ISSN 2078-9181
DOI 10.15622/ia.19.5
http://ia.spcras.ru

ТОМ 19 № 5

ИНФОРМАТИКА И АВТОМАТИЗАЦИЯ

INFORMATICS AND AUTOMATION

СПб ФИЦ РАН

Санкт-Петербург
2020

INFORMATICS AND AUTOMATION

Volume 19 № 5, 2020

Scientific and educational journal primarily specialized in computer science, automation, robotics, applied mathematics, interdisciplinary research
Founded in 2002

Founder and Publisher
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

Editorial office address

14-th line V.O., 39, St. Petersburg, 199178, Russia,
e-mail: ia@spcras.ru, web: http://ia.spcras.ru

The journal is indexed in Scopus

The journal is published under the scientific-methodological supervision of Department for Nanotechnology and Information Technology of the Russian Academy of Sciences

ИНФОРМАТИКА И АВТОМАТИЗАЦИЯ

Том 19 № 5, 2020

Научный, научно-образовательный журнал с базовой специализацией
в области информатики, автоматизации, робототехники, прикладной математики
и междисциплинарных исследований.
Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
«Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»
(СПб ФИЦ РАН)

Адрес редакции

199178, г. Санкт-Петербург, 14-я линия В.О., д. 39
e-mail: ia@spcras.ru, сайт: http://ia.spcras.ru

Журнал индексируется в международной базе данных Scopus

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий,
в которых должны быть опубликованы основные научные результаты диссертации
на соискание ученой степени доктора и кандидата наук»
Журнал выпускается при научно-методическом руководстве Отделения нанотехнологий
и информационных технологий Российской академии наук

CONTENTS

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Уважаемые читатели и авторы!

Редакционная коллегия журнала «Труды СПИИРАН» сообщает, что с № 5 2020 года журнал выходит под новым названием – «Информатика и автоматизация», зарегистрированным в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Изменение названия журнала обусловлено прошедшими научно-организационными событиями в деятельности Санкт-Петербургского института информатики и автоматизации Российской академии наук.

В соответствии с приказами Министерства науки и высшего образования Российской Федерации № 1399 от 18 декабря 2019 года и №768 от 08 июля 2020 года на базе Федерального государственного бюджетного учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) с присоединением Федерального государственного бюджетного учреждения науки института озероведения Российской академии наук (ИНОЗ РАН); Федерального государственного бюджетного учреждения науки Санкт-Петербургского научно-исследовательского центра экологической безопасности Российской академии наук (НИЦЭБ РАН); Федерального государственного бюджетного научного учреждения «Северо-Западный научно-исследовательский институт экономики и организации сельского хозяйства» (ФГБНУ СЗНИЭСХ); Федерального государственного бюджетного научного учреждения «Северо-Западный Центр междисциплинарных исследований проблем продовольственного обеспечения» (СЗЦППО); Федерального государственного бюджетного научного учреждения «Новгородский научно-исследовательский институт сельского хозяйства» (ФГБНУ «Новгородский НИИСХ») создано Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН).

Благодаря реорганизации СПИИРАН в Санкт-Петербурге образована крупная научная организация СПб ФИЦ РАН, ориентированная на проведение фундаментальных, поисковых и прикладных научных исследований в области информационной, экономической, продовольственной и экологической безопасности, которые направлены на получение новых

знаний в сфере информатики, автоматизации, робототехники, искусственного интеллекта, информационных и коммуникационных технологий, рационального использования почвенных, водных и генетических ресурсов сельского хозяйства Северо-Запада России, экономики агропромышленного комплекса и устойчивого развития сельских территорий, природоохранной деятельности, связанной с мониторингом и прогнозированием состояния окружающей среды и биоценоза, развитием отраслей традиционного природопользования в Арктической зоне, способствующих технологическому, экономическому, социальному и кадровому развитию. К основным научным направлениям Центра относятся:

– фундаментальные основы построения информационного общества с цифровой экономикой, фундаментальные, технологические, правовые и социально-экономические основы искусственного интеллекта, больших данных, информационной и кибербезопасности, постквантовых криптосистем, проактивного мониторинга и управления информационными процессами в сложных системах, создания интеллектуальных интегрированных систем поддержки принятия решений, технологий программно-определяемых систем, многомодальных пользовательских интерфейсов в человеко-машинных и робототехнических комплексах;

– фундаментальные основы рационального использования агроресурсного потенциала территорий, оптимизации и реконструкции мелиоративных систем, обеспечивающих сохранение природно-ресурсного потенциала и увеличения продуктивности агроландшафтов, сохранения и воспроизводства биологического разнообразия сельскохозяйственных животных и растений для обеспечения продовольственной и экологической безопасности РФ;

– фундаментальные и технологические основы управления продукционным процессом агроэкосистем и возделывания экономически значимых сельскохозяйственных культур в целях создания высокопродуктивных агрофитоценозов на основе адаптации, средообразования, биологизации и производства сбалансированного высококачественного агросырья, удовлетворяющего потребности различных групп населения, в том числе в Арктической зоне РФ;

– фундаментальные основы инновационно-инвестиционного развития сельских территорий, земельных отношений и землепользования на основе интеграционных процессов в региональных агропромышленных комплексах;

– эколого-экономические и правовые проблемы прогнозирования, диагностики и оперативного предупреждения угроз здоровью экосистем на различных жизненных циклах природно-хозяйственных объектов и реабилитации нарушенных, загрязненных техногенных ландшафтов и систем обращения с отходами;

– фундаментальные основы оценки и прогноза тенденций изменения природно-ресурсного потенциала озерного фонда России в различных физико-географических зонах с учетом природно-климатических и антропогенных факторов, его охрана и рациональное геостратегическое использование с учетом социально-экономического развития регионов.

В СПб ФИЦ РАН работает высокопрофессиональный коллектив, включающий свыше 500 сотрудников, в том числе 3 академика РАН, 4 члена-корреспондента РАН, 5 профессоров РАН, 84 доктора наук, 131 кандидата наук и обучается 42 аспиранта.

СПб ФИЦ РАН является соучредителем трех журналов: «Информатика и автоматизация» («Труды СПИИРАН»); «Региональная экология»; «Известия Российского географического общества».

Журнал «Информатика и автоматизация» издается в печатной и онлайн версиях. Печатная версия издается с 2002 г. Онлайн версия издается с 2010 г. Журнал входит с 06 мая 2011 года в «Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук» по специальностям из двух групп: 05.13.00 «Информатика, вычислительная техника и управление»; 01.01.00 «Математика». Журнал включен в международный каталог периодических изданий Ulrich's Periodicals Directory с 05 июня 2014 года. Журнал включен в специализированный референтный библиографический сервис CrossRef с 17 июля 2014 года. Все опубликованные статьи имеют цифровой идентификатор DOI. 12 июня 2016 года журнал включен в международную базу данных Scopus. 03 июля 2018 года журнал вошел в список журналов, включенных в базу данных RSCI на платформе Web of Science.

По итогам 2019 года в РИНЦ журнал «Информатика и автоматизация» занимает 11 место из 4036 научных журналов в общем рейтинге Science Index (в 2018 году – 25 место) и 1 место по тематикам «Автоматика. Вычислительная техника» и «Математика». Двухлетний импакт-фактор журнала в РИНЦ составляет 2,904 (в 2010 году – 0,321, в 2017 году – 1,539). В 2019 году журналу был присвоен квартиль Q3 в международной базе цитирования Scopus (SJR в 2019 году – 0.17, в 2020 году – 0.23). За 18 лет география авторов журнала существенно расширилась, опубликованы статьи ученых из Беларуси, Болгарии, Вьетнама, Великобритании, Германии, Индии, Ирана, Казахстана, Китая, Латвии, Мексики, Монголии, США, Турции, Украины, Франции, Японии и других.

С 2014 года журнал «Информатика и автоматизация» перешел на электронную редакционную платформу, которая регулярно обновляется и обладает рядом конкурентных преимуществ, включая импорт и экспорт

данных в глобальные индексы и агрегаторы научной информации, аналитику и визуализацию сведений о проиндексированных статьях. В настоящее время платформу используют еще 4 журнала: «Вестник защиты растений»; «Записки Горного института»; «Информационно-управляющие системы»; «Интеллектуальные системы на транспорте».

СПИИРАН за 40-летнюю историю закрепил за собой статус одного из ведущих научных центров Северо-Запада в области информатики, автоматизации, в том числе музейной деятельности. В здании СПб ФИЦ РАН располагаются Музей истории СПИИРАН и Музей школы К. Мая. Среди выпускников школы К. Мая 40 академиков Академии наук или Академии художеств, 156 докторов наук; 2 министра, 7 губернаторов, 4 члена Госсовета; 20 генералов и адмиралов, 3 Героя Социалистического труда, 2 летчика-космонавта (Г.М. Гречко, А.И. Борисенко). Используя потенциалы Музеев, сотрудники СПИИРАН ведут просветительскую и воспитательную работу со школьниками и студентами Санкт-Петербурга, пропагандируя лучшие научные, педагогические и культурно-нравственные традиции российского образования и науки.

В связи с расширением деятельности СПИИРАН – СПб ФИЦ РАН перечень специализаций журнала был увеличен, включая информатику, автоматизацию, робототехнику и прикладную математику. Сегодня журнал принимает статьи по следующим рубрикам:

- математическое моделирование и прикладная математика;
- цифровые информационно-коммуникационные технологии;
- искусственный интеллект, инженерия данных и знаний;
- робототехника, автоматизация и системы управления;
- информационная безопасность.

Редакционная коллегия поздравляет всех читателей, авторов, рецензентов и редакторов со значимым событием в истории журнала – изменением названия «Информатика и автоматизация» («Труды СПИИРАН»), произведенным с целью сохранения имени Санкт-Петербургского института информатики и автоматизации Российской академии наук и поддержания академических традиций преемственности.

Главный редактор
журнала «Информатика и автоматизация»,
руководитель научного направления СПИИРАН – СПб ФИЦ РАН,
член-корреспондент
Р.М. Юсупов

УДК 004.891;004.048;004.822 **DOI** 10.15622/ia.2020.19.5.1

А.В. Смирнов, Т.В. Левашова

КОНТЕКСТНО-УПРАВЛЯЕМЫЙ ПОДХОД К ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ЦИФРОВЫХ СЛЕДОВ ПОЛЬЗОВАТЕЛЕЙ

Смирнов А.В., Левашова Т.В. **Контекстно-управляемый подход к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей.**

Аннотация. Разрабатывается контекстно-управляемый подход к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей. Рассматриваются вопросы использования концепции жизни человека в цифровой среде при интеллектуальной поддержке принятия решений. Исследуются цели обращения к цифровым следам человека в различных проблемных областях и выявляются подходы к моделированию жизни человека в цифровой среде. Предлагается подход к интеллектуальной поддержке принятия решений, в котором цифровые следы служат источником информации для выявления предпочтений пользователей и их поведения при принятии решений. Развиваются взгляды на поддержку принятия решений на основе учета следов пользователей в цифровой среде. Результатами исследования являются спецификация требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователя, принципы, концептуальная и информационная модели такой поддержки.

Ключевые слова: интеллектуальная поддержка принятия решений, рекомендательные системы, цифровые следы, модель жизни пользователя в цифровой среде, группирование пользователей

1. Введение. Цифровая революция, начавшаяся в середине прошлого века, стирает границы между физической, цифровой и биологической областями [1]. Она влияет на все сферы жизнедеятельности человека: от экономики, науки и образования до образа жизни. Цифровые технологии сильно изменили модели бизнеса, социальные институты и общество в целом [2] и привели к такому явлению, как цифровой образ жизни, который тесно связан с общечеловеческой потребностью в «удобной жизни» [3].

Одним из следствий использования цифровых носителей и технологий в повседневной деятельности человека являются оставленные им цифровые следы этой деятельности, которые описывают жизнь данного человека в цифровой среде (digital life) [4, 5]. Цифровые следы зависят от видов деятельности человека в разные периоды его биологической жизни (возраста). В области поддержки принятия решений жизнь человека в цифровой среде является одним из источников исторических данных для прогностических решений [6-8].

Основная цель данного исследования – разработка принципов и концептуальной модели интеллектуальной поддержки принятия решений на основе учета следов пользователей в цифровой среде. Жизнь

пользователя в цифровой среде предложено использовать как один из источников исторических данных для формирования рекомендаций. Систематизировать информацию, которая присутствует в цифровых следах, предлагается посредством модели жизни пользователя в цифровой среде. Под моделью жизни понимается структура, описывающая типовые наборы данных, которые содержатся в цифровых следах. Для достижения цели исследования разработаны спецификация требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей, принципы, концептуальная и информационная модели такой поддержки.

2. Жизнь человека в цифровой среде в различных подходах. Использование цифровых следов пользователей для прогнозирования рекомендаций является новым направлением исследований в области интеллектуальной поддержки принятия решений. В данном разделе рассматриваются различные подходы, связанные с использованием концепции жизни человека в цифровой среде, с целью выяснения, каким образом используется и как моделируется жизнь человека в цифровой среде в различных проблемных областях.

Одним из крупных исследований, связанных с созданием описания жизни человека в цифровой среде, является исследовательский проект MyLifeBits компании «Микрософт» [9]. MyLifeBits (рис. 1) – система архивирования, которая позволяет хранить все события жизни человека в одном цифровом поисковом архиве. Для сбора информации о человеке используется специальное программное обеспечение, отслеживающее все его электронные взаимодействия, характеристики его состояния и делающее поминутные фото контекста этого человека (окружающей обстановки, ситуации, в которой человек находится, включая его действия, происходящие события, действия других объектов). Проект реализует концепцию цифровой памяти, то есть человек может осуществлять поиск по содержимому архива и предоставлять найденную информацию заинтересованным сторонам [10]. Модель MyLifeBits состоит из различных объектов (фото, документы) и типизированных отношений между этими объектами. Например, ссылка одного из контактов в списке контактов человека на фотографию может быть обозначена типом «человек на фотографии». Модель представляет собой ориентированный ацикличный граф, вершинами которого являются наборы объектов (collections), а дугами – отношения включения. Любой объект, как и сам набор, может принадлежать нескольким родовым наборам, при этом не должно существовать циклов, нарушающих ограничения ацикличного графа [11].

Рис. 1. Система MyLifeBits [9]

Проект SemanticLIFE [12] посвящен разработке системы управления персональной информацией с использованием онтологий в качестве семантической основы для представления этой информации. Система SemanticLIFE (рис. 2) предназначена для хранения, управления и извлечения информации, с которой когда-либо работал человек. Эта информация накапливается в течение многих лет и дополняется семантикой. Система позволяет собирать и хранить информационные объекты (сообщения электронной почты, просмотренные веб-страницы, телефонные звонки, изображения, контакты и другие) и снабжает их аннотациями. Предоставляемый системой механизм поиска основан на семантических запросах. Жизнь человека в цифровой среде реализована как онтологическое хранилище. Весомым аргументом в пользу использования онтологий служит то, что они поддерживают машиночитаемое представление данных и информации, что упрощает решение сложных задач, связанных с агрегированием информации из разных источников, таких как обработка семантических запросов, отслеживание жизненного пути и обработка событий в ходе жизни. В проекте параллельно поддерживаются два стандарта представления онтологии – RDF (Resource Description Framework) и Topic Maps.

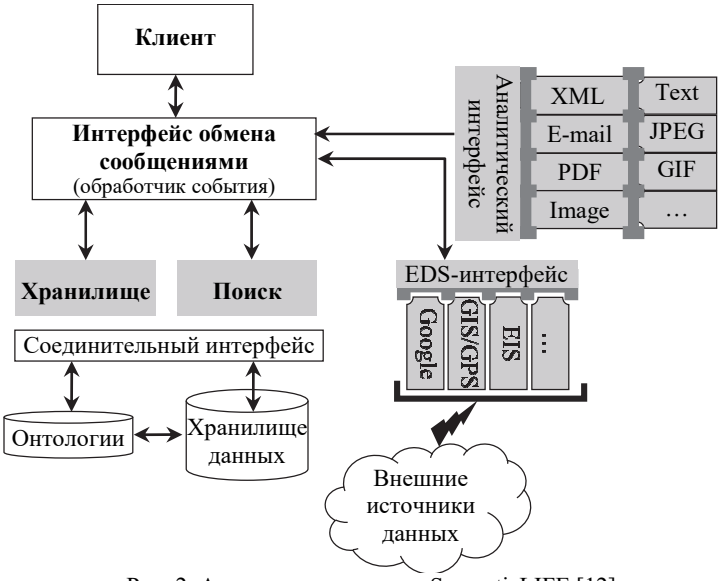


Рис. 2. Архитектура системы SemanticLIFE [12]

В архитектуре PersonisJ [13] модель жизни пользователя в цифровой среде используется для поддержки персонализации на стороне клиента (рис. 3). На концептуальном уровне эта модель представлена в виде иерархии контекстов. Каждый контекст может содержать в себе подлежащие моделированию компоненты. Например, в модели жизни пользователя может иметься контекст посещения пользователем музеев, а внутри этого контекста компоненты, которые моделируют предпочитаемые пользователем музеи. В течение жизни пользователя в компонентах накапливаются значения, на основании которых приложения, получившие от пользователя разрешение на использование конкретных данных, делают интересующие их выводы о пользователе (например, об его предпочтениях). Иерархия контекстов и компонентов представлена при помощи онтологии.

Проект по переосмыслению персональных данных (Rethinking Personal Data) [14], инициированный международным экономическим форумом в 2010 году, посвящен экосистемам персональных данных и напрямую не связан с моделированием жизни человека в цифровой среде. Персональными данными считаются цифровые записи всего, что человек когда-либо делал. Источниками таких данных являются результаты электронных взаимодействий человека (рис. 4), то есть в проекте используются те же типы источников, что и при моделировании жизни человека в цифровой среде. С точки зрения представления

цифровой жизни пользователей результаты проекта интересны тем, что в них предлагаются множество метаданных для описания персональных данных и начальный набор категорий для классификации информации о человеке. Множество метаданных включает три вида данных: добровольно предоставленные данные, данные наблюдений и логически выведенные данные. Предлагаемый набор категорий состоит из 8 категорий: цифровая идентичность; отношения с людьми и организациями; реальный мир и онлайн контекст, действия, интересы и поведение; коммуникационные данные и протоколы работы; выпущенная, просмотренная и перенаправленная аудиовизуальная информация; финансовая информация; медицинские данные; институциональные данные. Этот набор не является окончательным, так как информация, подлежащая хранению, чрезвычайно разнообразна, и постоянно появляются новые формы информации.

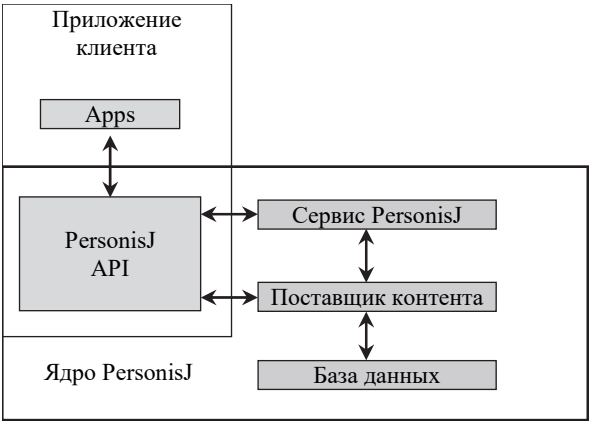


Рис. 3. Архитектура PersonisJ [13]

В модели, предназначенной для рекомендаций приложений владельцам смартфонов, жизнь пользователей в цифровой среде моделируется при помощи набора данных о том, в каком контексте владелец использует установленные на его смартфоне приложения. Используемые данные включают: день недели, время, тип дня (выходной или будний), местоположение, категория приложения, название приложения [15].

Жизнь человека в цифровой среде при принятии им потребительских решений в банковском секторе моделируется при помощи четырех категорий: поиск альтернатив, определение множества альтернатив, оценка множества альтернатив, потребительское решение (рис. 5). Каждая категория описывается множеством факторов, влияющих на выполнение

задачи, которая предполагается из названия категории. В частности, категория «поиск альтернатив» предполагает выполнение задачи поиска альтернатив, категория «определение множества альтернатив» связана с выполнением задачи определения множества альтернатив и так далее. Примерами факторов являются степень удовлетворенности клиента банком для категории «поиск альтернатив», лояльность клиента для категории «определение множества альтернатив» и другие. Для четырех категорий определено более 30 факторов. Значения этих факторов характеризуют конкретного клиента. В результате строится интегрированная модель принятия решений клиентом [16].

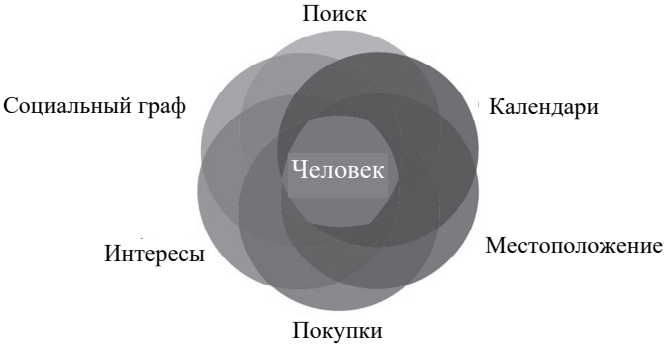


Рис. 4. Цифровые следы персональных данных [14]

В статистическом подходе, направленном на обработку данных в области здравоохранения, жизнь человека в цифровой среде является одним из источников статистических данных [5]. Выделяют следующие источники данных: социальные медиа, мобильные устройства (например, GPS-данные), Интернет-форумы, результаты вебскрейпинга, различные сенсоры (например, датчики здоровья, движения), Интернет вещей и другие.

Архитектура, предназначенная для обеспечения информационного суверенитета граждан в цифровой экосистеме (рис. 6) [17], ориентируется на моделирование жизни человека в цифровой среде в соответствии с архитектурой IDS (International Data Space) – международного пространства данных. Модель IDS представляет все объекты, включая человека, как их цифровых (виртуальных) двойников, называемых ресурсами. Представление ресурса имеет уникальный идентификатор. Для представления используются три уровня формализации: концептуальный, декларативный и программный (операционный) [18]. На концептуальном уровне ресурс представлен при помощи шести независимых аспектов: контент (content), контекст (context), концепт (concept), информационное взаимодействие (communication), ценность/полезность (commodity) (рис. 7).

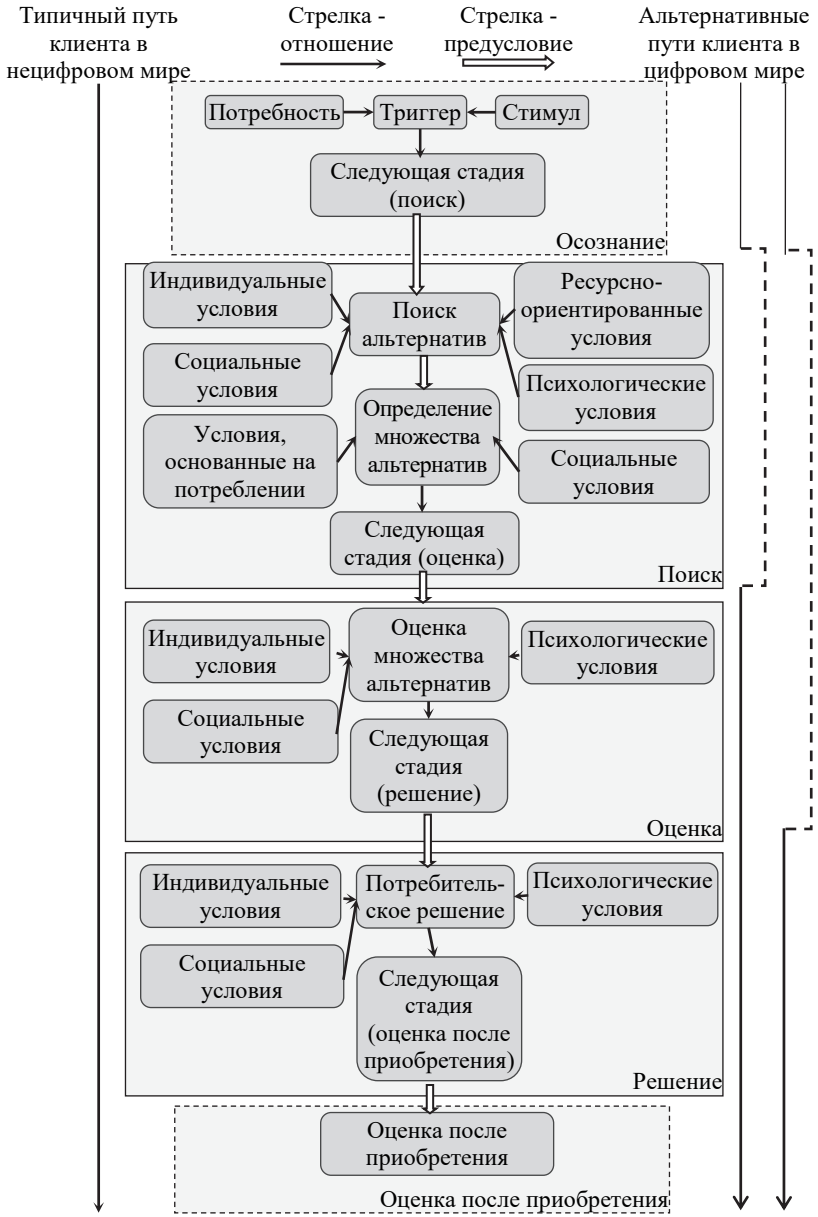


Рис. 5. Модель процесса принятия решений в банковском секторе [16]

Рис. 6. Архитектура для поддержки суверенитета граждан [17]

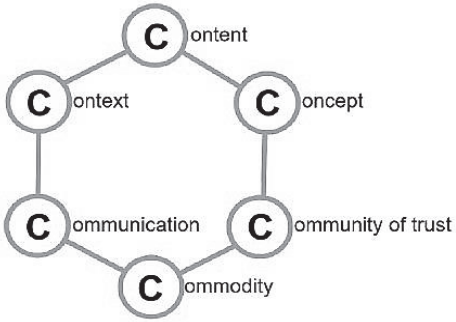


Рис. 7. Аспекты моделирования ресурса на концептуальном уровне в архитектуре IDS [18]

Для представления декларативного уровня используется онтология IDS. Программное представление обеспечивает отображение онтологии IDS на собственные структуры целевого языка программирования. Онтология [19] является единственной нормативной спецификацией модели. Она формализована в формате RDFS/OWL и представляет фундаментальные концепты архитектуры IDS – *цифровой контент*, которым обмениваются *участники* (ресурсы) посредством *компонентов инфраструктуры*. Представление ресурса на остальных уровнях не стандартизировано.

Таблица 1 обобщает способы моделирования жизни человека в цифровой среде, используемые в вышеописанных подходах.

Как видно из таблицы 1, все модели представления жизни человека в цифровой среде используют классификационные структуры. Такие структуры могут быть реализованы при помощи онтологической модели в терминах «класс – свойство» или отображены в такую модель.

Таблица 1. Способы моделирования жизни человека в цифровой среде

Подход	Модель	Проблемная область
MyLifeBits [9-11]	Граф: вершины – классы объектов, дуги – типизированные отношения	Цифровая память
SemanticLIFE [12]	Онтология	Управление персональной информацией
PersonisJ [13]	Онтология контекстов	Персонализированные сервисы
Rethinking Personal Data [14]	Метаданные	Экосистемы персональных данных
Рекомендация мобильных приложений [15]	Контекстно-управляемые данные	Рекомендующие системы
Принятие потребительских решений в банковском секторе [16]	Категорийно-факторная модель	Принятие решений
Сбор статистики на основе моделей цифровой жизни [5]	Данные	Планирование политики здравоохранения
Самоопределение граждан в цифровой экосистеме [17]	International Data Space (IDS)	Экосистемы персональных данных

Вышеописанные подходы использованы в качестве источников для спецификации требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей.

3. Спецификация требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей. Помимо подходов, связанных с использованием концепции жизни человека в цифровых средах, при разработке спецификации учитывались следующие концептуальные особенности современных интеллектуальных систем поддержки принятия решений как вида информационных систем. В информационных системах широко применяется профилирование пользователей. Профиль пользователя – это сводное описание его интересов, характеристик, поведения и предпочтений. Профилирование пользователей занимается сбором, организацией и логическим выводом информации о пользователе с последующим представлением ее в профиле [20]. Некоторые методы профилирования извлекают информацию из цифровых следов пользователей (например, [21]), в результате чего часть информации, описывающей жизнь пользователя, может быть представлена в его профиле. Одним из компонентов любой интеллектуальной информационной среды является база знаний [22], то

есть для интеллектуальной поддержки принятия решений требуется наличие знаний проблемной области. Практически все решения человек принимает в конкретной ситуации или контексте [23], поэтому при прогнозировании рекомендаций должен учитываться контекст пользователя.

Спецификация требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей включает три группы требований.

1. Общие требования:

– доступность профилей пользователей, созданных в различных проблемных областях, и цифровых следов пользователей;

– наличие моделей жизни пользователей, структурирующих контент жизни пользователей в цифровой среде;

– наличие онтологии для представления знаний проблемной области;

– наличие отношений между профилями пользователей, моделями жизни пользователей и онтологией проблемной области, позволяющих поддерживать актуальность представления информации о пользователях в онтологии;

– поддержка контекстно-зависимого предоставления рекомендаций;

– обеспечение конфиденциальности информации о пользователях.

2. Требования к профилям пользователей и к моделям жизни пользователей в цифровой среде:

– профили пользователей, помимо всего прочего, представляют предпочтения пользователей, выявленные в различных проблемных областях;

– профили пользователей и модели жизни пользователей представлены в виде онтологической модели или в виде, совместимом с такой моделью;

– модель жизни пользователя содержит структурные компоненты для представления когда-либо решаемых этим пользователем задач и принятых по этим задачам решений;

– представление задач в модели жизни пользователя содержит информацию о проблемной области, к которой эта задача относится;

– профили пользователей и модели жизни пользователей в цифровой среде предоставляют права на использование информации о пользователе в соответствии с применяемой политикой конфиденциальности.

3. Требования к онтологии проблемной области:

– онтология проблемной области содержит классы для представления типов лиц, принимающих решения, (ЛПР) и аксиомы, задающие принадлежность пользователей этим типам;

– онтология проблемной области содержит структурные элементы, позволяющие учитывать контекст пользователя;

– онтология проблемной области является обновляемой для учета новой информации о жизни пользователей.

4. Принципы интеллектуальной поддержки принятия решений на основе моделей жизни пользователей в цифровой среде. Исходя из спецификации требований к интеллектуальной поддержке принятия решений на основе моделей жизни пользователей в цифровой среде разработаны принципы, которые должны лечь в основу информационной среды интеллектуальной поддержки принятия решений. Множество принципов включает в себя:

П1. Поддержка принятия решений нацелена на рекомендацию пользователю решения.

П2. Пользователи с близкими предпочтениями и поведением при принятии решений объединены в группы.

П3. Предпочтения пользователей, принадлежащих одной группе, и их поведение при принятии решений описываются групповым паттерном. Групповой паттерн определяется как предпочтения и поведение, которые являются типичными для пользователей, принадлежащих одной группе.

П4. Рекомендации прогнозируются на основе групповых паттернов пользователей с близкими предпочтениями и поведением при принятии решений.

П5. Источниками информации о предпочтениях пользователей являются профили пользователей, существующие в различных проблемных областях. Для одного пользователя может существовать несколько профилей.

П6. Источником информации о поведении пользователя при принятии решений являются цифровые следы этого пользователя.

П7. Модель жизни пользователя в цифровой среде извлекается из цифровых следов. Она специфицирует задачи, с которыми пользователь когда-либо имел дело, со ссылкой на проблемную область этих задач и принятые пользователем решения.

П8. Модели профилей пользователя и жизни пользователя в цифровой среде совместимы с онтологической моделью знаний проблемной области.

П9. Задача принадлежности пользователя группе пользователей со сходными предпочтениями и поведением решается машиной логического вывода как задача классификации. Выбор машины вывода зависит

от языка представления онтологии, в которой специфицированы правила логического вывода. В настоящее время наиболее широко используется язык дескрипционных логик OWL [24]. Сравнение существующих машин вывода для дескрипционных логик может быть найдено в работах [25-27].

П10. Принадлежность пользователя группе пользователей со сходными предпочтениями и поведением зависит от контекста. В разных контекстах один и тот же пользователь может принадлежать разным группам.

В таблице 2 перечисленные принципы систематизированы относительно информационной структуры среды интеллектуальной поддержки принятия решений и ее ожидаемой функциональности.

Таблица 2. Принципы интеллектуальной поддержки принятия решений на основе моделей жизни пользователей в цифровой среде

Информационный уровень		
Информационные объекты	*Описание*	*Принцип(ы)*
Информационные ресурсы	Профили пользователей, цифровые следы пользователей, модели жизни пользователей в цифровой среде, онтология проблемной области	П5, П6. П9
Источники исторических данных для прогностических решений	Групповые паттерны пользователей с близкими предпочтениями и поведением при принятии решений	П3
Контекстная информация	Профили пользователей, модели жизни пользователей в цифровой среде, задача, проблемная область	П5, П7
Функциональный уровень		
Процесс	*Как обеспечивается*	*Принцип(ы)*
Поддержка процессов обмена информацией	Представление ресурсов, совместимое с онтологической моделью	П8
Создание групп пользователей со сходными предпочтениями и поведением при принятии решений	Кластеризация пользователей	П2
Категоризация пользователей в группы пользователей со сходными предпочтениями и поведением	Классификация пользователей, выполняемая онтологией	П9
Получение сведений о контексте	Мониторинг цифровых следов онлайн активности пользователей, логический вывод типа пользователя, поддерживаемый онтологией	П7, П9, П10
Прогнозирование решений	Сопоставление типа пользователя с групповыми паттернами	П4
Рекомендация решения	Поддержка принятия решений	П1

Разработанные принципы легли в основу концептуальной модели интеллектуальной поддержки принятия решений на основе цифровых следов пользователей.

5. Концептуальная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователей. Концептуальная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователей (рис. 8) предназначена для рекомендации пользователю решения, которое он принял бы в текущей ситуации (контексте). Основными блоками концептуальной модели являются профиль пользователя, модель жизни пользователя в цифровой среде, групповой паттерн пользователей с близкими предпочтениями и поведением при принятии решений и онтология ЛПР.

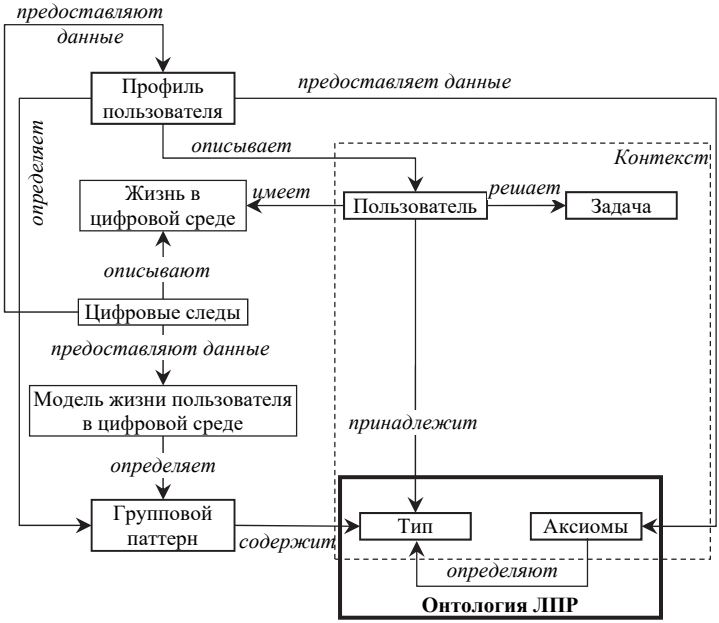


Рис. 8. Концептуальная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователя

Профиль пользователя представляет информацию, на основании которой можно охарактеризовать данного пользователя или построить его описательный портрет. Как правило, пользователь имеет несколько профилей, созданных в разных проблемных областях. Для создания портрета пользователя используются две группы характеристик: контекстно-независимые и контекстно-зависимые. Кон-

текстно-независимые характеристики (например, имя при рождении, возраст, образование) могут быть занесены самим пользователем при создании своего профиля; выявлены при регистрации пользователя в информационных системах и на сайтах; повторно использованы, если пользователь сделал их доступными для определенных проблемных областей; а также выявлены по результатам анализа цифровых следов пользователя.

Для определения контекстно-зависимых характеристик применяются специальные методы и процедуры. Например, процедуры, обрабатывающие данные сенсоров мобильных устройств пользователя, определяют типичные контекстно-зависимые характеристики, такие как текущее местоположение пользователя и время в зоне этого местоположения. Помимо типичных характеристик в проблемных областях выявляются характеристики пользователя, представляющие интерес для конкретной проблемной области. Например, для области Интернет-банкинга такими характеристиками являются добросовестность/неблагонадежность клиента-заемщика, сегмент клиента (группа клиентов с однотипными потребностями и поведенческими реакциями на продукт, к которой относится данный клиент), «продвинутость» клиента и другие. Так же как и контекстно-независимые характеристики, некоторые контекстно-зависимые характеристики могут быть выявлены по результатам анализа цифровых следов пользователя.

Ниже представлена модель профиля пользователя (1):

$$P = \langle User\_ID,\ P\_out, P\_in(C) \rangle, \tag{1}$$

где P – профиль пользователя; $User\_ID$ – уникальное имя пользователя; P_out – множество контекстно-независимых характеристик пользователя; P_in – множество контекстно-зависимых характеристик пользователя в контексте C.

Помимо вышеописанных характеристик пользователя важной частью профиля пользователя являются его предпочтения. В рассматриваемой концептуальной модели предполагается, что предпочтения пользователя могут меняться в зависимости от контекста, поэтому они отнесены к группе контекстно-зависимых характеристик. Для выявления предпочтений пользователя существует множество способов и методов, описание основных из них применительно к персонализации профиля пользователя в рекомендующих системах приведено в работе [28].

Среди цифровых следов есть следы взаимодействий пользователя с информационной средой при решении им различных задач.

Одним из результатов, который может быть получен вследствие анализа и обработки цифровых следов, является профиль задачи [29]. Профиль задачи – это комплексное формализованное описание процесса взаимодействия пользователя с информационной средой или сайтом проблемной области при решении конкретной задачи. На основании профилей задач можно определить виды задач, когда-либо решаемых пользователем в различных ситуациях (контекстах), и принятые пользователем решения. В рассматриваемой концептуальной модели профили задач, задачи и решения являются структурными компонентами модели жизни пользователя в цифровой среде (DL) (2).

$$DL = (PP, Problem(t_0, t_n), Domain, Decison(t_n), R_1, R_2),$$
$$R_{1\in} Problem \times Domain, R_2 \in Problem \times Decison, \tag{2}$$

где PP – идентификатор профиля задачи; $Problem$ – вид решаемой пользователем задачи; t_0 – время начала решения задачи; t_n – время принятия решения; $Domain$ – проблемная область, которой принадлежит задача; $Decision$ – принятое решение.

Предпочтения пользователя и модели жизни пользователей в цифровой среде являются источниками для выявления групп пользователей с близкими предпочтениями и поведением при принятии решений. Эти предпочтения и поведение обобщены в групповом паттерне пользователей с близкими предпочтениями и поведением при принятии решений (GP) (3). Виды групп зависят от проблемной области. В каждой проблемной области используются собственные способы группирования пользователей [30]. Для электронной торговли это могут быть виды сегментов покупателей (например «умные» покупатели, зависимые покупатели, нерискующие покупатели и другие), для туризма – группы туристов, имеющие психофизические барьеры (например, проблемы с коммуникацией, экономические трудности, культурный барьер и т.п.).

$$GP = \left\langle Group, Domain, Problem, Behaviour\_Type_g, Pr_g \right\rangle, \tag{3}$$

где $Group$ – имя группы пользователей с близкими предпочтениями Pr_g и поведением при принятии решений в проблемной области $Domain$ при решении задачи $Problem$; $Behaviour\_Type_g$ – вид пове-

дения, выделяемый в проблемной области *Domain* и соответствующий типовому поведению пользователей группы *Group*.

С точки зрения интеллектуальной поддержки принятия решений пользователь является ЛПР. Онтология ЛПР формализует знания, на основании которых пользователь может быть классифицирован в группы пользователей со сходными предпочтениями и поведением. В онтологии класс «тип» представляет тип ЛПР, который может быть сопоставлен с видами выявленных групп пользователей с близкими предпочтениями и поведением. Принадлежность ЛПР к тому или иному типу описывается аксиомами, определяемыми множеством свойств, которыми должен обладать ЛПР, чтобы принадлежать конкретному классу. Свойства конкретного пользователя, играющего в текущей ситуации роль ЛПР, – это характеристики пользователя, представленные в его профиле. На основании значений этих свойств формируются утверждения об индивидах (аксиомы, описывающие знания о конкретном пользователе) [31], решается задача классификации и определяется, к какому типу ЛПР относится данный пользователь. Так как часть характеристик пользователя являются контекстно-зависимыми, тип пользователя становится контекстно-зависимым, и один и тот же пользователь в разных контекстах может быть отнесен к разным типам ЛПР.

Интеллектуальная поддержка принятия решений в соответствии с вышеописанной концептуальной моделью осуществляется следующим образом. Когда пользователь сталкивается с задачей принятия решений, имеющаяся информация из профиля этого пользователя передается в аксиомы онтологии, описывающие принадлежность ЛПР классу «тип». Машина логического вывода решает задачу классификации и определяет, к какому типу ЛПР относится данный пользователь. Типу ЛПР соответствует группа, определяющая пользователей со сходными предпочтениями и поведением. Предпочтения и поведение пользователей, принадлежащих этой группе, описаны групповым паттерном групп пользователей с близкими предпочтениями и поведением при принятии решений. На основе этого паттерна прогнозируются предпочтения рассматриваемого пользователя. Для прогнозирования используются методы коллаборативной фильтрации, которые позволяют прогнозировать предпочтения конкретного пользователя на основе накопленной информации о предпочтениях других пользователей.

Информация о типе пользователя как ЛПР, задаче принятия решений, проблемной области и предпочтениях пользователя описывает

контекст (C) (4). Эта информация используется для рекомендации пользователю решения, которое пользователи его группы приняли бы в этом контексте (этой ситуации).

$$C(t) = (User\_ID, User\_Type(t), Domain, Problem(t), Pr_u, Pr_u(t), R_1, R_3), \quad Pr_u(t) \in Pr_u, R_3 \in Pr_u \times Domain, \tag{4}$$

где $User\_Type(t)$ – тип пользователя как ЛПР в контексте $C(t)$; $Domain$ – проблемная область; $Problem$ – вид задачи, решаемый пользователем в контексте $C(t)$; Pr_u – множество предпочтений пользователя, представляющих предпочитаемые пользователем критерии оценки альтернатив; $Pr_u(t)$ – множество предпочтений пользователя в контексте $C(t)$; t – рассматриваемый момент времени.

6. Информационная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователей. Информационная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователей (рис. 9) показывает информационные потоки между блоками концептуальной модели (рис. 8) и определяет информационные ресурсы, предоставляющие информацию в указанные блоки. В модели выделены внешние и внутренние ресурсы. Внешними ресурсами считаются ресурсы, которые существуют и поддерживаются вне концептуальной модели. К ним относятся ресурсы проблемной области. Внешние ресурсы включают в себя: профили пользователей, модели жизни пользователей в цифровой среде, сегменты пользователей (S), методы сегментации и методы профилирования. Так как в концептуальной модели предполагается группирование пользователей со сходным поведением при принятии решений, рассматриваются сегменты пользователей, полученные в результате поведенческой сегментации пользователей на основе моделей их жизни в цифровой среде. Название сегмента, к которому относится конкретный пользователь в данной проблемной области, представлено в профилях пользователей. В информационной модели профиль пользователя P (1) представлен выражением (5).

$$P = \langle User\_ID,\ P\_out, Pr(C), S(C) \rangle, \tag{5}$$

где $Pr(C)$ – множество предпочтений пользователя в контексте C $(Pr(C) \subset P\_in(C))$; $S(C)$ – сегмент пользователя в контексте C $(S(C) \subset P\_in(C))$

Внутренними ресурсами концептуальной модели, то есть ресурсами, которые разрабатываются и поддерживаются разработчиками среды интеллектуальной поддержки принятия решений, являются блоки – групповой паттерн и онтология ЛПР. В данной статье онтология ЛПР рассматривается только в части типизации пользователей, так как эта часть предоставляет основу для онтолого-ориентированной классификации пользователей.

