решения о прекращении выполнения отдельных видов работ (операций) с использованием трудовых ресурсов и средств труда ОАО «РЖД», утверждены распоряжением ОАО «РЖД» № 1486р от 26 июля 2017 г. (в ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 7 О принятии решения о прекращении выполнения отдельных видов работ с использованием трудовых ресурсов и средств труда ОАО «РЖД»: распоряжение ОАО «РЖД» № 1899р от 04.09.2013 г. (учитывать изменения, указанные в [6]).
- 8 Положение «О принятии решения о прекращении выполнения отдельных видов работ с использованием трудовых ресурсов и средств труда ОАО «РЖД», утверждены распоряжением ОАО «РЖД» № 1899р от 04 сентября 2013 г. (в ред. Распоряжений ОАО «РЖД» № 2798р от 01.12.2014, № 2995р от 18.12.2015, № 1486р от 26.07.2017, Приказа ОАО «РЖД» № 22 от 30.03.2015). (Учитывать изменения, указанные в [6]).
- 9 Приказ «О договорной и претензионной работе в ОАО «РЖД» № 15 от 30 марта 2016 г.
- 10 Распоряжение ОАО «РЖД» «Об организации работы ОАО «РЖД» в сфере аутсорсинга» № 1486р от 26 июля 2017 г. (в ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 11 Состав комиссии ОАО «РЖД» по аутсорсингу, утвержден распоряжением ОАО «РЖД» № 1486р от 26 июля 2017 г. (В ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 12 Положение о комиссии ОАО «РЖД» по аутсорсингу, утверждено распоряжением ОАО «РЖД» № 1486р от 26 июля 2017 г. (в ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 13 Положение о рабочей группе по аутсорсингу, утверждено распоряжением ОАО «РЖД» № 1486р от 26 июля 2017 г. (в ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 14 Состав рабочей группы по аутсорсингу, утвержден распоряжением ОАО «РЖД» № 1486р от 26 июля 2017 г. (В ред. Распоряжения ОАО «РЖД» № 1746р от 30.08.2017).
- 15 О принятии решения о прекращении выполнения отдельных видов работ с использованием трудовых ресурсов и средств труда ОАО «РЖД»: распоряжение ОАО «РЖД» № 1899р от 4 сентября 2013 г.
- 16 Методика экспертной оценки бизнес-процессов ОАО «РЖД» по критериям передачи на аутсорсинг, утверждена распоряжением ОАО «РЖД» № 173р от 31 января 2018 г.
- 17 Глоссарии терминов и определений в области управления процессами ОАО «РЖД», утверждены распоряжением ОАО «РЖД» № 2426р от 27.10.2017.
- 18 Методика проектирования, анализа и совершенствования процессов утверждена распоряжением ОАО «РЖД» № 2426р от 27 ноября 2017 г.
- 19 Об утверждении рекомендаций по применению проектного подхода при реализации аутсорсинг-инициатив: Распоряжение ОАО «РЖД» № 135р от 26 января 2018 г.
- 20 Положение о порядке распоряжения недвижимым имуществом ОАО «РЖД» утверждено приказом ОАО «РЖД» от 7 ноября 2008 г. № 150 (Список изменяющих документов в ред. приказов ОАО «РЖД»: № 120 от 15.06.2009, № 108 от 01.10.2012, № 17 от 08.04.2014, № 2666р от 10.11.2015, № 10 от 16.02.2017, № 119 от 11.12.2017, № 58 от 01.08.2018).

УДК 656.254

ОЦЕНКА НАРУШИТЕЛЕЙ ПО РЕАЛИЗАЦИИ УГРОЗ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

А. С. КАЗАКОВ

Белорусский государственный университет транспорта, г. Гомель

Безопасность движения поездов – один из основных критериев качества работы железной дороги. Постоянно совершенствуются системы железнодорожной автоматики и телемеханики (СЖАТ). В современных условиях это становится возможным за счет увеличения степени автоматизации, миниатюризации устройств, использования микропроцессорной элементной базы. Вследствие особенностей реализации современные СЖАТ стали более чувствительны к электромагнитному излучению, чем релейные аналоги. Вместе с этим развитие сверхширокополосных генераторов электромагнитного излучения привело к возможности проявления актов терроризма в отношении таких систем.

В существующих научных работах основной упор делается непосредственно на разработку методов оценки воздействующего сверхширокополосных излучения, его детекции, разработку методов защиты устройств. Подобное фокусирование оставляет без должного внимания другие аспекты атаки: сценарии атаки, характеристики злоумышленника, доступные средства и т. д.