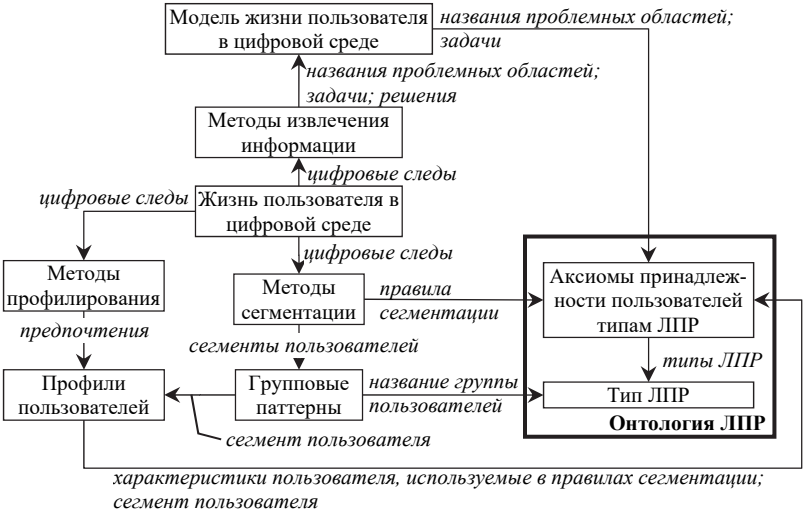


Рис. 9. Информационная модель интеллектуальной поддержки принятия решений на основе следов пользователя в цифровой среде

Реализация внутренних блоков предполагает решение следующих задач: 1) выявление групп пользователей с близкими предпочтениями (критериями оценки альтернатив) и поведением при принятии решений; 2) разработка групповых паттернов, описывающих группы пользователей с близкими предпочтениями и поведением; 3) определение классов онтологии для представления типов ЛПР; 4) формализация аксиом принадлежности пользователей типам ЛПР; 5) установка соответствий между видами групп пользователей и типами ЛПР. Модели решения перечисленных задач представлены в таблице 3, где каждая задача представлена ее номером.

Таблица 3. Модели решения задач

Задача	Источники информации	Исходные данные	Подход	Результат
1	Профили пользователей	Сегменты пользователей *S*	Пользователи, относящиеся к некоторому сегменту, образуют группу, название которой совпадает с названием сегмента	Группы пользователей (*G*), соответствующие сегментам проблемной области
2	2.1. Поведенческие методы сегментации пользователей; 2.2. Профили пользователей	2.1. Сегменты пользователей *S*; 2.2. Предпочтения пользователей	Анализ методов получения сегментов *S*, извлечение правил сегментации, извлечение предпочтений пользователей, входящих в сегменты *S*	2.1.Правила сегментации (*R*); 2.2. Предпочтения пользователей, входящих в группы *G*
3	Группы пользователей *G*	Названия групп из множества *G*	Выявление лексико-семантических зависимостей между названиями групп из множества *G*, составление необходимого и достаточного списка имен классов, соответствующих типам ЛПР	Список имен классов для представления типов ЛПР
4	4.1. Результаты решения задачи 2; 4.2. Профили пользователей; 4.3. Группы *G*	Правила сегментации *R*	Выбор правил сегментации, которые используют информацию из профилей пользователей. Формализация выбранных правил в виде аксиом. Обязательными концептами аксиом являются концепты, представляющие проблемную область и задачу	Множество аксиом, описывающих принадлежность объектов подклассам класса «тип»
5	5.1. Группы *G* 5.2. Онтология ЛПР	5.1.Названия групп из *G*; 5.2. Типы ЛПР	Установка соответствий экспертами	Множество отношений соответствия

7. Заключение. Представлены результаты исследований по разработке принципов и концептуальной модели интеллектуальной поддержки принятия решений на основе учета следов пользователей в цифровой среде. Для достижения цели решены следующие задачи: разрабо-

тана спецификация требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователя, разработаны принципы, концептуальная и информационная модели такой поддержки.

В процессе решения указанных задач выполнен анализ проектов и моделей, в которых используется концепция жизни человека в цифровой среде. Результаты анализа использованы для составления спецификации требований к интеллектуальной поддержке принятия решений на основе цифровых следов пользователей и разработки модели жизни пользователя в цифровой среде.

Сформулированы принципы интеллектуальной поддержки принятия решений на основе цифровых следов пользователей. Эти принципы постулируют цель поддержки принятия решений как предоставление рекомендаций, которые могут помочь пользователю в принятии решения, определяют виды и происхождение источников информации и знаний и фиксируют необходимые функциональные решения.

В соответствии с сформулированными принципами разработана концептуальная модель поддержки принятия решений на основе цифровых следов пользователей. Концептуальная модель позволяет рекомендовать пользователю решения, основываясь на знании о его типе как ЛПР, его предпочтениях, задаче принятия решений и проблемной области, которые сопоставляются со знаниями о группах пользователей, близких данному пользователю по предпочтениям и поведению при принятии решений. В результате пользователю рекомендуется решение, которое пользователи его группы приняли бы в схожем контексте. Выявление пользователей с близким поведением осуществляется методами поведенческой сегментации на основе цифровых следов этих пользователей.

Предложена информационная модель интеллектуальной поддержки принятия решений на основе цифровых следов пользователей. Модель представляет информационные потоки между блоками концептуальной модели, определяет информационные ресурсы, предоставляющие информацию в указанные блоки, и предлагает модели решения задач, связанных с реализацией информационных потоков.

Анализ проектов и моделей, в которых используется концепция жизни человека в цифровой среде, показал, что в настоящее время отсутствуют подходы к моделированию жизни человека в цифровой среде, а использование моделей жизни пользователей в такой среде в системах поддержки принятия решений является новым направлением. Предложенная в данной работе модель жизни пользователя в цифровой среде ориентирована именно на системы поддержки принятия решений и является новым результатом в этой области.

Во многих рекомендующих системах формирование рекомендаций осуществляется методами коллаборативной фильтрации. Эти методы используют накопленные оценки решений всех пользователей, а также результаты поиска пользователей-рекомендателей. Поиск пользователей-рекомендателей может быть основан на соседстве (простой метод), на статистической модели (метод, дорогой в реализации) или на гибридном методе (наиболее точный метод, но сложный и дорогой в реализации и применении). Новым в предложенной концептуальной модели поддержки принятия решений на основе цифровых следов пользователей является то, что для определения пользователей-рекомендателей используется логический вывод, поддерживаемый онтологией. Такой вывод позволяет определить пользователей-рекомендателей на основе информации о поведении и предпочтениях пользователя в различных проблемных областях, и информации о типах ЛПР, аксиоматически заданной в онтологии. Вывод типа ЛПР позволяет выбрать пользователей, предпочтения и поведение которых схоже с предпочтениями и поведением текущего пользователя. Такой подход приближает к решению двух проблем коллаборативной фильтрации – разреженности данных и «холодного старта» за счет использования информации о жизни пользователя в цифровой среде. Эта информация частично устраняет недостаток исходных данных, когда пользователи не предоставляют системе отклика и когда в системе появляется новый пользователь. Онтологический вывод в совокупности с групповыми паттернами, описывающими группы пользователей с близкими предпочтениями и поведением, является гибридным методом поиска пользователей-рекомендателей, то есть обеспечивающем достаточно точные рекомендации и таким образом качественную поддержку принятия решений.

Отличительной особенностью типа ЛПР является его зависимость от контекста, что является оригинальным решением авторов статьи. За счет использования контекстно-зависимого типа ЛПР среда поддержки принятия решений приобретает новое свойство, которое позволяет учесть тот факт, что одно и то же лицо в разных контекстах может принять разные решения по одному и тому же вопросу. Учет такой информации также повышает качество и эффективность поддержки принятия решений.

Модель жизни пользователя в цифровой среде, с одной стороны, предоставляет преимущества с точки зрения структуризации жизни пользователя в цифровой среде для целей поддержки принятия решений, а с другой стороны, эта модель накладывает определенные ограничения. Поскольку, как говорилось ранее, в настоящее

время нет научных работ, направленных на построение таких моделей, для выделения структурных компонентов модели требуются дополнительные исследования, связанные с разбором и структуризацией цифровых следов человека. Кроме того, предложенные модели ограничены уровнем доступа к информации в проблемных областях, а именно к профилям пользователей, правилам сегментации и цифровым следам.

Предложенные в работе модели интеллектуальной поддержки принятия решений целесообразно использовать при построении рекомендующих систем, предназначенных для проблемных областей, повседневная жизнь пользователей которых связана с активным использованием цифровых технологий (электронная торговля, банковский сектор, умные города и т.п.).

Литература

1. *Schwab K.* The Fourth Industrial Revolution: what it means, how to respond // World economic forum. 2016. vol. 14. no. 01. 346 p.
2. *Meffert J., Mendonça P.* Digital @scale : o manual que precisa para transformar a sua empres: 1st ed // Planeta. 2017. 320 p.
3. Strategic Research Agenda for Electronic Components & Systems // ECS Electronic Components + Systems. 2020. 368 p. URL: https://aeneas-office.org/wp-content/uploads/2020/07/ECS-SRA2020_L.pdf (дата обращения: 28.07.2020).
4. *Ayed G.B.* Architecting User-centric Privacy-as-a-set-of-services: Digital Identity-related Privacy Framework // Springer. 2014. 177 p.
5. *Seeskin Z.H. et al.* Uses of Alternative Data Sources for Public Health Statistics and Policymaking: Challenges and Opportunities // Proceedings of 2018 Joint Statistical Meetings. American Statistical Association. 2018. pp. 1822–1861.
6. *Araujo T., Helberger N., Kruikemeier S., de Vreese C.H.* AI We Trust? Perceptions about Automated Decision-Making by Artificial Intelligence // AI & SOCIETY. 2020. 13 p.
7. *Han M.L., Kwak B.I., Kim H.K.* CBR-Based Decision Support Methodology for Cybercrime Investigation: Focused on the Data-Driven Website Defacement Analysis // Security and Communication Networks. 2019. vol. 2019.
8. *Surendro K.* Predictive Analytics for Predicting Customer Behavior // 2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT). 2019. pp. 230–233.
9. MyLifeBits. 2001. URL: https://www.microsoft.com/en-us/research/project/mylifebits/ (дата обращения: 27.07.2020).
10. *Bell G., Gemmell J.* A Digital Life // Scientific American. 2007. vol. 296. no. 3. pp. 58–65.
11. *Gemmell J., Lueder R., Bell G.* The MyLifeBits Lifetime Store // Proceedings of the 2003 ACM SIGMM workshop on Experiential telepresence. ACM Press. 2003. pp. 80–83.
12. *Ahmed M. et al.* "SemanticLIFE"–A framework for managing information of a human lifetime //Proceedings of 6th International Conference on Information Integration and Web-based Applications and Services. 2004. pp. 725–734. URL: http://www.ifs.tuwien.ac.at/~tho/publications/iiWAS04-2.pdf (дата обращения: 28.07.2020).

13. *Gerber S. et al.* PersonisJ: Mobile, Client-Side User Modelling // International Conference on User Modeling, Adaptation, and Personalization.. 2010. pp. 111–122.
14. *Schwab K. et al.* Personal data: The emergence of a new asset class // An Initiative of the World Economic Forum. 2011. 40 p. URL: https://www.weforum.org/reports/personal-data-emergence-new-asset-class (дата обращения: 28.07.2020).
15. *Bahrainian S.A., Crestani F.* Tracking Smartphone App Usage for Time-Aware Recommendation // Digital Libraries: Data, Information, and Knowledge for Digital Lives. Springer. 2017. pp. 161–172.
16. *Pousttchi K., Dehnert M.* Exploring the Digitalization Impact on Consumer Decision-Making in Retail Banking // Electronic Markets. 2018. vol. 28. no. 3. pp. 265–286.
17. *Meister S., Otto B.* Digital Life Journey – Framework for a Self-Determined Life of Citizens in an Increasingly Digitized World // ISST Report. Fraunhofer ISST. 2019. 38 p.
18. *Otto B.* Reference Architecture Model // International Data Spaces Association. Report. Berlin. 2019. 118 p. URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf (дата обращения: 28.07.2020).
19. *Mader C. et al.* Industrial Data Space Information Model. Fraunhofer IAIS/EIS, Fraunhofer FIT. 2020. URL: https://w3id.org/idsa/core (дата обращения: 30.07.2020).
20. *Eke C.I, Norman A.A. Shuib L., Nweke H.F.* A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions // IEEE Access. 2019. vol. 7. pp. 144907–144924.
21. *Harkovchuk A., Korzun D.* Semantic Information Search Service by Person's Face Photo // Proceedings of the 24th Conference of Open Innovations Association FRUCT. 2019. pp. 821–823.
22. *Осипов Г.С.* Искусственный интеллект: состояние исследований и взгляд в будущее // Новости искусственного интеллекта. 2001. Вып. 43(1). URL: http://raai.org/about/persons/osipov/pages/ai/ai.html (дата обращения: 28.07.2020).
23. *Gen M., et al.* SMA White Paper: The Science of Decision Making across the Span of Human Activity. The US Department of Defense Strategic Multilayer Assessment (SMA). 2015. 78 p URL: https://nsiteam.com/social/wp-content/uploads/2016/01/The-Science-of-Decision-Making-across-the-Span-of-Human-Activity.pdf (дата обращения: 28.07.2020).
24. *McGuinness D.L., Harmelen F. van.* OWL Web Ontology Language Overview // W3C Recommendation. 2004. URL: https://www.w3.org/TR/owl-features/ (дата обращения: 31.07.2020).
25. *Dentler K. Cornet R., ten Teije A., de Keizer N.* Comparison of reasoners for large ontologies in the OWL 2 EL profile // Semantic Web. 2011. vol. 2. no. 2. pp. 71–87.
26. *Abburu S.* A Survey on Ontology Reasoners and Comparison // International Journal of Computer Applications. 2012. vol. 57. no. 17. pp. 33–39.
27. *Parsia B., Matentzoglu N., Gonçalves R.S.et al.* The OWL Reasoner Evaluation (ORE) 2015 Competition Report // Journal of Automated Reasoning. 2017. vol. 59. no. 4. pp. 455–482.
28. *Городецкий В.И., Тушканова О.Н.* Онтологии и персонификация профиля пользователя в рекомендующих системах третьего поколения // Онтология проектирования. 2014. Вып. 13. № 3. С. 7–31.
29. *Wong B. L. W., Keith S., Springett M.* Fit for Purpose Evaluation: The case of a public information kiosk for the socially disadvantaged // People and Computers XIX—The Bigger Picture. Springer. 2006. pp. 149–165.

30. *Bayer J.* Customer Segmentation in the Telecommunications Industry // Journal of Database Marketing & Customer Strategy Management. 2010. vol. 17. no. 3–4. pp. 247–256.
31. *Glimm B., Horrocks I., Motik B. et al.* A Novel Approach to Ontology Classification // Journal of Web Semantics. 2012. vol. 14. pp. 84–101.

Смирнов Александр Викторович — д-р техн. наук, заслуженный деятель науки РФ, главный научный сотрудник, лаборатория интегрированных систем автоматизации, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: конфигурирование систем, логистика знаний, поддержка принятия решений, социо-киберфизические системы. Число научных публикаций — 350. smir@iias.spb.su; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-20-73; факс: +7(812)328-44-50.

Левашова Татьяна Викторовна — канд. техн. наук, старший научный сотрудник, лаборатория интегрированных систем автоматизации, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: управление знаниями, поддержка принятия решений, контекстно-управляемые системы, социо-киберфизические системы. Число научных публикаций — 200. tatiana.levashova@iias.spb.su; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-80-71; факс: +7(812)328-44-50.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ. Обзор подходов, связанных с использованием жизни человека в цифровой среде (разд. 2), и онтологическая классификация пользователей (в составе разд. 5) выполнялись в рамках научного проекта № 20-07-00490. Спецификация требований к интеллектуальной поддержки принятия решений на основе моделей жизни пользователя в цифровой среде (разд. 3), принципы (разд. 4) и концептуальная модель такой поддержки (разд. 5) разработаны в рамках научного проекта № 20-07-00455, информационная модель интеллектуальной поддержки принятия решений на основе моделей жизни пользователей в цифровой среде (разд. 6) в части реализации групповых паттернов разработана в рамках научного проекта № 20-07-00490, в части реализации онтологии ЛПР – в рамках научного проекта № 20-07-00455. Контекстно-зависимая типизация пользователей является частью исследований по контекстно-ориентированному поведению пользователей, которые выполнялись в рамках бюджетной темы № 0073-2019-0005.

DOI 10.15622/ia.2020.19.5.1

A. SMIRNOV, T. LEVASHOVA

CONTEXT-AWARE APPROACH TO INTELLIGENT DECISION SUPPORT BASED ON USER DIGITAL TRACES

Smirnov A., Levashova T. **Context-Aware Approach to Intelligent Decision Support Based on User Digital Traces.**

Abstract. A context-aware approach to intelligent decision support based on user digital traces is proposed. The concept of human digital life with regard to intelligent decision support is discussed. The aims of addressing this concept in diverse domains are clarified and approaches to modelling human digital life are identified. In the proposed approach, digital traces serve as a source of information to reveal user preferences and decision-making behaviour. Perspectives on decision support based on user digital traces are developed. The research outcomes are the specification of requirements to intelligent decision support based on user digital traces, the principles, conceptual framework and information model of such support. The principles form the basis for the conceptual framework of intelligent decision support based on user digital traces. Components of the conceptual model are user profiles; a user digital life model that structures information containing in the digital traces; group patterns that describe preferences and decision-making behavior shared by a user group; and a decision maker ontology. The information model defines information flows between the framework's components, identifies tasks that require solutions to implement the framework and offers techniques for this. The novelties of the research are applying the concept of human digital life to intelligent decision support and context-dependent ontological inference of the type of user as a decision-maker, which determines a group of users sharing their preferences and behaviours with the active user, to predict a recommended decision. The paper contributes to the areas of modelling human digital life and intelligent decision support.

Keywords: Intelligent Decision Support, Recommending Systems, Digital Traces, Model of User Digital Life, User Classification

Smirnov Alexander — Ph.D., Dr.Sci., Honored Scientist of Russian Federation, Chief Researcher, Laboratory of Computer-Aided Systems, St.-Petersburg Federal Research Center of the Russian Academy of Sciences (SPb FRC RAS). Research interests: system configuring, knowledge logistics, decision support, socio-cyber-physical systems. The number of publications — 350. smir@iias.spb.su; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-20-73; fax: +7(812)328-44-50.

Levashova Tatiana — Ph.D., Senior Researcher, Laboratory of Computer-Aided Systems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: knowledge management, decision support, context-aware systems, and socio-cyber-physical systems. The number of publications — 200. tatiana.levashova@iias.spb.su; 39, 14-th line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-80-71; fax: +7(812)328-44-50.

Acknowledgements. The research overview is due to project number 20-07-00490 from RFBR (sec. 2), the requirements to and principles of intelligent decision support based on user digital life (sec. 3 and 4) are due to project number 20-07-00455 from RFBR, the conceptual framework (sec. 5) in parts of user digital life modelling and group patterns revealing is due to project number 20-07-00455 from RFBR, in part of ontology-based user classification is due to project number 20-07-00490 from RFBR, and in part of context-dependent user categorization is due to State Research, project number 0073-2019-0005. The information model of intelligent

decision support based on user digital life (sec. 6) in part of the group patterns implementation is due to project number 20-07-00455 from RFBR and in part of the implementation of the decision maker ontology is due to project number 20-07-00490 from RFBR.

References

1. Schwab K. The Fourth Industrial Revolution: what it means, how to respond World economic forum. 2016. vol. 14. no. 01. 346 p.
2. Meffert J., Mendonça P. Digital @scale : o manual que precisa para transformar a sua empres: 1st ed. Planeta. 2017. 320 p.
3. Strategic Research Agenda for Electronic Components & Systems. ECS Electronic Components + Systems, 2020. Available at: https://aeneas-office.org/wp-content/uploads/2020/07/ECS-SRA2020_L.pdf (accessed: 28.07.2020).
4. Ayed G.B. Architecting User-centric Privacy-as-a-set-of-services: Digital Identity-related Privacy Framework. Springer. 2014. 177 p.
5. Seeskin Z.H. et al. Uses of Alternative Data Sources for Public Health Statistics and Policymaking: Challenges and Opportunities. Proceedings of 2018 Joint Statistical Meetings. American Statistical Association. 2018. pp. 1822–1861.
6. Araujo T., Helberger N., Kruikemeier S., de Vreese C.H. AI We Trust? Perceptions about Automated Decision-Making by Artificial Intelligence. *AI & SOCIETY*. 2020. 13 p.
7. Han M.L., Kwak B.I., Kim H.K. CBR-Based Decision Support Methodology for Cybercrime Investigation: Focused on the Data-Driven Website Defacement Analysis. *Secur. Commun. Networks.* 2019. vol. 2019.
8. Surendro K. Predictive Analytics for Predicting Customer Behavior. 2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT). 2019. pp. 230–233.
9. MyLifeBits. 2001. Available at: https://www.microsoft.com/en-us/research/project/mylifebits/ (accessed: 07.05.2020).
10. Bell G., Gemmell J. A Digital Life. *Sci. Am.* 2007. vol. 296. no. 3. pp. 58–65.
11. Gemmell J., Lueder R., Bell G. The MyLifeBits Lifetime Store. Proceedings of the 2003 ACM SIGMM workshop on Experiential telepresence – ETP ’03. ACM Press. 2003. pp. 80–83.
12. Ahmed M. et al. "SemanticLIFE"–A framework for managing information of a human lifetime //Proceedings of 6th International Conference on Information Integration and Web-based Applications and Services. 2004. pp. 725–734. Available at: http://www.ifs.tuwien.ac.at/~tho/publications/iiWAS04-2.pdf (accessed: 28.07.2020).
13. Gerber S. et al. PersonisJ: Mobile, Client-Side User Modelling. International Conference on User Modeling, Adaptation, and Personalization. 2010. pp. 111–122.
14. Schwab K. et al. Personal data: The emergence of a new asset class // An Initiative of the World Economic Forum. 2011. 40 p. Available at: https://www.weforum.org/reports/personal-data-emergence-new-asset-class (accessed: 28.07.2020).
15. Bahrainian S.A., Crestani F. Tracking Smartphone App Usage for Time-Aware Recommendation. Digital Libraries: Data, Information, and Knowledge for Digital Lives. Springer. 2017. pp. 161–172.
16. Pousttchi K., Dehnert M. Exploring the digitalization impact on consumer decision-making in retail banking. *Electron. Mark*. 2018. vol. 28. no. 3. pp. 265–286.
17. Meister S., Otto B. Digital Life Journey – Framework for a Self-Determined Life of Citizens in an Increasingly Digitized World. ISST Report. Fraunhofer ISST. 2019. 38 p.
18. Otto B. Reference Architecture Model. International Data Spaces Association. Report. Berlin. 2019. 118 p. Available at: https://www.internationaldataspaces.org/wp-

content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf (accessed: 28.07.2020).
19. Mader C., Pullmann J., Petersen N. et al. Industrial Data Space Information Model. Fraunhofer IAIS/EIS. Fraunhofer FIT. 2020. Available at: https://w3id.org/idsa/core (accesses: 30.07.2020).
20. Eke C.I, Norman A.A. Shuib L., Nweke H.F. A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions. *IEEE Access*. 2019. vol. 7. pp. 144907–144924..
21. Harkovchuk A., Korzun D. Semantic Information Search Service by Person's Face Photo. Proceedings of the 24th Conference of Open Innovations Association FRUCT. 2019. pp. 821–823.
22. Osipov G.S. [Atrificial Intelligence: State of Research and Looking to the Future]. *Novosti iskusstvennogo intellekta – Artificial Intelligence News*. 2001. vol. 43. no. 1. (In Russ.). Available at: http://raai.org/about/persons/osipov/pages/ai/ai.html (accessed: 28.07.2020).
23. Gen M. et al. SMA White Paper: The Science of Decision Making across the Span of Human Activity. The US Department of Defense Strategic Multilayer Assessment (SMA). 2015. 78 p. Available at: https://nsiteam.com/social/wp-content/uploads/2016/01/The-Science-of-Decision-Making-across-the-Span-of-Human-Activity.pdf (accessed: 28.07.2020).
24. McGuinness D.L., Harmelen F. van. OWL Web Ontology Language Overview W3C Recommendation; 2004. Available at: https://www.w3.org/TR/owl-features/ (accessed: 25.03.2020).
25. Dentler K. Cornet R., ten Teije A., de Keizer N. Comparison of reasoners for large ontologies in the OWL 2 EL profile. *Semant. Web*. 2011. vol. 2. no. 2. pp. 71–87.
26. Abburu S. A Survey on Ontology Reasoners and Comparison. *International Journal of Computer Applications*. 2012. vol. 57. no. 17. pp. 33–39.
27. Parsia B., Matentzoglu N., Gonçalves R.S. et al. The OWL Reasoner Evaluation (ORE) 2015 Competition Report. *Journal of Automated Reasoning.* 2017. vol. 59. no. 4. pp. 455–482.
28. Gorodetsky V.I., Tushkanova O.N. [Ontology-Based User Profile Personification in 3G Recommender Systems]. *Ontologiya proektirovaniya – Ontology of designing*, 2014. vol. 13. no. 3. pp. 7–31. (In Russ.).
29. Wong B.L.W., Keith S., Springett M. Fit for Purpose Evaluation: The case of a public information kiosk for the socially disadvantaged. People and Computers XIX—The Bigger Picture. 2006. pp. 149–165.
30. Bayer J. Customer segmentation in the telecommunications industry. *Journal of Database Marketing & Customer Strategy Management*. 2010. vol. 17. no. 3–4. pp. 247–256.
31. Glimm B. et al. A Novel Approach to Ontology Classification. *Journal of Web Semantics*., 2012. vol. 14. pp. 84–101.

DOI 10.15622/ia.2020.19.5.2

T. ENDO , R. MAEDA , F. MATSUNO

STABILITY ANALYSIS OF SWARM HETEROGENEOUS ROBOTS WITH LIMITED FIELD OF VIEW

Endo T., Maeda R., Matsuno F. **Stability Analysis of Swarm Heterogeneous Robots with Limited Field of View.**

Abstract. This paper presents a stability analysis of swarm robots, a group of multiple robots. In particular, we focus on robot swarms with heterogeneous abilities, in which each robot has a different sensing range and physical limitations, including maximum velocity and acceleration. In addition, each robot has a unique sensing region with a limited angle field of view. We previously proposed a decentralized navigation method for such heterogeneous swarm robots consisting of one leader and multiple followers. With the decentralized navigation method, a single leader can navigate for followers while maintaining connectivity and satisfying the physical limitations unique to each robot; i.e., each follower has a target robot and follows it without violating its physical limitations. In this paper, we focus on a stability analysis of such swarm robots. When the leader moves at a constant velocity, we mathematically prove that the shape and orientations of all robots eventually converge to the equilibrium state. For this, we must first prove that the equilibrium state exists. Then, we show the convergence of the state to its equilibrium. Finally, we carry out experiments and numerical simulations to confirm the stability analysis, i.e., the convergence of the swarm robots to the equilibrium states.

Keywords: stability, swarm robots, navigation, decentralized controller.

1. Introduction. Swarm robots are a group of multiple robots that aim to achieve robust, scalable, and flexible coordinated collective behavior [1-6]. For robot swarms, it is important to control the robots in a decentralized manner by utilizing locally available information for each robot, so that the system can deal with increases in the number of robots. Swarm robots are expected to be applicable to various situations, such as cooperative coverage [7, 8], surveillance [9, 10], target-capturing [11, 12], transport [13, 14], and visually appealing entertainment [15, 16]. One of the essential functions of such tasks is to move swarm robots as a flock to the desired location.

Although many studies have investigated the connectivity maintenance of swarm robots, most have considered homogeneous swarm robots, which consist of robots with the same ability and performance. On the other hand, heterogeneous swarms consist of robots with different abilities and performance. Heterogeneous swarm robots have the ability to handle a wide range of tasks that homogeneous swarms cannot. This is because they cooperate with each other while taking advantage of each robot's characteristics [17]. For example, several studies [18-20] proposed decentralized control methods for connectivity maintenance of a group of heterogeneous robots characterized by a different communication radius. Another study [21] also proposed a decentralized control method for connectivity maintenance of a robotic swarm

with heterogeneous abilities, including sensing range, maximum velocity, and acceleration. However, these studies assumed that all robots could sense all directions.

In practical situations, many sensors and cameras have angle limitations in addition to distance ones in the sensing range. Thus, to propose a decentralized control method for connectivity maintenance of a heterogeneous robotic swarm, in which each robot has both a different sensing range with a limited field of view and a limited sensing distance, is a practical challenge. A few studies [22-26] have considered the navigation of robots having cameras with a limited field of view. In three [22-24], control methods were proposed for visibility maintenance of homogeneous robots; i.e., each robot had the same sensing region, and a cooperative visibility maintenance method was proposed in [25] for multiple robots with different sensing regions but the same performance.

However, there are no studies about decentralized control methods for connectivity maintenance of a heterogeneous robotic swarm characterized by sensing distance, limited field of view, and maximum velocity and acceleration. We previously proposed a decentralized navigation strategy for swarm robots with heterogeneous abilities, including the angle of field of view, velocity, and acceleration [26]. Our method ensured that the leader could guide the followers. At the same time, they maintained a certain distance from their target and did not exceed their unique physical limitations such as maximum velocity and acceleration. However, we did not conduct a stability analysis of swarm robots.

In this paper, we present the stability analysis of swarm robots with heterogeneous abilities for velocity and acceleration, and sensing region with a limited angle of view, and limited sensing distance. We discuss the stability of the whole swarm shape, and the orientation of each follower robot with omni-directional mobility; i.e., we discuss the convergence of the shape of the whole swarm and the orientation of all followers to the equilibrium state. The stability of the swarm shape predicts the shape of the swarm, which is useful in controlling formation or avoiding obstacles. On the other hand, the stability of followers' orientation greatly influences on their ability to keep the target robot in their sensing range, which is important in connectivity maintenance with robots having a limited field of view. Thus, we prove that the swarm shape and the orientation of all followers converge to an equilibrium state. Further, we present experimental results and numerical simulation results to confirm the validity of our stability analysis. The preliminary version of this paper has been published [27]. This extended version contains a new proof of the boundedness of perturbation, that is required in the stability of the whole

swarm. Furthermore, this paper includes new simulation results to investigate the stability of the swarm robots by our control method for a more significant number of robots.

The main contributions of this paper are as follows. We deal with a heterogeneous swarm of robots in which each robot has a different sensing range, limited field of view, and physical limitations, such as maximum velocity and acceleration. Such robotic swarms have the potential to deal with a wider variety of tasks. When a leader robot guiding follower robots moves at a constant speed in a constant direction, the shape of the whole swarm and all followers' orientations converge to an equilibrium point. We mathematically prove that this convergence is achieved, and carry out an experiment and numerical simulation to confirm the stability.

This paper is organized as follows. In Section 2, we present the problem settings. Section 3 introduces our navigation method. Section 4 describes the mathematical analysis of stability. Section 5 provides the experimental results and Section 6 the results of the numerical simulations to confirm the stability analysis. Finally, Section 7 concludes the paper.

2. System Description. Let us consider $n+1$ agents in a two-dimensional (2-D) plane without obstacles. ID $1,2,\ldots,n$ are assigned to followers, and $n+1$ to the leader. The position vector and orientation of agent i in the absolute coordinate system at time t are $\boldsymbol{x}_i(t) = [x_i(t), y_i(t)]^T \in \mathbb{R}^2$ and $\eta_i(t) \in \mathbb{R}$, respectively, and the equations of motion of agent i are described as follows:

$$\dot{\boldsymbol{x}}_i(t) = \boldsymbol{u}_i(t); \tag{1}$$

$$\dot{\eta}_i(t) = \omega_i(t), \tag{2}$$

where $\boldsymbol{u}_i(t) \in \mathbb{R}^2$ is translational velocity input, and $\omega_i(t) \in \mathbb{R}$ is angular velocity input. Follower i has the following physical limitations:

$$\begin{cases} \|\boldsymbol{u}_i(t)\| \leqslant U_i, \quad \|\dot{\boldsymbol{u}}_i(t)\| \leqslant A_i, \quad |\omega_i(t)| \leqslant \Omega_i, \quad |\dot{\omega}_i(t)| \leqslant B_i; \\ \boldsymbol{u}_i(t) \text{ and } \omega_i(t) \text{ are continuous for } t, \end{cases} \tag{3}$$

where $\dot{\boldsymbol{u}}_i(t)$ is the semi-derivative of $\boldsymbol{u}_i(t)$, whose norm is larger if $\boldsymbol{u}_i(t)$ is left or right semi-differentiable, and $\dot{\omega}_i(t)$ is defined in the same manner. In addition, U_i, A_i, Ω_i, and B_i are the upper limits of the translational velocity, translational acceleration, angular velocity, and angular acceleration, respectively, and $\|\cdot\|$ denotes the Euclidean norm.

The sensing region of follower i is defined as follows:

$$S_i(t) = \left\{ \boldsymbol{x}(t) \in \mathbb{R}^2 \ : \ r_i(t) \leqslant \rho_i, \ |\phi_i(t)| \leqslant \psi_i \right\}, \tag{4}$$

where $\boldsymbol{x}(t) = [x(t), y(t)]^T \in \mathbb{R}^2$ is a position vector, $r_i(t) = \|\boldsymbol{x}(t) - \boldsymbol{x}_i(t)\| \in \mathbb{R}$ is the distance between $\boldsymbol{x}(t)$ and follower i, ρ_i is the maximum sensing distance, $\phi_i(t)$ is the bearing angle from follower i to $\boldsymbol{x}(t)$, which is defined by $\phi_i(t) = \text{atan2}(y(t) - y_i(t), \ x(t) - x_i(t)) - \eta_i(t)$, and $2\psi_i(t)$ is the angle of the sensing region as shown in Figure 1 (a). If agent j is in the sensing region $S_i(t)$, follower i can measure the relative distance $r_{ij}(t) = \|\boldsymbol{x}_j(t) - \boldsymbol{x}_i(t)\|$ and bearing angle $\phi_{ij}(t) = \text{atan2}(y_j(t) - y_i(t), \ x_j(t) - x_i(t)) - \eta_i(t)$.

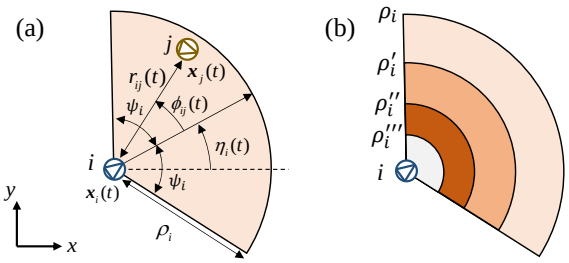


Fig. 1. Sensing region of follower i: (a) relative position between follower i and its target; (b) division of sensing region

We assume that the leader knows the specifications of all followers, but cannot access global real-time information. Meanwhile, followers can obtain only local information from their own sensing.

3. Previously Proposed Navigation Method. In this section, we briefly introduce our previously proposed decentralized navigation method [26] for heterogeneous swarm robots with a limited field of view, which ensures connectivity maintenance.

The translational velocity input of follower i is set as the following form:

$$\boldsymbol{u}_i(t) = u_{ir}(t)\boldsymbol{e}_{ir}(t) + u_{i\theta}(t)\boldsymbol{e}_{i\theta}(t), \tag{5}$$

where the target of follower i is agent j, $\boldsymbol{e}_{ir}(t)$ is a unit vector defined by $\boldsymbol{e}_{ir}(t) = (\boldsymbol{x}_j(t) - \boldsymbol{x}_i(t))/r_{ij}$, and $\boldsymbol{e}_{i\theta}(t)$ is a unit normal vector of $\boldsymbol{e}_{ir}(t)$ (see Figure 2 (a)). We define positive constants ρ_i', ρ_i'', and ρ_i''', which satisfy $0 < \rho_i''' < \rho_i'' < \rho_i' < \rho_i$, respectively, and divide the sensing region as shown in Figure 1 (b). Then, the components of $\boldsymbol{u}_i(t)$ are designed as follows:

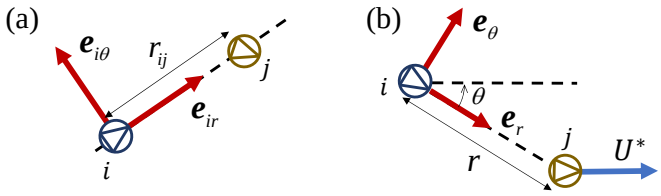


Fig. 2. Relationship between follower i and its target j: (a) local coordinate system; (b) definition of angle θ

1. If $\rho_i''' \leqslant r_{ij}(t) \leqslant \rho_i''$;

$$\begin{cases} u_{ir}(t) = a_i'(r_{ij}(t) - \rho_i''), \\ u_{i\theta}(t) = 0. \end{cases} \tag{6}$$

2. If $\rho_i'' < r_{ij}(t) < \rho_i'$;

$$\begin{cases} u_{ir}(t) = 0, \\ u_{i\theta}(t) = 0. \end{cases} \tag{7}$$

3. If $\rho_i' \leqslant r_{ij}(t) < \rho_i' + \frac{U_i'(t)}{2a_i}$;

$$\begin{cases} u_{ir}(t) = a_i(r_{ij}(t) - \rho_i'), \\ u_{i\theta}(t) = \sigma_i u_{ir}(t). \end{cases} \tag{8}$$

4. If $\rho_i' + \frac{U_i'(t)}{2a_i} \leqslant r_{ij}(t) \leqslant \rho_i' + \frac{U_i'(t)}{a_i}$;

$$\begin{cases} u_{ir}(t) = a_i(r_{ij}(t) - \rho_i'), \\ u_{i\theta}(t) = \sigma_i(U_i'(t) - u_{ir}(t)). \end{cases} \tag{9}$$

Here, $a_i = U_i/(\rho_i - \rho_i')$, $a_i' = V_i(\rho_i'' - \rho_i''')$, $\sigma_i(t) \in [-1, 1]$, V_i is a parameter satisfying $V_i \leqslant U_i$ (the definition is described in [26]), and $U_i'(t) = \max_{0 \leqslant \tau \leqslant t} u_{ir}(\tau)$. By this control method, the relations

$$\rho_i''' \leqslant \rho_i'' - \frac{U_{n+1}}{a_i'} < r_{ij}(t) \leqslant \rho_i' + \frac{U_i'(t)}{a_i} \tag{10}$$

always hold [26], and thus it is enough to design the translational velocity input in the above range. In addition, the parameter $\sigma_i(t)$ affects the shape of the swarm. The larger $|\sigma_i(t)|$, the wider the swarm shape becomes. The control input (6) moves the follower away from its target when they are too close. By (8) and (9), the follower maintains connectivity with its target while satisfying translational limitations (first and second limitations in (3)).

On the other hand, angular velocity input $\omega_i(t)$ is given by

$$\omega_i(t) = k_i \phi_{ij}(t). \tag{11}$$

Here, the feedback gain k_i satisfies

$$\frac{K_i}{\psi_i} \leqslant k_i \leqslant \min\left\{ \frac{\Omega_i}{\psi_i}, \frac{-K_i + \sqrt{K_i^2 + 4\psi_i B_i}}{2\psi_i} \right\}, \tag{12}$$

where $K_i = \max\{V_i/\rho_i''', 3a_iV_i/(2a_i\rho_i' + V_i)\}$. By the control input (11), the follower turns to its target while satisfying rotational limitations (third and fourth limitations in (3)).

When the followers are controlled by (5)–(9) and (11), connectivity maintenance of the whole swarm is achieved by introducing some proper velocity constraints for the leader. Details of leader constraints, the definition of connectivity, the target determination method, and proof of satisfying physical limitations and connectivity maintenance are described in our previous paper [26].

Here, note that we did not consider the case of failure of the leader robot. Robustness against failure is an important issue we leave for future study.

4. Stability Analysis. We show that the shape of the whole swarm and orientation of all followers converge to the equilibrium state when the leader moves at a constant velocity. Since in Sections 4.1 and 4.2 we mainly consider two agents, i and its target j, we hereafter omit the subscripts i and ij for parameters and variables. In addition, let us define the following:

$$r_c := \rho' + \frac{U'}{2a}, \quad r_e := \rho' + \frac{U'}{a}, \quad r_d := \rho'' - \frac{U_{n+1}}{a'}. \tag{13}$$

We assume that agent j moves at constant velocity $\|\boldsymbol{u}_j\| = U^*$, and thus we also assume that σ is a constant. Here, we consider only the case of $\sigma \geqslant 0$, because $\sigma \geqslant 0$ and $\sigma \leqslant 0$ are physically symmetric from the definition of $u_{i\theta}$. By defining θ as the angle between $\boldsymbol{e}_r$ and the moving direction of agent j as

shown in Figure 2 (b), the kinematic model of this motion is given by

$$\dot{r} = U^* \cos\theta - u_{ir}, \tag{14}$$

$$\dot{\theta} = \frac{1}{r}(u_{i\theta} - U^* \sin\theta), \tag{15}$$

$$\dot{\phi} = \frac{1}{r}(U^* \sin\theta - u_{i\theta}) - k\phi = -\dot{\theta} - k\phi. \tag{16}$$

First, we define the equilibrium point.

Definition 1. (Equilibrium point): The equilibrium for a parameter U^* is a point (r_0, θ_0, ϕ_0) that satisfies $\dot{r}|_{r=r_0} = 0$, $\dot{\theta}\big|_{\theta=\theta_0} = 0$, and $\dot{\phi}\big|_{\phi=\phi_0} = 0$, for fixed $U^* \in (0, U']$.

We prove an equilibrium exists for $U^* \in (0, U']$. On the other hand, from (14)–(16), r and θ are independent of ϕ. Therefore, we discuss the convergence of relative position (r, θ) first, and then that of bearing angle ϕ in the following subsection. We hereafter consider θ in $(-\pi, \pi]$.

4.1. Equilibrium point of relative position.

Lemma, 1. (Existence of the equilibrium): Let us consider the system (14) *and* (15). *For $U^* \in (0, U']$, one stable equilibrium point exists in an area $\rho' < r \leqslant r_e$ and $0 \leqslant \theta \leqslant \tan^{-1}\sigma$. Moreover, there is one saddle point in an area $r_d \leqslant r < \rho''$. The equilibrium point (r_0, θ_0) is continuous for U^*, and r_0 is monotonically increasing for U^* if $r > \rho'$, and monotonically decreasing if $r < \rho''$.*

Proof. We divide the proof into two steps:

(step 1): We show the existence of the equilibrium.

1) If $r_d \leqslant r < \rho''$, from (6), (14), (15), and Definition 1, (r_0, θ_0) should satisfy $U^* \cos\theta_0 - a'(r_0 - \rho'') = 0$ and $U^* \sin\theta_0 / r_0 = 0$. Then, we obtain $(r_0, \theta_0) = (\rho'' - U^*/a', \pi)$. We call this point P and define $r_p := \rho'' - U^*/a'$. Point P is obviously continuous and monotonically decreasing for U^*.

2) If $\rho'' \leqslant r \leqslant \rho'$, from (7), (14), and (15), (r_0, θ_0) should satisfy $U^* \cos\theta_0 = 0$ and $-U^* \sin\theta_0 / r_0 = 0$. However, there is no (r_0, θ_0) satisfying these equations simultaneously because of $U^* > 0$.

3) If $\rho' < r < r_c$, from (8), (14), and (15), the equilibrium satisfies

$$\begin{cases} U^* \cos\theta_0 - a(r_0 - \rho') = 0, \\ \sigma a(r_0 - \rho') - U^* \sin\theta_0 = 0. \end{cases} \tag{17}$$

Since $U^* > 0$ and $r_0 > \rho'$, $\sin\theta_0 \geqslant 0$ and $\cos\theta_0 \geqslant 0$ must hold. Then $0 \leqslant \theta_0 \leqslant \pi/2$. From (17), we obtain $\sin\theta_0 - \sigma\cos\theta_0 = 0$ and $\theta_0 = \tan^{-1}\sigma$. Considering $0 \leqslant \theta_0 \leqslant \pi/2$ gives $\cos\theta_0 = 1/\sqrt{1+\sigma^2}$, substituting this into

the first equation in (17), we obtain $(r_0, \theta_0) = (\rho' + U^*/(\sqrt{1+\sigma^2}a), \tan^{-1}\sigma)$ for $U^* \in (0, \sqrt{1+\sigma^2}U'/2)$. This point is continuously in $\rho' < r < r_c$, and r_0 is monotonically increasing for U^*.

4) If $r_c \leqslant r \leqslant r_e$, the equilibrium point satisfies

$$\begin{cases} U^* \cos\theta_0 - a(r_0 - \rho') = 0, \\ a(U' - a(r_0 - \rho')) - U^* \sin\theta_0 = 0, \end{cases} \tag{18}$$

from (9), (14), and (15). Since $U^* > 0$ and $r_0 > \rho'$, $\sin\theta_0 \geqslant 0$ and $\cos\theta_0 > 0$ must hold, and these lead to $0 \leqslant \theta_0 < \pi/2$. From (18), we obtain

$$\sin\theta_0 + \sigma\cos\theta_0 = \frac{\sigma U'}{U^*}, \tag{19}$$

and a condition of existence of θ_0 is $U^* \geqslant \sigma U'/\sqrt{1+\sigma^2}$. Since $\sigma U'/\sqrt{1+\sigma^2} \leqslant \sqrt{1+\sigma^2}U'/2$ holds for any $\sigma \in [0,1]$ and $U' > 0$, the equilibrium point exists continuously in $r_c \leqslant r \leqslant r_e$ for $U^* \in [\sqrt{1+\sigma^2}U'/2, U']$. Since θ_0 ($\geqslant 0$) is monotonically decreasing for U^* from (19), and $\theta_0 = \tan^{-1}\sigma$ at $U^* = \sqrt{1+\sigma^2}U'/2$, we have $\theta_0 \leqslant \tan^{-1}\sigma$. Moreover, r_0 is monotonically increasing for U^*.

(step 2): Next, we discuss the stability of the equilibrium point.

1) If $r_d \leqslant r < \rho''$, from (14) and (15), Jacobi matrix J at equilibrium point P is calculated as follows:

$$J = \begin{bmatrix} \frac{\partial \dot{r}}{\partial r} & \frac{\partial \dot{r}}{\partial \theta} \\ \frac{\partial \dot{\theta}}{\partial r} & \frac{\partial \dot{\theta}}{\partial \theta} \end{bmatrix} = \begin{bmatrix} -a' & 0 \\ 0 & \frac{U^*}{r_0} \end{bmatrix}. \tag{20}$$

The eigenvalue of J is $\lambda = -a', U^*/r_0$, one of which is a negative real number, and the other a positive real number. Thus, P is a saddle point.

2) If $\rho' < r \leqslant r_e$, from (8) and (9), Jacobi matrix J at equilibrium point P is as follows:

$$J = \begin{bmatrix} -a & -U^* \sin\theta_0 \\ J_{21} & -\frac{U^*}{r_0}\cos\theta_0 \end{bmatrix}, \tag{21}$$

where $J_{21} = a\sigma/r_0$ when $\rho' < r_0 < r_c$, and $J_{21} = -a\sigma/r_0$ when $r_c \leqslant r_0 \leqslant r_e$. The characteristic equation of J is $\lambda^2 - (\mathrm{tr}J)\lambda + \det J = 0$, where λ is the

eigenvalue of J. Since $0 \leqslant \theta_0 \leqslant \tan^{-1}\sigma \leqslant \pi/4$ from lemma 1,

$$\mathrm{tr}J = -a - \frac{U^*}{r_0}\cos\theta_0 < 0 \tag{22}$$

$$\begin{aligned}\det J &= \frac{aU^*}{r_0}\cos\theta_0 \pm \frac{aU^*\sigma}{r_0}\sin\theta_0 \\ &\geqslant \frac{aU^*}{r_0}(\cos\theta_0 - \sigma\sin\theta_0) \geqslant 0\end{aligned} \tag{23}$$

are obtained. Here, note that $\det J = 0$ holds if and only if $\sigma = 1$, $U^* = U'/\sqrt{2}$, and $r_c \leqslant r_0 \leqslant r_e$. When $\det J \neq 0$, we have $\mathrm{Re}\lambda < 0$ from Hurwitz's theorem. Moreover, since

$$\begin{aligned}&(\mathrm{tr}J)^2 - 4\det J \\ &\quad = a^2 + \frac{U^{*2}}{r_0^2}\cos\theta_0 + \frac{aU^*}{r_0}(\cos\theta_0 - \sigma\sin\theta_0) > 0\end{aligned} \tag{24}$$

holds, λ is real and $\lambda < 0$.

Thus, the equilibrium is stable.

Next, let us consider the case of $\det J = 0$. In this case, the equilibrium is $(r_0, \theta_0) = (r_c, \pi/4)$, and one of the eigenvectors corresponding to $\lambda = 0$ is $[U^*/(\sqrt{2}a), -1]^T$. Since $\det J = 0$ does not hold in the direction of $r < r_c$, it is enough to consider the direction of the vector $[\Delta r, \Delta\theta]^T = \varepsilon[U^*/(\sqrt{2}a), -1]^T$ for $\varepsilon > 0$. Using a Taylor series in (14) and (15) around the equilibrium (r_0, θ_0), and substituting $[\Delta r, \Delta\theta]^T = \varepsilon[U^*/(\sqrt{2}a), -1]^T$ into them gives

$$\begin{aligned}\dot{r}(r_0 + \Delta r, \theta_0 + \Delta\theta) &= -a\Delta r - U^*\sin\theta_0\Delta\theta - \frac{U^*\cos\theta_0}{2}(\Delta\theta)^2 + \dots \\ &= -\frac{\varepsilon a}{2\sqrt{2}}\Delta r,\end{aligned} \tag{25}$$

$$\begin{aligned}\dot{\theta}(r_0 + \Delta r, \theta_0 + \Delta\theta) &= -\frac{\sigma a}{r_0}\Delta r - \frac{U^*\cos\theta_0}{r_0}\Delta\theta + \frac{\sigma a}{r_0^2}(\Delta r)^2 \\ &\quad + \frac{U^*\sin\theta_0}{2r_0}(\Delta\theta)^2 + \frac{U^*\cos\theta_0}{r_0^2}\Delta r\Delta\theta + \dots \\ &= -\frac{U^*\varepsilon}{2\sqrt{2}r_0}\Delta\theta.\end{aligned} \tag{26}$$

These show the equilibrium attracts points in the direction of $\varepsilon[U^*/(\sqrt{2}a), -1]^T$, and thus the equilibrium point (r_0, θ_0) is stable. □

Now, we discuss the convergence to the equilibrium point. First, we show the convergence of (r, θ), where $r \leqslant \rho'$.

Lemma, 2. (Convergence where $r \leqslant \rho'$): Let us consider the area $r \leqslant \rho'$. If $\theta = \pi$, (r, θ) converges to the saddle point P. If $\theta \neq \pi$, (r, θ) moves to the area $r > \rho'$ through $-\pi/2 \leqslant \theta \leqslant \pi/2$.

Proof. First, we consider the case in which the state converges to the saddle point P. Suppose $\theta(t') = \pi$ at the initial time t'. If $\rho'' < r(t') \leqslant \rho'$ and $\theta(t') = \pi$, we obtain $\dot{r} = -U^*$ and $\theta(t) = \pi$ from (7), (14), and (15). This means that r monotonically decreases until $r \leqslant \rho''$, while $\theta(t) = \pi$ is maintained. If r becomes $r \leqslant \rho''$, we obtain $\dot{r} = -U^* - a'(r - \rho'')$ and $\theta(t) = \pi$ from (6). Solving this equation under the initial condition $r(t_0) = \rho''$ gives $r(t) = \rho'' - U^*(1 - \exp(-a'(t - t_0)))/a' \to r_p$ as $t \to \infty$. Thus, (r, θ) converges to the saddle point P. The same discussion also holds if $r_d \leqslant r(t') \leqslant \rho''$.

Next, we consider the case in which $\theta \neq \pi$. Figure 3 shows the vector field where $r_d \leqslant r \leqslant \rho'$. Here, note that $r \geqslant r_d$ always holds as shown in [26]. The curved line in the area $r_p \leqslant r \leqslant \rho''$ shows $\theta = \cos^{-1}\{a'(r - r_p)/U^* - 1\}$, and $\dot{r} = 0$ holds on this line. Further, point (r, π) and $(r, -\pi)$ are the same point in the 2-D environment. Since the vector field is symmetrical concerning $\theta = 0$, we hereafter discuss the case where $\theta \geqslant 0$.

Let us divide the area $r \in [r_d, \rho']$ and $\theta \in [0, \pi)$ into the following four regions, as shown in Figure 3. The arrows in Figure 3 show the direction of velocity vector; that is, the possible region to which the state moves.

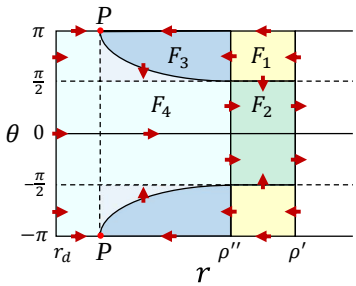


Fig. 3. Velocity field for $r \leqslant \rho'$

1) If (r, θ) is in the region F_1, $\theta = \pi$ will never hold, and the state moves to F_2 or F_3.

2) If (r, θ) is in the region F_2, $\theta < 0$ will never hold, and the state moves to the area $r > \rho'$.

3) If (r, θ) is in the region F_3, $\theta = \pi$ will never hold, and the state moves to F_4.

4) If (r,θ) is in the region F_4, $\theta=\pi$ and $\theta<0$ will never hold, and the state moves to F_2.

From these we find that (r,θ) always moves to the area $r>\rho'$ via the region F_2. Here, note that the same result is achieved in the case of $\theta\geqslant 0$ because of the symmetry of the vector field concerning to $\theta=0$. □

Note also that the convergence to the saddle point occurs only in limited situations, such as when the leader moves straight toward the follower whose target is the leader.

Next, we show the convergence of (r,θ) where $r>\rho'$. If the state starting from $r>\rho'$ becomes $(r,\theta)=(\rho',\pi)$, the state converges to the saddle point P from Lemma 2. Thus, we hereafter discuss the other case. First, we introduce the following theorems used in the proof.

Theorem, 1. (Poincaré-Bendixson Theorem [28]): Let $\boldsymbol{f}\in\mathbb{R}^2$ be a C^1 function $\mathbb{R}^2\to\mathbb{R}^2$. If the equilibrium points of the differential equation $\dot{\boldsymbol{x}}=\boldsymbol{f}(\boldsymbol{x})$ are isolated, and the solution is bounded for $t\geqslant 0$, then either

1. $\omega(\boldsymbol{x}(0))$ is an equilibrium point, or

2. $\omega(\boldsymbol{x}(0))$ is a periodic orbit, or

3. $\alpha(\boldsymbol{y})$ and $\omega(\boldsymbol{y})$ are equilibrium points for each $\boldsymbol{y}\in\omega(\boldsymbol{x}(0))$,

where $\alpha(\boldsymbol{x}(0))$ and $\omega(\boldsymbol{x}(0))$ are an α-limit set and ω-limit set, respectively, of $\dot{\boldsymbol{x}}=\boldsymbol{f}(\boldsymbol{x})$ with the initial condition $\boldsymbol{x}(0)$.

Since our system has non-C^1 input $u_{i\theta}$, we divide the whole region into the following four subregions to apply theorem 1 to our problem:

$$D_1=\left\{(r,\theta)\ :\ \rho'<r<\rho'+\frac{U^*}{a}\cos\theta,\ -\frac{\pi}{2}<\theta<\frac{\pi}{2}\right\}, \tag{27}$$

$$D_2=\begin{cases}\left\{(r,\theta)\ :\ \rho'<r<\min\left\{r_e,\rho'+\frac{U^*}{\sigma a}\sin\theta\right\},\ 0<\theta<\pi\right\} & \\ \qquad\qquad (0<\sigma\leqslant 1), & \\ \{(r,\theta)\ :\ \rho'<r<r_e,\ 0<\theta<\pi\} \qquad (\sigma=0), & \end{cases} \tag{28}$$

$$D_3=\begin{cases}\left\{(r,\theta)\ :\ \max\left\{\rho',r_e-\frac{U^*}{\sigma a}\sin\theta\right\}<r<r_e,\ 0<\theta<\pi\right\} & \\ \qquad\qquad (0<\sigma\leqslant 1), & \\ \{(r,\theta)\ :\ \rho'<r\leqslant r_e,\ 0<\theta<\pi\} \qquad (\sigma=0), & \end{cases} \tag{29}$$

$$D_4=\left\{(r,\theta)\ :\ \rho'<r\leqslant r_e,\ -\pi<\theta\leqslant\pi\right\}\setminus(D_1\cup D_2\cup D_3). \tag{30}$$

Here, note that $\dot{r}>0$ on D_1 from (14), and $\dot{\theta}<0$ on D_2 and D_3 from (15).

Since the characteristics of the velocity field are changed according to (r_0,θ_0) and σ, we consider the convergence in the following four cases: case 1 ($\sigma=0$); case 2 ($\sigma\neq 0$ and $U^*<U'/2$); case 3 ($\sigma\neq 0$ and $U'/2\leqslant U^*<$

$\sqrt{1+\sigma^2}U'/2$); and case 4 ($\sigma \neq 0$ and $\sqrt{1+\sigma^2}U'/2 \leqslant U^* \leqslant U'$). Figure 4 shows the subregions D_1, D_2, D_3, and D_4 for the corresponding cases, and the arrows show the direction of the velocity field on the boundaries of the regions. In case 1, we define the following region D as shown in Figure 5 (a):

$$D = \left\{ (r,\theta) \ : \ \rho' < r \leqslant r_e, \ |\theta| < \frac{\pi}{2} \right\}. \tag{31}$$

For case 2, any r on D_1 satisfies $r < r_c$. A region D for case 2 is defined as follows (see Figure 5 (b)):

$$D = \left\{ (r,\theta) \ : \ \rho' < r < \min\left\{ \rho' + \frac{U^*}{\sigma a}, \ r_c \right\}, \ |\theta| < \frac{\pi}{2} \right\}. \tag{32}$$

For case 3, there exists an r satisfying $r \geqslant r_c$ on D_1, and $r_0 < r_c$. A region D in this case is defined as shown in Figure 5 (c). In case 4, there exists an r satisfying $r \geqslant r_c$ on D_1, and $r_0 \geqslant r_c$. A region D in this case is defined as shown in Figure 5 (d). Now, we show that the trajectory is included in the region D after a certain time.

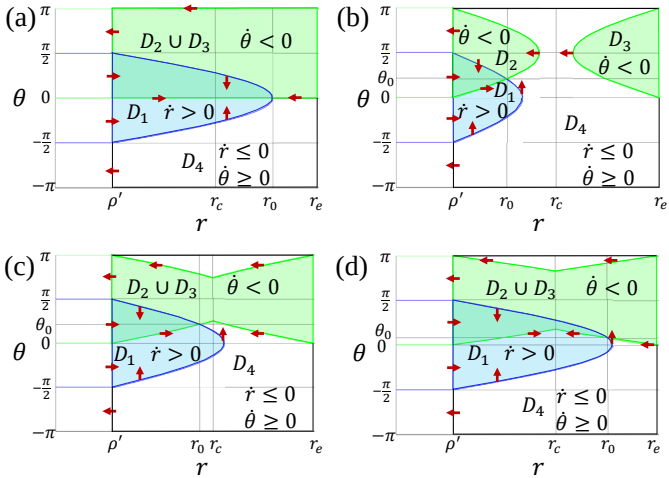


Fig. 4. Velocity fields: (a) Case 1; (b) Case 2; (c) Case 3; (d) Case 4

Lemma, 3. For any initial state $(r(0),\theta(0)) \in (\rho', r_e] \times (-\pi, \pi]$, *there exists* $\tau \geqslant 0$ *such that* $(r(t),\theta(t)) \in D$ *for any* $t \geqslant \tau$.

Proof. For case 1, we divide the whole region into the subregions as shown in Figure 4 (a). Because of the characteristics of the velocity field in

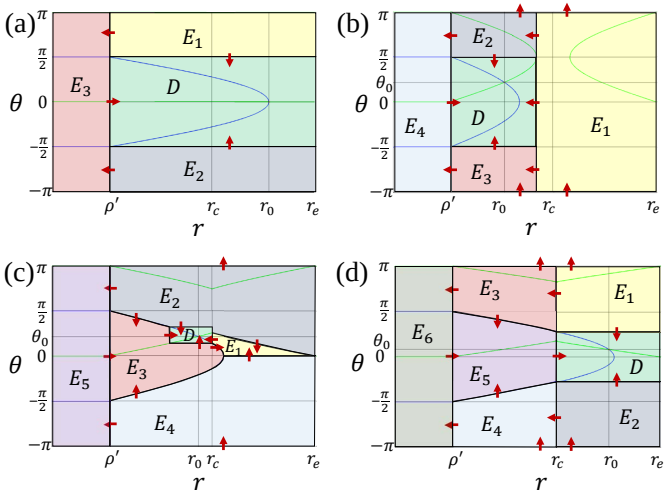


Fig. 5. Divided regions: (a) case 1; (b) case 2; (c) case 3; (d) case 4

case 1, once the trajectory goes inside region D, it stays in D. Thus, we discuss the cases where the initial state is not on D:

1) If (r, θ) is in region E_1 defined in Figure 5 (a); the state goes into D or E_3 defined in Figure 5 (a).

2) If (r, θ) is in the region E_2 defined in Figure 5 (a); the state goes into D or E_3.

3) If (r, θ) is in the region E_3; the state goes into D by Lemma 2.

Thus, in case 1, we found that the state goes into D from any initial state. In other cases, we can show that the state goes into D in the same manner. Therefore, the state goes into D from any initial state in all cases. □

For case 1, $\dot{r}$ and $\dot{\theta}$ in D are C^1 functions of r and θ from (8) and (9). The trajectory is bounded after the state enters D from Lemma 3. Further, the equilibrium is isolated from Lemma 1. Thus, the trajectory behavior for $t \to \infty$ is limited to three cases in Theorem 1.

Since

$$\frac{\partial \dot{r}}{\partial r} + \frac{\partial \dot{\theta}}{\partial \theta} = -a - \frac{U^*}{r} \cos\theta < 0 \tag{33}$$

on D from (8), (9), (14), and (15), there is no periodic orbit by Bendixson's criterion [29], and thus the second case in Theorem 1 is negated. In addition, since there is just one equilibrium on D and there is no trajectory that starts from the equilibrium from Lemma 1, the third case in Theorem 1 is also

negated. Thus, the trajectory that starts from any point on D converges to the equilibrium. The trajectory after a certain time is included in D from Lemma 3, and thus the trajectory from any initial state converges to the equilibrium. For cases 2, 3, and 4, we can show that the trajectory from any initial state converges to the equilibrium in the same manner as in case 1.

4.2. Equilibrium point of bearing angle.

Lemma, 4. (Convergence of bearing angle): Consider the system (16). *For any initial condition* $\phi(t') \in [-\psi, \psi]$, $\phi(t) \to 0$ *as* $t \to \infty$.

Proof. From section 4.1, $\dot{\theta} \to 0$ as $t \to \infty$. If $\dot{\theta}(t) = 0$, solving (16) gives $\phi(t) = \exp(-k(t-t'))\phi(t')$. For arbitrary initial value $\phi(t') \in [-\psi, \psi]$, $\phi(t)$ converges to 0 as $t \to \infty$. Moreover, $\phi(t) \in [-\psi, \psi]$ always holds as shown in [26]. Therefore, from the converging-input and converging-state theorem [30], $\phi(t) \to 0$ as $t \to \infty$. □

The equilibrium state of bearing angle $\phi = 0$ means that the agent is always aiming at its target. Since the relative positions of follower i and its target j converges, the orientation η of follower i converges to the equilibrium state.

4.3. Stability of the whole swarm. Sections 4.1 and 4.2 show that the relative position, bearing angle, and orientation of agent i and its target j converge to the equilibrium if the target j moves at a constant velocity. When the leader moves at a constant velocity, the velocity of follower j, whose target is the leader, converges to that of the leader. Now, let agent k be an agent whose target is agent j, and define r_k, θ_k, and α_j as shown in Figure 6.

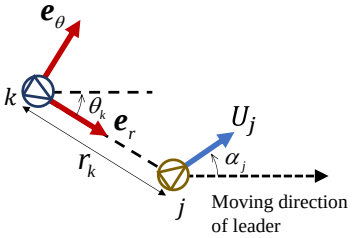


Fig. 6. Definition of r_k, θ_k, and α_j

In this subsection, we hereafter omit the subscript k. The kinematic model of this motion is written as follows:

$$\dot{r} = U_j \cos(\theta + \alpha_j) - u_{kr}, \tag{34}$$

$$\dot{\theta} = \frac{1}{r}\{u_{k\theta} - U_j \sin(\theta + \alpha_j)\}, \tag{35}$$

where U_j is the velocity of agent j, θ is the angle between $\boldsymbol{e}_r$ and the moving direction of the leader, and α_j is the angle between U_j and the moving direction of the leader.

Here, note that kinematic model (34) and (35) become (14) and (15) when $U_j = U^*$. To show the stability of the system (34) and (35), we need to show the boundedness of r and θ. From [26], r is bounded. To show the boundedness of θ, we rewrite (34) and (35) as follows:

$$\dot{r} = U^* \cos\theta - u_{kr} + \mu_r, \tag{36}$$

$$\dot{\theta} = \frac{1}{r}(u_{k\theta} - U^* \sin\theta + \mu_\theta), \tag{37}$$

where $\mu_r = U_j \cos(\theta + \alpha_j) - U^* \cos\theta$, and $\mu_\theta = -U_j \sin(\theta + \alpha_j) + U^* \sin\theta$.

Here, μ_r and μ_θ are bounded because U_j and U^* are bounded. Moreover, since $U_j \to U^*$ and $\alpha_j \to 0$ as $t \to \infty$ from Section 4.1, $\mu_r \to 0$ and $\mu_\theta \to 0$ as $t \to \infty$. That is, for any $\varepsilon > 0$, there exists $T > 0$ such that $|\mu_r| < \varepsilon$ and $|\mu_\theta| < \varepsilon$ hold for $t > T$. This means that we can consider arbitrarily small μ_r and μ_θ (i.e., arbitrarily small $|U_j - U^*|$ and $|\alpha_j|$) after a sufficient period of time.

Here, note that $\dot{\theta}$ is bounded [26], and thus θ is bounded within a sufficiently large finite time. Therefore, we investigate the boundedness of θ after a sufficient period of time.

To show the boundedness of θ after a large enough lapse of time – that is, (34) and (35) with arbitrarily small $|U_j - U^*|$ and $|\alpha_j|$ – we use the same procedures described in Section 4.1. Now, we divide the whole region into the following four subregions:

$$D_1 = \left\{ (r,\theta) \ : \ 0 < r < \rho' + \frac{U_j}{a}\cos(\theta + \alpha_j),\ -\frac{\pi}{2} < \theta + \alpha_j < \frac{\pi}{2} \right\}. \tag{38}$$

$$D_2 = \begin{cases} \left\{ (r,\theta) \ : \ 0 < r < \min\left\{ r_e, \rho' + \frac{U^*}{\sigma a}\sin(\theta + \alpha_j) \right\},\ 0 < \theta + \alpha_j < \pi \right\} \\ \qquad\qquad (0 < \sigma \leqslant 1), \\ \left\{ (r,\theta) \ : \ 0 < r < r_e,\ 0 < \theta + \alpha_j < \pi \right\} \qquad (\sigma = 0), \end{cases} \tag{39}$$

$$D_3 = \begin{cases} \left\{ (r,\theta) \ : \ \max\left\{ 0, r_e - \frac{U^*}{\sigma a}\sin(\theta + \alpha_j) \right\} < r \leqslant r_e,\ 0 < \theta + \alpha_j < \pi \right\} \\ \qquad\qquad (0 < \sigma \leqslant 1), \\ \left\{ (r,\theta) \ : \ 0 < r \leqslant r_e,\ 0 < \theta + \alpha_j < \pi \right\} \qquad (\sigma = 0). \end{cases} \tag{40}$$

Here, note that $\dot{r} > 0$ on D_1 from (34), and $\dot{\theta} < 0$ on D_2 and D_3 from (35), and the remaining part, D_4, is (30).

In addition, we consider the following four cases; case 1 ($\sigma = 0$); case 2 ($\sigma \neq 0$ and $U^* \leqslant U'/2$); case 3 ($\sigma \neq 0$ and $U'/2 < U^* < \sqrt{1+\sigma^2}U'/2$); and case 4 ($\sigma \neq 0$ and $\sqrt{1+\sigma^2}U'/2 \leqslant U^* \leqslant U'$). Figure 7 (a), (b), (c), and (d) show the properties of the velocity fields for cases 1, 2, 3, and 4, respectively.

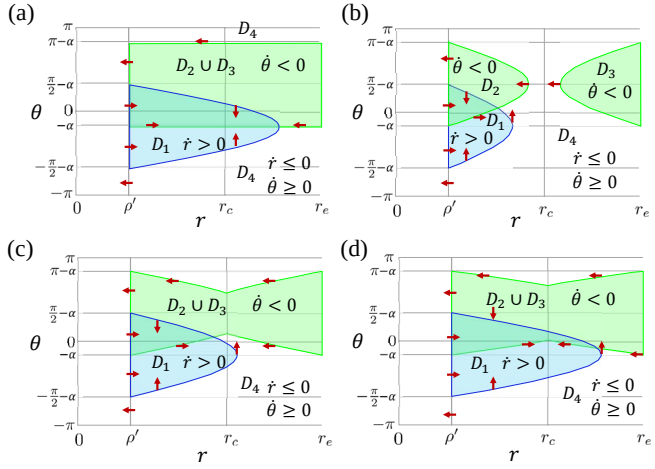


Fig. 7. Properties of the velocity fields

Lemma, 5. (Boundedness of perturbation): In all cases, θ of the kinematic model (34) *and* (35) *with arbitrarily small $|U_j - U^*|$ and $|\alpha_j|$ is bounded.*

Proof. For cases 1, 3, and 4, we found that $D_2 \cap D_3 \neq \emptyset$. Further, from the characteristics of the velocity fields (Fig. 7 (a), (c), and (d)), the state cannot move by stepping over $D_2 \cup D_3$. Thus, θ is bounded. On the other hand, in case 2, we can show that the state goes into D and it stays in D forever, as shown in the proof of Lemma 3, where

$$D = \left\{ (r,\theta) \ : \ \rho' < r < \min\left\{ r_e, \rho' + \frac{U^*}{\sigma a} \right\}, \right. \\ \left. -\frac{\pi}{2} - \alpha_j < \theta < \frac{\pi}{2} - \alpha_j \right\}. \qquad (41)$$

Thus, θ is bounded for case 2. □

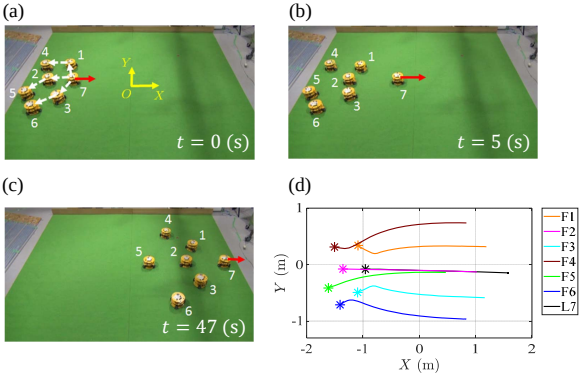


Fig. 8. Experimental environment and trajectories of agents: (a)–(c) Screenshots of experiment; (d) trajectories of all agents

To summarize, the kinematic model (36) and (37) has the following properties: $\mu_r \to 0$ and $\mu_\theta \to 0$ as $t \to \infty$; (36) and (37) become (14) and (15) when $\mu_r = 0$ and $\mu_\theta = 0$; and r and θ are bounded.

Applying the converging-input and converging-state theorem [30], we found that the state (r, θ) of agent k converges to the equilibrium, and its translational velocity converges to that of the leader. Then, since $\dot{\theta} \to 0$, bearing angle ϕ of agent k also converges to the equilibrium point from the Section 4.2. This procedure can be applied to any agent l, whose target is the leader, or agent j, or agent k. Therefore, all agents eventually converge to the equilibrium, and the velocity consensus is achieved. Finally, this section is summarized in the following theorem.

Theorem, 2. (Stability of the whole swarm): If the leader moves at a constant velocity, the control inputs (5)–(9) *and* (11) *realize the following: the shape of the swarm and orientation of all followers converge to the equilibrium state, and the velocity consensus is achieved for all agents.*

5. Experimental Results. We carried out an experiment to confirm the stability of the swarm robots by our control method. We used 7 omnidirectional robots controlled by velocity commands via Bluetooth. Here, the translational velocity and angular velocity of robots could be controlled independently. A motion-capture system measured the positions and orientations of robots. The system was centrally controlled, but the controller for each agent used only local information. Therefore, the controller in this experiment was decentralized. The sampling time was 0.1 (s), and the specifications of follower i are listed in Table 1.

Table 1. Specifications of Followers in the Experiment

Follower i	1	2	3	4	5	6
ρ_i	1.00	0.90	1.00	0.85	0.95	0.80
ρ_i'	0.60	0.55	0.60	0.55	0.55	0.50
ρ_i''	0.40	0.35	0.40	0.40	0.35	0.30
ψ_i	$\pi/4$	$\pi/6$	$\pi/5$	$\pi/4$	$\pi/5$	$\pi/5$
A_i	0.5	0.5	0.5	0.5	0.5	0.5
Ω_i	$2\pi/5$	$\pi/3$	$2\pi/5$	$2\pi/5$	$3\pi/5$	$2\pi/5$
B_i	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$
σ_i	1.0	0.0	-1.0	1.0	0.0	-1.0
V_i	0.19	0.16	0.18	0.19	0.17	0.15
k_i	1.00	1.22	1.12	1.00	1.12	1.12

Table 2. Specifications of Followers in the Numerical Simulation.

i	1	2	3	4	5	6	7	8	9	10
ρ_i	4.1	4.0	4.0	4.8	5.3	4.2	5.9	5.0	6.7	4.0
ρ_i'	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
ρ_i''	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
ψ_i	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$
A_i	0.3	0.4	0.6	0.5	0.5	0.9	0.9	0.7	0.4	0.6
Ω_i	$3\pi/4$	$2\pi/3$	$\pi/2$	$2\pi/3$	$2\pi/3$	$\pi/2$	$2\pi/3$	$3\pi/4$	$2\pi/3$	$2\pi/3$
B_i	π	$3\pi/4$	$\pi/2$	$2\pi/3$	$3\pi/4$	π	$\pi/2$	π	$3\pi/4$	$3\pi/4$
σ_i	0.0	0.0	1.0	1.0	1.0	-1.0	-1.0	-1.0	0.0	1.0
V_i	0.30	0.34	0.36	0.36	0.37	0.47	0.41	0.43	0.34	0.39
k_i	1.37	1.50	1.22	1.41	1.50	1.73	1.22	1.73	1.50	1.50

The leader moved in a straight line at a moving speed first of 0.15 (m/s), then decelerating to 0.045 (m/s) at $t = 5$ (s). This motion makes U' larger for each robot, which resulted in the wider shape of the swarm. Here, note that the purpose of this experiment is not to show that the proposed controller is also applicable when the speed of the leader changes. Figure 8 contains screenshots and shows the trajectories of all agents. In Figure 8 (a), the red arrow shows the leader's moving direction, and the white arrows indicate connectivity, pointing from a follower to a target. Here, the symbol '$*$' shows the initial position of the corresponding robot, and F1, $\cdots$, F6 are the followers, while L7 is the leader. On the other hand, Figure 9 (a), (b), and (c) show the error between each state and its equilibrium point $r - r_0$, $\theta - \theta_0$, and $\phi - \phi_0$, respectively. From these results, the errors converge to zero, and thus the convergence of the state (r, θ, ϕ) is confirmed.

6. Simulation Results. We carried out a numerical simulation to investigate the stability of the swarm robots by our control method for a larger number of robots. In the simulation, we used one leader and 10 followers, and the specifications of follower i are listed in Table 2. In the

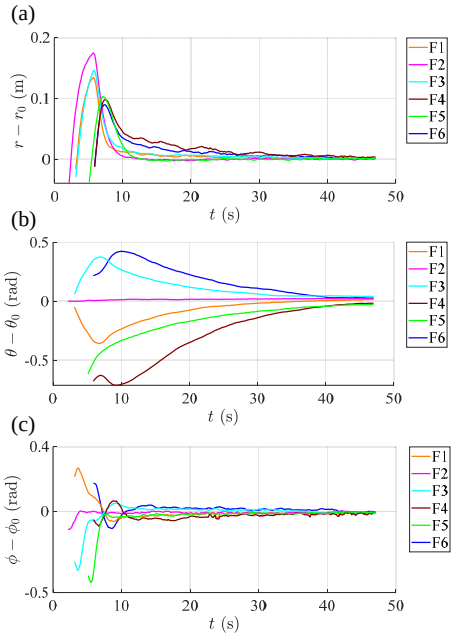


Fig. 9. Experimental results: (a) $r - r_0$. (b) $\theta - \theta_0$. (c) $\phi - \phi_0$

numerical simulation, the leader moved in a straight line, and the leader's initial moving speed was 0.30 (m/s), followed by deceleration to 0.15 (m/s) at $t = 25$ (s), as in the case of the experiment.

Figure 10 shows the simulation results. Figure 10 (a) shows the trajectories of all agents. In this figure, all agents were near the origin at the initial time, then moved in the positive X-axis direction, where F1, $\cdots$, F10 are the followers, while L11 is the leader. On the other hand, Figure 10 (b), (c), and (d) show the error between each state and its equilibrium point $r - r_0$, $\theta - \theta_0$, and $\phi - \phi_0$, respectively. From these results, we found that the errors converge to zero, and thus the convergence of the state (r, θ, ϕ) is confirmed by the numerical simulation.

7. Conclusions. This paper presented a stability analysis of a decentralized navigation method for heterogeneous swarm robots with a limited field of view. Each robot had unique abilities in terms of velocity, acceleration, and sensing region. We proved that the swarm shape and orientation of the followers converged to the equilibrium state when the leader moved at a constant velocity. We also confirmed the stability of an experiment and

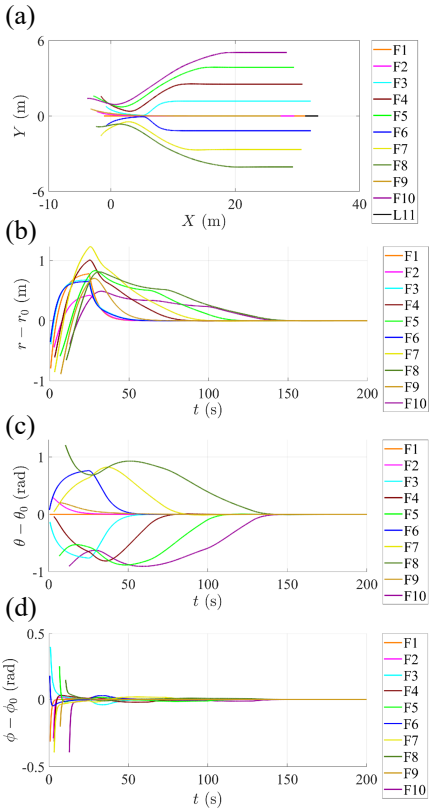


Fig. 10. Simulation results: (a) trajectories of all agents; (b) $r - r_0$; (c) $\theta - \theta_0$; (d) $\phi - \phi_0$

numerical simulation. Future work will be focused on collision avoidance with robots or environmental obstacles by designing the $\boldsymbol{e}_\theta$ component of the control input. We will also investigate line-of-sight (LOS) maintenance between robots, which is important if the robot is equipped with a distance or visual sensor.

References

1. E. Şahin, Swarm Robotics: From Sources of Inspiration to Domains of Application. Swarm Robotics. 2005. pp. 10–20.
2. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective. *Swarm Intell*. 2013. vol. 7. pp. 1–41.
3. Bayindir L. A review of swarm robotics tasks. *Neurocomputing*. 2016. vol. 172. pp. 292–321.

4. Ge X. et al. A survey on recent advances in distributed sampled-data cooperative control of multi-agent systems. *Neurocomputing*. 2018. vol. 275. pp. 1684–1701.
5. Chung S. et al. Survey on Aerial Swarm Robotics. *IEEE Trans. Robot.*. 2018. vol. 34. pp. 837–855.
6. Nedjah N., Junior L.S. Review of methodologies and tasks in swarm robotics towards standardization. *Swarm and Evolutionary Computation*. 2019. vol. 50. pp. 100565.
7. Kantaros Y., Thanou M., Tzes A. Distributed coverage control for concave areas by a heterogeneous Robot-Swarm with visibility sensing constraints. *Automatica*. 2015. vol. 53. pp. 195–207.
8. Teruel E., Aragues R., López-Nicolás G. A distributed robot swarm control for dynamic region coverage. *Robot. Auton. Syst.*. 2012. vol. 32. pp. 81–95.
9. Durham J.W., Franchi A., Bullo F. Distributed pursuit-evasion without mapping or global localization via local frontiers. *Auton. Robot.*. 2012. vol. 32. pp. 81–95.
10. Garcia-Aunon P., Roldán J., Barrientos A. Monitoring traffic in future cities with aerial swarms: Developing and optimizing a behavior-based surveillance algorithm. *Cognitive Systems Research*. 2019. vol. 54. pp. 273–286.
11. Kim T., Sugie T. Cooperative control for target-capturing task based on a cyclic pursuit strategy. *Automatica*. 2007. vol. 43. pp. 1426–431.
12. Kawakami H., Namerikawa T. Cooperative target-capturing strategy for multivehicle systems with dynamic network topology. Proc. of 2009 American Control Conference. 2009. pp. 635–640.
13. Miyata N., Ota J., Arai T., Asama H. Cooperative transport by multiple mobile robots in unknown static environments associated with real-time task assignment. *IEEE Trans. Robot. Autom.*. 2002. vol. 18. pp. 769–780.
14. Chen J. et al. Occlusion-Based Cooperative Transport with a Swarm of Miniature Mobile Robots. *IEEE Trans. Robot.*. 2015. vol. 31. pp. 307–321.
15. Xu M. et al. Collective Crowd Formation Transform with Mutual Information–Based Runtime Feedback. *Comput. Graph. Forum.*. 2015. vol. 34. pp. 60–73.
16. Kobayashi Y., Endo T., Matsuno F. Distributed formation for robotic swarms considering their crossing motion. *Journal of the Franklin Institute*. 2018. vol. 355. pp. 8698–8722.
17. Dorigo M. et al. Swarmanoid: A Novel Concept for the Study of Heterogeneous Robotic Swarms. *IEEE Robot. Autom. Mag.*. 2013. vol. 20. pp. 60–71.
18. Sabattini L., Secchi C., Chopra N. Decentralized Estimation and Control for Preserving the Strong Connectivity of Directed Graphs. *IEEE Trans. Cybern.*. 2015. vol. 45. pp. 2273–2286.
19. Filotheou A., Nikou A., Dimarogonas D.V. Robust decentralised navigation of multi-agent systems with collision avoidance and connectivity maintenance using model predictive controllers. *Int. J. Control*. 2020. vol. 93. no. 6. pp. 1470–1484.
20. Yoo S.J., Park B.S. Connectivity preservation and collision avoidance in networked nonholonomic multi-robot formation systems: Unified error transformation strategy. *Automatica*. 2019. vol. 103. pp. 274–281.
21. Yoshimoto M., Endo T., Maeda R., Matsuno F. Decentralized navigation method for a robotic swarm with nonhomogeneous abilities. *Auton. Robots*. 2018. vol. 42. pp. 1583–1599.
22. Panagou D., Kumar V. Cooperative Visibility Maintenance for Leader–Follower Formations in Obstacle Environments. *IEEE Trans. Robot.*. 2014. vol. 30. pp. 831–844.
23. Delimpaltadakis I.M., Bechlioulis C.P., Kyriakopoulos K.J. Decentralized Platooning With Obstacle Avoidance for Car-Like Vehicles With Limited Sensing. *IEEE Robot. Autom. Lett.*. 2018. vol. 3. pp. 835–840.
24. Liu X., Ge S.S., Goh C. Vision-Based Leader–Follower Formation Control of Multiagents With Visibility Constraints. *IEEE Trans. Control Syst. Technol.*. 2019. vol. 27. pp. 1326–1333.

25. Poonawala H.A., Spong M.W. Cooperative visibility maintenance in SE(3) for multirobot-networks with limited field-of-view sensors. *Control Theory Technol.*. 2017. vol. 15. pp. 246–257.
26. Maeda R., Endo T. Matsuno F. Decentralized Navigation for Heterogeneous Swarm Robots With Limited Field of View. *IEEE Robotics and Automation Letters*. 2017. vol. 2. pp. 904–911.
27. Endo T., Maeda R. Matsuno F. Stability Analysis for Heterogeneous Swarm Robots with Limited Field of View. Proc. of 2019 Developments in eSystems Engineering (DeSE). 2019. pp. 27–32.
28. Alligood K.T., Sauer T.D., Yorke J.A. Chaos: An introduction to dynamical systems. Springer. 1996. 358 p.
29. Li Y., Muldowney J.S. On Bendixson's criterion. *J. Differ. Equations*. 1993. vol. 106. pp. 27–39.
30. Sontag E.D. A remark on the converging-input converging state property. *IEEE Trans. Automat. Contr.*. 2003. vol. 48. pp. 313–314.

Takahiro Endo — Ph.D., Associate Professor, Kyoto University. Research interests: robotics, haptics, and control of infinite dimensional system. The number of publications — 43. endo@me.kyoto-u.ac.jp; C3, Kyodai Katsura, Nishikyo-ku, 615-8540, Kyoto, Japan; office phone: 81-75-383-3595; fax: +81-75-383-3595.

Ryuma Maeda — Master's Student, Department of Mechanical Engineering and Science, Kyoto University. Research interests: control of multi-agent system. The number of publications — 3. ray501.itsme182@gmail.com; C3, Kyodai Katsura, Nishikyo-ku, 615-8540, Kyoto, Japan; office phone: +81-75-383-3595; fax: +81-75-383-3595.

Fumitoshi Matsuno — Ph.D., Professor, Department of Mechanical Engineering and Science, Kyoto University. Research interests: robotics, swarm intelligence, control of distributed parameter system and nonlinear system, rescue support system in disaster. The number of publications — 181. matsuno@me.kyoto-u.ac.jp; C3, Kyodai Katsura, Nishikyo-ku, 615-8540, Kyoto, Japan; office phone: +81-75-383-3595; fax: +81-75-383-3595.

Acknowledgements. This work was supported in part by JST SICORP Grant Number JP-MJSC18E4, Japan.