Европейским союзом в рамках «Seventh Framework Programme» в проекте SECRET (SECurity of Railways against Electromagnetic aTtacks), основной целью которого является оценка рисков и по-

следствий электромагнитных (ЭМ) атак на системы железнодорожной автоматики и телемеханики, было выделено три основных вида ЭМ-атак:

1 ЭМ-атаки, целью которых является разрушение электронного оборудования.

2 ЭМ-атаки, целью которых является изменение передаваемой информации для отправки ложной информации компонентам железнодорожных систем.

3 ЭМ-атаки, которые нацелены на блокировку передаваемой информации между компонентами железнодорожной системы, чтобы нарушить работу системы и повлиять на ее возможности.

Экспертами наиболее вероятной признана атака, направленная на блокировку передаваемой информации, что является нарушением доступности устройств системы посредством блокировки информации, необходимой для их нормального функционирования. Главным защищаемым объектом в области информационной безопасности (ИБ) является информация. Одним из ключевых принципов информационной безопасности является доступность информации. Отсюда следует, что некоторые аспекты электромагнитной атаки, например, характеристика злоумышленника, мотивы атаки, сценарии атаки, могут быть описаны с точки зрения аналогичных понятий информационной безопасности.

Правильная оценка характеристик злоумышленника позволяет определить наиболее вероятные сценарии атаки, используемые средства, цели атаки, а также подобрать наиболее подходящие методы реагирования. В 2015 году Федеральной службой по техническому и экспортному контролю (ФСТЭК) России была сформулирована и опубликована «методика определения угроз безопасности информации в информационных системах», в которой сформулированы принципы оценки нарушителей информационной системы.

Микропроцессорные системы железнодорожной автоматики и телемеханики, являясь критически важными объектами инфраструктуры (КВОИ), представляют интерес в качестве цели для различных видов злоумышленников. Ниже (таблица 1), приведены характеристики наиболее вероятных субъектов, осуществляющих атаку, с учетом факторов, влияющих на их деятельность. Используются принципы, описанные в методике ФСТЭК.

При оценке возможностей злоумышленников необходимо исходить из условий, что для повышения своих возможностей «спецслужбы» могут вступать в сговор с сотрудниками, обслуживающими объект. Опираясь на приведенные в методике ФСТЭК оценки потенциала злоумышленника, сотрудники, специалисты, обслуживающие систему управления (профессионалы) и не обслуживающие систему (непрофессионалы), являются нарушителями с базовым (низким) потенциалом.

Таблица 1 – Характеристики вероятных нарушителей, факторы влияющие на их деятельность

Факторы	Субъекты			
	Специальные службы иностранных государств (блоков государств)	Террорист	Сотрудник организации, не обслуживающий объект (непрофессионал)	Сотрудник, специалист, обслуживающий объект (профессионал)
Временной	Ограничение по срокам выполнения поставленной задачи	Отсутствует	Отсутствует	Отсутствует
Территориальный	Ограничен территорией собственного государства	Отсутствует	Ограничен территорией ЖД	Ограничен территорией ЖД
Набор средств для осуществления задачи	Широкие возможности выбора средств	Более ограниченный набор средств, чем у спецслужб	Случайные средства	Более ограниченный набор средств, чем у спецслужб
Условия работы (наличие инструкций)	Присутствуют	Отсутствуют	Отсутствуют	Отсутствуют
Условия работы (секретность)	Присутствует	Присутствует	Отсутствует	Присутствует
Условия работы (методы воздействий)	Стандартные (рекомендованные)	Нестандартные или (и) стандартные	Случайные	Нестандартные или (и) стандартные
Условия работы (характер выбора объекта воздействия)	Обязательный	Необязательный	Случайный	Необязательный

Такие нарушители имеют возможность получить информацию об уязвимостях отдельных компонентов системы, имеют возможность получить информацию о методах и средствах реализации угроз безопасности, опубликованных в общедоступных источниках, и (или) самостоятельно создают методы и средства реализации атак и осуществляют их. Террористы обладают всеми возможностями злоумышленников с базовым потенциалом, однако имеют большее количество ресурсов, та-

ким образом, относятся к злоумышленникам со средним потенциалом и являются наиболее вероятным вариантом злоумышленника. Спецслужбы являются нарушителями с самым высоким потенциалом. Они обладают широкими возможностями по выбору средств, экспертными знаниями в целевой области, большими ресурсами, однако имеют ограничение по времени, сложности с работой на территории иностранных государств и ограничены внутренними инструкциями.