УДК 004.9 **DOI** 10.15622/ia.2020.19.5.2

Т. Эндо, Р. Маэда, Ф. Мацуно

АНАЛИЗ УСТОЙЧИВОСТИ РОЯ ГЕТЕРОГЕННЫХ РОБОТОВ С ОГРАНИЧЕННЫМ ПОЛЕМ ЗРЕНИЯ

Эндо Т., Маэда Р., Мацуно Ф. **Анализ устойчивости роя гетерогенных роботов с ограниченным полем зрения.**

Аннотация. Представлен анализ устойчивости роя роботов – группы различных роботов. Исследование ориентировано на рой роботов с гетерогенными способностями, где каждый робот имеет разный уровень чувствительности сенсоров и различные физические ограничения, включая максимальную скорость движения и ускорения. Каждый робот обладает уникальной областью восприятия в условиях ограниченного угла обзора. Изначально предлагался децентрализованный метод навигации для роя роботов с гетерогенными способностями, состоящего из ведущего робота и многочисленных ведомых роботов. С децентрализованным методом навигации ведущий робот может направлять ведомых, поддерживая соединение и учитывая физические ограничения, уникальные для каждого робота; то есть каждый ведомый робот имеет ведущего робота и следует за ним с учетом его физических ограничений. Данное исследование сосредоточено на анализе устойчивости такого роя роботов с гетерогенными способностями. С математической точки зрения доказывается, что когда ведущий робот двигается с постоянной скоростью, форма и направления всех остальных ведомых роботов в конечном счете стремятся к равновесию. Чтобы продемонстрировать совпадение этого состояния равновесия, сперва необходимо доказать, что оно существует. Проводятся эксперименты и численные моделирования, чтобы подтвердить наличие стабильности, то есть достижение роем роботов состояния равновесия.

Ключевые слова: устойчивость, рой роботов, навигация, децентрализованный контроллер

Эндо Такахиро — Ph.D., доцент, Киотский университет. Область научных интересов: робототехника, тактильные ощущения и управление бесконечномерными системами. Число научных публикаций — 43. endo@me.kyoto-u.ac.jp; Кёдай Катсура, Нисикё-ку, С3, 615-8540, Киото, Япония; р.т.: 81-75-383-3595; факс: +81-75-383-3595.

Маэда Рёма — студент магистратуры, кафедра машиностроения и науки, Киотский университет. Область научных интересов: управление мультиагентной системой. Число научных публикаций — 3. ray501.itsme182@gmail.com; Кёдай Катсура, Нисикё-ку, С3, 615-8540, Киото, Япония; р.т.: +81-75-383-3595; факс: +81-75-383-3595.

Мацуно Фумитоси — Ph.D., профессор, кафедра машиностроения и науки, Киотский университет. Область научных интересов: робототехника, разведка роя, управление системой распределенных параметров и нелинейной системой, система поддержки спасения при бедствиях. Число научных публикаций — 181. matsuno@me.kyoto-u.ac.jp; Кёдай Катсура, Нисикё-ку, С3, 615-8540, Киото, Япония; р.т.: +81-75-383-3595; факс: +81-75-383-3595.

Поддержка исследований. Работа выполнена при частичной финансовой поддержке Японского агентсва науки и технологий "Программа стратегических международных совместных исследований" (номер гранта JPMJSC18E4).

Литература

1. *Şahin E.* Swarm Robotics: From Sources of Inspiration to Domains of Application // Swarm Robotics. 2005. pp. 10–20.
2. *Brambilla M., Ferrante E., Birattari M., Dorigo M.* Swarm robotics: a review from the swarm engineering perspective // Swarm Intell. 2013. vol. 7. pp. 1–41.
3. *Bayindir L.* A review of swarm robotics tasks // Neurocomputing. 2016. vol. 172. pp. 292–321.
4. *Ge X. et al.* A survey on recent advances in distributed sampled-data cooperative control of multi-agent systems // Neurocomputing. 2018. vol. 275. pp. 1684–1701
5. *Chung S. et al.* Survey on Aerial Swarm Robotics // IEEE Trans. Robot. 2018. vol. 34. pp. 837–855.
6. *Nedjah N., Junior L.S.* Review of methodologies and tasks in swarm robotics towards standardization // Swarm and Evolutionary Computation. 2019. vol. 50. pp. 100565.
7. *Kantaros Y., Thanou M., Tzes A.* Distributed coverage control for concave areas by a heterogeneous Robot-Swarm with visibility sensing constraints // Automatica. 2015. vol. 53. pp. 195–207.
8. *Teruel E., Aragues R., López-Nicolás G.* A distributed robot swarm control for dynamic region coverage // Robot. Auton. Syst. 2019. vol. 119. pp. 51–63.
9. *Durham J.W., Franchi A., Bullo F.* Distributed pursuit-evasion without mapping or global localization via local frontiers // Auton. Robot. 2012. vol. 32. pp. 81–95.
10. *Garcia-Aunon P., Roldán J., Barrientos A.* Monitoring traffic in future cities with aerial swarms: Developing and optimizing a behavior-based surveillance algorithm // Cognitive Systems Research. 2019. vol. 54. pp. 273–286.
11. *Kim T., Sugie T.* Cooperative control for target-capturing task based on a cyclic pursuit strategy // Automatica. 2007. vol. 43. pp. 1426–431.
12. *Kawakami H., Namerikawa T.* Cooperative target-capturing strategy for multivehicle systems with dynamic network topology // Proc. of 2009 American Control Conference. 2009. pp. 635–640.
13. *Miyata N., Ota J., Arai T., Asama H.* Cooperative transport by multiple mobile robots in unknown static environments associated with real-time task assignment // IEEE Trans. Robot. Autom. 2002. vol. 18. pp. 769–780.
14. *Chen J. et al.* Occlusion-Based Cooperative Transport with a Swarm of Miniature Mobile Robots // IEEE Trans. Robot. 2015. vol. 31. pp. 307–321.
15. *Xu M. et al.* Collective Crowd Formation Transform with Mutual Information–Based Runtime Feedback // Comput. Graph. Forum. 2015. vol. 34. pp. 60–73.
16. *Kobayashi Y., Endo T., Matsuno F.* Distributed formation for robotic swarms considering their crossing motion // Journal of the Franklin Institute. 2018. vol. 355. pp. 8698–8722.
17. *Dorigo M. et al.* Swarmanoid: A Novel Concept for the Study of Heterogeneous Robotic Swarms // IEEE Robot. Autom. Mag. 2013. vol. 20. pp. 60–71.
18. *Sabattini L., Secchi C., Chopra N.* Decentralized Estimation and Control for Preserving the Strong Connectivity of Directed Graphs // IEEE Trans. Cybern. 2015. vol. 45. pp. 2273–2286.
19. *Filotheou A., Nikou A., Dimarogonas D.V.* Robust decentralised navigation of multi-agent systems with collision avoidance and connectivity maintenance using model predictive controllers // Int. J. Control. 2020. vol. 93. no. 6. pp. 1470–1484.
20. *Yoo S.J., Park B.S.* Connectivity preservation and collision avoidance in networked nonholonomic multi-robot formation systems: Unified error transformation strategy // Automatica. 2019. vol. 103. pp. 274–281.

21. *Yoshimoto M., Endo T., Maeda R., Matsuno F.* Decentralized navigation method for a robotic swarm with nonhomogeneous abilities // Auton. Robots. 2018. vol. 42. pp. 1583–1599.
22. *Panagou D., Kumar V.* Cooperative Visibility Maintenance for Leader–Follower Formations in Obstacle Environments // IEEE Trans. Robot. 2014. vol. 30. pp. 831–844.
23. *Delimpaltadakis I.M., Bechlioulis C.P., Kyriakopoulos K.J.* Decentralized Platooning With Obstacle Avoidance for Car-Like Vehicles With Limited Sensing // IEEE Robot. Autom. Lett. 2018. vol. 3. pp. 835–840.
24. *Liu X., Ge S.S., Goh C.* Vision-Based Leader–Follower Formation Control of Multiagents With Visibility Constraints // IEEE Trans. Control Syst. Technol. 2019. vol. 27. pp. 1326–1333.
25. *Poonawala H.A., Spong M.W.* Cooperative visibility maintenance in SE(3) for multirobot-networks with limited field-of-view sensors // Control Theory Technol. 2017. vol. 15. pp. 246–257.
26. *Maeda R., Endo T. Matsuno F.* Decentralized Navigation for Heterogeneous Swarm Robots With Limited Field of View // IEEE Robotics and Automation Letters. 2017. vol. 2. pp. 904–911.
27. *Endo T., Maeda R. Matsuno F.* Stability Analysis for Heterogeneous Swarm Robots with Limited Field of View // Proc. of 2019 Developments in eSystems Engineering (DeSE). 2019. pp. 27–32.
28. *Alligood K.T., Sauer T.D., Yorke J.A.* Chaos: An introduction to dynamical systems // Springer. 1996. 358 p.
29. *Li Y., Muldowney J.S.* On Bendixson's criterion // J. Differ. Equations. 1993. vol. 106. pp. 27–39.
30. *Sontag E.D.* A remark on the converging-input converging state property // IEEE Trans. Automat. Contr. 2003. vol. 48. pp. 313–314.

УДК 621.391 **DOI** 10.15622/ia.2020.19.5.3

А.В. Паршуткин, Д.И. Бучинский

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ КАНАЛА СПУТНИКОВОЙ СВЯЗИ В УСЛОВИЯХ ИСКАЖЕНИЙ СЛУЖЕБНОЙ ЧАСТИ КАДРОВ НЕСТАЦИОНАРНЫМИ ПОМЕХАМИ

Паршуткин А.В., Бучинский Д.И. **Модель функционирования канала спутниковой связи в условиях искажений служебной части кадров нестационарными помехами.**

Аннотация. Рассмотрены основные способы организации современных спутниковых систем связи и используемые в них способы синхронизации и передачи служебной информации, а также механизм кадровой синхронизации с точки зрения помехоустойчивости. На основании проведенного анализа предложена структурная схема имитационной модели для исследования влияния непреднамеренных помех на каналы современных спутниковых систем связи. Предлагаемая модель воздействия нестационарных помех на канал спутниковой связи учитывает влияние помех на символьную и кадровую синхронизации, механизмы выделения границ кадра, а также действие современных кодов исправления ошибок. Модель позволяет оценить влияние нестационарных помех как на информационную, так и на служебную части кадра современных систем широкополосной спутниковой связи. В качестве показателя помехоустойчивости канала спутниковой связи используется вероятность потери кадра, то есть пропуска кадра ввиду нарушения в системе кадровой синхронизации, неверного выделения границ кадра либо наличия в кадре ошибок, которые не были исправлены корректирующими кодами. С использованием указанной модели проведено исследование влияния нестационарных помех различной длительности на информационную и служебную части кадра, сравнение результатов воздействия нестационарных помех различной длительности с воздействием белого гауссовского шума. Показано, что нестационарные помехи, представляющие собой короткие шумовые импульсы, которые не влияют на информационную часть кадра, из-за исправления кодами коррекции могут снижать качество приема ввиду нарушения работы кадровой синхронизации и искажения служебной информации о сигнально-кодовой конструкции и длине кадра.

Ключевые слова: *DVB*-S2, *DVB-RCS*, кадровая синхронизация, нестационарная помеха, помехоустойчивость, широкополосная спутниковая связь

1. Введение. В настоящее время возрастают требования пользователей к объемам передаваемых данных и скорости передачи информации через спутниковые системы связи. Эффективное использование ограниченного частотного ресурса обеспечивается созданием сетей широкополосной спутниковой связи с применением временного и частотного разделения каналов, а также протоколов, адаптивных к условиям распространения *DVB-S2X* и *DVB-RCS* (*Digital Video Broadcasting – Return Channel via Satellite*) [1-4].

Широко известны исследования помехозащищенности каналов спутниковой связи для стационарных помех [5-10], в то время как для нестационарных помех такие исследования проведены только для частных случаев [11-15]. Процесс влияния импульсных и структурных помех на процессы синхронизации при передаче данных описан в [11, 12], однако влияние помех на служебную часть кадра современных систем широкополосной спутниковой связи не исследовалось.

В [14, 15] описано воздействие нестационарных помех на каналы спутниковой связи, использующие протоколы *DVB-S*2 и *DVB-RCS*, исследованы результаты воздействия непреднамеренных стационарных и нестационарных помех с равной средней мощностью. Однако в работе не рассматривалось влияние нестационарных помех на процессы синхронизации и демультиплексирования кадров физического уровня. Описанная в [14] модель не позволяет исследовать влияние согласованности повторения импульсных помех и длительности кадра на характеристики помехоустойчивости.

Целью статьи является исследование помехозащищенности канала спутниковой связи при воздействии нестационарных помех с учетом их влияния на подсистему кадровой и символьной синхронизаций и передачи служебной информации.

2. Способы синхронизации и передачи служебной информации в сетях широкополосной спутниковой связи с коммутацией пакетов. Как известно, свод правил, определяющих взаимодействие функциональных блоков одного уровня в сети связи, называется протоколом [3]. Анализ различных протоколов спутниковой связи показывает, что в достаточно общем случае служебная информация передаваемого кадра включает:

– синхросигнал, обеспечивающий канал подстройки частоты, канал временной синхронизации;

– адресную часть с информацией о параметрах системы, идентификатор отправителя и назначение;

– блок контроля достоверности кадра;

– блок управления;

– элементы внутреннего и иного (расширенного) взаимодействия, относящиеся к фирменной части оборудования, как правило, их назначение не разглашается даже при применении открытых стандартов связи [3].

Блок управления, в свою очередь, может включать следующие элементы:

– каналы управления общие (поиска и запроса доступа на связь);

– каналы управления качеством канала связи (управления мощностью передатчика, сигнально-кодовой конструкцией, видом кодирования);

– выделенные каналы управления, в которых в зависимости от напряженности трафика и вида используемого протокола могут формироваться подканалы, обеспечивающие требуемый вид обслуживания [2].

Рассмотрим, как реализуются процессы синхронизации и передачи служебной информации физического и канального

уровней в современных сетях широкополосной спутниковой связи на примере сетей, использующих протоколы *DVB-S*2, *DVB-S*2*X*, *DVB-RCS*, *DVB-RCS*2.

Особенностью протоколов *DVB-S*2, *DVB-S*2*X* является механизм адаптации к помеховой обстановке и меняющимся условиям распространения сигнала, что особенно актуально, так как данные протоколы рассчитаны на использование в диапазонах K_u и K_a, для которых характерно существенное влияние погодных условий на величину затухания сигнала. Адаптация достигается введением режимов переменного кодирования и модуляции (англ. *Variable Coding and Modulation*) и адаптивного кодирования и модуляции (англ. *Adaptive Coding and Modulation*) [16]. Суть первого режима состоит в использовании различных видов модуляции и кодирования для передачи информации, имеющей разный приоритет. Второй режим предполагает выбор оптимального режима кодирования и модуляции в зависимости от условий на трассе распространения сигнала и приема. Оба режима реализованы посредством введения кадров физического уровня с заголовками, включающими информацию о режиме использованного в кадре кодирования и модуляции, а также синхроинформации. Введение в протоколы кадров физического уровня обусловлено тем, что служебная информация, содержащаяся в этих кадрах, необходима для выполнения функций, свойственных физическому уровню модели *OSI* (*Open System Interconnection*). Несмотря на фиксированный размер кадра в битах, за счет возможности изменения модуляции меняется и длительность кадра, что обуславливает использование старт-стопной кадровой синхронизации.

Протоколы *DVB-S*2, *DVB-S*2*X*, *DVB-RCS*, *DVB-RCS*2 предполагают возможность организации сетей с топологией звезда (рис. 1а) и ячеистой топологией (рис. 1б). В первом случае все абоненты (A_1, A_2 … A_m) связаны между собой через центральную земную станцию (ЦЗС).

Прямой канал, то есть канал от ЦЗС до абонентов представляет собой непрерывный широкополосный поток, состоящий из кадров физического уровня с заголовками (ЗГ). В прямом канале применяется временное разделение. Пакеты и кадры протоколов более высоких уровней передаются с помощью непрерывного сигнала с использованием инкапсуляции общего потока (англ. *Generic Stream Encasualtion*). Абоненты принимают весь поток прямого канала, осуществляют его анализ и демультиплексирование. Данные от абонентов до ЦЗС передается по обратному каналу, который в указанных протоколах организуется по технологии *MF-TDMA* (*Multi-Frequency Time-Division Multiple Access)*, обеспечивающей

эффективное использование доступного частотного ресурса [16-19]. Таким образом, обратный канал представляет собой совокупность частотных каналов (f_1 … f_n) и временных слотов (ВС1, ВС2 и т.д.), которые динамически распределяются между абонентами. Причем одному абоненту выделяются в различные временные слоты различные частоты, как показано на рисунке 1в. В каждый временной интервал, который может состоять из нескольких временных слотов, на одной частоте излучается отдельная посылка.

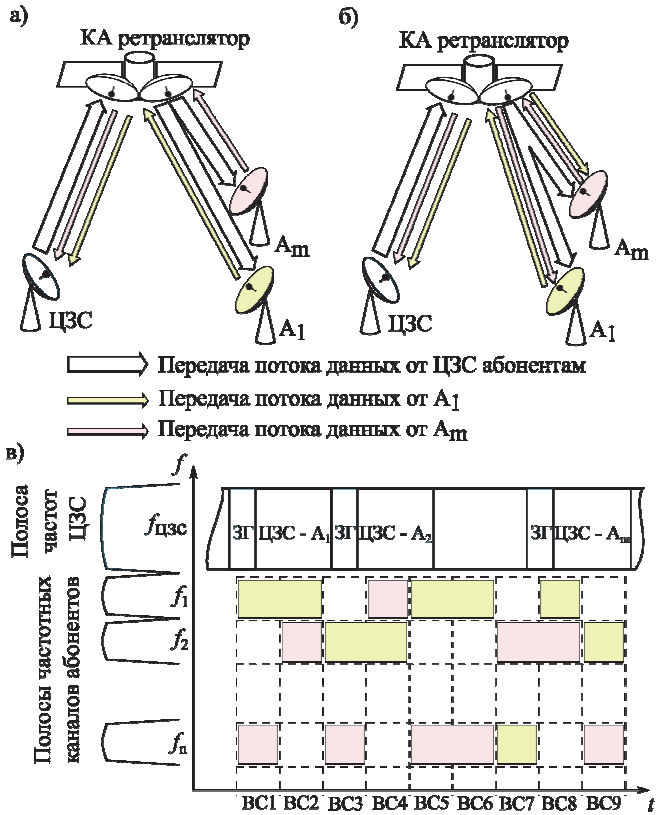


Рис. 1. Топологии сетей спутниковой связи и каналы передачи данных: а) топология звезда; б) ячеистая топология; в) частотно-временная структура каналов передачи данных

Очевидным недостатком такой топологии является двойная передача части трафика и существенная задержка сигнала при двойной ретрансляции сигнала спутником в случае связи абонентов между собой.

Например, для передачи данных от абонента A_1 абоненту A_m необходимо сначала передать их по обратному каналу на ЦЗС, где они будут включены в общий поток и переданы по прямому каналу. Однако такая организация сети позволяет обойтись абонентам лишь *DVB-S*2 совместимыми приемниками, которые значительно проще приемников *DVB-RCS*2. Кроме того, нередки случаи, когда трафик между отдельными абонентами незначителен, а обмен информацией происходит в основном между абонентом и ЦЗС. Это уменьшает количество информации, которую необходимо передавать через спутник дважды.

Другой предусмотренной стандартом *DVB-RCS*2 топологией спутниковой сети связи является ячеистая топология [2]. В данном случае абоненты также используют обратный канал, организованный по технологии *MF-TDMA*, а ЦЗС – прямой канал, представляющий собой непрерывный *DVB-S*2 поток. Основным отличием является возможность прямой передачи данных от одного абонента другому, минуя центральную земную станцию. Это требует от абонентов возможности принимать обратный канал, а значит, использовать более сложные *DVB-RCS*2 приемники.

Важно отметить, что во всех рассмотренных топологиях для корректной реализации технологии *MF-TDMA* необходимо, чтобы каждая земная станция излучала посылки в строго отведенных временных слотах и на определенных частотах. При этом необходимо учитывать тот факт, что ввиду различного пути распространения задержка сигнала от разных земных станций будет отличаться. Для того чтобы не происходило наложения посылок из соседних тайм слотов, необходимо их излучать с определенными задержками. Кроме того, важное значение имеет оптимальное распределение имеющегося частотного ресурса между земными станциями с учетом их приоритета. Поэтому необходима синхронизация всей сети. В обоих рассмотренных случаях функцию синхронизации и согласования сети выполняет центральная земная станция путем передачи пакетов синхронизации сети (*Network Clock Reference*), пакетов и таблиц со специальной информацией. Причем как пакеты синхронизации сети, так и служебная информация передается в виде *DVB-S2* или *DVB-S2X* потока. На рисунке 2 показан принцип формирования и передачи пакета синхронизации [2].

Заголовок кадра физического уровня состоит из последовательности начала кадра (ПНК), называемой в стандарте [1] *SOF* (*Start of Frame*) и информационной части заголовка (ИЧЗ) соответственно – *PLSCODE* (*Physical Layer Signaling Code*). В определенные ЦЗС моменты времени заголовок кадра физического уровня формирует пусковой сигнал. Регистр-защелка по этому сигналу запоминает значение счетчика опорного генератора сети и записывает

его в специальное поле пакета синхронизации сети, который передается в теле n + 2-го кадра физического уровня. Поэтому синхронизация всей системы зависит от возможности абонентов корректно принимать *DVB-S*2 сигнал.

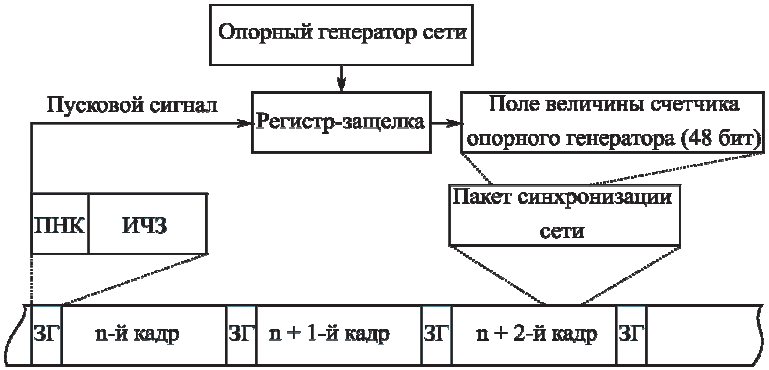


Рис. 2. Порядок формирования пакетов синхронизации сети и передачи их в *DVB-S*2 потоке

Синхронизация абонентов в сетях широкополосной спутниковой связи обеспечивается как по элементам сигнала (тактовая, символьная синхронизация), так и по различным блокам (группам) этих элементов (кадровая синхронизация) [1, 3, 14]. Для непрерывного контроля за состоянием системы синхронизации синхросигналы передаются в каждом кадре. Рассмотрим порядок работы блока кадровой синхронизации (рис. 3) [1].

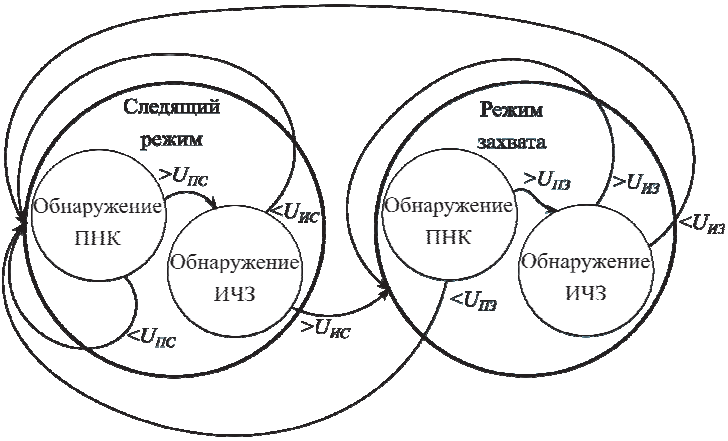


Рис. 3. Структурно-логическая схема кадровой синхронизации

Сначала блок кадровой синхронизации, находясь в следящем режиме, ищет последовательность начала кадра путем корреляционной свертки со всеми поступающими отсчетами. Сразу после превышения порога обнаружения ПНК в следящем режиме $U_{ПС}$ (0,61) производится корреляционное сравнение последующих 64 символов со всеми 128 возможными вариантами ИЧЗ. Если при этом будет превышен порог для ИЧЗ в следящем режиме $U_{ИС}$ (0,88), то принимается решение об обнаружении кадра, а блок кадровой синхронизации переходит в режим захвата.

В режиме захвата блок кадровой синхронизации не производит корреляционной свертки со всеми поступающими отсчетами, а на основании информации, полученной из ИЧЗ, вычисляет, где должна появиться следующая последовательность начала кадра. Начиная с предполагаемого места производится вычисление величины корреляции с последовательностью начала кадра. Если порог обнаружения ПНК в режиме захвата $U_{ПЗ}$ (0,36) не превышен, то блок возвращается в режим слежения, если же порог превышен, то производится проверка следующих 64 символов на наличие в них ИЧЗ аналогично тому, как это происходило в режиме слежения, но с использованием порога для ИЧЗ в режиме захвата $U_{ИЗ}$ (0,65). Если принимается решение, что обнаружен кадр, то блок остается в режиме захвата, в противном случае блок переходит в режим слежения [2]. Относительно высокие пороги в следящем режиме позволяют достичь малых величин ложной тревоги, и в то же время относительно малые пороги в режиме захвата обеспечивают низкую вероятность пропуска кадра.

Известно, что в сетях широкополосной спутниковой связи используется синхронный метод обеспечения кадровой синхронизации, при котором синхроинформация, заложенная в принимаемом сигнале, играет корректирующую роль для запуска приемника. С позиций помехоустойчивости спутниковой системы связи это означает, что искажение элемента синхронизации не сразу приводит к выходу из синхронизма и искажению сообщения, что обеспечивает относительно высокую помехозащищенность системы кадровой синхронизации [10].

В отличии от синхросигнала, остальные элементы служебной части кадра необходимы для корректного восстановления принятой информации и ошибки при ее приеме могут приводить к потере переданной информации с необходимостью ее повторной передачи. А в ряде случаев при использовании в протоколе кадров переменной длины эта информация необходима и для поддержания кадровой синхронизации [20, 21].

Наличие выделенных элементов синхронизации и иных блоков служебной информации в структуре кадра приводит к возможности возникновения сбоев в выделении границ кадра при воздействии помех на эти элементы. Причем качество приема информации существенно зависит от того, в какую часть передаваемого кадра попадает помеха. Для исследования данной зависимости разработана имитационная модель функционирования канала спутниковой связи в условиях воздействия нестационарных помех.

3. Модель канала спутниковой связи в условиях воздействия нестационарных помех. Для исследования влияния нестационарных помех на канал передачи информации от ЦЗС абонентам была использована имитационная модель, схема которой показана рисунке 4.

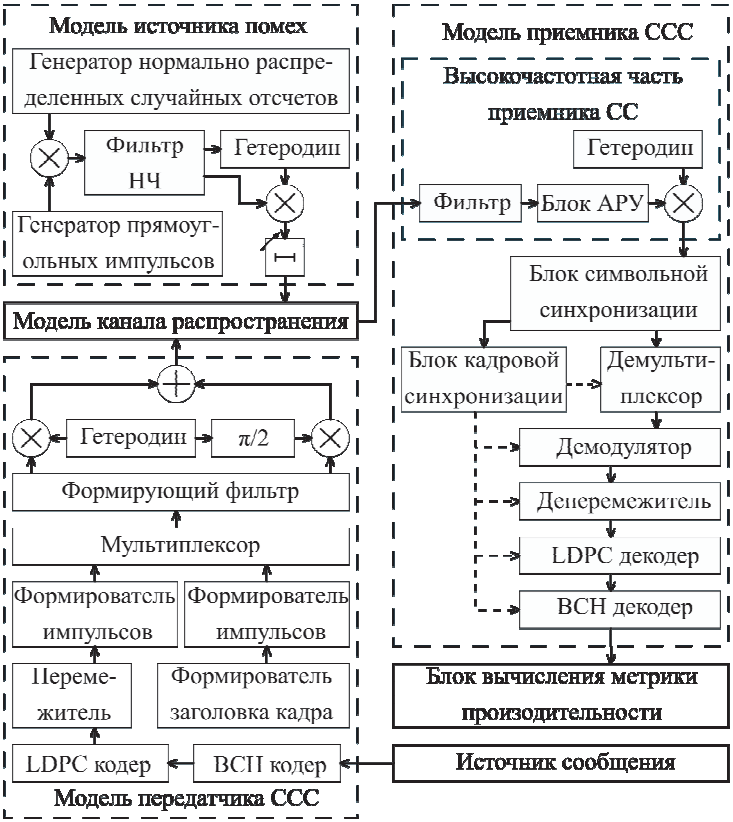


Рис. 4. Структурная схема имитационной модели спутникового канала связи

Модель предусматривает внутреннее и внешнее кодирование источника сообщения с использованием *LDPC* (*Low Density Parity Check*) кодов и кодов Боуза – Чодхури – Хоквингема (БЧХ), а также перемежение. Добавление заголовка кадра физического уровня в зависимости от выбранного вида модуляции и режима кодирования, состоящего из последовательности начала кадра длиной 26 бит и семи битов служебной информации, которые закодированы в 64 бита ИЧЗ. Из битов заголовка и информационной части кадра получают канальные символы, соответствующие используемой модуляции, с последующей повышающей передискретизацией. Недостающие отсчеты заполняют нулями, и получается последовательность канальных импульсов. Они сглаживаются формирующим фильтром с амплитудно-частотной характеристикой $H(f)$ типа корень квадратный из приподнятого косинуса [1]:

$$H(f)=\begin{cases}1.0 & ,|f|\le\dfrac{1-\alpha}{2T};\\ \dfrac{1}{\sqrt{2}}\sqrt{1+cos\left(\dfrac{\pi T}{\alpha}\left[|f|-\dfrac{1-\alpha}{2T}\right]\right)} & ,\dfrac{1-\alpha}{2T}<|f|\le\dfrac{1+\alpha}{2T};\\ 0 & ,\text{в других случаях,}\end{cases} \qquad (1)$$

где f – частота; α – фактор сглаживания фильтра; T – период следования канальных импульсов.

Импульсная характеристика $h(t)$ такого фильтра имеет вид:

$$h(t)=\begin{cases}\dfrac{1}{T}\left(1+\alpha\left(\dfrac{4}{\pi}-1\right)\right) & ,t=0;\\ \dfrac{\alpha}{T\sqrt{2}}\left[\left(1+\dfrac{2}{\pi}\right)sin\left(\dfrac{2}{4\alpha}\right)+\left(1-\dfrac{2}{\pi}\right)cos\left(\dfrac{2}{4\alpha}\right)\right] & ,t=\pm\dfrac{T}{4\alpha};\\ \dfrac{1}{T}\dfrac{sin\left[\pi(t/T)(1-\alpha)+4\alpha(t/T)cos\left[\pi(t/T)(1+\alpha)\right]\right]}{\pi(t/T)\left[1-\left(4\alpha(t/T)\right)^2\right]} & ,\text{в других случаях.}\end{cases} \qquad (2)$$

В качестве фактора сглаживания фильтра использовался $\alpha = 0{,}35$, поскольку в этом случае сигнал наиболее устойчив к выбранному типу помех, а период следования канальных импульсов выбран $T = 1$мкс. Выбор параметра сглаживания обусловлен тем, что

такой параметр сглаживания обеспечивает наибольшую устойчивость к используемому типу непреднамеренных помех. Полученные импульсы поступают в квадратурный модулятор, который формирует сигнал на промежуточной частоте.

Применение таких фильтров обусловлено необходимостью предотвращения межсимвольного искажения при ограничении полосы излучения. Однако, как видно из формулы (2), импульсная характеристика фильтра в моменты времени $t = nT$, $n \in \mathbb{N}$ не равна нулю, то есть такой фильтр не обеспечивает отсутствие межсимвольного искажения в моменты дискретизации. Это связано с тем, что на приемной стороне сигнал будет подвергнут обработке согласованным фильтром, то есть фильтром с такой же импульсной и амплитудно-частотной характеристиками. Такой подход позволяет повысить отношение сигнал-шум за счет использования согласованного фильтра и избежать межсимвольного искажения в моменты дискретизации при ограниченной полосе излучения.

Синфазная $I_{tx}(t)$ и квадратурная $Q_{tx}(t)$ составляющие видеосигнала после формирующего фильтра представляют собой:

$$I_{tx}(t) = \sum_{n=0}^{N-1} \int_{-\infty}^{+\infty} I_n \delta(\tau - nT) h(t-\tau) d\tau; \tag{3}$$

$$Q_{tx}(t) = \sum_{n=0}^{N-1} \int_{-\infty}^{+\infty} Q_n \delta(\tau - nT) h(t-\tau) d\tau, \tag{4}$$

где I_n – n-й канальный символ синфазного канала; Q_n – n-й канальный символ квадратурного канала; $h(\tau)$ – импульсная характеристика формирующего фильтра, связанная с $H(f)$ преобразованием Фурье; N – количество символов в кадре.

Затем для получения сигнала на промежуточной частоте $S(t)$ синфазная и квадратурная составляющие умножаются на гармонические колебания промежуточной частоты f_{np}, сдвинутые на $\pi/2$, и складываются:

$$S(t) = I_{tx}(t)\cos(2\pi f_{np} t) - Q_{tx}(t)\sin(2\pi f_{np} t). \tag{5}$$

В модели канала распространения формируется аддитивная смесь сигнала $S(t)$, нестационарной помехи $\xi(t)$ в виде помехового импульса длительностью τ_n и белого гауссовского шума $\eta(t)$,

соответствующего приведенным ко входу собственным шумам приемника. Полученная смесь обрабатывается моделью приемника спутникового канала связи. В высокочастотной части производится обработка полученного сигнала блоком автоматической регулировки усиления (АРУ) и перенос на видеочастоту с получением синфазной $I_{rx}(t)$ и квадратурной $Q_{rx}(t)$ составляющих принятой реализации.

Затем сигнал поступает в блок символьной синхронизации, схема которого представлена на рисунке 5.

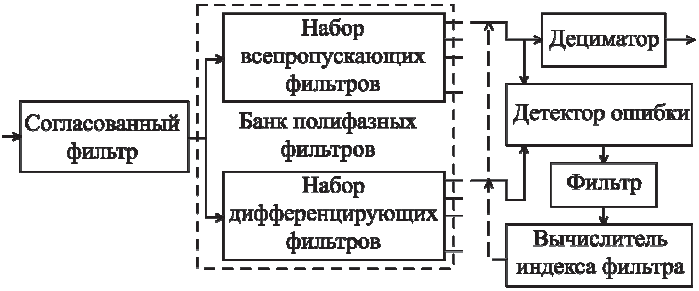


Рис. 5. Структурная схема блока символьной синхронизации

В блоке символьной синхронизации поступающий сигнал подвергается обработке согласованным фильтром. Таким образом, канальные импульсы в спутниковом канале подвергаются последовательной обработке двумя фильтрами с импульсной характеристикой (2). Один раз при формировании видеосигнала на стороне передатчика и один раз на приемной стороне, что эквивалентно обработке их одним фильтром импульсная характеристика которого $h_{\Sigma}(t)$ представляет собой свертку импульсных характеристик формирующего и согласованного фильтров:

$$h_{\Sigma}(\mathrm{t}) = \sin\left(\frac{t}{T}\right)\frac{\cos\left(\dfrac{\pi\alpha t}{T}\right)}{1-\dfrac{4\alpha^2 t^2}{T^2}}. \qquad (6)$$

Как видно из формулы (6), отклик фильтров на каждый канальный импульс равен амплитуде импульса в момент времени $t = 0$ и равен нулю в моменты времени, кратные периоду повторения

импульсов T. Поскольку формирующий и согласованный фильтры являются линейными элементами, то отклик от последовательности канальных импульсов равен сумме откликов от каждого импульса в последовательности. Поэтому импульсы не будут влиять друг на друга в моменты времени $t = nT$, $n \in \mathbb{N}$ и могут быть точно восстановлены на принимающей стороне. При этом полоса частот, занимаемая сигналом, ограничена, и сигнал не оказывает помехового воздействия на соседние каналы.

В реальном приемнике тактовая частота опорного генератора может отличаться от таковой частоты опорного генератора передатчика, время распространения сигнала неизвестно и может меняться, а для корректного восстановления исходного сигнала необходимо выбрать значения отсчетов в моменты времени, когда отсутствует межсимвольное искажение. Для этого сигнал после согласованного фильтра поступает в банк полифазных фильтров, который состоит из двух наборов фильтров. Первый представляет собой набор всепропускающих параллельных фильтров с различными постоянными групповыми временами задержки $\tau_{ГВЗi}$, второй – набор дифференцирующих параллельных фильтров с такими же постоянными групповыми временами задержки. То есть в банке для каждого значения группового времени задержки присутствует пара фильтров – всепропускающий и дифференцирующий. Сигнал с одной из таких пар поступает в блок вычисления ошибки, где формируется сигнал ошибки дискретизации. Сглаживаемый фильтром сигнал ошибки служит для вычисления номера пары фильтров, отсчеты которых наилучшим образом соответствуют моментам дискретизации в передатчике.

На рисунке 6 приведены примеры сигналов на выходах трех пар фильтров. Сигналы на выходе всепропускающих фильтров $S_{api}(t,\tau_{ГВЗi})$ показаны сплошными линиями, а их значения в моменты дискретизации – точками. Жирными точками обозначены отсчеты, которые будут оставлены для дальнейшей обработки после децимации. Сигналы, обработанные дифференцирующими фильтрами $S_{difi}(t,\tau_{ГВЗi})$, показаны пунктиром, а их значения в моменты дискретизации – квадратами. Как видно из рисунка 6, сигналу на выходе дифференцирующего фильтра с нулевым значением отсчета в момент времени t = 3 мкс соответствует интерполирующий фильтр с идеальными моментами дискретизации.

Затем в блоке символьной синхронизации сигнал, обработанный выбранным фильтром, время групповой задержки которого обеспечивает наилучшую символьную синхронизацию, поступает в

дециматор, где осуществляется понижающая дискретизация путем оставления отсчета, который соответствует моменту времени с отсутствием межсимвольных искажений. Остальные отсчеты отбрасываются. За счет выбора способа формирования сигнала ошибки такой алгоритм символьной синхронизации соответствует алгоритму Гарднера [22].

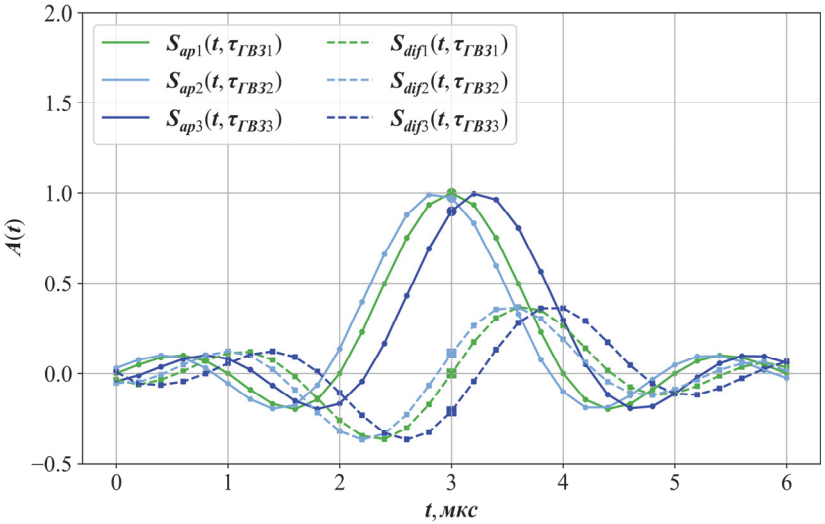


Рис. 6. Пример сигналов на выходах интерполирующих и дифференцирующих фильтров блока символьной синхронизации

После обработки блоком символьной синхронизации сигнал, представленный одним отсчетом на символ, поступает в блок кадровой синхронизации, который формирует кадровые синхроимпульсы. С их помощью в демультиплексоре определяются границы кадра и выделяется информационная часть кадра. Последняя подвергается демодуляции, деперемежению, декодированию *LDPC* и БЧХ декодерами и передается в блок вычисления метрики производительности. В этом блоке происходит сравнение переданной и принятой информации для вычисления метрики производительности спутникового канала передачи данных.

Временные диаграммы полученных сигналов и помех представлены на рисунке 7.

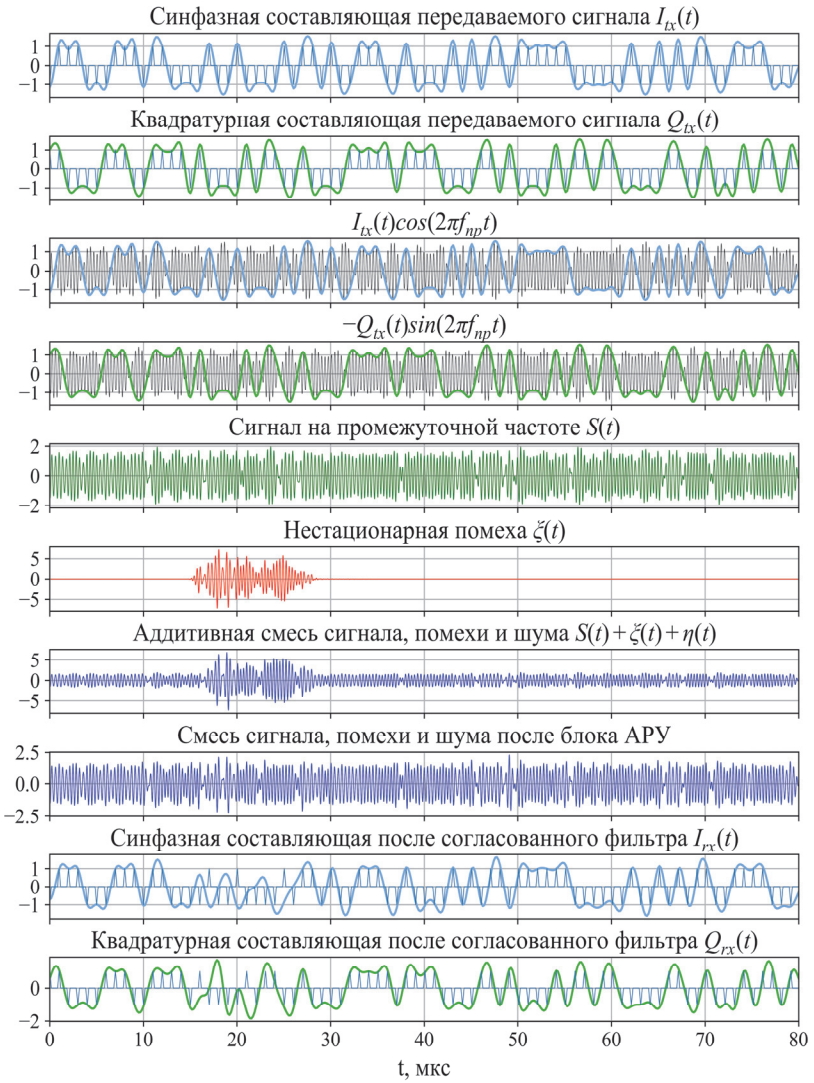


Рис. 7. Временные диаграммы передаваемого и принятого сигналов и помехи

4. Анализ устойчивости каналов спутниковой связи к воздействию нестационарных помех. С помощью описанной выше имитационной модели было проведено исследование устойчивости каналов спутниковой связи к воздействию нестационарных помех. Моделировалось воздействие импульсной помехи, период следования

помеховых импульсов которой в какие-то моменты времени может совпадать с периодом следования кадров физического уровня, а ширина спектра равна ширине спектра полезного сигнала. В качестве показателя качества функционирования спутниковой связи использовалась вероятность потери кадра физического уровня. Кадр считался потерянным, если после применения кодов исправления ошибок кадр содержал неисправленные ошибки либо если кадр не был корректно выделен блоком кадровой синхронизации. Моделировался канал с периодом повторения канальных символов в 1 мкс, различными кодовыми скоростями и видами модуляции (*QPSK* 1/4, *QPSK* 1/3, *QPSK* 2/5, *QPSK* 3/4, *QPSK* 1/2, 8*PSK* 3/5, 8*PSK* 2/3, 8*PSK* 3/4).