УДК 656.256:519.683.7

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРОГРАММИРОВАНИЯ И КОНФИГУРИРОВАНИЯ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

А. Ю. КАМЕНЕВ, А. А. ЛАПКО

Украинский государственный университет железнодорожного транспорта, г. Харьков

Подготовка к эксплуатации современных систем железнодорожной автоматики реализуется еще на этапе их разработки. Важной составляющей данного этапа является автоматизированное проектирование и конфигурирование программно-аппаратных средств систем управления транспортного назначения. Для повышения эффективности процесса конфигурирования программно-аппаратных средств систем железнодорожной автоматики важным направлением является синтез и интеграция современных научных методов и прикладных САД и САЕ-систем.

В недавнем времени для решения указанных задач специалистами Украинского государственного университета железнодорожного транспорта и Научно-производственного предприятия «Желдоравтоматика» (г. Харьков) были разработаны методы графоаналитического моделирования распределенных объектов, которые были интегрированы в состав САЕ-системы EPlan. Пример человеко-машинного интерфейса САЕ-системы, использующей функциональные вершины смешанных графов для задач автоматизированного проектирования, приведен на рисунке 1. При этом показан принцип воспроизведения программно-аппаратных блоков устройств железнодорожной автоматики функциональными вершинами графической модели.

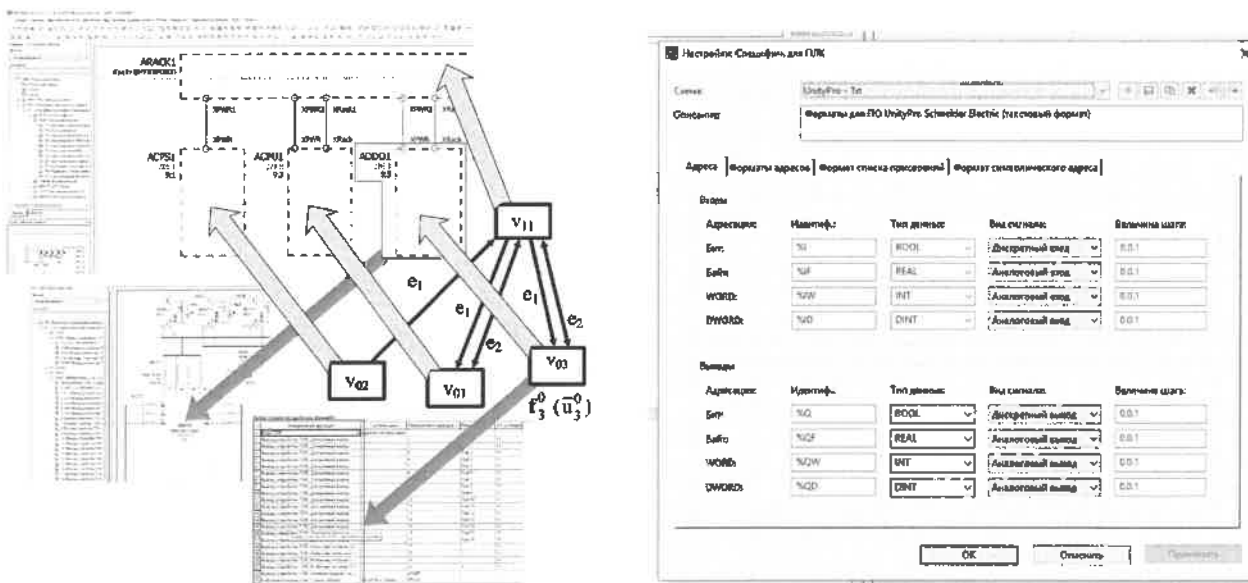


Рисунок 1 – Человеко-машинный интерфейс и принцип графо-функционального моделирования в САЕ-системе EPlan

В особенности вопрос касается микропроцессорных систем железнодорожной автоматики, главным образом – централизации стрелок и сигналов. Технологическим объектом таких систем является путевое развитие железнодорожных станций, исследованию графоаналитического воспроизведения которого посвящен ряд научных трудов авторов данного доклада. Отдельного внимания заслуживает при этом совершенствование методов конфигурирования моделей для испытаний таких систем.