На рисунке 8 изображена зависимость вероятности потери кадра P_0 от длительности помехового импульса τ_n и времени задержки начала помехового импульса относительно начала заголовка кадра физического уровня $\tau_з$. При этом фиксировалось отношение мгновенной мощности помехи к мощности сигнала $Q = 10$ дБ. Как видно из рисунка 8, зависимость вероятности потери кадра $P_0(\tau_з)$ имеет несимметричный вид, что свидетельствует о различной помехоустойчивости информационной части заголовка и последовательности начала кадра. Поверхности, образованные зависимостью вероятности пропуска кадра физического уровня от длительности помехового импульса и задержки, имеют два выраженных плато. Первое образуется, когда помеха начинает воздействовать на последовательность начала кадра. Причем первое плато ниже, то есть помехоустойчивость последовательности начала кадра выше, чем информационной части заголовка, хотя длина ПНК, составляющая 26 символов (26 мкс), меньше длины ИЧЗ, составляющей 64 символа (64 мкс). Это объясняется меньшим порогом для принятия решения о наличии ПНК в принятой реализации.

Кроме того, из семейства графиков видно, что для помех с длительностью 40 мкс и менее наблюдается снижение вероятности потери кадра P_0 при попадании помехи на стык ПНК и ИЧЗ. При этом энергия помехи распределяется между двумя частями заголовка, ПНК и ИЧЗ. Помехи, длительность которых не превышает 15 мкс, не влияют на процесс кадровой синхронизации и выделения границ кадра, так как такие помехи не могут вызвать достаточного количества ошибок для перехода одного кодового слова в другое либо достаточного количества ошибок для того, чтобы порог обнаружения ИЧЗ не был превышен.

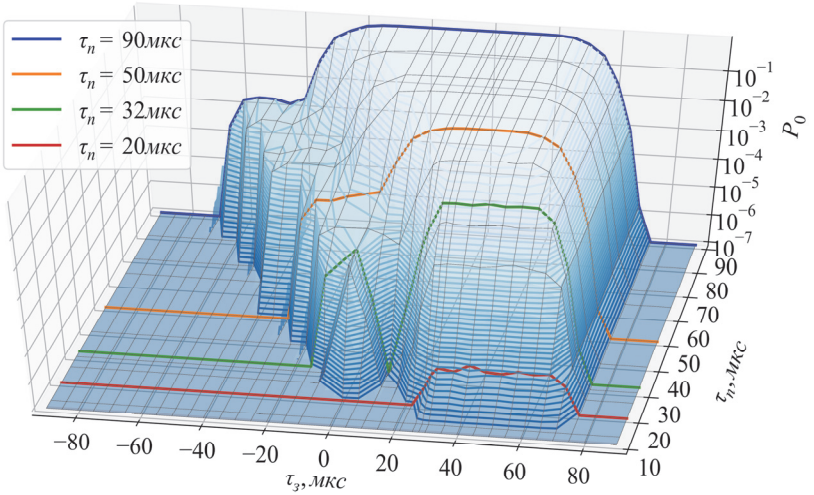


Рис. 8. Зависимость вероятности потери кадра P_0 от длительности помехового импульса $\tau_п$ и времени задержки начала помехового импульса относительно начала заголовка кадра физического уровня $\tau_з$ при фиксированном отношении мгновенной мощности помехи к мощности сигнала Q = 10 дБ

Для тех же исходных данных была построена зависимость вероятности потери кадра физического уровня P_0 от отношения мгновенной мощности помехи к мощности сигнала Q и времени задержки начала помехового импульса от начала заголовка кадра физического уровня $\tau_з$ при фиксированной длительности помехи $\tau_п$ = 32 мкс. Полученная зависимость изображена на рисунке 9.

Данная зависимость иллюстрирует наличие снижения вероятности потери кадра физического уровня при попадании помехи между частями заголовка кадра. Существование данного провала при высоких мгновенных мощностях обусловлено в том числе ограниченным временем воздействия помехи, а значит, и ограниченным количеством искажаемых символов. Это приводит как к снижению вероятности пропуска информационной части заголовка, так и к невозможности возникновения ошибки в распознавании сообщения в информационной части заголовка вследствие того, что количество искаженных символов не может превысить половины минимального расстояния Хэмминга для используемого кода.

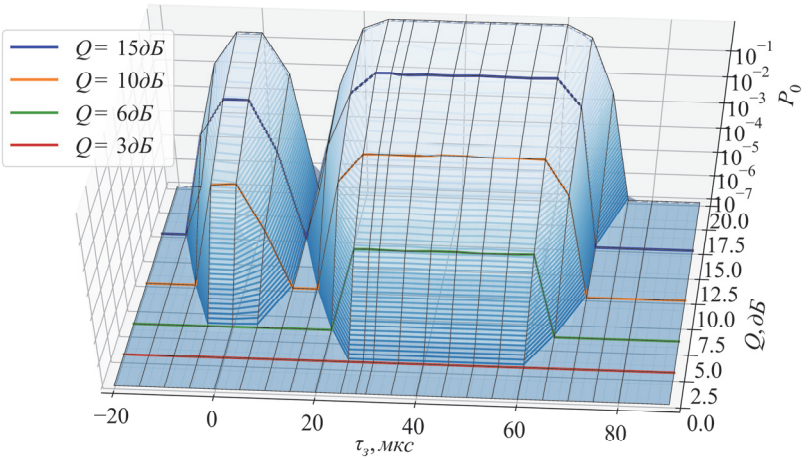


Рис. 9. Зависимость вероятности потери кадра P_0 от отношения мгновенной мощности помехи к мощности сигнала Q и времени задержки начала помехового импульса от начала заголовка кадра физического уровня $\tau_з$ при фиксированной длительности помехи $\tau_п$

Была исследована зависимость вероятности потери кадра физического уровня P_0 от длительности задержки начала воздействия нестационарной помехи $\tau_з$ относительно начала кадра физического уровня. Моделировались различные длительности нестационарной помехи $\tau_п$. Мгновенная мощность помехи выбиралась исходя из обеспечения постоянной средней мощности помехи, соответствующей отношению сигнал-шум 16,05 дБ [1]. Такое отношение сигнал-шум обеспечивает квазибезошибочный прием, то есть прием с вероятностью кадровой ошибки менее 10^{-7} для режима с использованием модуляции 32*APSK* (*Amplitude Phase Shift Keying*) и скорости кодирования 9/10 [1, 7]. Это наименее помехоустойчивый режим функционирования, предусмотренный стандартом *DVB-S*2. Результаты моделирования представлены на рисунке 10.

Как видно из графиков, такая помеха обладает средней мощностью, обеспечивающей квазибезошибочную работу в наименее помехоустойчивом режиме, и способна существенно негативно повлиять на работу приемника спутниковой связи. Причем наибольшую опасность представляет помеха, длительность которой совпадает с длительностью информационной части заголовка, так как она приводит к наибольшим вероятностям потери кадров физического уровня и действует в достаточно широком интервале временных задержек.

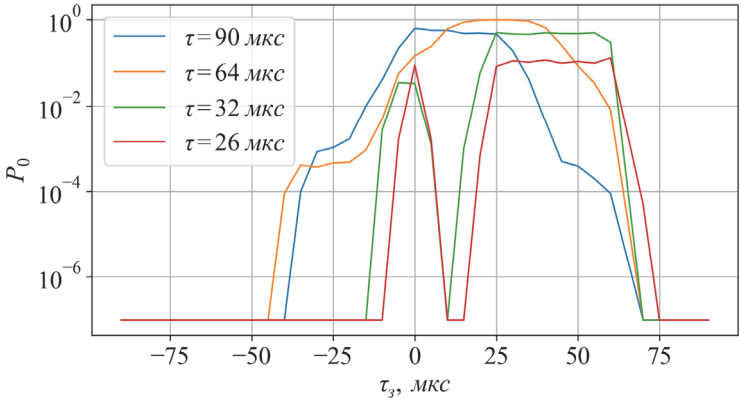


Рис. 10. Зависимость вероятности потери кадра физического уровня P_0 от времени задержки начала воздействия помехи $\tau_з$ для различных длительностей помехового воздействия $\tau_п$ при фиксированной средней мощности

Для всех рассмотренных длительностей помеховых импульсов воздействие помех на информационную часть кадра не приводит к потере пакетов. Это обусловлено тем, что применяемые в стандартах *DVB-S*2, *DVB-S*2*X* декодеры полностью исправляют ошибки, возникающие в результате коротких помеховых воздействий. Эти результаты согласуется с ранее полученными результатами исследования воздействия нестационарных помех на информационную часть кадра широкополосных систем спутниковой связи [14].

Адекватность разработанной модели и достоверность полученных результатов подтверждается совпадением в частных случаях с ранее полученными результатами и известными аналитическими выражениями. При значениях времени задержки помехового воздействия, превышающего длительность заголовка кадра физического уровня, результаты совпадают с результатами, полученными в [14]. В случае, когда длительность помехи равна длительности кадра, а задержка равна нулю, то есть когда помеха превращается в непрерывную шумовую, полученные результаты согласуются с данными по кадровой ошибке, которые приведены в [1], а вероятность битовой ошибки согласуется с аналитическими выражениями, которые были представлены в [23].

5. Заключение. Разработана модель канала спутниковой связи в условиях воздействия нестационарных помех. Особенностью модели является учет влияния применяемых в современных спутниковых системах связи модуляции, демодуляции и фильтрации сигналов,

символьной и кадровой синхронизации, кодов исправления ошибок. Это позволило исследовать влияние помех на различные фрагменты заголовка и сравнить это воздействие с воздействием на информационную часть кадра.

Результаты моделирования показали, что информационная часть заголовка обладает меньшей помехоустойчивостью по сравнению с последовательностью начала кадра, несмотря на меньший размер. Этот факт объясняется как существенно меньшим порогом обнаружения последовательности начала кадра, так и возможностью ошибочного распознавания информационной части, обусловленной случайными изменениями символов, вызванных помеховым воздействием. Существенное значение имеют длительность помехового воздействия и положение начала помехового воздействия относительно начала заголовка. Показано, что нестационарные помехи, обладающие незначительной средней мощностью, способны существенно нарушить процесс кадровой синхронизации и выделения кадров физического уровня при условии их попадания в заголовок кадра за счет нарушения приема служебной информации.

Полученные результаты могут использоваться при уточнении оценок помехоустойчивости каналов спутниковой связи, использующих протоколы *DVB-S*2, *DVB-S*2*X* в условиях нестационарных помех.

Литература

1. ETSI EN 302 307 V1.2.1 Digital Video Broadcasting (DVB);Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2). 2009-04.
2. ETSI EN 301 545-2 V1.1.1 Digital Video Broadcasting (DVB); Second generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower layers for Satellite standard. 2012-01.
3. *Челышев В.Д., Якимовец В.В.* Зарубежные радиоэлектронные системы наземного и спутникового мобильного радиосервиса // СПб: ВАС. 2012. 388 с.
4. *Bejarano J.R., Miguel N.C., Ruiz P.F.J.* MF-TDMA Scheduling Algorithm for Multi-Spot Beam Satellite Systems Based on Co-Channel Interference Evaluation // IEEE Access. 2019. vol. 7. pp. 4391–4399.
5. *Черноусов А.В.* Анализ воздействия аддитивных помех на широкополосный сигнал // Решетневские чтения. 2016. Т. 1 С. 306–308.
6. *Дворников С.В., Пшеничников А.В., Манаенко С.С., Глухих И.Н.* Интегральная модель помехозащищенных линий радиосвязи // Радиопромышленность. 2018. № 4(28). С. 8–14.
7. *Sormunen L., Puttonen J., Kurjenniemi J.* System level modelling of DVB-S2X in high throughput satellite system // 36th International Communications Satellite Systems Conference (ICSSC 2018). 2018. pp. 1–4.
8. *Wang G. et al*. Performance Evaluation of SATCOM Link in the Presence of Radio Frequency Interference // 2016 IEEE Aerospace Conference. 2016. pp. 1–10.

9. *Кантор Л.Я.* Электромагнитная совместимость систем спутниковой связи // М.: НИИР. 2009. 280 с.
10. *Puzko D. et al*. Evaluation of Finite Discrete RRC-Pulse Parameters to Simulate DVB-S2 with LDM // 2019 IEEE International Conference on Electrical Engineering and Photonics (EExPolytech). 2019. pp. 140–143.
11. *Агиевич С.Н., Борисов В.В., Дворников С.В., Луценко С.А.* Предложения по оценке эффективности преднамеренных помех элементам синхронизации сигналов спутниковых систем // Вопросы оборонной техники. 2019. № 5-6. С. 114–120.
12. *Луценко С.А.* Подход к расчету энергетического выигрыша при постановке помех системе цикловой синхронизации спутниковых линий связи // Журнал радиоэлектроники. 2019. № 3. 15 р.
13. *Перегудов М.А., Семченко И.А.* Оценка эффективности случайного множественного доступа к среде типа ALOHA при голосовых соединениях, передаче служебных команд, текстовых сообщений и мультимедийных файлов в условиях деструктивных воздействий // Труды СПИИРАН. 2019. Вып. 18. С. 887–911.
14. *Паршуткин А.В., Маслаков П.А.* Исследование помехоустойчивости современных стандартов спутниковой связи к воздействию нестационарных помех // Труды СПИИРАН. 2017. Вып. 53. С. 159–177.
15. *Маслаков П.А., Паршуткин А.В., Фомин А.В.* Модель функционирования канала спутниковой связи при воздействии нестационарных помех // Труды Военно-космической академии им. А.Ф.Можайского. 2016. Вып. 651. С. 78–83.
16. *Kim P., Lee I., Oh D., Ryu J.* Robust initial access technique of spread spectrum based on DVB-RCS2 standard for mobile application // 36th International Communications Satellite Systems Conference (ICSSC 2018). 2018. pp. 1–5.
17. *He R., Yang D., Wang H., Kuang J.* Adaptive hierarchical coding and modulation scheme over satellite channels // IET Communications. 2018. vol. 13. no. 17. pp. 2834–2839.
18. *Joudeh H., Clerckx B.* Robust transmission in downlink multiuser miso systems: A rate-splitting approach // IEEE Transactions on Signal Processing. 2016. vol. 64. pp. 6227–6242.
19. *Perez-Neira A. et al*. Signal Processing for High Throughput Satellite Systems: Challenges in New Interference-Limited Scenarios // 2018. arXiv preprint arXiv:1802.03958.
20. *Ali B.A.B., Zhour M., Ahmed M.* Modeling and Design of a DVB-S2X system // 2019 5th International Conference on Optimization and Applications (ICOA). 2019. pp. 1–5.
21. *Hao H., Chen J., Zhou Y.* An irregular row weight problem resolution for DVB-S2 LDPC short frame // 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC). 2017. pp. 45–48.
22. *Floyd M.G.* Interpolation in Digital Modems – Part I: Fundamentals // IEEE Transactions on Communications. 1993. vol. 41. No. 3. pp. 501–507.
23. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: пер. с англ. // М.: Вильямс. 2003. 1104 с.

Паршуткин Андрей Викторович — д-р техн. наук, профессор, профессор, кафедра систем и средств радиоэлектронной борьбы космического назначения, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: радиоэлектронная защита радиоэлектронных средств и систем, методы оценивания результативности помех и радиоэлектронных воздействий, методы создания интеллектуальных помех и защиты от них, методы и средства технической

защиты информации. Число научных публикаций — 97. andydc2010@mail.ru; ул. Ждановская, 13, 197198, Санкт-Петербург, Россия; р.т.: +7(812)347-95-35; факс: +7(812) 237-12-49.

Бучинский Дмитрий Игоревич — адъюнкт, кафедра систем и средств радиоэлектронной борьбы космического назначения, Военно-космическая академия имени А.Ф.Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: радиоэлектронная защита радиоэлектронных средств и систем, методы создания интеллектуальных помех, помехоустойчивость систем спутниковой связи. Число научных публикаций — 3. reys-rd@ya.ru; ул. Ждановская, 13, 197198, Санкт-Петербург, Россия; р.т.: +7(926)015-82-74; факс: +7(812) 237-12-49.

DOI 10.15622/ia.2020.19.5.3

A. PARSHUTKIN, D. BUCHINSKIY

MODEL OF SATELLITE COMMUNICATION CHANNEL FUNCTIONING UNDER CONDITIONS OF DISTURBANCES OF SERVICE PART OF FRAMES BY UNSTEADY INTERFERENCE

Parshutkin A., Buchinsky D. **Model of Satellite Communication Channel Functioning under Conditions of Disturbances of Service Part of Frames by Unsteady Interference.**

Abstract. The paper describes the main ways of organizing modern satellite communication systems and the methods of synchronization and transmission of service information used in them, the frame synchronization mechanism from the view point of noise immunity. Based on the analysis, a block diagram of a simulation model is proposed for studying the influence of unintentional interference on the channels of modern satellite communication systems. The proposed model of the impact of non-stationary interference on a satellite communication channel takes into account the effect of interference on symbolic, frame synchronization, mechanisms for extracting frame boundaries, as well as the effect of modern error correction codes. The model allows evaluating the impact of non-stationary interference on both the information and the service side of the frame of modern systems of broadband satellite communications. As an indicator of the noise immunity of a satellite communication channel, there was used probability of frame loss, i.e. frame skipping due to a violation in the frame synchronization system, incorrect allocation of frame boundaries, or the presence of errors in the frame that were not repaired by corrective codes. Using this model, we studied the effect of non-stationary interference of various durations on the information and service parts of the frame, compared the results of the impact of non-stationary interferences of various durations with the effect of white Gaussian noise. It is shown that non-stationary interference, which are short noise pulses that do not affect the information part of the frame due to reparation by correction codes, can significantly reduce the reception quality due to disruption of frame synchronization and distortion of service information about the signal-code structure and frame length.

Keywords: DVB-S2, DVB-RCS, Frame Synchronization, Non-stationary Interference, Noise Immunity, Satellite Broadband

Parshutkin Andrey — Ph.D., Dr.Sci., Professor, Professor, Department of Systems and Electronic Warfare Systems for Space Applications, Mozhaisky Military Space Academy. Research interests: electronic protection of electronic equipment and systems, methods of estimating the impact of noise and electronic influences, methods of creation of intellectual interference and protection, methods and means of technical protection of information. The number of publications — 97. andydc2010@mail.ru; 13, Zhdanovskaya str., 197198, St. Petersburg, Russia; office phone: +7(812)347-95-35; fax: +7(812) 237-12-49.

Buchinskiy Dmitriy — Ph.D. Student, Department of Systems and Electronic Warfare Systems for Space Applications, Mozhaisky Military Space Academy. Research interests: electronic protection of electronic equipment and systems, methods of estimating the impact of noise and electronic influences, methods of creation of intellectual interference and protection, immunity of satellite communication systems. The number of publications — 3. reys-rd@ya.ru; 13, Zhdanovskaya str., 197198, St. Petersburg, Russia; office phone: +7(926)015-82-74; fax: +7(812) 237-12-49.

References

1. ETSI EN 302 307 V1.2.1 Digital Video Broadcasting (DVB);Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2). 2009-04.
2. ETSI EN 301 545-2 V1.1.1 Digital Video Broadcasting (DVB); Second generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower layers for Satellite standard. 2012-01.
3. Chelyshev V.D., Yakimovec V.V. *Zarubezhnye radioelektronnye sistemy nazemnogo i sputnikovogo mobilnogo radioservisa* [Foreign radio electronic systems of terrestrial and satellite mobile radio service]. SPb.: VAS. 2012. 388 p. (In Russ.).
4. Bejarano J.R., Miguel N.C., Ruiz P.F.J. MF-TDMA Scheduling Algorithm for Multi-Spot Beam Satellite Systems Based on Co-Channel Interference Evaluation. *IEEE Access.* 2019. vol. 7. pp. 4391–4399.
5. Chernousov A.V. [Analysis of the impact of additive interference on a broadband signal]. *Reshetnevskie chteniya* [Reshetnev readings]. 2016. Issue 1. pp. 306–308. (In Russ.).
6. Dvornikov S.V., Pshenichnikov A.V., Manaenko S.S., Gluhih I.N. [Integral model of noise-immune radio communication lines]. *Radiopromyshlennost – Radio industry.* 2018. vol. 4(28). pp. 8–14. (In Russ.).
7. Sormunen L., Puttonen J., Kurjenniemi J. System level modelling of DVB-S2X in high throughput satellite system. 36th International Communications Satellite Systems Conference (ICSSC 2018). 2018. pp. 1–4.
8. Wang G. et al. Performance Evaluation of SATCOM Link in the Presence of Radio Frequency Interference. 2016 IEEE Aerospace Conference. 2016. pp. 1–10.
9. Kantor L.Ya. *Elektromagnitnaya sovmestimost sistem sputnikovoj svyazi* [Electromagnetic compatibility of satellite communication systems]. M.: NIIR. 2009. 280 p. (In Russ.).
10. Puzko D. et al. Evaluation of Finite Discrete RRC-Pulse Parameters to Simulate DVB-S2 with LDM. 2019 IEEE International Conference on Electrical Engineering and Photonics (EExPolytech). 2019. pp. 140–143.
11. Agievich S.N., Borisov V.V., Dvornikov S.V., Lucenko S.A. [Proposals for evaluating the effectiveness of intentional interference to synchronization elements of satellite systems]. *Voprosy oboronnoj tekhniki – Military Enginery.* 2019. vol. 5-6. pp. 114–120. (In Russ.).
12. Lucenko S.A. [Approach to calculating the energy gain when jamming the system of cyclic synchronization of satellite communication lines]. *Zhurnal radioelektroniki – Journal of Radio Electronics.* 2019. vol. 3. (In Russ.).
13. Peregudov M.A., Semchenko I.A. [Evaluation of Efficiency of Random Multiple Access to ALOHA Type Environment with Voice Connections, Transfer of Service Commands, Text Messages and Multimedia Files in Destructive Impact Conditions]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2019. vol. 18. pp. 887–911. (In Russ.).
14. Parshutkin A.V., Maslakov P.A. [Study of the Noise Immunity of Modern Standards of Sat-ellite Communications to the Impact of Non-Stationary Interference]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2017. vol. 53. pp. 159–177. (In Russ.).
15. Maslakov P.A., Parshutkin A.V., Fomin A.V. [A model of the functioning of a satellite communication channel under the influence of non-stationary interference]. *Trudy Voenno-kosmicheskoj akademii im. A.F.Mozhajskogo – Proceedings of the Mozhaisky Military Space Academy.* 2016. vol. 651. pp.78–83. (In Russ.).

16. Kim P., Lee I., Oh D., Ryu J. Robust initial access technique of spread spectrum based on DVB-RCS2 standard for mobile application. 36th International Communications Satellite Systems Conference (ICSSC 2018). 2018. pp. 1–5.
17. He R., Yang D., Wang H., Kuang J. Adaptive hierarchical coding and modulation scheme over satellite channels. *IET Communications.* 2018. vol. 13. no. 17. pp. 2834–2839.
18. Joudeh H., Clerckx B. Robust transmission in downlink multiuser miso systems: A rate-splitting approach. *IEEE Transactions on Signal Processing.* 2016. vol. 64. pp. 6227–6242.
19. Perez-Neira A. et al. Signal Processing for High Throughput Satellite Systems: Challenges in New Interference-Limited Scenarios. 2018. arXiv preprint arXiv:1802.03958.
20. Ali B.A.B., Zhour M., Ahmed M. Modeling and Design of a DVB-S2X system. 2019 5th International Conference on Optimization and Applications (ICOA). 2019. pp. 1–5.
21. Hao H., Chen J., Zhou Y. An irregular row weight problem resolution for DVB-S2 LDPC short frame. 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC). 2017. pp. 45–48.
22. Floyd M.G. Interpolation in Digital Modems – Part I: Fundamentals. *IEEE Transactions on Communications.* 1993. vol. 41. no. 3. pp. 501–507.
23. Sklar B. *Digital communications* // Prentice Hall. 2001. pp. 1093–1099. (Russ. ed.: Sklyar B. Tsifrovaya svyaz. *Teoreticheskiye osnovy i prakticheskoye primeneniye.* M.: Viliams. 2003. 1104 p.).

УДК 621.31 **DOI** 10.15622/ia.2020.19.5.4

В.Б. Авдеев, В.А. Трушин, М.А. Кунгуров

УНИФИЦИРОВАННАЯ РЕЧЕПОДОБНАЯ ПОМЕХА ДЛЯ СРЕДСТВ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Авдеев В.Б., Трушин В.А., Кунгуров М.А. **Унифицированная речеподобная помеха для средств активной защиты речевой информации.**

Аннотация. Рассматривается возможность создания речеподобной помехи для средств виброакустической защиты речевой информации на основе таблиц слогов и слов русского языка. Обосновывается выбор направлений исследований и условий проведения эксперимента: синтез звуковых файлов путем случайной выборки элементов речи из базы данных, исследование спектров синтезированных помех, алгоритм создания помехи типа «речевой хор», исследование автокорреляционных функций синтезированных РП-помех, а также их плотности распределения вероятностей. Показано, что спектральные и статистические характеристики синтезированных речеподобных помех типа «речевой хор» из пяти голосов близки к аналогичным характеристикам реальных речевых сигналов. При этом речевой хор формировался путем усреднения мгновенных значений временных реализаций звуковых файлов. Показано, что спектральная плотность мощности речеподобной помехи типа «речевой хор» практически не изменяется при числе усредняемых «голосов» начиная с пяти. Плотность распределения вероятностей значения речеподобной помехи при увеличении числа голосов в «речевом хоре» приближается к нормальному закону (в отличие от реального речевого сигнала, чья плотность вероятности близка к распределению Лапласа). Оценка автокорреляционной функции показала интервал корреляции в несколько миллисекунд. Проведенные артикуляционные испытания разборчивости речи при использовании синтезированных речеподобных помех с различными отношениями «сигнал/шум» показали возможность снижения интегрального уровня помехи на 12-15 дБ по сравнению с шумоподобной помехой. Построены зависимости словесной разборчивости от интегрального отношения «сигнал/помеха» на основе полиномиальной и кусочно-линейной аппроксимации. Проведена предварительная оценка возможного влияния речеподобных помех на психоэмоциональное состояние человека. Обсуждается направление дальнейших исследований по повышению эффективности алгоритмов формирования речеподобных помех.

Ключевые слова: защита речевой информации, разборчивость речи, унифицированная речеподобная помеха, базы слогов и слов, спектральная плотность мощности, плотность распределения вероятностей, автокорреляционная функция, артикуляционные испытания

1. Введение. Для защиты речевой информации от утечки по техническим каналам широко применяются активные средства защиты – генераторы акустического и виброакустического шума. Такие генераторы построены в основном с использованием в качестве задающего белого шума с нормальным законом распределения вероятности значений. Естественно, что встает вопрос о выборе такой помехи, которая при обеспечении требуемого показателя защищенности (в общем случае – это коэффициент словесной разборчивости речи W) дает минимальное значение интегрального уровня помехи, то есть вносит минимальные дискомфорт и демаскирующие признаки при

проведении переговоров. Так, доказано, что для шумовых помех такими являются формантоподобные, то есть помехи, имеющие огибающую спектра, подобную спектру формант [1].

Исследования в области психоакустики показали [2], что гораздо более эффективной является речеподобная помеха, имеющая не только огибающую спектра подобную речевому сигналу, но и его «тонкую» структуру. При этом наибольшей эффективностью обладает помеха типа «речевой хор».

Известные на рынке активные средства защиты информации – генераторы речеподобной помехи (ГРП) используют разные алгоритмы ее формирования. Например, в комплексе виброакустической защиты «Барон», речеподобная помеха формировалась от трех внешних радиостанций с использованием дополнительного фонемного клонера из голосов говорящих. В генераторах «Факир», «Шаман», «Бубен» используется псевдослучайный сигнал типа «речевой хор». Однако принципы формирования речеподобных (РП) помех в этих устройствах не раскрываются.

Вместе с тем анализ публикаций по данному вопросу позволяет выявить два основных подхода в формировании РП-помехи:

1. От различных внешних источников.
2. От внутренних источников прибора.

В первом случае на внешний вход ГРП (например, микрофонный) подаются реальные речевые сигналы конкретных лиц (участников переговоров) или сигналы от других источников (например, радиостанций) [3-8]. Во втором случае РП-помеха формируется внутри ГРП самыми различными способами: синтез РП-помехи из заранее записанных в память ГРП элементов речи с выборкой по случайному закону; формирование РП-помехи из «псевдотекстов» с оптимизацией помехи путем клонирования основных фонемных составляющих голосов конкретных лиц; с использованием заранее сформированных баз аллофонов и тому подобное [9-15].

Естественно, существуют и комбинированные решения, совмещающие два указанных подхода. Необходимо отметить, что не существует какой-либо классификации РП-помех. Наиболее полные обзоры методов формирования РП-помех приведены в работах [7, 8].

К сожалению, в большинстве перечисленных работ не приводятся количественные данные об эффективности формируемых РП-помех. Исключение составляют работы [9, 10]. Так в работе [9] говорится об энергетическом выигрыше в 9 дБ при использовании помехи типа «фонемный хор» по сравнению с белым шумом (для слоговой разборчивости); в работе [10] – о выигрыше порядка 15 дБ для обеспечения словесной разборчивости 0,1-0,3.

Что касается самого понятия РП-помехи, в работах [8, 16] дается следующее определение: «Синтезируемый по случайному закону акустический сигнал, который по своим основным характеристикам соответствует речевому сигналу, но не содержит смысловой информации». При этом под основными характеристиками понимается их усредненные спектральные и временные характеристики без раскрытия этих понятий и критериев соответствия.

На данный момент не существует нормативной базы, регулирующей принципы формирования РП-помехи в средствах виброакустической защиты речевой информации, что не позволяет их унифицировать и делает невозможной сертификацию таких устройств.

Целью настоящей работы является исследование возможности создания унифицированной РП-помехи для ее дальнейшего использования при создании средств активной защиты речевой информации.

Суть предлагаемого подхода заключается в следующем:

1. Для формирования РП-помехи используются базы элементов русской речи: слогов и слов из ГОСТ.
2. Выборка элементов речи из баз осуществляется по случайному алгоритму.
3. Из случайной выборки с помощью программы-звукосинтезатора формируются звуковые файлы.
4. Формируется РП-помеха типа «речевой хор» из нескольких голосов путем наложения их звуковых файлов.

При этом необходимо решить следующие задачи:

– оценить влияние длительности аудиосигнала на его энергетический спектр;

– оценить влияние вида элементов речи (слоги, слова и др.) на его энергетический спектр;

– выбрать механизм создания РП-помехи типа «речевой хор» и оценить его энергетический спектр;

– провести артикуляционные испытания разборчивости речи с различными видами РП-помехи при разных отношениях «сигнал/помеха»;

– оценить плотности вероятностей и автокорреляционные функции синтезированных РП-помех.

2. Основные условия проведения исследований. За основу при создании РП-помех взяты артикуляционные слоговые и словесные таблицы из ГОСТ 16600-72 [17]. Для сравнения рассматривались также связные (смысловые) тексты [11, 18]. Формирование РП-помехи на основе звуков не рассматривалось, так как разборчивость звуков зависит от их сочетаний с другими звуками [19].

В качестве алгоритма случайной выборки речи из соответствующей базы использовался метод RNGCripto-ServiceProvider, реализованный на языке C#.

Программа-синтезатор – Vocalizer. Выбор данной программы обусловлен возможностью изменения таких параметров, как частота дискретизации, установка скорости речи, добавление других голосов и сохранение записи в файл.

Запись аудиофайлов производилась с частотой дискретизации 44,1 кГц, 16 бит, моно. Для обработки аудиосигналов и получения их спектров использовалась программа Adobe Audition 3.0. Создание РП-помехи производилось при среднем уровне речи 70 дБ.

3. Оценка влияния длительности аудиосигнала на его энергетический спектр. Для оценки влияния длительности аудиосигнала были использованы различные по длительности (1, 5, 15 и 30 минут) отрезки звуковых файлов, записанные одним диктором. С помощью программы Adobe Audition 3.0 для каждого отрезка построены спектры речевых сигналов и рассчитаны интегральные уровни в 7 октавных полосах. Полученные результаты представлены в таблице 1.

Таблица 1. Влияние длительности аудиосигнала на спектр

Октавные полосы, Гц	Интегральные уровни спектра речи, дБ			
	1 мин	5 мин	15 мин	30 мин
125	54,21	54,71	55,00	54,93
250	65,76	66,06	66,09	66,14
500	67,23	67,04	66,99	66,97
1000	55,40	54,09	54,18	54,27
2000	48,74	48,25	47,94	47,90
4000	50,38	50,59	50,36	50,06
8000	51,76	52,46	52,50	52,24

Различия спектров речи от длительности аудиосигнала составляет примерно 1 дБ. Таким образом, можно сделать вывод, что длительность аудиосигнала не имеет существенного влияния на спектр речевого сигнала (при времени усреднения не менее 1 минуты).

4. Оценка влияния вида элементов речи на его спектр. Слоги и слова были взяты из ГОСТ 16600-72, связный текст –отрывок из произведения М. А. Булгакова «Мастер и Маргарита». Длительность записи аудиофайлов – одна минута. Эксперимент проводился для 5 «синтезированных» дикторов. Пример полученных результатов для диктора Алены по слогам, словам и связным текстам приведен в таблице 2 и на рисунке 1.

Таблица 2. Спектральные уровни речи для диктора Алена по октавным полосам для слогов, слов и связных текстов

Октавные полосы, Гц	125	250	500	1000	2000	4000	8000
Слоги, дБ	54,16	65,75	67,25	55,01	48,56	51,05	51,87
Слова, дБ	55,66	66,00	66,94	55,43	48,23	50,98	52,17
Связные тексты, дБ	55,96	66,44	66,67	53,63	47,00	49,74	52,36

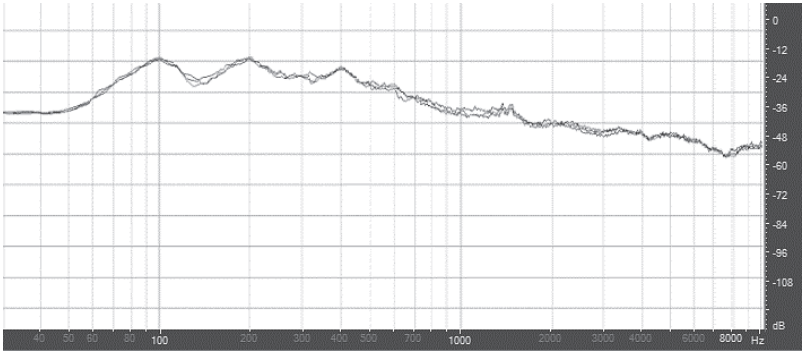


Рис. 1. Спектры речи Алены по слогам, словам и связным текстам

Приведенные результаты показывают, что разница спектров при использовании различных элементов речи составляет примерно 1 дБ.

5. Создание РП-помехи типа «речевой хор». Для создания речевого хора в качестве дикторов использовались компьютерные голоса, записанные с помощью программы-синтезатора Vocalizer. Запись производилась с одинаковой скоростью произношения, громкостью (небольшие расхождения в спектрах были выровнены по общему интегральному уровню) и длительностью в одну минуту (табл. 3). Создание речевого хора осуществлялось путем усреднения мгновенных значений временных реализаций (табл. 3, 4, рис. 2).

Таблица 3. Интегральные уровни спектров речи пяти дикторов

Октавные полосы, Гц	Интегральные уровни спектра речи, дБ				
	Алёна	Юрий	Милена	Катя	Николай
125	55,98	65,70	56,56	65,12	63,61
250	66,06	66,01	67,13	66,47	65,06
500	66,83	62,23	64,81	62,48	63,97
1000	55,53	53,12	59,58	54,86	61,07
2000	48,95	52,59	51,03	51,19	57,83
4000	51,37	52,95	50,99	49,36	48,85
8000	52,56	46,06	53,10	43,13	46,31

Таблица 4. Интегральные уровни в октавных полосах речевого хора с разным количеством дикторов

Октавные полосы, Гц	125	250	500	1000	2000	4000	8000
Хор из 3 голосов, дБ	63,48	65,77	64,62	56,93	54,52	52,40	51,42
Хор из 5 голосов, дБ	62,27	65,91	65,04	57,63	54,44	53,08	52,12
Хор из 10 голосов, дБ	62,31	65,70	65,07	57,61	55,84	52,58	53,56
Усредненный спектр речи по Покровскому, дБ	53,00	66,00	66,00	61,00	56,00	53,00	49,00

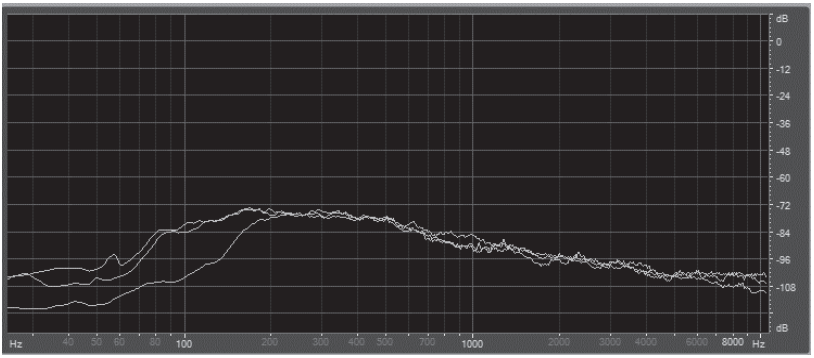


Рис. 2. Спектры речевого хора из 3, 5 и 10 голосов

Из таблицы 4 следует, что увеличение количества голосов в речевом хоре свыше пяти практически не влияет на его спектр и интегральные уровни в октавных полосах (различия около 1 дБ). Вместе с тем, имеются существенные различия октавных уровней в первой и седьмой полосе между спектром речевого хора и усредненным спектром по Покровскому [19] (10 и 4 дБ соответственно). По-видимому, это объясняется различием подходов в получении усредненных спектров. Дело в том, что в работе [19] фактически усреднялись сами спектры конкретных голосов (5 мужских и 5 женских) [19]. Однако такого спектра в природе не существует. На практике происходит суммирование мгновенных значений речевых сигналов (т.е. временных сигналов) на барабанной перепонке уха человека или чувствительном элементе первичных преобразователей – микрофона, акселерометра.

6. Организация артикуляционных испытаний с РП-помехой. Согласно требованиям ГОСТ [17] испытания проводятся бригадой

операторов, которая включает в себя как дикторов, так и аудиторов в возрасте от 18 до 30 лет, не имеющих явных дефектов речи и слуха. Каждый аудитор во время испытаний заполняет принятые элементы в специальный бланк, после чего для каждого измерения вычисляется среднее значение разборчивости W по формуле (1):

$$W_{cp} = \frac{1}{K}\sum_{i=1}^{K} W_i, \tag{1}$$

где W_i – результат единичного измерения, выраженный в процентах; $K = m*n$ – общее число таблиц, принятых всеми аудиторами; m – число аудиторов; n – число таблиц.

Далее происходит обработка результатов, а именно выявление сомнительных значений W_i, которые отбрасывают и вычисляют новое значение W. Среднеквадратическое отклонение рассчитывают по формуле (2):

$$\sigma_W \sqrt{\frac{1}{K-1}\sum_{i=1}^{K}(W_i - W_{cp})^2}. \tag{2}$$

Если $\left|W_i - W_{cp}\right| \geq 3\sigma_W$, то данные результаты следует исключить и вычислить повторно по формуле (1) с учетом уменьшенного числа измерений.

При заданном классе качества разборчивости, при обработке результатов измерений используют метод доверительного интервала:

С доверительной вероятностью 95% определяют по формуле (3) нижнюю границу разборчивости:

$$W_н = W_{cp} - C_K\sigma_W, \tag{3}$$

где C_K – коэффициент, учитывающий доверительную вероятность (находится по специальной таблице).

При проведении артикуляционных испытаний в качестве помехи использовался речевой хор из трех голосов, а в качестве сигналов–аудиозаписи четырех дикторов, созданные в программе-синтезаторе Vocalizer:

Диктор 1 – синтезированный женский голос не участвующий в помехе;

Диктор 2 – отрывок из фильма, в котором присутствуют и мужские и женские голоса, отличающиеся по уровню громкости;

Диктор 3 – синтезированный мужской голос, не участвующий в помехе;

Диктор 4 – синтезированный мужской голос, участвующий в помехе.

В аудиоредакторе Adobe Audition путем наложения двух аудиозаписей (РП-помехи и сигнала) были получены аудиозаписи с определенными отношениями сигнал/шум q (-15, -12, -10, -8, -5, -2, 0, 2, 5, 8, 10дБ), после чего группа аудиторов в составе семи человек прослушивала их. В связи с очень большим объемом проведенных артикуляционных испытаний (более 900) ниже в качестве примера представлены результаты испытаний с РП-помехой «речевой хор» на основе таблицы слов для диктора 4 (табл. 5).

Таблица 5. Результаты артикуляционных испытаний для Диктора 4 с помехой типа речевой хор, созданной на основе слов

q, дБ	$W_{ауд1}$	$W_{ауд2}$	$W_{ауд3}$	$W_{ауд4}$	$W_{ауд5}$	$W_{ауд6}$	$W_{ауд7}$	$W_{ср.}$
10	0,96	0,96	0,94	0,96	0,82	1,00	0,88	0,93
8	0,96	0,96	0,94	0,90	0,67	0,98	0,77	0,88
5	0,93	0,93	0,91	0,81	0,49	0,89	0,62	0,80
2	0,90	0,87	0,87	0,61	0,16	0,80	0,33	0,65
0	0,74	0,64	0,60	0,52	0,02	0,29	0,09	0,41
-2	0,48	0,44	0,27	0,33	0,00	0,04	0,06	0,23
-5	0,24	0,13	0,09	0,02	0,00	0,02	0,00	0,07
-8	0,09	0,04	0,00	0,00	0,00	0,00	0,00	0,02
-10	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
-12	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
-15	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

По усредненным значениям артикуляционных испытаний семи аудиторов для всех дикторов созданы графики аппроксимаций для РП-помех из слогов и слов, представленные на рисунках 3-6.

Средняя ошибка аппроксимации – среднее отклонение расчетных значений от фактических:

$$\overline{A} = \frac{1}{n}\sum \frac{|y_i - y_x|}{y_i} * 100\%, \qquad (4)$$

где y_i – фактические значения; y_x – значения аппроксимирующей функции.

При этом средняя ошибка аппроксимации не определена для нулевых значений. Значение ошибки аппроксимации до 15% свидетельствует о хорошо подобранной модели уравнения.

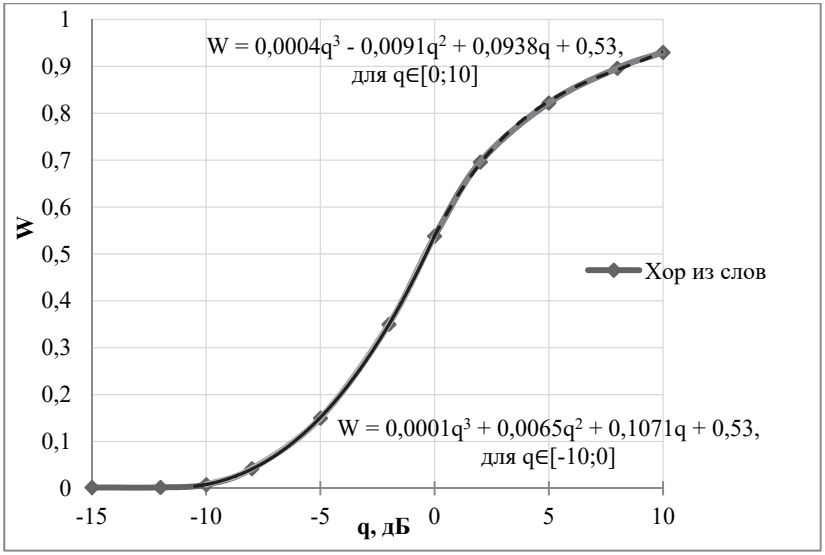


Рис. 3. График аппроксимации для РП помехи из слов

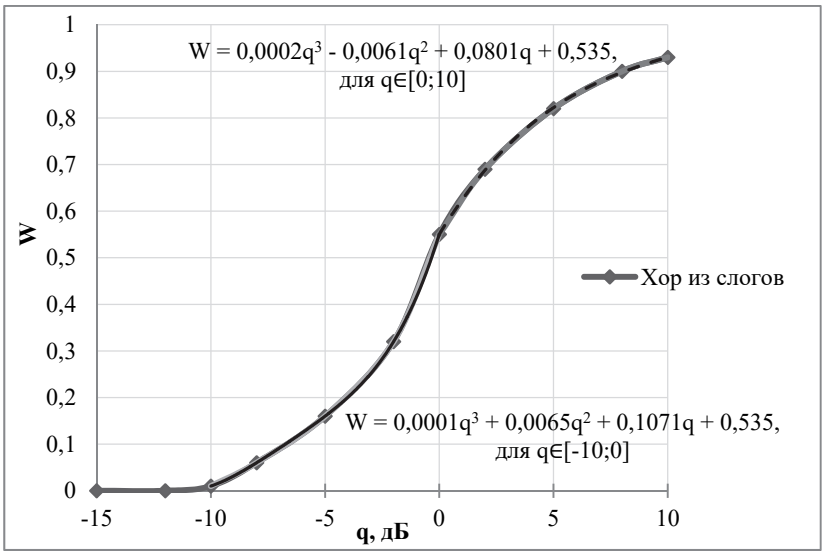


Рис. 4. График аппроксимации для РП помехи из слогов

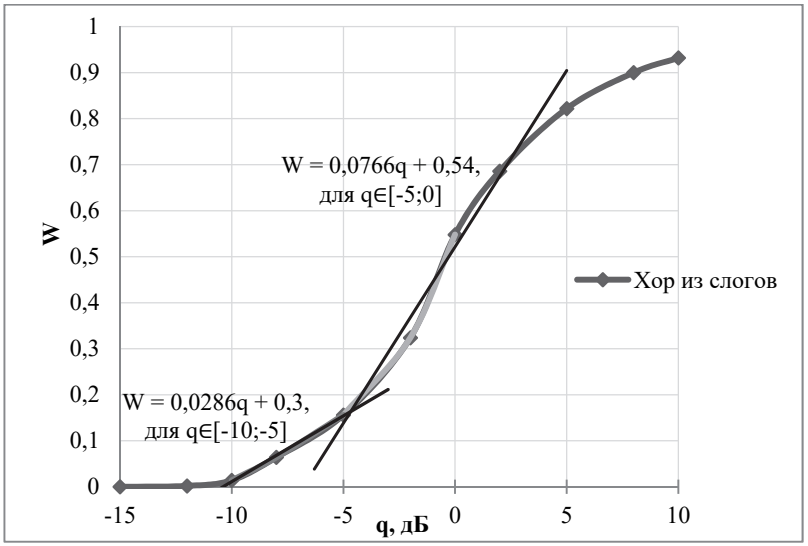


Рис. 5. График составной линейной аппроксимации для РП помехи из слогов

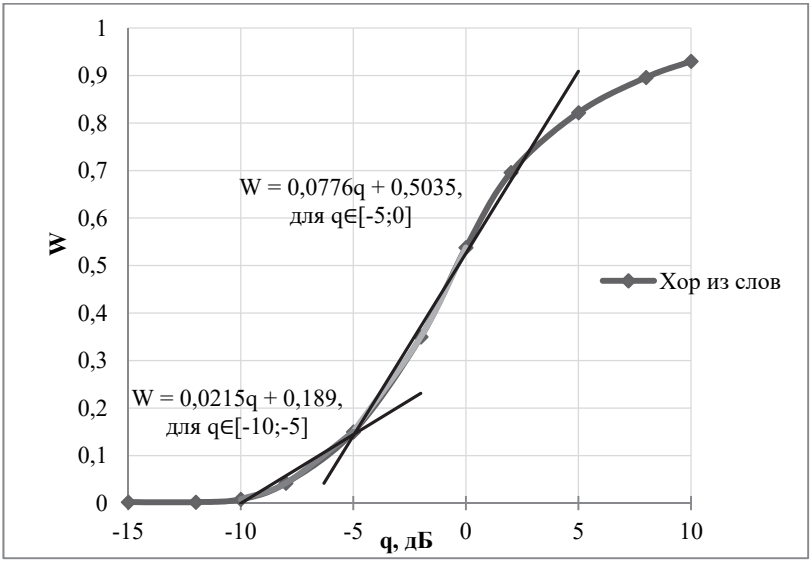


Рис. 6. График составной линейной аппроксимации для РП помехи из слов

Средняя ошибка аппроксимаций графиков 3-6 лежит в пределах 5-10%.

7. Оценка влияния вида элементов речи на разборчивость. Для проведения такой оценки были построены зависимости разборчи-

вости W от интегрального отношения сигнал/шум q для РП-помех, полученных из различных элементов речи для всех дикторов. Примеры таких графиков приведены на рисунках 7, 8.

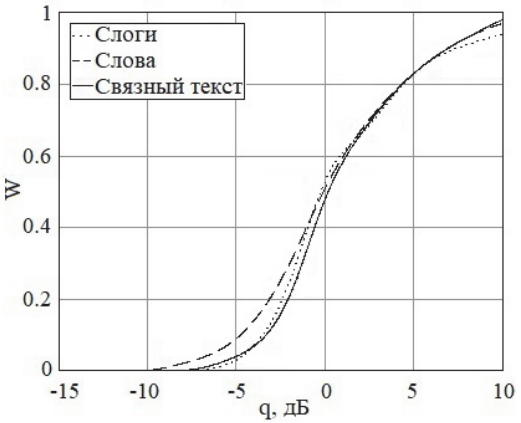


Рис. 7. Зависимость W для синтезированного женского голоса Катя и РП-помехи «речевой хор» по слоговым и словесным таблицам и связным текстам

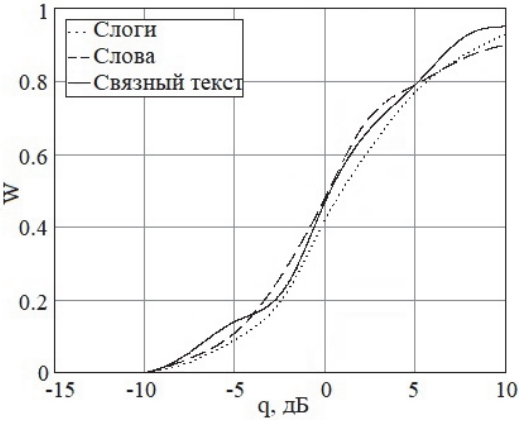


Рис. 8. Зависимость W для синтезированного мужского голоса Николай и РП-помехи «речевой хор» по слоговым и словесным таблицам и связным текстам

Анализ всех полученных зависимостей не выявил значительных различий в разборчивости при использовании РП-помех разного ви-

да (разброс по q не превышает 2-3 дБ). При этом выигрыш в интегральном отношении сигнал/шум по сравнению с помехой «белый шум» [10, 18, 20, 21] составляет 10-15 дБ.

8. Оценка плотности распределения вероятностей синтезированных РП-помех. Важной статистической характеристикой речи является плотность распределения вероятностей ее значений, которая чаще всего аппроксимируется распределениями Лапласа (двойная экспонента) или многочленом третьего порядка по системе экспоненциальных функций [22, 23]. На рисунке 9 для примера приведена экспериментальная плотность вероятностей значений РП-сигнала (слоги), построенная по 10000 отчетам с частотой дискретизации 44,1 кГц [23]. Очевидно визуальное сходство с распределением Лапласа.

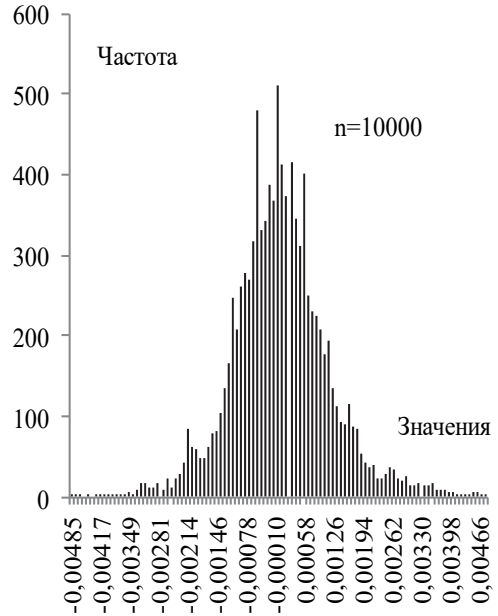


Рис. 9. Частотная гистограмма, построенная по 10000 значений сигнала «слова»

Однако для РП-сигнала (помехи) типа «речевой хор» плотность распределения вероятностей изменяется и при увеличении числа голосов приближается к нормальному закону (рис. 10-12), что естественно согласно центральной предельной теореме.

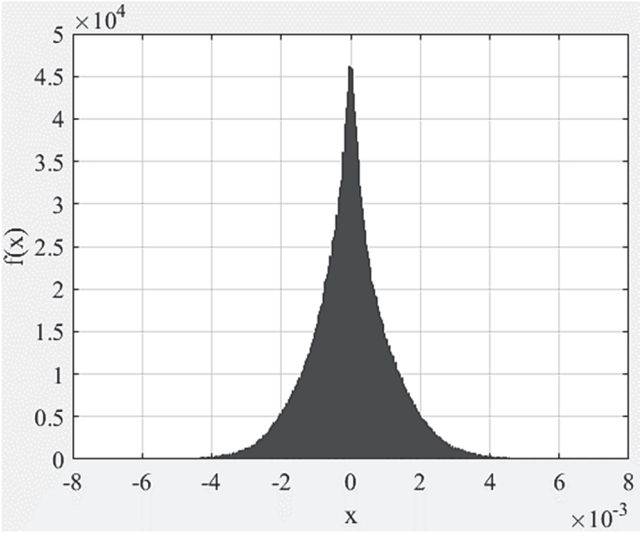


Рис. 10. Гистограмма плотности вероятности речевого хора из 3 голосов

Исходя из результатов сравнения спектров речевого хора для различного числа голосов (табл. 4, рис. 2) наибольший интерес для дальнейшего количественного анализа представляет плотность распределения вероятностей речевого хора из 5 голосов (рис. 11).

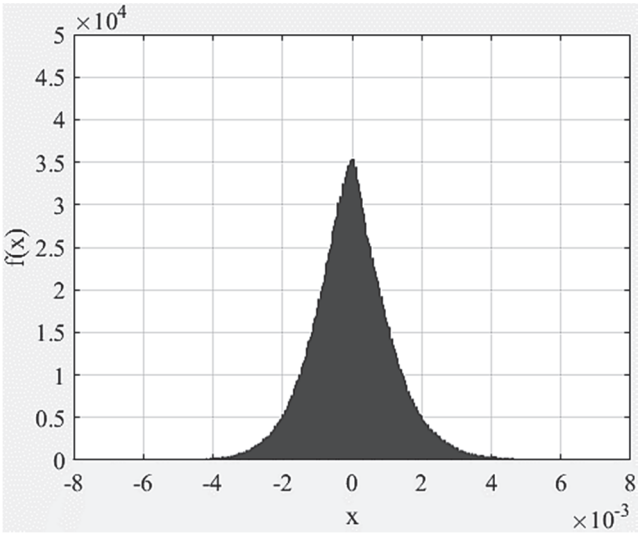


Рис. 11. Гистограмма плотности вероятности речевого хора из 5 голосов

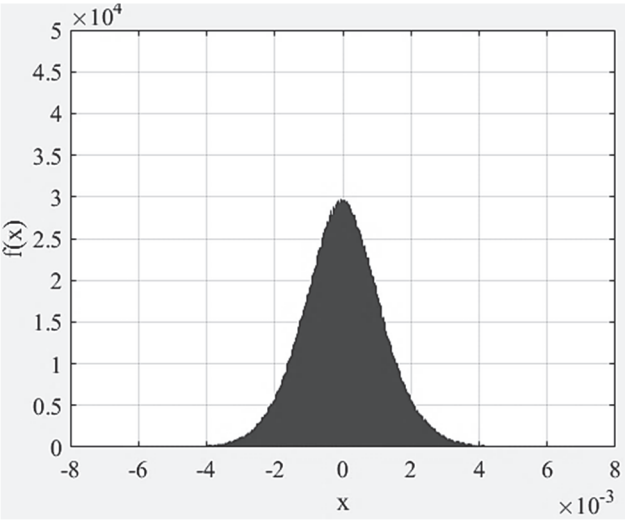


Рис. 12. Гистограмма плотности вероятности речевого хора из 10 голосов

9. Оценка автокорреляционной функции синтезированных РП-помех. На рисунке 13 представлена типичная автокорреляционная функция (АКФ) речевого сигнала в частотном диапазоне 100 Гц-8 кГц, полученная по известному спектру русской речи [19]. При этом интервал корреляции оценивается от 1 мс до 8 мс [24].

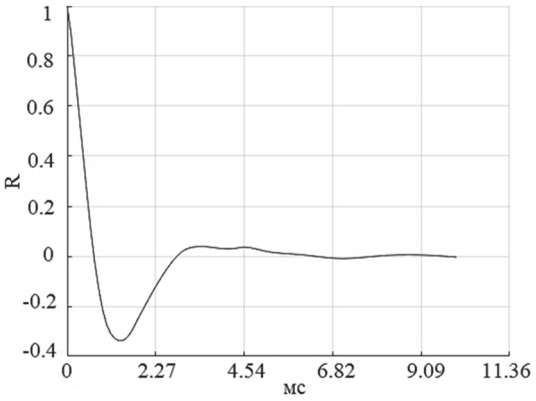


Рис. 13. АКФ русской речи [19]

Для сравнения на рисунке 14-16 приведены графики АКФ РП-сигналов типа «речевой хор» для различного количества голосов (3, 5, 10). Графики построены в среде Matlab с помощью стандартных средств. При этом частота дискретизации аудиозаписей равнялась 44,1 кГц, длина аудиофайла 1 мин., количество отсчетов – 1000.

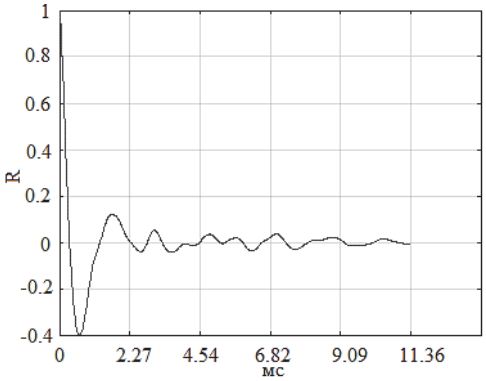


Рис. 14. АКФ речевого хора из 3 голосов

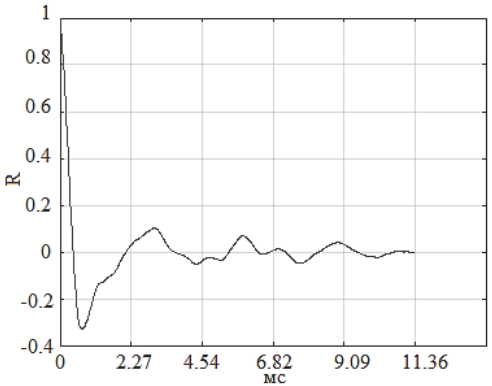


Рис.15. АКФ речевого хора из 5 голосов

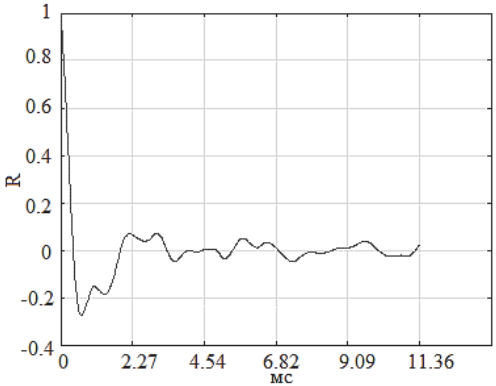
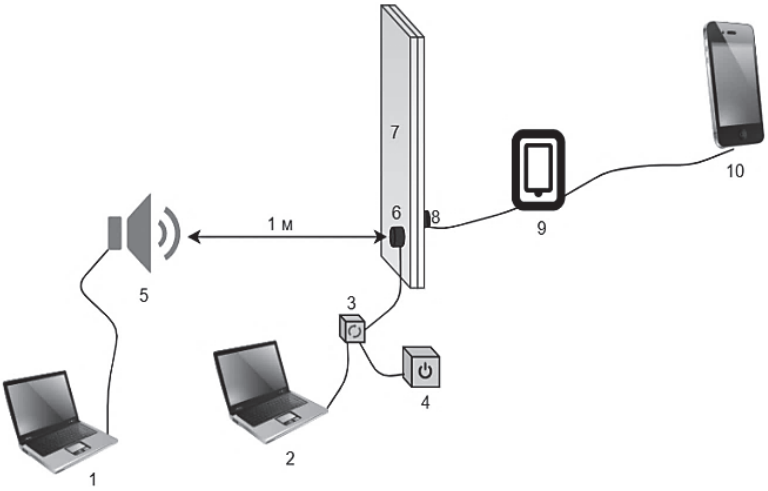


Рис. 16. АКФ речевого хора из 10 голосов

10. Организация и результаты натурных испытаний на реальном объекте. На рисунках 17, 18 приведен экспериментальный макет, его состав и соответствующая блок-схема. Расположение вибровозбудителей и акселерометров на стекле показано на рисунках 19, 20.



1 – Ноутбук с записью переговоров
2 – Ноутбук с записанной речеподобной помехой
3 – НЧ усилитель звука на TDA2030
4 – Блок питания для усилителя
5 – Акустоизлучатель “Волна”
6 – Вибровозбудитель (электроакустический преобразователь)
7 – Двойной стеклопакет
8 – Акселерометр тестового устройства AS-4
9 – Тестовое устройство AA-012GL
10 – Смартфон с диктофоном

Рис. 17. Экспериментальный макет

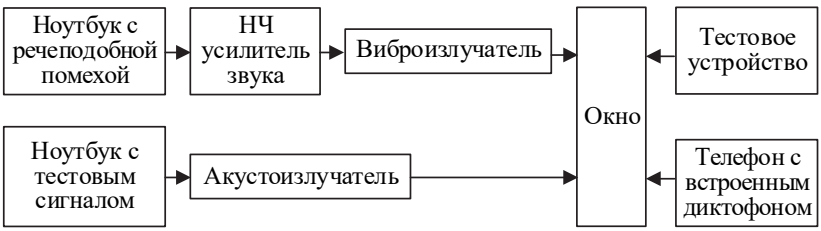
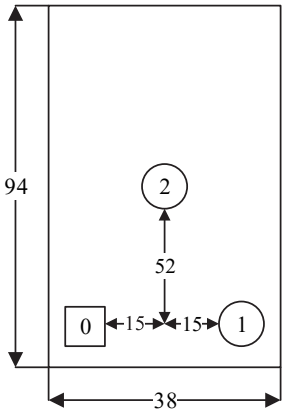
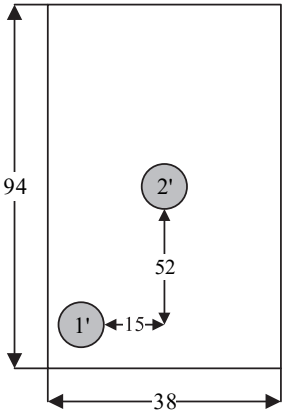


Рис.18. Блок-схема экспериментального макета



0 – Место установки вибровозбудителя генератора РП-помех
1, 2 – Места установки акселерометра шумомера

Рис. 19. Схема расположения устройств на внутренней стороне стекла



1`, 2` – Места установки акселерометра тестового устройства

Рис. 20. Схема расположения устройств на внешней стороне стекла

Все измерения и расчеты проводились по общепринятой методике [20] с использованием аттестованного шумомера-виброметра «Октава 110А» (табл. 6).

Таблица 6. Результаты оценки разборчивости речи

Номер КТ		V_c, дБ	$V_п$, дБ	q, дБ	W
1	Артикуляционные испытания	87,3	97,3	-10	0,00
	Расчет по Покровскому	87,7	97,4	-9,7	0,38
2	Артикуляционные испытания	94,5	96,3	-1,8	0,00
	Расчет по Покровскому	96,0	96,9	-0,9	0,40

Результаты проведенных испытаний подтвердили приведенные выше данные и выводы об эффективности синтезированных РП-помех.

В процессе выполнения данной работы был изготовлен и испытан действующий макет генератора речеподобных помех (ГРП), в котором реализован предложенный принцип формирования РП-помехи. Для упрощения конструкторского решения за основу создания ГРП был взят аудио-модуль mp3, который позволяет подключать выносную microSD карту. На карту памяти предполагается запись уже предварительно подготовленной РП-помехи. Питание генератора осуществляется от сети. Блок-схема устройства показана на рисунке 21.

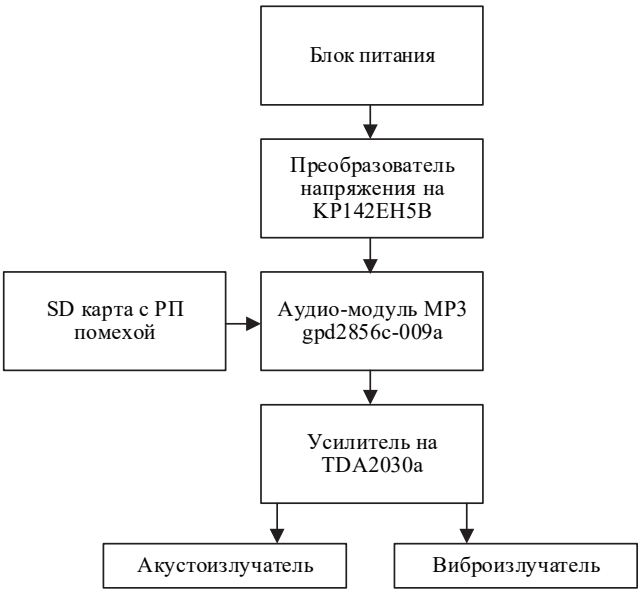


Рис. 21. Блок-схема макета ГРП

Основные характеристики разработанного ГРП:

– диапазон частот: 175…11200 Гц;

– вид помехи – РП помеха типа «речевой хор» из словесных артикуляционных таблиц;

– время непрерывной работы – 8 часов;

– регулировка уровней помехи – на этапе записи помех.

11. Воздействие РП-помехи на человека. При создании средств активной защиты информации от утечки по техническим каналам, в том числе по акустическим и виброакустическим кана-

лам, разработчики обязаны учитывать возможность их вредного влияния на организм человека. Для средств защиты речевой информации с шумовой помехой регламентирующими документами для разработчиков являются санитарные нормы, основанные на предельно допустимых уровнях (ПДУ) звуковых давлений и времени их воздействия на человека [25]. Вместе с тем у специалистов возникает много вопросов в части выбора ПДУ, времени экспозиции и методов их определения.

Что касается РП-помех, то в доступной литературе не удалось найти никакой информации об их воздействии на человека, кроме работы [20], где говорится: «В процессе экспериментальных исследований также установлено, что по сравнению с шумовыми «речеподобные комбинированные (реверберационные и инверсионные) помехи оказывают значительно меньшее раздражающее воздействие на нервную систему человека» [20].

Проведенная авторами весьма предварительная оценка возможного влияния РП-помех на человека показала, что они имеют место при $W \le 0{,}2$. Оценка проведена в соответствии с рисунком 13 для речевого хора из слогов, при трех аудиторах, располагавшихся на расстоянии 2 метров от окна. При отношении «сигнал/помеха» 11 дБ ($W = 0{,}3$) и 7 дБ ($W = 0{,}21$) все три аудитора никакого раздражающего воздействия в течение 30 минут не почувствовали; при отношении «сигнал/помеха» - 2,5 дБ ($W = 0{,}1$) один аудитор (женщина) ощутил некий дискомфорт (не удавалось сосредоточиться при чтении текста).

Для объективизации и получения количественной оценки влияния РП-помех на психоэмоциональное состояние человека были проведены эксперименты с использованием тестов Торндайка и Крепелина с участием трех аудиторов – молодых людей в возрасте 22 лет (двое мужчин и одна женщина). Для сравнения был также использован «белый шум».

Длительность эксперимента для каждого вида помех составляла 90 минут; контрольные тестирования проводились перед включением генератора помехи, а также через каждые 30 минут действия помехи. При этом эксперимент проводился в два этапа: на первом испытуемые занимались чтением текста, на втором этапе их внимание было сосредоточено на художественных и документальных видеопрограммах. Анализ результатов эксперимента позволил сделать следующие выводы:

– проведенное тестирование не выявило количественных зависимостей результатов тестирования от вида и продолжительности РП-

помех, более того, у двух испытуемых результаты тестирования после воздействия помех улучшились;

– субъективная оценка испытуемыми своего состояния говорит о повышении утомляемости, появлении раздражительности и головных болях, при этом наименьшее воздействие оказывал «белый шум», наибольшее – РП-помеха «речевой хор» из слоговых артикуляционных таблиц. Негативное влияние из словесных артикуляционных таблиц занимает промежуточное положение, по-видимому, в данной помехе меньше выражен эффект какофонии (т.е. случайных и бессмысленных сочетаний неприятных для слуха звуков);

– уровень негативного влияния помех зависит от характера деятельности испытуемых: существенно меньше при концентрации испытуемых на содержании видеопрограмм.

Был также проведен эксперимент по оценке негативного воздействия модифицированных РП-помех, в которых были «обрезаны» на 5% пики максимальной амплитуды (уменьшения пик-факторов). Результаты данного эксперимента показали значительное уменьшение негативных воздействий на испытуемых, в частности ощущение дискомфорта при воздействии такой помехи на основе словесных таблиц возникает не ранее, чем через час. При этом РП-помехи сохранили свои маскирующие свойства, что подтверждено соответствующими артикуляционными испытаниями (табл. 7). В качестве информативного сигнала использовалась аудиозапись беседы двух мужчин.

Таблица 7. Результаты артикуляционных испытаний

Отношение «сигнал/шум», дБ	W_1		W_2	
	1-е прослушивание	*2-е прослушивание*	*1-е прослушивание*	*2-е прослушивание*
-15	0,000	0,000	0,000	0,000
-12	0,000	0,000	0,000	0,000
-10	0,000	0,000	0,000	0,000
-8	0,009	0,033	0,000	0,007
-5	0,096	0,147	0,121	0,125
-2	0,219	0,252	0,250	0,268
0	0,500	0,542	0,329	0,350

Очевидно, что требуются дополнительные специальные исследования с большим числом испытуемых и контрольных тестов.

12. О расчетно-экспериментальной оценке эффективности средств защиты речевой информации с РП-помехой. В настоящее время для оценки защищенности речевой информации от утечки по акустическим и виброакустическим каналам, а также эффективности активных средств защиты используется расчетно-экспериментальная

методика, основанная на формантном методе Покровского [19, 20], однако данная методика применима только для помехи типа «белый шум». Изменение характеристик классического «белого шума», в частности, создание формантоподобной огибающей приводит к существенным различиям оценки W по методике и артикуляционным испытаниям. Это относится и к РП-помехам. Так в работе [26] отмечается, что при отношении «сигнал/шум» 5 дБ W составляет 11% по артикуляционным испытаниям и 88% по методике, что объясняется, по-видимому, тем, что методика не учитывает особенностей восприятия человеком речи в условиях РП-помех.

В данной ситуации возможны два подхода. Первый – корректировка существующей методики для каждого вида помех, второй – создание универсальной методики, не зависящей от параметров используемых помех (шумов). Естественно, второй подход представляется более перспективным, но в то же время требует дополнительных серьезных исследований. В этой связи в работе [27] предлагается использовать для анализа речевых сигналов подход, соответствующий «парадигме антропоморфической обработки сигналов, согласно которой обработка информации должна строиться на тех же принципах, что и в слуховой системе человека» [27]. В работе [28], посвященной анализу формантного метода оценки разборчивости речи как метода выполнения косвенных измерений, предлагается создание методики, основанной на информационно-измерительной модели периферической слуховой системы человека. Данная модель реализована в среде LabVIEW и проходит экспериментальные исследования.

13. Заключение. Показана возможность создания унифицированной РП-помехи на основе таблиц слогов и слов русского языка из ГОСТ в следующей последовательности:

– осуществляется случайная выборка элементов речи из соответствующей базы;

– из случайной выборки элементов речи создаются звуковые файлы;

– формируется РП-помеха путем усреднения звуковых (т.е. временных) файлов разных голосов.

Показано, что для получения стабильного долговременного спектра речи достаточно аудиосигнала с длительностью 1 минута, при которой разница спектров РП-помехи при различных элементах речи (слогов и слов) не превышает 1дБ; при этом полученные спектры соответствуют спектру связного текста. Созданная путем усреднения звуковых файлов разных голосов РП-помеха типа «речевой хор» имеет

спектр, который практически не изменяется (± 1 дБ) при увеличении числа голосов больше пяти.

Проведены репрезентативные артикуляционные испытания по оценке разборчивости речи для разных видов РП-помехи типа «речевой хор» согласно требованиям действующих ГОСТ, которые показали снижение интегрального отношения «сигнал/шум» в среднем на 10-15 дБ.

Оценка плотности вероятности значений РП-помех показала, что при увеличении числа усредняемых голосов, она изменяется и стремится к нормальному закону распределения в отличие от плотности речевого сигнала, которая соответствует распределению Лапласа. Оценка АКФ РП-помехи «речевой хор» показала ее схожесть с АКФ реального речевого сигнала. Натурные испытания эффективности РП-помех на реальном объекте подтвердили справедливость полученных результатов.

Представлены результаты предварительных исследований по оценке влияния РП-помех на психоэмоциональное состояние человека и возможности его уменьшения. Поставлен вопрос о необходимости создания универсальной методики оценки эффективности средств активной защиты речевой информации, независящей от вида и характеристик используемых помех.

Авторы выражают благодарность студентам кафедры защиты информации НГТУ-НЭТИ А. И. Заводовской, И. А. Овешникову и Э. В. Топорищеву за проведение экспериментальных исследований по оценке влияния РП-помех на психоэмоциональное состояние человека в рамках выполнения бакалаврских ВКР.

Литература

1. *Трушин В.А., Иванов А.В.* Возможности снижения интегрального уровня помехи в средствах активной защиты информации речевой информации (состояние и перспективы) // Доклады ТУСУР. 2018. Т. 21. № 2. С. 38–42.
2. *Алдошина И., Притц Р.* Музыкальная акустика // СПб.: Композитор. 2006. 720 с.
3. *Blintsov V., Nuzhniy S., Kasianov Y., Korytskyi V.* Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels // Technology audit and production reserves. 2019. vol. 5. no. 2(49). pp. 19–26.
4. *Davydau H.V. et al.* Method for protecting speech information // Doklady BGUIR. 2015. vol. 8(94). pp. 107–110.
5. *Blintsov V., Nuzhniy S., Parkhuts L., Kasianov Y.* The objectified procedure and a technology for assessing the state of complex noise speech information protection // Eastern-European Journal of Enterprise Technologies. 2018. vol 5. no. 9(95). pp. 26–34.
6. *Ахатаева С.М. и др.* Способ формирования речеподобного помехового сигнала // Патент Республики Казахстан №26413. 2012. Бюл.11.
7. *Воробьев В.И., Давыдов А.Г., Давыдов Г.В.* Речеподобные сигналы: разновидности, основные параметры, способы формирования, области применения // Минск: Доклады БГУИР. 2009. №3. С. 9-16.
8. *Зельманский О.Б.* Методика синтеза речеподобных сигналов на разных языках для систем защиты информации // Информационные системы и технологии. 2012. № 4. С. 122–133.

9. *Гордиевич П., Средяк В., Омельчук Я., Порошин И.* Формирование защитной речеподобной помехи путем генерации фонемных последовательностей // Правове, нормативне та метрологічне забеспечення захисту інформаціів. 2009. С. 129–132.
10. *Horev A.A, Tsarev N.V.* The method and algorithm of speech-like noise formation // 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2017. pp. 419–422.
11. *Трушин В.А., Попов Д.Е., Кунгуров М.А., Марченко Д.Л.* Создание речеподобной помехи на основе связных текстов // Проблемы правовой и технической защиты информации. 2018. Вып. 6. С.79–85.
12. *Асяев Г.Д., Антясов И.С.* Оценка эффективности применения шумовых «речеподобных» помех для защиты акустической информации // Вестник УрФО 2018. № 2(28). С. 19–24.
13. *Mostafa T. et al.* An efficient speech generative model based on deterministic/stochastic separation of spectral envelopes // Doklady BGUIR. 2020. vol. 18(2). pp. 23–29.
14. *Yerzhan N. et al*. Intelligibility of the kazakh speechwhen it's PROTECTED with combined masking signals // Doklady BGUIR. 2015. vol. 8(94). pp. 67–73.
15. *Koul R.K., Allen G.D.* Segmental intelligibility and speech interference thresholds of high-quality synthetic speech // Journal of speech & hearing research, American Speech-Language-Hearing Association. 1993. vol. 36. no. 4. pp. 790–798.
16. ITU-T P.501 Test signals for use in telephonometry/ Series P: Telephone Transmission Quality. Objective measuring apparatus. 2004. pp. 27.
17. ГОСТ 16600-72. Межгосударственный стандарт. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений // М.: Стандарт Информ. 2007. 74 с.
18. *Трушин В.А, Рева И.Л, Иванов А.В.* Усовершенствованная методика оценки разборчивости речи в задачах защиты информации // Ползуновский вестник. 2012. №3/2. С. 238–241.
19. *Покровский Н.Б.* Расчет и измерение разборчивости речи // М.: Связь-издат. 1962.
20. *Хорев А.А, Макаров Ю.К.* К оценке эффективности защиты акустической (речевой) информации // Специальная техника. 2000. № 5. С. 46–56.
21. *Авдеев В.Б.* О некоторых направлениях совершенствования методических подходов, применяемых при оценке эффективности технической зашиты информации // Специальная техника. 2013. № 3. С. 26–36.
22. *Trushin V.A., Khitsenko V.E.* About the methods of forming a test signal in the instrumental evaluation // Journal of Physics: Conference Series of speaker clearance. 2020.
23. *Кропотов Ю.А.* Модель одномерной плотности вероятности речевых сигналов // Системы управления, связи и безопасности. 2015. № 4. С. 158–170.
24. *Быков А.А., Кропотов Ю.А.* Исследование автокорреляционных функций речевых сигналов // Радиотехника. 2008. № 9. С. 107–111.
25. СН 2.2.4/2.1.8.562-96. Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки // Санитарные нормы. М.: Минздрав России. 1996.
26. *Хорев А.А., Царев Н.В.* Способ и алгоритм формирования речеподобной помехи // Вестник ВГУ, серия: Системный анализ и информационные технологии. 2017. № 1. С. 57–67.
27. *Вашкевич М.И., Азаров И.С.* Определение патологии голосового аппарата человека на основе анализа модуляционного спектра речи в критических полосах // Труды СПИИРАН. 2020. Т. 19(2). С. 249–276.
28. *Trushin V.A.* The analysis of the formant method of speech intelligibility estimation as a method of performing indirect measurements // Научный вестник НГТУ. 2019. № 4 С. 135–146.

Авдеев Владимир Борисович — д-р техн. наук, профессор, главный научный сотрудник, Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»). Область научных интересов: техническая защита информации. Число научных публикаций — 166. avb1952@mail.ru; ул. 9 Января, 280А, 394020, Воронеж, Россия; р.т.: +7-903-653-55-20.

Трушин Виктор Александрович — канд. техн. наук, доцент, старший научный сотрудник, кафедра защиты информации, Новосибирский государственный технический университет (НГТУ); ведущий инженер, ФГУП «НТЦ «Атлас». Область научных интересов: техническая защита информации. Число научных публикаций — 162. rastr89@mail.ru; пр. Карла Маркса, 20, 630092, Новосибирск, Россия; р.т.: +7-903-900-19-82.

Кунгуров Михаил Александрович — магистрант, кафедра защиты информации, Новосибирский государственный технический университет (НГТУ); инженер, ФГУП «НТЦ «Атлас». Область научных интересов: техническая защита информации. Число научных публикаций — 1. mixailkungurov@gmail.com; пр. Карла Маркса, 20, 630092, Новосибирск, Россия; р.т.: +7-996-381-12-97.

DOI 10.15622/ia.2020.19.5.4

V. AVDEEV, V. TRUSHIN, M. KUNGUROV

UNIFIED SPEECH-LIKE INTERFERENCE FOR ACTIVE PROTECTION OF SPEECH INFORMATION

Avdeev V., Trushin V., Kungurov M. **Unified Speech-Like Interference for Active Protection of Speech Information.**

Abstract. The paper considers the possibility of creating a speech-like interference for the means of vibro-acoustic protection of speech information based on tables of syllables and words of the Russian language. The choice of research directions and experimental conditions is substantiated: synthesis of sound files by random sampling of speech elements from a database, research of spectra of synthesized noise, algorithm for creating interference of the "speech choir" type, study of autocorrelation functions of synthesized speech-like interference, as well as their probability distribution density. It is shown that the spectral and statistical characteristics of the synthesized speech-like interference type "speech choir" of five voices are close to similar characteristics of real speech signals. At the same time, the speech choir was formed by averaging the instantaneous values of temporary realizations of sound files. It is shown that the spectral power density of the speech-like interference of the "speech choir" type practically is not changed with the number of averaged "voices" starting from five. The probability density distribution of the speech-like interference value with an increase in the number of voices in the "speech choir" approaches the normal law (unlike a real speech signal whose probability density is close to the Laplace distribution). Evaluation of the autocorrelation function gave a correlation interval of several milliseconds. The articulation tests of speech intelligibility using synthesized speech-like interference with different signal-to-noise ratios showed the possibility of reducing the integral noise level by 12-15 dB compared to noise-like interference. The dependencies of verbal intelligibility on the integral signal-to-noise ratio are constructed on the basis of polynomial and piecewise linear approximations. A preliminary assessment of a possible impact of speech-like interference on the psycho-emotional state of a person was performed. The direction of further research on increasing the efficiency of algorithms for generating speech-like interference is discussed.

Keywords: Protection of Speech Information, Speech Intelligibility, Unified Speech-Like Interference, Base Syllables and Words, Power Spectral Density, Probability Density Distribution, Autocorrelation Function, Articulation Tests

Avdeev Vladimir — Ph.D., Dr.Sci., Professor, Chief Researcher, Federal Autonomous Institution "State Research and Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control ("FAI "GNII PTZI FSTEC of Russia"). Research interests: technical information protection. The number of publications — 166. avb1952@mail.ru; 280A, str. January 9, 394020, Voronezh, Russia; office phone: +7-903-653-55-20.

Trushin Viktor — Ph.D., Associate Professor, Senior Researcher, Department of Information Security, Novosibirsk State Technical University (NSTU); Leading Engineer, FSUE STC "Atlas". Research interests: technical information protection. The number of publications — 162. rastr89@mail.ru; 20, pr. Karla Marksa, 630092, Novosibirsk, Russia; office phone: +7-903-900-19-82.

Kungurov Mihail — Master's Student, Department of Information Security, Novosibirsk State Technical University (NSTU); Engineer, FSUE STC "Atlas. Research interests: technical information protection. The number of publications — 1. mixailkungurov@gmail.com; 20, pr. Karla Marksa, 630092, Novosibirsk, Russia; office phone: +7-996-381-12-97.

References

1. Trushin V.A., Ivanov A.V [Possibilities of reducing the integral level of interference in the means of active protection of voice information information (state and prospects)] *Doklady TUSUR – TUSUR reports.* 2018. Issue 21. vol. 2. pp. 38–42. (In Russ.).
2. Aldoshina I., Pritc R. *Muzykal'naja akustika* [Musical acoustics]. SPb: Compozitor. 2006. 720 p. (In Russ.).
3. Blintsov V., Nuzhniy S., Kasianov Y., Korytskyi V. Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels. *Technology audit and production reserves.* 2019. vol. 5. no. 2(49). pp. 19–26.
4. Davydau H.V. et al. Method for protecting speech information. *Doklady BGUIR.* 2015. vol. 8(94). pp. 107–110.
5. Blintsov V., Nuzhniy S., Parkhuts L., Kasianov Y. The objectified procedure and a technology for assessing the state of complex noise speech information protection. *Eastern-European Journal of Enterprise Technologies*. 2018. vol 5. no. 9(95). pp. 26–34.
6. Ahataeva S.M. et al. [The method of forming a speech-like interfering signal]. Patent of the Republic of Kazakhstan no. 26413. 2012. bul. 11.
7. Vorob'ev V.I., Davydov A.G., Davydov G.V. [Speech-like signals: varieties, basic parameters, methods of formation, fields of application]. *Doklady BGUIR – BSUIR reports.* 2009. vol. 3. pp. 9–16. (In Russ.).
8. Zel'manskij O.B. [Synthesis technique of speech-like signals in different languages for information protection systems]. *Informacionnye sistemy i tekhnologii – Information systems and technologies.* 2012. vol. 4. pp. 122–133. (In Russ.).
9. Gordievich P., Sredjak V., Omel'chuk Ja., PoroshinI. [The formation of protective speech-like interference by generating phonemic sequences]. Pravove, normativne ta metrologichne zabespecheniya zahistu informaciiv – Legal, normative and metrological support of information protection in. 2009. pp. 129–132. (In Russ.).
10. Horev A.A, Tsarev N.V. The method and algorithm of speech-like noise formation // 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2017. pp. 419–422.
11. Trushin V.A., Popov D.E., Kungurov M.A., Marchenko D.L. [Speech-like interference based on coherent texts]. *Problemy pravovoj I tehnicheskoj zashhity informacii – Problems of legal and technical protection of information*. 2018. pp. 79–85. (In Russ.).
12. Asjaev G.D., Antjasov I.S. [Evaluation of the effectiveness of the use of noise "speech-like" interference to protect acoustic information] *Vestnik UrFO – Bulletin of the Ural Federal District.* 2018. vol. 2(28). pp. 19–24. (In Russ.).
13. Mostafa T. et al. An efficient speech generative model based on deterministic/stochastic separation of spectral envelopes. *Doklady BGUIR.* 2020. vol. 18(2). pp. 23–29.
14. Yerzhan N. et al. Intelligibility of the kazakh speechwhen it's PROTECTED with combined masking signals. *Doklady BGUIR.* 2015. vol. 8(94). pp. 67–73.
15. Koul R.K., Allen G.D. Segmental intelligibility and speech interference thresholds of high-quality synthetic speech. *Journal of speech & hearing research, American Speech-Language-Hearing Association*. 1993. vol. 36. no. 4. pp. 790–798.
16. ITU-T P.501 [Test signals for use in telephonometry] Series P: Telephone Transmission Quality. Objective measuring apparatus. 2004. 27 p.
17. GOST 16600-72. [Interstate standard. Voice transmission to radiotelephone communications. Speech intelligibility requirements and articulatory measurement methods] M.: Standart Inform. 2007. 74 p. (In Russ.).

18. Trushin V.A, Reva I.L, Ivanov A.V. [Improved method for assessing speech intelligibility in information security tasks]. *Polzunovskijvestnik – Polzunovsky Bulletin*. 2012. vol. 3/2. pp. 238–241. (In Russ.).
19. Pokrovskiĭ N.B. Raschet i izmerenie razborchivosti rechi [Calculation and measurement of speech intelligibility]. M.: Svjaz'-izdat. 1962. (In Russ.).
20. Horev A.A, Makarov Ju.K. [To assess the effectiveness of protection of acoustic (speech) information]. *Special'naja tehnika – Special equipment*. 2000. vol. 5. pp. 46–56. (In Russ.).
21. Avdeev V.B. [On some areas of improving the methodological approaches used in assessing the effectiveness of technical protection of information]. *Special'naja tehnika – Special equipment*. 2013. vol. 3. pp. 26–36. (In Russ.).
22. Trushin V.A., Khitsenko V.E. About the methods of forming a test signal in the instrumental evaluation. *Journal of Physics: Conference Series of speaker clearance.* 2020.
23. Kropotov Ju.A. [Model of one-dimensional probability density of speech signals]. *Sistemy upravlenija, svjazi i bezopasnosti – Management, communication and security systems*. 2015. vol. 4. pp. 158–170. (In Russ.).
24. Bykov A.A., Kropotov Ju.A. [The study of autocorrelation functions of speech signals]. *Radiotehnika – Radiotechnics*. 2008. vol. 9. pp. 107–111. (In Russ.).
25. Sanitary standards 2.2.4/2.1.8.562-96. [Noise at workplaces, in the premises of residential, public buildings and in residential areas] *Sanitarnye normy.* M.: Minzdrav Rossii. 1996. (In Russ.).
26. Horev A.A., Carev N.V. [Method and algorithm for the formation of speech-like noise]. *Vestnik VGU – VSU Bulletin, ser. Systems analysis and information technology*. 2017. vol. 1. pp. 57–67. (In Russ.).
27. Vashkevich M.I., Azarov I.S. [Determination of the pathology of the human vocal apparatus based on the analysis of the modulation spectrum of speech in critical bands] *Trudy SPIIRAN – SPIIRAS Proceedings*. 2020. Issue 19(2). pp. 249–276. (In Russ.).
28. Trushin V.A. [The analysis of the formant method of speech intelligibility estimation as a method of performing indirect measurements] *Nauchnyj vestnik NGTU – Science Bulletin of the NSTU*. 2019. vol. 4. pp. 135–146. (In Russ.).

УДК 004.738.5 **DOI** 10.15622/ia.2020.19.5.5

Р.В. Максимов, С.П. Соколовский, И.С. Ворончихин

АЛГОРИТМ И ТЕХНИЧЕСКИЕ РЕШЕНИЯ ДИНАМИЧЕСКОГО КОНФИГУРИРОВАНИЯ КЛИЕНТ-СЕРВЕРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Максимов Р.В., Соколовский С.П., Ворончихин И.С. **Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей.**

Аннотация. Проанализированы основные факторы, обуславливающие расширение возможностей и повышение результативности сетевой разведки по идентификации состава и структуры клиент-серверных вычислительных сетей вследствие стационарности их структурно-функциональных характеристик. Вскрытые особенности защиты клиент-серверных вычислительных сетей, основанных на реализации принципов пространственного обеспечения безопасности, а также формализация и внедрение множества запрещающих регламентов обосновывают актуальность задачи динамического управления структурно-функциональными характеристиками клиент-серверных вычислительных сетей, функционирующих в условиях сетевой разведки.

Представлена математическая модель, позволяющая находить оптимальные режимы динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей для различных ситуаций. Приведены результаты расчетов. Представлен алгоритм решения задачи динамической конфигурации структурно-функциональных характеристик клиент-серверной вычислительной сети, обеспечивающий уменьшение времени достоверности добываемых сетевой разведкой данных. Показаны результаты практических испытаний разработанного на основе алгоритма динамического конфигурирования клиент-серверных вычислительных сетей программного обеспечения. Полученные результаты свидетельствуют, что использование представленного решения по динамическому конфигурированию клиент-серверных вычислительных сетей позволяет повысить результативность защиты за счет изменения структурно-функциональных характеристик клиент-серверных вычислительных сетей в рамках нескольких подсетей. При этом достигнуто поддержание критически важных соединений, а интервалы времени изменения структурно-функциональных характеристик адаптивны к условиям функционирования и действиям злоумышленника.

Новизна разработанной модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей. Новизна разработанного алгоритма состоит в применении модели динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей для динамического управления структурно-функциональными характеристиками клиент-серверной вычислительной сети в условиях сетевой разведки.

Ключевые слова: сетевая разведка, клиент-серверные вычислительные сети, технология движущейся цели, компьютерная атака, киберманеврирование

1. Введение. Развитие высоких технологий напрямую сопряжено с развитием компьютерных сетей. Все компьютерные сети по своему назначению делятся на вычислительные, информационные и смешанные. Наибольший практический интерес представляют собой вы-

числительные сети, которые предназначены для распределенного решения вычислительных задач в крупных научных центрах, предприятиях аэрокосмической отрасли и нефтегазовой промышленности, а также в оборонном секторе.

Вычислительные сети представляет собой совокупность компьютеров, соединенных между собой с каналами связи в единую систему и использующих общие ресурсы. В клиент-серверной архитектуре вычислительных сетей задания, или сетевая нагрузка, распределены между серверами (поставщиками услуг) и клиентами (клиентами). Фактически клиент и сервер – это программное обеспечение, размещенное на ЭВМ и взаимодействующее через вычислительную сеть.

В общем случае клиент-серверная вычислительная сеть (КС ВС) представляет собой совокупность клиентов, периферийного и коммуникационного оборудования, объединенного физическими линиями связи. В состав КС ВС также могут входить серверы управления данными, которые используются в совокупности с системами управления базами данных. Все эти элементы определяются идентификаторами, в качестве которых в наиболее распространенном семействе протоколов *TCP/IP* используются сетевые адреса (*IP*-адреса). Для взаимодействия с клиентами сервер выделяет необходимые ресурсы для работы и ожидает запросы на открытие соединения (или запросы на предоставляемый сервис) [1, 2]. Формат запросов клиента и сервера определяется протоколом.

Рассматриваются без детализации функций содержательной обработки информации КС ВС, элементы которых функционируют под управлением *DHCP*-сервера. Для получения элементами КС ВС сетевых параметров, таких как *IP*-адрес, время продолжительности аренды *IP*-адреса, номер подсети (маска) и других, используется протокол *DHCP* (*Dynamic Host Configuration Protocol* – протокол динамической настройки узла) [3], который позволяет автоматически назначать параметры на определенный срок, называемый временем аренды. *DHCP*-сервер функционирует на прикладном уровне эталонной модели взаимодействия открытых систем, однако он реализует распределение параметров сетевого уровня. По истечении времени аренды *IP*-адрес вновь считается свободным, и клиент обязан запросить новый или же продлить арендуемый ранее. Кроме того, клиент сам может отказаться от полученного адреса. Динамическое (по сути – автоматическое) распределение *IP*-адресов является единственным, которое позволяет централизованно управлять адресным пространством КС ВС и политикой безопасности, избегая конфликтов распределения сетевых параметров, рационально используя незадействованные или временно сво-

бодные *IP*-адреса. Процесс инициализации клиента в КС ВС известен и включает четыре этапа получения *IP*-адреса в аренду [3].

Использование именно этого клиент-серверного протокола позволяет за счет вариации параметров динамической конфигурации структурно-функциональных характеристик КС ВС в условиях сетевой разведки скрыть состав, структуру и алгоритмы функционирования КС ВС от сетевой разведки и перевести КС ВС в заранее заданную конфигурацию при реализации злоумышленником компьютерной атаки (КА).

2. Анализ объекта исследования. Конвергенция информационных технологий и инфраструктуры, приобретающих глобальный трансграничный характер, вызывает негативные процессы, которые порождают угрозы национальной безопасности государства в экономической, оборонной, информационной и других сферах.

Этому способствует:

– наращивание злоумышленниками ассортимента средств сетевой разведки и организация их непосредственного контакта с элементами КС ВС через организацию интерфейсов сетевой разведки с элементами КС ВС;

– организация составных каналов утечки и создание виртуальных точек присутствия, обусловленная открытостью архитектуры КС ВС и протоколов информационного обмена (семейства *TCP/IP*);

– использование недекларированных возможностей аппаратного и программного обеспечения, обусловленных применением в КС ВС зарубежной технологической базы.

В большинстве случаев успешной компьютерной атаке на КС ВС всегда предшествуют процессы сетевой разведки. Сетевая разведка (СР) представляет собой процесс добывания и обработки данных о КС ВС, используемых устройствах и программном обеспечении, их уязвимостях, средствах защиты, а также путях проникновения в КС ВС. СР направлена на получение структурно-функциональных характеристик КС ВС.

Под структурно-функциональными характеристиками (СФХ) в работе понимаются структура, состав, физические, логические, функциональные и технологические взаимосвязи между сегментами КС ВС, применяемые информационные технологии и особенности их функционирования.

Под динамической конфигурацией СФХ КС ВС в работе понимается такое управление сетевыми параметрами и взаимосвязями элементов КС ВС, при котором длительность стационарного состояния КС ВС изменяется адаптивно, и может быть установлено таким, что

будет меньше длительности времени сбора злоумышленником информации о структуре КС ВС ВН. Следовательно, так называемый динамический способ распределения *IP*-адресов, реализуемый протоколом *DHCP*, является разновидностью автоматического (автоматизированного) распределения и не учитывает сценариев развития и длительности времени сбора злоумышленником информации.

Периодичность динамической конфигурацией СФХ КС ВС задается декларативно и может быть определена в диапазоне от минимального до максимального значения времени работы сетевого сканера злоумышленника. Значения времени работы сетевого сканера определяется в зависимости от средств СР.

Применение в КС ВС традиционных средств защиты информации, таких как межсетевые экраны, системы обнаружения атак и вторжений, а также криптографических средств защиты, не позволяет обеспечить конфиденциальность информации о ее составе и структуре. Это обусловлено, во-первых, тем, что информационные системы (ИС) используют при передаче по КС ВС *IP*-пакетов адресную и другую служебную (технологическую) информацию [4]. Во-вторых, тем, что подавляющему большинству современных КС ВС присущи свойства детерминированности, статичности и однородности. Так, свойство статичности КС ВС заключается в наличии инвариантов структуры КС ВС, к которым можно отнести схему информационных связей и саму структуру КС ВС. Свойство однородности подразумевает наличие инвариантов состава КС ВС, к нему можно отнести множество элементов оборудования, которым представлены узлы КС ВС и установленное на узлах КС ВС программное обеспечение [5]. Свойство детерминированности сводится к наличию инвариантов алгоритмов функционирования КС ВС, к которым можно отнести интенсивность информационного обмена клиентов КС ВС, протоколы их взаимодействия, физические и логические адреса элементов КС ВС, топологию КС ВС, множество функций и иерархическую структуру клиентов КС ВС [6].

Злоумышленники, использующие данные обстоятельства, получают преимущество в использовании временного и вычислительного ресурса для ведения СР, чем достигают:

– высокой достоверности результатов СР в течение длительного времени, что позволяет осуществлять планирование, выбор времени и технологического процесса КС ВС для начала КА;

– возможности бескомпроматного применения средств СР и реализации КА в любое удобное для этого время за счет заблаговременного (планового) формирования и применения их рационального состава;

– возможности неоднократного поиска и анализа уязвимостей аппаратного и программного обеспечения с последующим их тестированием на проникновение для конкретной цели;

– возможности с небольшими ресурсными затратами проводить крупномасштабную КА после обобщения частных результатов СР.

Непосредственное влияние на возникновение данных обстоятельств оказывают, с одной стороны, требования нормативных правовых актов (НПА), определяющих топологию и типологию КС ВС, с другой стороны, требования НПА к ассортименту и особенностям применения средств защиты информации, применяемых в КС ВС.

В то же время регуляторы в качестве основных мер и рекомендаций по защите КС ВС указывают:

– сокрытие архитектуры и конфигурации информационной (автоматизированной) системы (Приказ ФСТЭК России № 239 от 25.07.2019);

– управление изменениями конфигурации информационной системы и системы защиты персональных данных (Приказ ФСТЭК России № 239 от 25.07.2019);

– перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, которая обеспечивает защиту информации в случае возникновения отказов (сбоев) в защите информационной системы (Приказ ФСТЭК России № 27 от 15.02.2017).

Реализовать данные меры на текущий момент не представляется возможным, так как отсутствуют необходимые для этого технологии, и, соответственно, невозможно предъявлять требования к разработке и применению средств и систем защиты на основе этих технологий.

Внедрение ассортимента запрещающих регламентов, основанных на обнаружении и реагировании на факт ведения СР, не способны эффективно противостоять современным средствам СР [7]. В связи с этим требуются принципиально новые подходы к построению систем безопасности.

Если заменить статические параметры КС ВС динамическими, то злоумышленник не может получить окончательную и актуальную информацию, позволяющую реализовать вскрытые уязвимости программного обеспечения КС ВС. Данная концепция получила название «Защита на основе движущейся цели» (*Moving Target Defense*, *MTD*) [8-10]. Проведенный анализ научных работ в рассматриваемой предметной области [11-14] показал настолько высокую эффективность этой концепции, что за последние годы к исследованиям и разработке систем защиты в этом направлении привлечены научные кол-

лективы более чем в 30 странах мира. Существующий тренд исследований свидетельствует о том, что *MTD* может стать одной из основных парадигм построения систем информационной безопасности в ближайшем будущем.

Одним из направлений концепции *MTD* является динамическое изменение параметров КС ВС, таких как применяемые сетевые протоколы, значения *IP*- и *MAC*-адресов, номер подсети (маска), номера сетевых портов, применяемые алгоритмы шифрования, а также маршруты передачи трафика (информационные направления). Следовательно, при реализации концепции *MTD* в маскировании состава и структуры КС ВС направлением первоочередной разработки является динамическое изменение параметров сети (в рамках данной статьи – динамическое управления сетевым адресным пространством). Анализ научных работ в рассматриваемой предметной области показал, что для динамического изменения параметров КС ВС применяются методы киберманеврирования (*cyber maneuvering*) [11], которые заключаются в периодическом (синхронизированном по времени) или неуправляемом (случайном) изменении СФХ абонентов КС ВС с использованием различных способов [15-17]. При технической реализации киберманеврирования применяется *DHCP*-сервер с расширенными настройками, обеспечивающий динамическое конфигурирование СФХ КС в соответствии с разработанными алгоритмами при наступлении заданного события безопасности.

В то же время следует отметить, что известные технические решения, реализующие методы киберманеврирования, еще недостаточно проработаны и обладают существенными недостатками, а задачи приведения в соответствие таких мер защиты КС ВС (централизованному) замыслу противодействия средствам СР только начинают формулироваться отдельными авторами и их кооперациями [18-21], что обуславливает актуальность проводимого исследования.

3. Постановка задачи. Формализованную постановку задачи на динамическое конфигурирование СФХ КС ВС можно представить следующим образом:

$$< MIP, Z > \rightarrow \min P_{ABD} = \lim_{t \to \infty} P_{ABD}(t) \mid P_{ABD} \in \{P_i\},\ i = 1, 2, \ldots, h \qquad (1)$$

для минимизации вероятности вскрытия (от англ. *abduction*) структуры КС ВС злоумышленником;

$$< MIP, Z > \rightarrow \max P_{AC} = \lim_{t \to \infty} P_{AC}(t) \mid P_{AC} \in \{P_i\},\ i = 1, 2, \ldots, h \qquad (2)$$

для максимизации вероятности доступности (от англ. *access*) информации клиентам КС ВС в связи со сменой СФХ КС ВС.

В выражениях (1) и (2) введены следующие переменные:

– Z – множество внутренних параметров модели, $Z \subseteq \{S_i, \Lambda_j\}$,

где $S_i = \{S_1, \ldots, S_h\}$ – перечень моделируемых состояний КС ВС, $\Lambda_j = \{\lambda_1, \lambda_2, \ldots, \lambda_J\}$ – интенсивности потоков событий в ней;

– MIP – множество входных параметров модели, параметров СФХ КС ВС (от англ. *Model Input Parameters*) $MIP \subseteq \{IP, D, TM\}$, где IP – значение *IP*-адресов сетевых устройств вычислительной сети, являющихся клиентами *DHCP*-сервера;

– $D = [1, 2, \ldots, 32]$ – номер вычислительной сети *DHCP*-сервера (длина маски подсети) и клиентов КС ВС, максимальное значение составляет 32, а минимальное – 0;

– $TM = [0, 1, \ldots, 2592000]$ – значение времени аренды всех *IP*-адресов вычислительной сети.

Под доступностью информации будем понимать состояние информации (ресурсов КС ВС), при котором клиенты, обладающие правами доступа, могут реализовывать их беспрепятственно. Потоки событий от клиентов к *DHCP*-серверу и от *DHCP*-сервера к клиентам представляют собой последовательность управления сетевыми параметрами и СФХ КС ВС, приводящими к изменению доступности информации клиентам и к изменению возможностей злоумышленников по вскрытию структуры КС ВС.

4. Модель динамического конфигурирования клиент-серверных вычислительных сетей. Пусть имеется КС ВС, СФХ которой могут изменяться администратором в ручном и автоматическом режимах, а также имеется узел КС ВС – *DHCP*-сервер, обеспечивающий формирование и назначение СФХ сетевым устройствам, таких как *IP*-адреса, время их аренды, маска подсети и *IP*-адрес *DHCP*-сервера, который может функционировать в том числе и в качестве средства защиты информации о составе и структуре КС ВС от СР.

Моделируемая система S с течением времени меняет свое состояние (переходит из одного состояния в другое) с интенсивностью потоков событий λ, потенциально переводящих КС ВС в состояния, когда обеспечивается или не обеспечивается скрытие структуры КС ВС при ведении СР злоумышленником. Необходимые для исследования состояния КС ВС представлены в таблице 1.

Смена состояний $S_1 – S_5$ обуславливается возможностью нарушения штатного режима функционирования КС ВС под воздействием на нее средств СР и КА, которые могут создавать внеочередные заявки,

влияющие на доступность информации клиентов КС ВС. В случае, если длительность цикла ведения СР меньше длительности периода стационарности СФХ КС ВС, то можно полагать, что КС ВС может быть вскрыта средствами СР. Конструктивное использование результатов СР – это КА, влияющие на ухудшение основных качеств КС ВС.

Таблица 1. Дискретные состояния КС ВС

Переменная	Состояния
S_1	Состояние покоя КС ВС. Признаки СР и КА отсутствуют
S_2	Состояние изменения СФХ (перевод КС ВС в заранее определенную конфигурацию)
S_3	Состояние обнаружения средств СР штатными средствами защиты КС ВС
S_4	Состояние идентификации средствами СР СФХ КС ВС с некоторой полнотой
S_5	Состояние невозможности вскрытия СФХ КС ВС средствами СР злоумышленника

Следовательно, для снижения результативности СР и возможности последующей реализации КА на КС ВС необходимо сокращение времени пребывания СФХ КС ВС в стационарном состоянии (так чтобы длительность времени аренды *IP*-адресов и других сетевых параметров была меньше длительности времени ведения СР). Однако это может привести к тому, что КС ВС в некоторый момент времени не сможет обеспечить доступность информации клиентам КС ВС.

Эффективность функционирования КС ВС будет оцениваться как способность КС ВС обеспечивать доступность информации клиентам КС ВС при реализации динамического конфигурирования СФХ в условиях воздействия средств СР.

Моменты возможных переходов моделируемой системы из состояния в состояние неопределенны, случайны и происходят под действием событий, характеризующихся интенсивностями λ (табл. 2). Интенсивность события λ – это среднее число событий, приходящихся на единицу времени.

Оценка эффективности процессов функционирования КС ВС при использовании динамического конфигурирования СФХ связана с необходимостью моделирования данного процесса в реальном времени, что обусловливает целесообразность использования математического аппарата марковских процессов, необходимые условия которого: потоки событий являются простейшими (обладают свойствами стационарности, ординарности и не имеют последействий). Таким образом, процесс функционирования КС ВС в условиях динамического конфи-

гурирования ее СФХ можно представить как марковский случайный процесс с дискретными состояниями и непрерывным временем.

Таблица 2. Интенсивности потоков событий

Переменная	Описание потока событий
λ_{12}	Заявки на штатное формирование и назначение СФХ клиентам КС ВС (средств СР не обнаружено)
λ_{21}	Заявки на распределение СФХ клиентам КС ВС
λ_{13}	Заявки на обнаружение средств СР
λ_{32}	Заявки на внештатное изменение СФХ клиентам КС ВС
λ_{25}	Заявки на оценку результативности защиты от средств СР
λ_{51}	Заявки на продление текущих сетевых параметров клиентам КС ВС
λ_{24}	Заявки на оценку результативности средств СР
λ_{43}	Заявки скомпрометированного средства СР на вскрытие СФХ клиентов КС ВС
λ_{41}	Заявки нескомпрометированного средства СР на вскрытие СФХ клиентов КС ВС

На рисунке 1 представлен граф состояний моделируемой системы. Рассмотрим сценарий перехода моделируемой системы из состояния S_i в состояние S_j под воздействием потоков событий с интенсивностями λ_{ij}.

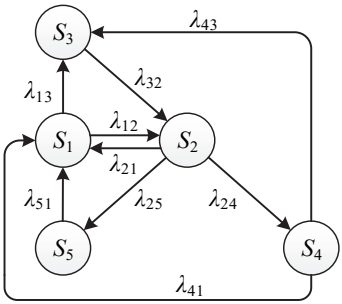


Рис. 1. Граф состояний процесса функционирования КС ВС

Пусть КС ВС функционирует в штатном режиме, между клиентами и серверами осуществляется информационный обмен, всем сетевым устройствам распределены *IP*-адреса и другие СФХ, сетевые устройства взаимодействуют между собой, воздействия средств СР отсутствуют, тогда S_1 – начальное состояние моделируемой системы (состояние покоя системы). Динамическое изменение сетевых параметров клиентов КС ВС в штатном режиме S_2 осуществляется под

воздействием λ_{12} и λ_{21} – заявок на штатное продление времени аренды *IP*-адресов и установление сетевых параметров новым клиентам. После изменения СФХ под воздействием заявок λ_{12} КС ВС переходит из состояния S_2 в состояние покоя S_1 с интенсивностью λ_{21}. В состояние S_3 система переходит под воздействием заявок на обнаружение средств СР λ_{13}. С увеличением интенсивности заявок λ_{32} на внештатное изменение СФХ клиентов КС ВС переходит из состояния S_3 в состояние S_2.

Увеличение потока заявок на оценку результативности средств СР с интенсивностью λ_{24}, означает переход системы в состояние S_4, в котором злоумышленник с использованием средств СР идентифицировал состав, структуру и алгоритмы функционирования КС ВС с некоторой полнотой.

Увеличение интенсивности применения средств СР злоумышленником λ_{43} на определенном этапе приведет к компрометации средств СР и переходу системы из состояния S_4 в состояние S_3.

Процесс бескомпроматной идентификации СФХ КС ВС средствами СР злоумышленника потоком заявок с интенсивностью λ_{41} означает штатную работу КС ВС при наличии средства СР, работающего в резидентном режиме, и переход системы в состояние S_1. Переход системы из состояния S_2 в S_5 осуществляется под воздействием заявок на оценку результативности защиты от СР λ_{25} и означает отсутствие идентификации СФХ КС ВС средствами СР. Это приведет к тому, что изменение СФХ сетевых устройств КС ВС осуществляется в штатном режиме, по расписанию.

В случае привлечения для динамического распределения СФХ сетевым устройствам КС ВС *DHCP*-сервера его функционирование осуществляется в пределах одной подсети, без использования агентов-ретрансляторов, предназначенных для распределения сетевых параметров между сетевыми устройствами, которые находятся в разных подсетях. Максимальное число клиентов *DHCP*-сервера определяется выбранным классом сети, что в соответствии с рассматриваемым типом КС ВС будет составлять 255 (компьютерные сети класса *C*).

По размеченному графу состояний составлены уравнения Колмогорова – дифференциальные уравнения (3) с неизвестными функциями $p_i(t)$.

Используя известный порядок решения системы линейных дифференциальных уравнений методом Рунге – Кутты [22, 23] и учитывая вектор вероятностей начальных состояний $p_i(0)$, интервал интегрирования t_0, t_1 и число этапов интегрирования n, произведен расчет для заданных значений интенсивностей событий $\lambda_{ij} = \text{const}$ (марковский однородный процесс), что позволило получить числовые таблицы

приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0, t_1]$. Таким образом, получены вероятностные и временные характеристики, описывающие состояния процесса функционирования КС ВС при изменении СФХ в различных условиях функционирования КС ВС (ситуациях).

$$\left.\begin{aligned}
&\frac{dp_1(t)}{dt} = \lambda_{21}p_2(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t) + \lambda_{41}p_4(t) - \lambda_{13}p_1(t),\\
&\frac{dp_2(t)}{dt} = \lambda_{12}p_1(t) + \lambda_{32}p_3(t) - \lambda_{21}p_2(t) - \lambda_{24}p_2(t) - \lambda_{25}p_2(t),\\
&\frac{dp_3(t)}{dt} = \lambda_{13}p_1(t) - \lambda_{32}p_3(t) + \lambda_{43}p_4(t),\\
&\frac{dp_4(t)}{dt} = \lambda_{24}p_2(t) - \lambda_{43}p_4(t) - \lambda_{41}p_4(t),\\
&\frac{dp_5(t)}{dt} = \lambda_{25}p_2(t) - \lambda_{51}p_5(t),\\
&\sum_{i=1}^{5} p_i(t) = 1.
\end{aligned}\right\} \qquad (3)$$

Рассмотрим использование модели при вариациях исходных данных, определяющих следующие ситуации.

В исходной ситуации КС ВС функционирует без воздействия средств СР, в штатном режиме, СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств КС ВС они штатно изменяются в ручном или автоматическом режиме администратором.

Ситуация C_1. КС ВС функционирует в условиях воздействия средств СР злоумышленника. Средства СР не обнаружены штатными средствами защиты КС ВС и функционируют бескомпроматно. СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ КС ВС они штатно изменяются в ручном или автоматическом режиме администратором. Средства СР направляют к КС ВС поток заявок на идентификацию СФХ сетевых устройств КС ВС с интенсивностью, позволяющей при постоянной интенсивности заявок на внештатное изменение СФХ сетевых устройств КС ВС, а также постоянной интенсивности заявок на обнаружение и оценку результативности обнаружения средств СР со стороны штатных средств защиты, к некоторому моменту времени вскрыть СФХ сетевых устройств КС ВС с некоторой полнотой.

Ситуация C_2. КС ВС функционирует в условиях воздействия средств СР злоумышленника. Средства СР обнаружены штатными средствами защиты КС ВС. СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств КС ВС они штатно изменяются в ручном или автоматическом режиме администратором. При отсутствии возможности увеличения интенсивности заявок на внештатное изменение СФХ сетевых устройств КС ВС, чтобы предотвратить вскрытие средствами СР злоумышленника СФХ сетевых устройств КС ВС, штатные средства защиты наращивают интенсивность потока заявок на обнаружение средств СР и оценку результативности обнаружения средств СР.

Ситуация C_3. КС ВС функционирует без воздействия средств СР, в штатном режиме, СФХ сетевым устройствам распределены, осуществляется информационный обмен. СФХ КС ВС внештатно изменяются *DHCP*-сервером в динамическом режиме с уменьшением временных интервалов изменения СФХ. Интенсивность изменения СФХ сетевых устройств КС ВС *DHCP*-сервером может увеличиваться до тех пор, пока минимальное значение интервала времени, через который изменяются СФХ сетевых устройств, не примет пороговое значение, после прохождения которого КС ВС не сможет выполнять свою целевую функцию и будет перегружена ввиду невозможности сетевых устройств завершить текущий цикл получения распределенных им СФХ и установления ими сетевых соединений до наступления очередного цикла изменения СФХ.

При $t \to \infty$ в моделируемой системе устанавливается стационарный режим, когда КС ВС случайным образом меняет свои состояния и ее вероятности $p_1(t), p_2(t), \ldots, p_5(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.

Приближенные значения p_i на интервале $t \in [0,5]$ с фиксированным шагом интегрирования 10^3 для значений интенсивностей потоков событий ситуации C_1 имеют значения $p_1 = 0{,}2$, $p_2 = 0{,}05$, $p_3 = 0$, $p_4 = 0{,}75$, $p_5 = 0$, сплайн-интерполяция значений представлена на графиках зависимостей вероятностей состояний от времени (рис. 2).

На интервале времени [0; 1,63] графика, представленного на рисунке 2, моделируемая система находится в переходном состоянии, наблюдается всплеск значений вероятности состояния $p_2(t)$, $p_4(t)$ и значительное снижение вероятности $p_1(t)$ пребывания моделируемой системы в состоянии штатного режима функционирования, что соответствует вскрытию КС ВС с вероятностью 0,77 уже через 1,6 секунды бескомпроматного функционирования средств СР.

Это возможно при постоянной интенсивности заявок на штатное изменение СФХ сетевых устройств КС ВС, а также постоянной интенсивности заявок на обнаружение средств СР и оценку его результативности.

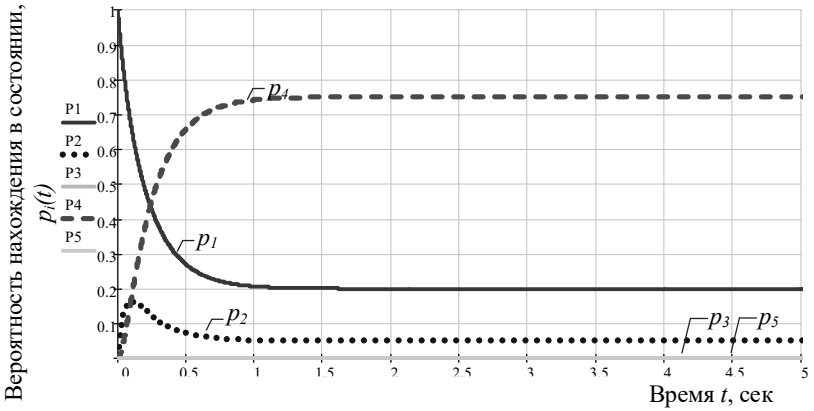


Рис. 2. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_1

Финальные вероятности для ситуации C_2 имеют следующие значения $p_1 = 0{,}114$, $p_2 = 0{,}047$, $p_3 = 0{,}475$, $p_4 = 0{,}032$, $p_5 = 0{,}332$ и представлены на рисунке 3.

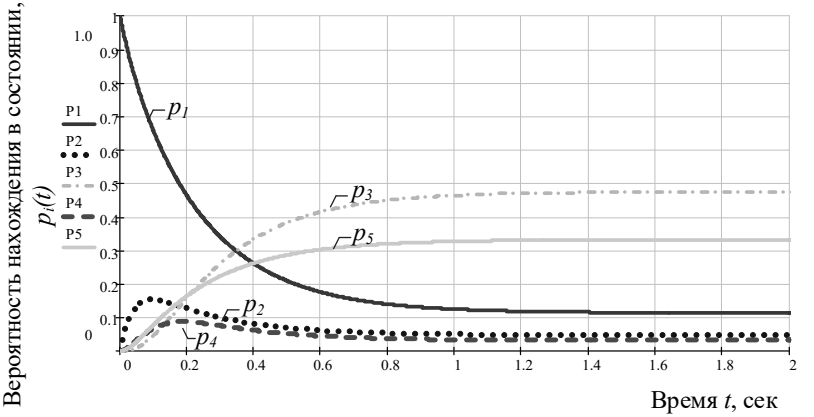


Рис. 3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_2

На рисунке 4 представлены результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации C_3, когда воздействия средств СР на КС ВС отсутствуют, а для динамического распределения СФХ сетевых устройств КС ВС задействован *DHCP*-сервер, постепенно уменьшающий временные интервалы, через которые осуществляется изменение СФХ до исчерпания ресурса КС ВС на реконфигурацию и последующей ее перегрузки. Данные зависимости позволяют определить пороговое значение интервала времени, через которое возможна последующая реконфигурация СФХ сетевых устройств без перегрузки системы, выполняющей свою целевую функцию, в условиях, когда воздействия средств СР отсутствуют. Финальные вероятности для ситуации C_3, для соответствующих значений интенсивностей потоков событий имеют следующие значения $p_1 = 1{,}429 \cdot 10^{-3}$, $p_2 = 2{,}02 \cdot 10^{-3}$, $p_3 = 0$, $p_4 = 0{,}997$, $p_5 = 0$.

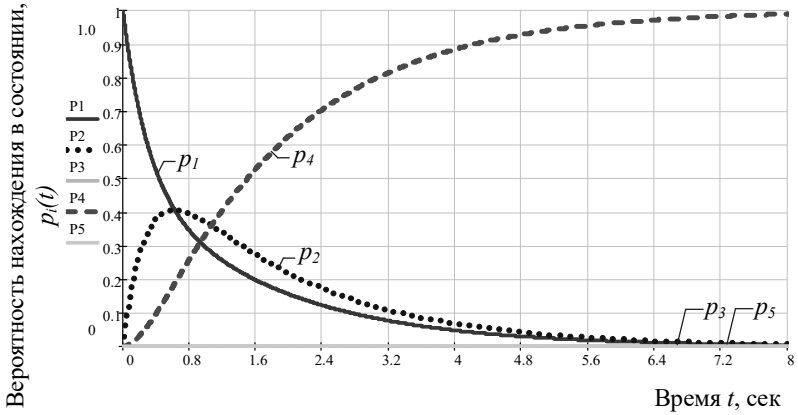


Рис. 4. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3

На рисунках 5 и 6 представлены графики зависимостей вероятностей пребывания моделируемой системы в различных состояниях от времени для ситуации C_3 при внештатном увеличении интенсивности изменения СФХ КС ВС *DHCP*-сервером в 3 и в 6 раз соответственно, по сравнению с пороговым значением.

В ситуации C_3 состояние S_3 трактуется как состояние перегрузки системы и наступления отказа в обслуживании. Пороговое значение интенсивности – это такая интенсивность изменения СФХ КС ВС *DHCP*-сервером, при которой КС ВС не сможет выполнять свою целевую функцию и будет перегружена. Сетевые устройства не могут завершить теку-

щий цикл получения распределенных им СФХ, установления сетевых соединений и передачи сообщений, до наступления очередного цикла изменения СФХ. Финальные вероятности для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 3 раза для соответствующих значений интенсивностей потоков событий имеют следующие значения $p_1 = 0{,}145$, $p_2 = 0{,}078$, $p_3 = 0$, $p_4 = 0{,}777$, $p_5 = 0$ (рис. 5).

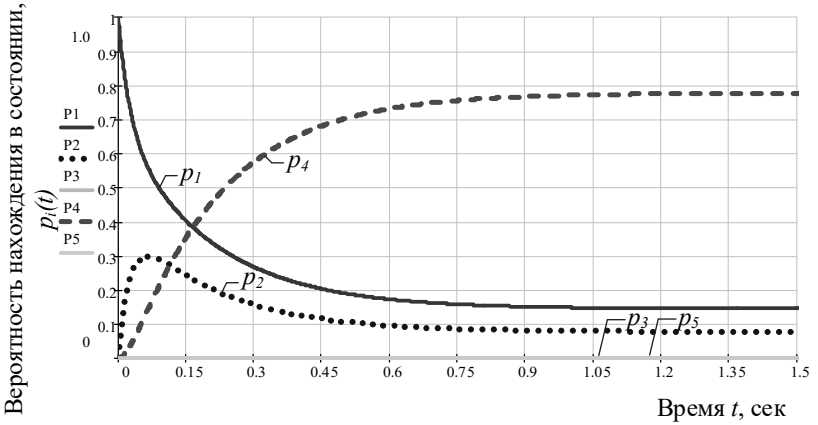


Рис. 5. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 3 раза

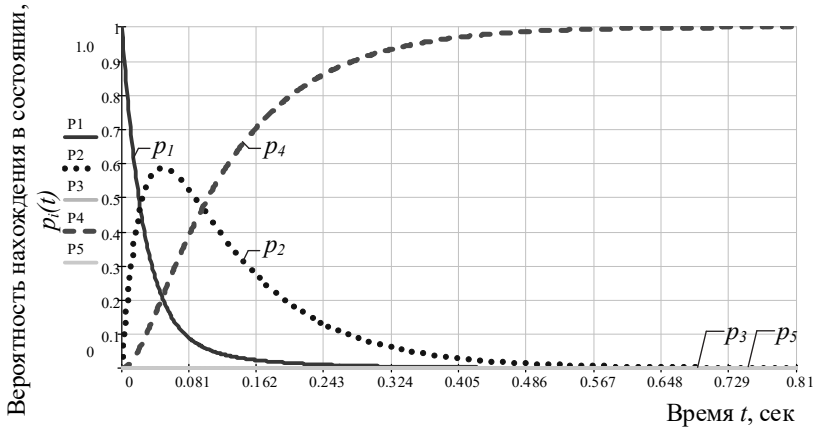


Рис. 6. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 6 раз

Финальные вероятности для ситуации C_3 при внештатном увеличении интенсивности изменения СФХ КС ВС *DHCP*-сервером в 6 раз имеют следующие значения $p_1 = 0$, $p_2 = 0$, $p_3 = 0$, $p_4 = 1$, $p_5 = 0$ и представлены на рисунке 6.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверной вычислительной сети.

Практическая значимость заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования клиент-серверной вычислительной сети при различных условиях динамического конфигурирования структурно-функциональных характеристик.

5. Алгоритм динамического конфигурирования клиент-серверных вычислительных сетей. Назначением разработанного алгоритма является динамическая конфигурация СФХ сетевых устройств КС ВС, обеспечивающая повышение результативности и снижение ресурсоемкости защиты за счет изменения значений *IP*-адресов клиентов в зависимости от условий функционирования КС ВС и действий злоумышленника в рамках задаваемого перечня подсетей без разрыва активных соединений.

Наиболее близким аналогом по своей технической сущности к представленному научно-методическому аппарату является [14], где обеспечивается повышение защищенности вычислительных сетей от несанкционированных воздействий за счет постоянного изменения *IP*-адресов в рамках одной подсети через равные, предварительно заданные интервалы времени. Это может привести к возможности вскрытия злоумышленником алгоритма изменения значений *IP*-адресов узлов защищаемой вычислительной сети и принятию им мер по обходу системы защиты.

Недостатками известных алгоритмов являются:

– относительно низкая результативность защиты КС ВС, обусловленная возможностью ложного срабатывания системы защиты и перегрузкой КС ВС [24];

– высокая ресурсоемкость защиты, обусловленная необходимостью применения дополнительного специального программного обеспечения, расходующего ресурсы сети на преобразование исходящих пакетов в свой собственный протокол, а также изменением *IP*-адресов сетевых устройств защищаемой КС ВС через фиксированные промежутки времени вне зависимости от условий функционирования и действий средств СР злоумышленника [25-29];

– относительно узкая область применения, обусловленная разрывом всех активных соединений между сетевыми устройствами при изменении СФХ КС ВС в случае обнаружения воздействия средств СР, а также изменением *IP*-адресов клиентов защищаемой вычислительной сети в рамках только одной подсети [30, 31].

Физическая (содержательная) постановка задачи. Стационарность значений СФХ сетевых устройств КС ВС, распределенных в большинстве случаев на все время функционирования КС ВС [32], позволяет злоумышленнику бескомпроматно вскрывать их средствами СР в реальном масштабе времени и в последующем успешно подвергать воздействию КА [33-36]. К тому же блокирование запросов СР штатными средствами защиты приводит к компрометации средств защиты и вынуждает злоумышленника менять пути их обхода и/или стратегию воздействия. В связи с этим для уменьшения времени актуальности и снижения достоверности добытых СР данных необходимо динамическое конфигурирование изначально стационарных СФХ сетевых устройств КС ВС с продолжительностью цикла их конфигурирования меньшей, чем продолжительность цикла добывания данных средствами СР, что заставит злоумышленника для компенсации мер защиты увеличивать интенсивность применения средств СР и в итоге приведет уже к его компрометации.

Конфигурирование СФХ *DHCP*-сервером осуществляют через интервалы времени, изменяемые адаптивно в зависимости от условий функционирования и действий злоумышленника. Другой особенностью алгоритма является то, что конфигурирование СФХ сетевых устройств КС ВС в рамках одной подсети, состоящей из относительно большого количества *IP*-адресов, накладывает ограничение на используемый диапазон их перестройки, к тому же при внештатном изменении СФХ недопустим разрыв критически важных активных соединений, например по протоколам *FTP, HTTPS, POP3, SMTP, VoIP, H.323*, между сетевыми устройствами КС ВС. В связи с этим в разработанном алгоритме для предотвращения реализации злоумышленником мер по обходу системы защиты изменение *IP*-адресов производят в рамках задаваемого диапазона подсетей без разрыва критически важных активных соединений.

Ограничения и допущения. Информация о легитимности и нелегитимности клиентов КС ВС, устанавливающих соединения, считается достоверной за счет применения комплекса средств защиты. Исходя из определения понятия легитимный, то есть соответствующий закону, под легитимностью клиента понимается его законное право находиться в составе КС ВС, установленное политикой безопасности сети, требова-

ниями и рекомендациями по обеспечению безопасности информации в КС ВС. Проверка на легитимность клиента должна производиться перед установлением соединений в КС ВС. Для получения численных оценок процесса защиты от средств СР используется разработанная модель функционирования КС ВС. Конфигурация СФХ КС ВС заключается в управлении формируемыми и распределяемыми *DHCP*-сервером значениями параметров сетевых устройств КС ВС, таких как *IP*-адреса, время продолжительности их аренды, *IP*-адрес *DHCP*-сервера, номер подсети.

Показатели и критерии. Показателем эффективности динамической конфигурации СФХ КС ВС является максимизация вероятности доступности информации клиентами КС ВС в связи со сменой СФХ $P_{AC}(t) \to \max$:

$$< MIP, Z > \to \max P_{AC} = \lim_{t \to \infty} P_{AC}(t) \mid P_{AC} \in \{P_i\},\ i = 1, 2, \ldots, h. \qquad (4)$$

Теоретическая основа алгоритма – теории систем управления, вероятности, массового обслуживания, исследования операций.

Блок-схема алгоритма динамического конфигурирования КС ВС, представленная на рисунке 7, включает следующие этапы:

1. Задают основные исходные данные, обозначение и описание которых приведены в таблице 3.

2. Подключают сетевые устройства к подсети.

3. Задают сетевым устройствам *IP*-адреса, время продолжительности их аренды $t^d_{\max}$, номер d сети *DHCP*-сервера и *IP*-адрес IP^d_{dhcp} выбранного *DHCP*-сервера, временные параметры синхронизации времени.

4. Устанавливают соединения между сетевыми устройствами.

5. Назначают установленным соединениям CIP_m.

6. Принимают из канала связи пакет сообщения.

7. Выделяют CIP_m из заголовка принятого пакета и сравнивают их с идентификаторами санкционированных информационных потоков *TS*.

8. В случае их совпадения передают пакет сообщений получателю и принимают из канала связи следующий пакет сообщения.

9. В ином случае сравнивают *IP*-адрес получателя с *FIP*.

10. В случае их несовпадения игнорируют пакет сообщений.

11. В ином случае сравнивают *IP*-адрес отправителя пакетов сообщений с каждым *IP*-адресом из множества IP^d.

12. В случае их совпадения блокируют *IP*-адрес отправителя и тем самым изолируют злоумышленника от дальнейшего информационного обмена в подсети при последующем изменении *IP*-адресов сетевых устройств.

Таблица 3. Обозначение и описание основных исходных данных

Переменная	Описание
D	Массив памяти (байт) для хранения номера подсети *DHCP*-сервера, где $D = [1, 2, \ldots, z]$, а z – максимальное количество номеров подсетей
$t^d_{\max}$	Максимальное значение времени аренды всех *IP*-адресов подсети с номером d, где d – номер подсети *DHCP*-сервера, $d = 1, 2 \ldots z$
CIP_m	Идентификатор соединения между сетевыми устройствами
C_i	Массив памяти (байт) для хранения идентификаторов соединения между сетевыми устройствами CIP_m, который содержит в себе *IP*-адрес отправителя – c, и получателя – b, тип протокола взаимодействия, порты взаимодействия, где m – максимальное допустимое количество соединений между сетевыми устройствами
CC	Массив памяти (байт) для хранения идентификаторов критически важных соединений между сетевыми устройствами, которые не подлежат разрыву, где $CC = [CIP^c_1, CIP^c_2 \ldots CIP^c_m]$, а CIP^c_m – идентификатор критических соединений между сетевыми устройствами
N_A	Массив памяти (байт) для хранения матрицы соответствия n-му *IP*-адресу сетевого устройства l-го *MAC*-адреса, где l – максимальное количество сетевых устройств в подсети, а n – максимальное допустимое значение количества *IP*-адресов сетевых устройств в подсети
d	Подмножество во множестве *IP*-адресов сетевых устройств подсети $IP^d = \{IP^d_1, IP^d_2 \ldots IP^d_n\}$
IP^d_{dhcp}	*IP*-адреса доверенных *DHCP*-серверов, где IP^d_{dhcp} – *IP*-адрес *DHCP*-сервера для подмножества d, $IP^d_{dhcp} \in IP^d$, чем обеспечивают невозможность использования ложного *DHCP*-сервера злоумышленником
FIP	Множество предварительно заданных ложных *IP*-адресов клиентов
C	Множество всех возможных соединений между сетевыми устройствами, $C = \{CIP_1, CIP_2 \ldots CIP_m\}$
A_m	Маркер активности соединения
TS	Множество идентификаторов санкционированных информационных потоков, $TS \geq 1$
FIP^d	Множество *IP*-адресов ложных клиентов вычислительной сети d, $FIP^d = \{FIP^d_1, FIP^d_2 \ldots FIP^d_n\}$, где n – максимальное допустимое количество *IP*-адресов сетевых устройств ВС

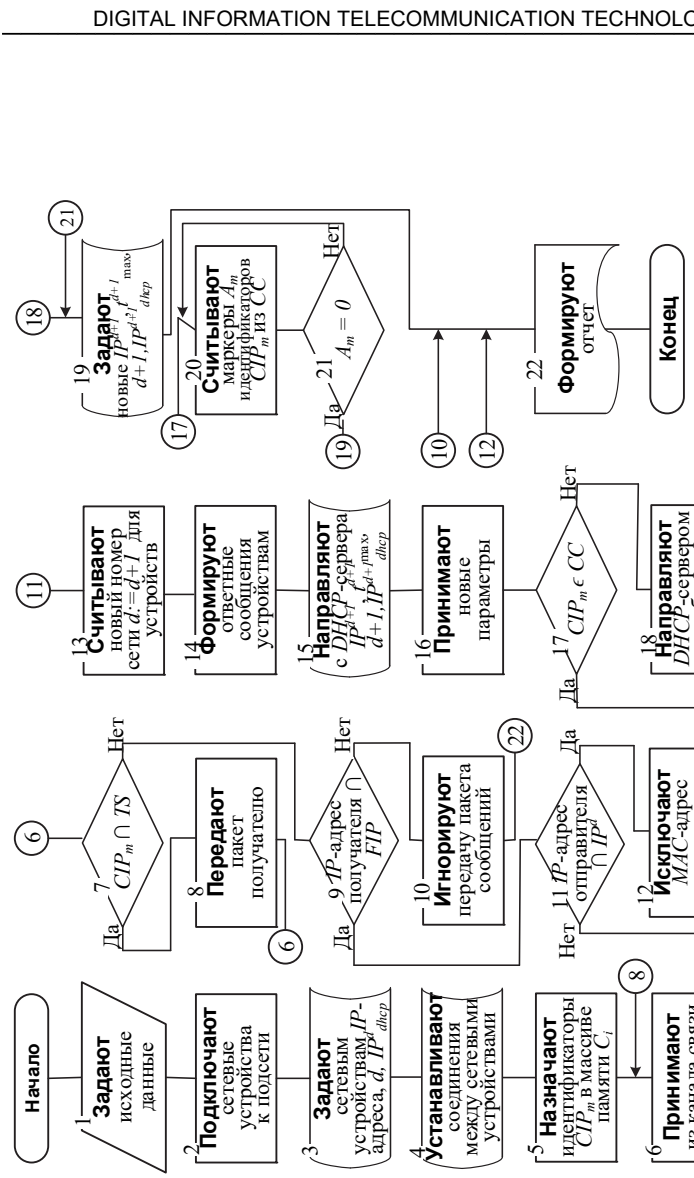


Рис. 7. Блок-схема последовательности действий, реализующих алгоритм динамического конфигурирования КС ВС

13. В ином случае изменяют СФХ сетевых устройств. Для этого считывают *DHCP*-сервером очередной номер подсети путем увеличения текущего номера сети d на единицу.

14. Формируют *DHCP*-сервером ответные сообщения каждому сетевому устройству.

15. Направляют сообщения с новыми сетевыми параметрами для каждого из сетевых устройств.

16. Принимают сообщения каждым из сетевых устройств.

17. Сравнивают, принадлежит ли идентификатор соединения между сетевыми устройствами множеству идентификаторов критических соединений.

18. В случае, если $CIP_m \notin CC$, направляют с *DHCP*-сервера сообщение сетевым устройствам, содержащее значение $t^d_{\max} = 0$ (прекращение аренды действующего *IP*-адреса).

19. Задают каждому сетевому устройству принятые новые параметры сетевой конфигурации.

20. В случае, если $CIP_m \in CC$ (прерываемые соединения является критическими), считывают маркеры активности соединений идентификаторов из множества *CC*.

21. В случае, если критическое соединение не активно ($A_m = 0$), то сетевым устройствам задают новые сетевые параметры. В ином случае ($A_m \neq 0$) вновь считывают маркеры активности соединений до тех пор, пока критическое соединение станет не активным.

22. Формируют отчет.

Для минимизации возможностей злоумышленника по реконструкции СФХ КС ВС в разработанном алгоритме в качестве функции выбора значения номера подсети *DHCP*-сервера используют последовательность чисел Фибоначчи, значение времени продолжительности аренды *IP*-адресов сетевых устройств *DHCP*-сервер выбирают случайным образом в пределах от 700 до 2592000 секунд, очередной номер подсети *DHCP*-сервера d вычисляют как $d = d+1$, а в качестве функции выбора значений *IP*-адресов сетевых устройств используют последовательность чисел Люка.

Для оценки вероятности вскрытия структуры КС ВС средствами СР в разработанном алгоритме используется модель функционирования клиент-серверной ВС в условиях ведения СР злоумышленником. При этом интенсивность потоков события λ_{25} интерпретируется как интенсивность заявок на оценку перегрузки КС ВС. Для этого рассмотрены следующие две ситуации.

Ситуация C_4. Средства СР обнаружены штатными средствами защиты КС ВС, поток заявок на обнаружение и оценку результативности обнаружения средств СР злоумышленника постоянный. Для упре-

ждения злоумышленника по вскрытию СФХ КС ВС сразу после компрометации средств СР *DHCP*-сервером увеличивается интенсивность потока заявок на внештатное изменение СФХ КС ВС. Финальные вероятности для ситуации C_4 имеют следующие значения: $p_1 = 0.353$, $p_2 = 0.294$, $p_3 = 0$, $p_4 = 0.059$, $p_5 = 0.294$ (рис. 8).

Из рисунка 8 видно, что для предотвращения вскрытия СФХ КС ВС средствами СР необходимо увеличение интенсивности заявок на внештатное изменение СФХ КС ВС *DHCP*-сервером таким образом, чтобы цикл динамической конфигурации СФХ заканчивался ранее цикла их вскрытия средствами СР злоумышленника.

Ситуация C_5. КС ВС функционирует в условиях ведения СР злоумышленником. Средства СР не обнаружены штатными средствами защиты КС ВС, поток заявок на обнаружение и оценку результативности обнаружения средств СР злоумышленника постоянный. Для предупреждения воздействия средств СР по вскрытию СФХ КС ВС, *DHCP*-сервером осуществляется периодическое внештатное изменение СФХ КС ВС.

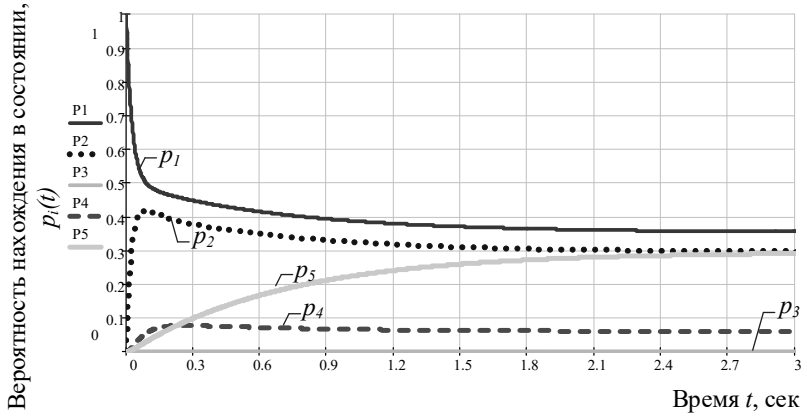


Рис. 8. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_4

На интервале времени [0; 7] на рисунке 9 КС ВС находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояния $p_2(t)$ и $p_5(t)$, а также незначительный всплеск значения вероятности состояния $p_4(t)$, что соответствует нахождению моделируемой системы в состоянии внештатного изменения СФХ КС ВС с интенсивностью потока заявок, обеспечивающей дискриминацию воздействий средств СР.

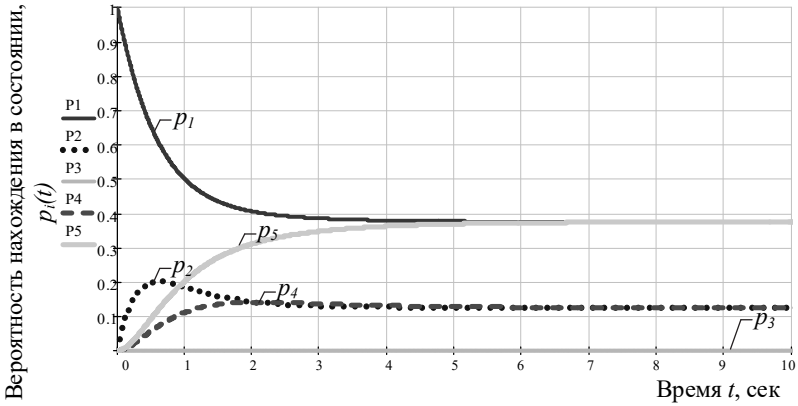


Рис. 9. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_5, с низкой интенсивностью внештатного изменения СФХ КС ВС *DHCP*-сервером

Из рисунка 9 видно, что периодическое внештатное изменение с низкой интенсивностью СФ Х КС ВС *DHCP*-сервером в целях усложнения процедуры реконструкции злоумышленником алгоритма перестройки *IP*-адресов и других СФХ элементов КС ВС поможет скрыть состав, структуру и алгоритмы функционирования КС ВС от СР и переведет КС ВС в заранее заданную конфигурацию при реализации злоумышленником КА. Финальные вероятности для ситуации C_5 имеют следующие значения: $p_1 = 0.375$, $p_2 = 0.125$, $p_3 = 0$, $p_4 = 0.125$, $p_5 = 0.375$.

6. Результаты исследований. Результативность разработанного алгоритма была проверена путем его программной реализации и проведения натурного эксперимента в среде виртуализации *EVE-NG* с использованием операционных систем *Linux Kali* и *Linux Debian*.

Схема моделируемой КС ВС представлена на рисунке 10 и включает в себя две рабочие станции *Workstation* 1, 2, *DHCP*-сервер, средство СР – *Intruder* и коммутатор.

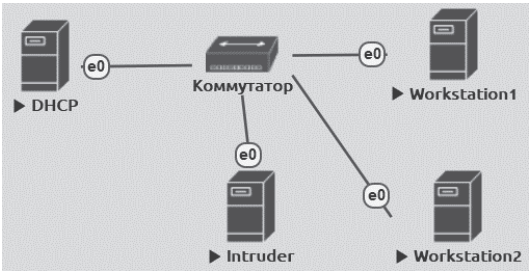


Рис. 10. Схема КС ВС

В ходе первого этапа эксперимента исследована возможность обнаружения злоумышленником изначально заданных *IP*-адресов сетевых устройств КС ВС: *DHCP*-сервера с *IP*-адресом 10.10.0.1/32 (рис. 11) и заданных им *IP*-адресов рабочих станций *Workstation* 1 и 2, имеющих значения 10.10.0.3/32 и 10.10.0.2/32 соответственно (рис. 12).

Рис. 11. Параметры *DHCP*-сервера

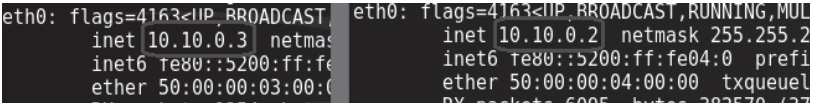


Рис. 12. Сетевые параметры рабочих станций

Для обнаружения активных *IP*-адресов в сети злоумышленником применялся сетевой сканер *NMAP* с использованием официального графического интерфейса *Zenmap*, отображающего следующую группу параметров, которая представлена на рисунке 13: «*Target*» – цель сканирования; «*Host*» – найденные устройства в сети; «*Nmap output*» – отчет и уязвимости найденных устройств в сети.

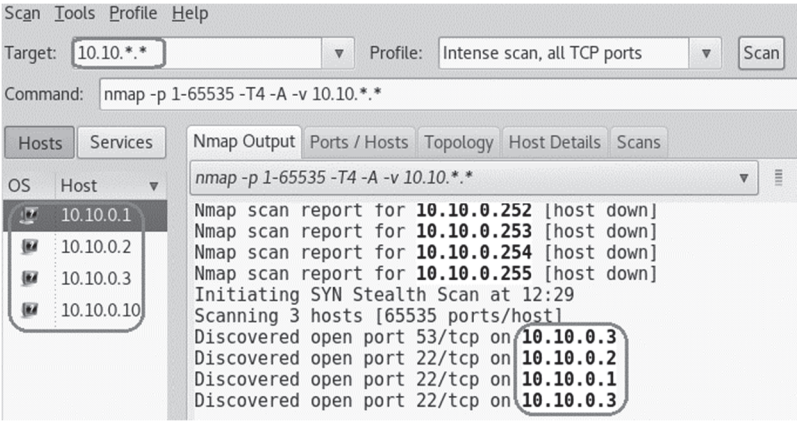


Рис. 13. Сканирование КС ВС злоумышленником

Поиск сетевых устройств осуществлялся в сети 10.10.*.*. Для идентификации узлов сети (*host detection*) злоумышленником с применением сканера *Nmap* направлялись запросы *ECHO_REQUEST* с использованием протокола *ICMP*. Применение режима *Decoy* в сканере

Nmap при каждом его запросе позволило злоумышленнику сфальсифицировать свой истинный *IP*-адрес (адрес источника). Такой набор средств сканирования достаточно эффективен и для противодействия ему необходимо применить средства анализа трафика или систем обнаружения атак.

По результатам проведенного сетевого сканирования средством *NMAP* был построен графический рисунок с изображением топологии сети и *IP*-адресами сетевых устройств КС ВС (рис. 14), а также сформирован отчет, отображающий открытые сетевые порты рабочих станций КС ВС, которые в дальнейшем могут использоваться злоумышленником в целях проведения КА (рис. 13).

В ходе второго этапа эксперимента в качестве средства защиты был применен *DHCP*-сервер, реализующий функцию динамического конфигурирования СФХ КС ВС. *DHCP*-сервером осуществлялась фиксация запросов *ECHO_REQUEST* и сравнение *IP*-адреса отправителя этих запросов с *IP*-адресами, хранящимися во множестве предварительно заданных ложных *IP*-адресов, обращение к которым исключено для легитимных клиентов КС ВС и свидетельствует о факте воздействия средств СР. В случае их совпадения *DHCP*-сервер осуществлял реконфигурацию значений ранее распределенных СФХ рабочих станций КС ВС (рис. 15), а именно значений *IP*-адресов, времени их аренды и номера подсети рабочих станций (рис. 16 и 17).

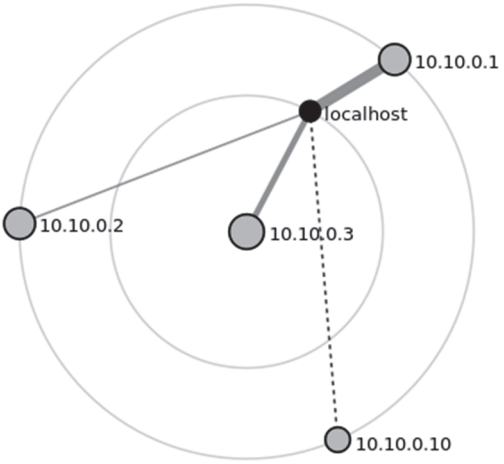


Рис. 14. Результат работы сканера *Nmap*

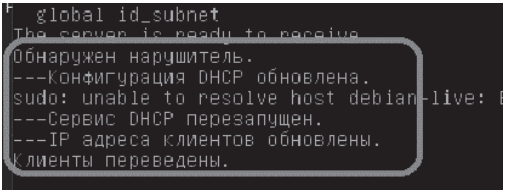


Рис. 15. Работа *DHCP*-сервера

Рис. 16. Новые сетевые параметры *DHCP*-сервера

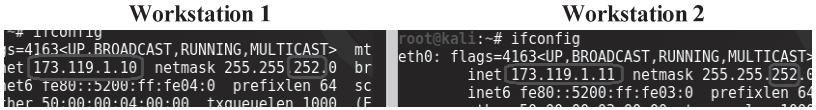


Рис. 17. Новые сетевые параметры рабочих станций

Представленная на рисунке 18 экранная форма наглядно демонстрирует, что после реконфигурации сетевых параметров рабочих станций КС ВС злоумышленник не может идентифицировать их значения. Таким образом, у него возникает необходимость повторного подбора параметров сканирования КС ВС либо расширения области сканирования, что в обоих случаях значительно увеличивает затрачиваемый им вычислительный и временной ресурс.

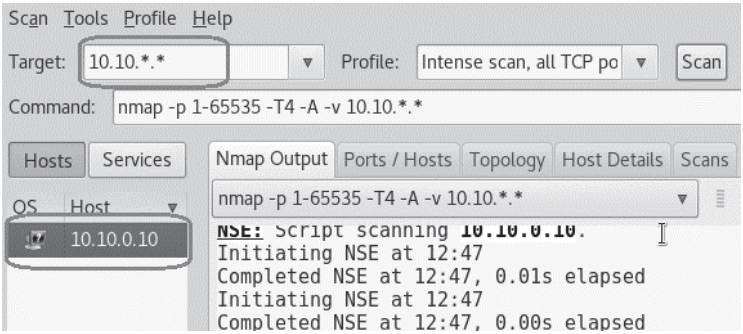


Рис. 18. Повторное сканирование КС ВС злоумышленником

7. Заключение. Расширение возможностей и повышение результативности сетевой разведки обусловлены стационарностью структурно-функциональных характеристик клиент-серверных вычис-

лительных сетей. В этой связи актуальной является задача динамического управления структурно-функциональными характеристиками клиент-серверных вычислительных сетей, функционирующих в условиях сетевой разведки.

Процесс функционирования клиент-серверной вычислительной сети в условиях динамического конфигурирования ее структурно-функциональных характеристик представлен как марковский случайный процесс с дискретными состояниями и непрерывным временем, что позволило находить оптимальные режимы для различных ситуаций.

Получены вероятностные и временные показатели, описывающие функционирование клиент-серверной вычислительной сети при различных ситуациях динамического управления ее структурно-функциональными характеристиками. Показано, что если длительность цикла динамического конфигурирования будет меньше длительности цикла сетевой разведки, то вскрытие состава и структуры сети будет сорвано, а получаемая сетевой разведкой информация не будет достоверной.

Новизна полученных результатов заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей.

Разработанные алгоритм и технические решения практически испытаны – достигнуто поддержание критически важных соединений, а интервалы времени изменения структурно-функциональных характеристик адаптивны к условиям функционирования и действиям злоумышленника.

Литература

1. *Jajodia S. et al.* Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats // Springer. 2011. 184 p.
2. *Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П.* Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6(34). С. 92–101.
3. RFC 2131. Dynamic Host Configuration Protocol. 1997. URL: https://tools.ietf.org/html/rfc2131 (дата обращения: 04.04.2020).
4. RFC 826. An Ethernet Address Resolution Protocol. 1982. URL: https://tools.ietf.org/html/rfc826 (дата обращения: 05.04.2020).
5. *Sokolovsky S.P., Telenga A.P., Voronchikhin I.S.* Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии: Сб. материалов XIX междунар. научн.-методич. конф. 2019. С. 639–643.
6. *Максимов Р.В., Соколовский С.П., Шарифуллин С.Р., Чернолес В.П.* Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3(233). С. 28–35.
7. *Eskridge T.C. et al.* Integrated decision engine for evolving defenses // Patent US 20180309794A1, pub. 25.10.2018.

8. *Котенко И.В., Саенко И.Б., Коцыняк М.А., Лаута О.С.* Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. Вып. 6(55). С. 160–184.
9. *Jafarian J.H., Al-Shaer E., Duan Q.* Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers // Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 69–78.
10. *MacFarland D.C., Shue C.A.* The SDN shuffle: creating a moving-target defense using host-based software-defined networking // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 37–41.
11. Cyber Maneuvering and Morphing. 2012. URL: https://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html (дата обращения: 31.04.2020).
12. What is Moving Target Defense. 2017. URL: https://www.cryptomove.com/what-is-mtd.html (дата обращения: 31.04.2020).
13. *Максимов Р.В., Соколовский С.П., Ворончихин И.С.* Способ защиты вычислительных сетей // Патент на изобретение RU 2716220, опубл. 06.03.20. Бюл. № 7. 33 с.
14. *Antonatos S., Akritidis P., Markatos E., Anagnostakis K.* Defending against Hitlist Worms using Network Address Space Randomization // 2005 ACM Workshop on Rapid Malcode. 2005. pp. 30–40.
15. *Cai G., Wang B., Wang X., Yuan Y., Li S.* An introduction to network address shuffling // 2016 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 185–190.
16. *Luo Y.B. et al.* RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries // Trustcom/BigDataSE/ISPA. 2015. pp. 263–270.
17. *Green M., MacFarland D.C., Smestad D.R., Shue C.A.* Characterizing network-based moving target defenses // ACM CCS Workshop on Moving Target Defense. 2015. pp. 31–35.
18. *Zhuang R., DeLoach S.A., Ou X.* Towards a theory of moving target defense // Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 31–40.
19. *Antonatos S., Anagnostakis K.G.* Tao: Protecting against hitlist worms using transparent address obfuscation // Communications and Multimedia Security. 2006. pp. 12–21.
20. *Wang A. et al.* Scotch: Elastically scaling up SDN control-plane using vs witch based overlay // ACM International on Conference on Emerging Networking Experiments and Technologies. 2014. pp. 403–414.
21. *Zhuang R., Bardas A.G., DeLoach S.A., Ou X.* A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 11–20.
22. *Вентцель Е.С.* Исследование операций: задачи, принципы, методология. 2-е изд. // М.: Наука. 1988. 208 с.
23. *Максимов Р.В., Орехов Д.Н., Соколовский С.П.* Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50–99.
24. *Zhao Z.Y., Guo Y.B., Liu W.* The Design and Research for Network Address Space Randomization in OpenFlow Network // Journal of Computer and Communications. 2015. № 3. pp. 203–211.
25. *Ganga G. et al.* Adaptor implementation for Internet Protocol address and port hopping // Patent US 20160036691A1. pub. 04.02.2016.
26. *Cruz A. et al.* Method for selection of unique next-time interval Internet Protocol address and port // Patent US 20150236752A1. pub. 20.08.2015.
27. *Fink R.A., Bubnis E.A., Keller T.E.* Method and apparatus for anonymous IP datagram exchange using dynamic network address translation // Patent US 20120117376A1. pub. 04.05.2012.
28. *Kravcov K.N.* Data transmission in networks with address space dynamic randomization // Selected Papers of the 17th International Conference on Data Analytics and Management in Data Intensive Domains. 2015. pp. 273–277.

29. *Котенко И.В., Саенко И.Б., Кушнеревич А.Г.* Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей интернета вещей // Труды СПИИРАН. 2018. Вып. 4(59). С. 5–30.
30. *Ellard D.J. et al.* Method for selection of unique next-time interval Internet Protocol address and port // Patent US 20150236752A1, pub. 20.08.2015.
31. *Котенко И.В., Саенко И.Б., Полубелова О.В.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Вып.1 (20). С. 27–56.
32. *Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P.* Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines // Вопросы кибербезопасности. 2019. № 1 (29). С. 10–17.
33. *Крупенин А.В., Соколовский С.П., Хорев Г.А., Калач А.В.* Маскирование идентификаторов канального уровня средств проактивной защиты интегрированных сетей связи специального назначения // Вестник Воронежского института ФСИН России. 2018. № 3. С. 81–89.
34. *Шерстобитов Р.С., Шарифуллин С.Р., Максимов Р.В.* Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136–175.
35. *Crouse M., Prosser B., Fulp E.W.* Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 21–29.
36. *Okhravi H. et al.* Creating a cybermoving target for critical infrastructure applications using platform diversity // International Journal of Critical Infrastructure Protection. 2015. № 5(1). pp. 30–39.

Максимов Роман Викторович — д-р техн. наук, профессор, специальная кафедра, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности, синтез и системный анализ систем защиты информации критически важных объектов, маскирование информационных ресурсов интегрированных ведомственных сетей связи. Число научных публикаций — 210. rvmaxim@yandex.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7(928)037-96-63.

Соколовский Сергей Петрович — канд. техн. наук, доцент, докторант, специальная кафедра, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности, синтез и системный анализ систем защиты информации критически важных объектов, маскирование информационных ресурсов интегрированных ведомственных сетей связи. Число научных публикаций — 200. mtd.krd@mail.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7(951)851-5408.

Ворончихин Иван Сергеевич — адъюнкт, специальная кафедра, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности, системный анализ систем защиты информации критически важных объектов, рандомизация сетевого адресного пространства. Число научных публикаций — 22. 5.00@mail.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7 (996) 379-34-22.

DOI 10.15622/ia.2020.19.5.5

R. MAXIMOV, S. SOKOLOVSKY, I. VORONCHIKHIN

ALGORITHM AND TECHNICAL SOLUTIONS FOR DYNAMIC CONFIGURATION OF CLIENT-SERVER COMPUTING NETWORKS

Maximov R., Sokolovsky S., Voronchikhin I. **Algorithm and Technical Solutions for Dynamic Configuration of Client-Server Computing Networks.**

Abstract. The main factors that determine the expansion of capabilities and increase the effectiveness of network intelligence to identify the composition and structure of client-server computer networks due to the stationarity of their structural and functional characteristics are analyzed. The substantiation of an urgent problem of dynamic management of structurally-functional characteristics of the client-server computer networks functioning in the conditions of network reconnaissance is resulted on the grounds of the revealed protection features of client-server computer networks at the present stage that is based on realization of principles of spatial safety maintenance, and also formalization and introduction of forbidding regulations.

The mathematical model allowing to find optimum modes for dynamic configuration of structurally-functional characteristics of client-server computer networks for various situations is presented. Calculation results are given. An algorithm is presented that makes it possible to solve the problem of dynamic configuration of the structural and functional characteristics of a client-server computer network, which reduces the reliability time of data obtained by network intelligence. The results of practical tests of software developed on the basis of the dynamic configuration algorithm of client-server computer networks are shown. The obtained results show that the use of the presented solution for the dynamic configuration of client-server computer networks allows to increase the effectiveness of protection by changing the structural and functional characteristics of client-server computer networks within several subnets without breaking critical connections through time intervals that are adaptively changed depending on the functioning conditions and the attacker's actions.

The novelty of the developed model lies in the application of the mathematical apparatus of the Markov's theory of random processes and Kolmogorov's solution of equations to justify the choice of dynamic configuration modes for the structural and functional characteristics of client-server computer networks. The novelty of the developed algorithm is the use of a dynamic configuration model for the structural and functional characteristics of client-server computer networks for the dynamic control of the structural and functional characteristics of a client-server computer network in network intelligence.

Keywords: Network Intelligence, Client-server Computer Networks, Moving Target Technology, Computer Attack, Cybermaneuvering

Maximov Roman — Ph.D., Dr.Sci., Professor, Special Department, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security, synthesis and system analysis of information security systems of critical objects, masking and simulation of information resources of integrated departmental communication networks. The number of publications — 210. rvmaxim@yandex.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7(928)037-96-63.

Sokolovsky Sergey — Ph.D., Associate Professor, Doctoral Student, Special Department, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: nformation security, synthesis and system analysis of information security systems of critical objects, masking and simulation of information resources of integrated departmental communication networks. The number of publications — 200. mtd.krd@mail.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7(951)851-5408.

Voronchikhin Ivan — Ph.D. Student, Special Department, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security, system analysis of information security systems of critical objects, network address space randomization. The number of publications — 22. 5.00@mail.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7 (996) 379-34-22.

References

1. Jajodia S. et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Springer. 2011. 184 p.
2. Voronchikhin I.S., Ivanov I.I., Maximov R.V., Sokolovsky S.P. [Masking the structure of distributed information systems in cyberspace]. *Voprosy kiberbezopasnosti – Cybersecurity issues*. 2019. vol. 6 (34). pp. 92–101. (In Russ).
3. RFC 2131. Dynamic Host Configuration Protocol. 1997. Available at: https://tools.ietf.org /html/rfc2131 (accessed: 04.04.2020).
4. RFC 826. An Ethernet Address Resolution Protocol. 1982. Available at: https://tools.ietf.org /html/rfc826 (accessed: 05.04.2020).
5. Sokolovsky S.P., Telenga A.P., Voronchikhin I.S. [Moving target defense for securing Distributed Information Systems] *Informatika: problemy, metodologija, tehnologii: Sb. materialov XIX mezhdunar. nauchn.-metodich. konf.* [Informatics: problems, methodology, technologies: collection of materials of the XIX international scientific and methodological conference]. 2019. pp. 639–643.
6. Maximov R.V., Sokolovsky S.P., Sharifullin S.R., Chernoles V.P. [Innovative information technologies in the context of ensuring national security of the state]. *Innovacii – Innovations*. 2018. vol. 3(233). pp. 28–35. (In Russ).
7. Eskridge T.C. et al. Integrated decision engine for evolving defenses. Patent US 20180309794A1, pub. 25.10.2018.
8. Kotenko I.V., Saenko I.B., Kozinak M.A., Louth O.S. [Estimation of cyber stability of computer networks based on simulation of cyber attacks using stochastic network transformation method]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2017. vol. 6(55). pp. 160–184. (In Russ).
9. Jafarian J.H., Al-Shaer E., Duan Q. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers. *Proceedings of the First ACM Workshop on Moving Target Defense.* 2014. pp. 69–78.
10. MacFarland D.C., Shue C.A. The SDN shuffle: creating a moving-target defense using host-based software-defined networking. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 37–41.
11. Cyber Maneuvering and Morphing. 2012. Available at: https://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html (accessed: 31.04.2020).
12. What is Moving Target Defense. 2017. Available at: https://www.cryptomove.com/what-is-mtd.html (accessed: 31.04.2020).
13. Maximov R.V., Sokolovsky S.P. Voronchikhin I.S. *Sposob zashchity vychislitel'nih setey* [Method of Protection of Computer Networks]. Patent Russia, no. 2716220, 06.03.2020. (In Russ.).
14. Antonatos S., Akritidis P., Markatos E., Anagnostakis K. Defending against Hitlist Worms using Network Address Space Randomization. 2005 ACM Workshop on Rapid Malcode. 2005. pp. 30–40.
15. Cai G., Wang B., Wang X., Yuan Y., Li S. An introduction to network address shuffling. 2016 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 185–190.
16. Luo Y.B. et al. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries. Trustcom/BigDataSE/ISPA. 2015. pp. 263–270.
17. Green M., MacFarland D.C., Smestad D.R., Shue C.A. Characterizing network-based moving target defenses. ACM CCS Workshop on Moving Target Defense. 2015. pp. 31–35.

18. Zhuang R., DeLoach S.A., Ou X. Towards a theory of moving target defense. Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 31–40.
19. Antonatos S., Anagnostakis K.G. Tao: Protecting against hitlist worms using transparent address obfuscation. Communications and Multimedia Security. 2006. pp. 12–21.
20. Wang A. et al. Scotch: Elastically scaling up SDN control-plane using vs witch based overlay. ACM International on Conference on Emerging Networking Experiments and Technologies. 2014. pp. 403–414.
21. Zhuang R., Bardas A.G., DeLoach S.A., Ou X. A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 11–20.
22. Ventcel' E.S. *Issledovanie operacij: zadachi, principy, metodologija* [Operations research: objectives, principles, and methodology]. M.: Nauka. 1988. 208 p. (In Russ).
23. Maximov R.V., Orehov D.N., Sokolovsky S.P. [Model and algorithm of functioning of the client-server information system in the conditions of network intelligence]. *Sistemy upravlenija, svjazi i bezopasnosti – Management, communication and security systems.* 2019. vol. 4. pp. 50–99. (In Russ).
24. *Zhao Z.Y., Guo Y.B., Liu W.* The Design and Research for Network Address Space Randomization in OpenFlow Network. *Journal of Computer and Communications*. 2015. vol. 3. pp. 203–211.
25. Ganga G. et al. Adaptor implementation for Internet Protocol address and port hopping. Patent US 20160036691A1. pub. 04.02.2016.
26. Cruz A. et al. Method for selection of unique next-time interval Internet Protocol address and port. Patent US 20150236752A1. pub. 20.08.2015.
27. Fink R.A., Bubnis E.A., Keller T.E. Method and apparatus for anonymous IP datagram exchange using dynamic network address translation. Patent US 20120117376A1. pub. 04.05.2012.
28. Kravcov K.N. Data transmission in networks with address space dynamic randomization. Selected Papers of the 17th International Conference on Data Analytics and Management in Data Intensive Domains. 2015. pp. 273–277.
29. Kotenko I.V., Saenko I.B., Kushnerevich A.G. [Architecture of a parallel big data processing system for monitoring the security of Internet of things networks]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2018. vol. 4(59). pp. 5–30. (In Russ).
30. Ellard D.J. et al. Method for selection of unique next-time interval Internet Protocol address and port. Patent US 20150236752A1, pub. 20.08.2015.
31. Kotenko I.V., Saenko I.B., Polubelova O.V. [Applying information and security event management technology to protect information in critical infrastructures]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2012. vol. 1(20). pp. 27–56. (In Russ).
32. Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. [Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines]. *Cybersecurity issues*. 2019. vol. 1(29). pp. 10–17.
33. Krupenin A.V., Sokolovsky S.P., Horev G.A., Kalach A.V. [Masking channel-level identifiers for proactive protection of integrated special-purpose communication networks]. *Vestnik Voronezhskogo instituta FSIN Rossii – Bulletin of the Voronezh Institute of the Federal penitentiary service of Russia.* 2018. vol. 3. pp. 81–89. (In Russ).
34. Sherstobitov R.S., Sharifullin S.R., Maksimov R.V. [Masking integrated communication networks for departmental purposes]. *Sistemy upravlenija, svjazi i bezopasnosti – Systems of Control, Communication and Security.* 2018. vol. 4. pp. 136–175. (In Russ).
35. Crouse M., Prosser B., Fulp E.W. Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 21–29.
36. Okhravi H. et al. Creating a cybermoving target for critical infrastructure applications using platform diversity. *International Journal of Critical Infrastructure Protection*. 2015. vol. 5(1). pp. 30–39.

УДК 004.056 **DOI** 10.15622/ia.2020.19.5.6

Д.С. Левшун, Д.А. Гайфулина, А.А. Чечулин, И.В. Котенко

ПРОБЛЕМНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. **Проблемные вопросы информационной безопасности киберфизических систем.**

Аннотация. Представляются анализ и систематизация современных исследований в области обеспечения информационной безопасности киберфизических систем. Рассматриваются проблемные вопросы, связанные с информационной безопасностью подобных систем: «Что атакуют?», «Кто атакует?», «Почему атакуют?», «Как атакуют?» и «Как защититься?». В качестве ответа на первый вопрос даются определение и классификация киберфизических систем по таким атрибутам этих систем, как сложность, связность, критичность и социальный аспект. В качестве ответа на второй и третий вопросы предлагается классификация атакующих по таким атрибутам, как тип доступа, способ доступа, намерения, знания и ресурсы. В качестве ответа на четвертый вопрос рассматривается классификация атакующих действий по таким атрибутам, как субъект и объект, способ воздействия, предпосылки и последствия. В качестве ответа на пятый вопрос предлагается классификация методов и средств защиты по таким атрибутам, как принцип работы, объект защиты и решаемая задача. Научная значимость статьи заключается в систематизации современного состояния исследований в предметной области. Практическая значимость статьи заключается в предоставлении информации о проблемных вопросах безопасности, которые характерны для киберфизических систем, что позволит учитывать их при разработке, администрировании и использовании таких систем.

Ключевые слова: информационная безопасность, киберфизическая система, цель атакующего, модель атакующего, модель атакующих действий, метод и средство защиты.

1. Введение. Киберфизические системы стали неотъемлемой частью нашей жизни: от электроэнергетики, производства и транспорта, до медицины, торговли и личного пользования [1]. Таким образом, обеспечение защищенности таких систем представляет собой критически важную задачу, решить которую в полной мере, как показывает практика в России и за рубежом, пока не удалось [2]. Это подтверждается, например, тем, что все чаще появляются новости о ботнетах из умных микроволновок и холодильников, используемых для проведения DDoS-атак, а также о взломе изолированных сетей критически важных предприятий через умные датчики и камеры [3]. Этим же обусловлена высокая актуальность выбранной темы.

Предполагается, что данная работа станет отправной точкой для разработчиков, исследователей и системных администраторов в понимании различных аспектов информационной безопасности киберфизических систем. Научная значимость статьи заключается в систематизации современного состояния исследований в предметной области. Практическая значимость статьи заключается в том, что ознакомление с ней позволит лучше понять, какие проблемы информационной безопасности характерны для киберфизических систем с точки зрения объекта атаки, злоумышленника, цели и мотива атаки, способа атаки, а также методов и средств защиты, и учитывать их при разработке, администрировании и использовании таких систем. Даются ответы на следующие вопросы: (1) что является объектом атаки? («Что атакуют?»); (2) кто является субъектом атаки? («Кто атакует?»); (3) каковы намерения атакующих? («Почему атакуют?»); (4) каков способ реализации атаки? («Как атакуют?»); (5) какие методы и средства защиты могут быть применены? («Как защититься?»).

В качестве ответа на первый вопрос в разделе 2 предлагаются определение и классификация киберфизических систем. Данная классификация позволяет оценить критичность системы или ее элементов в соответствии с зависящими от них бизнес-процессами, сложность в соответствии с функциональными возможностями и связность в соответствии с используемыми интерфейсами и протоколами передачи данных. Кроме того, данная классификация позволяет учесть социальный аспект работы системы в соответствии с задействованным персоналом и возможными пользователями.

В качестве ответа на второй и третий вопросы в разделе 3 разрабатывается классификация атакующих. Данная классификация позволяет оценить возможности атакующих в соответствии с типом доступа к системе, уровнем знаний и доступных ресурсов. Кроме того, предложенная классификация позволяет учесть возможные намерения атакующих, в том числе связанные с нарушением конфиденциальности и целостности информации, а также нарушением доступности устройств и перехватом управления ими.

В качестве ответа на четвертый вопрос в разделе 4 формируется классификация атакующих действий. Данная классификация позволяет установить взаимосвязь между атакующим и атакующими действиями в соответствии со знаниями и ресурсами, необходимыми злоумышленнику для их реализации, а также целью, которой соответствует их применение. Кроме того, данная классификация устанавливает взаимосвязь между

атакующими действиями и элементами киберфизической системы, в соответствии с которыми они могут быть реализованы.

В качестве ответа на пятый вопрос в разделе 5 предлагается классификация методов и средств защиты. Данная классификация позволяет оценить возможность реализации атакующих действий в соответствии с используемыми методами и средствами защиты. В разделе 6 представляются основные выводы по каждому из вопросов.

При этом ответы на упомянутые выше вопросы, точно также как и классификации, предложенные в качестве ответа на них, связаны между собой (рис. 1).

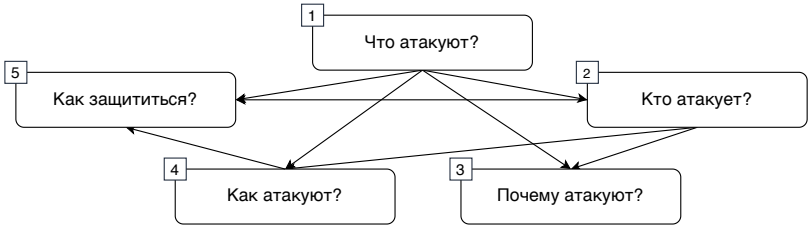


Рис. 1. Взаимосвязь между проблемными вопросами информационной безопасности

Взаимосвязь между вопросами показана направленными стрелками. При этом процесс выстраивания взаимосвязей изначально построен на двух основных понятиях информационной безопасности: злоумышленник («Кто атакует?») и объект атаки («Что атакуют?»). Затем, на основе информации об объекте атаки и злоумышленнике можно предположить цель атакующих («Почему атакуют?), а также используемые им инструменты и подходы («Как атакуют?»). Кроме того, при расширении информации об объекте атаки и злоумышленнике данными об используемых злоумышленником инструментах и подходах, становится возможным предположить эффективные способы противодействия («Как защититься?»). Отметим, что на рисунке показана прямая связь между вопросами, в то время как косвенные связи не отображены – в противном случае была бы связь все ко всем. Каждый из данных вопросов, точно также как и ответы на них, будут рассмотрены более подробно в последующих разделах.

2. Определение и классификация киберфизических систем. Применение киберфизических систем становится все более распространенным и востребованным, так как в этих системах реализована интеграция информационных технологий и устройств взаимодействия с

физическими процессами и объектами. Важно отметить, что в научной литературе пока не существует единого определения киберфизической системы, и в ряде работ присутствуют различные его описания. Термин киберфизическая система впервые был предложен в 2006 году для обозначения комплексов, состоящих из природных объектов, искусственных подсистем и контроллеров [4]. Кроме того, популяризация данного термина связана с проектом Индустрия 4.0 [5], в основе которого лежит внедрение данных систем в промышленность. Так в работе [6] представлен обзор различных типов систем и связанных с ними процессов перехода от мехатроники к облачным системам Интернета вещей или киберфизическим системам. Как правило, следующие системы относят к киберфизическим [7]: системы управления производством; Интернет вещей; «умный дом»; робототехнические системы; беспилотные летательные аппараты; беспилотные автомобили; системы военного назначения.

В исследовании [8] киберфизическая система определяется как новый тип системы, которая является результатом объединения встроенных программных систем, связанных, с одной стороны, с их физической средой с помощью датчиков и исполнительных механизмов, а с другой стороны, с глобальными сетями, такими как Интернет с его данными и услугами. Согласно [9] киберфизическая система представляет собой комплексную техническую систему, которая объединяет сенсорные технологии и технологии вычислений, связи и управления. Оборудование и программное обеспечение системы тесно связаны через сеть, формируя четыре процесса: сбор данных, анализ данных, принятие решений и их выполнение. В работе [10] используется понятие киберфизического пространства для обозначения условной среды, в которой в неразрывной связи существуют физические объекты и их информационные сущности. А в работе [7] понятие киберфизической системы представляется в качестве удобной концепции для представления технологических систем как результата интеграции физических процессов и информационной среды.

Резюмируя, можно выделить следующие характеристики, позволяющие отнести систему к киберфизической: (1) интеграция информационных технологий с физической средой; (2) наличие процессов сбора, хранения, анализа, обработки и предоставления данных; (3) наличие надежной среды передачи данных между элементами системы. Это означает, что киберфизическая система может быть определена как система, которая выполняет функции сбора, хранения, анализа, обработки и предоставления данных от устройств, взаимодействующих с физическими процессами и объектами, а также их тесную интеграцию с информационными технологиями в рамках надежной среды передачи данных. Под информационной безопас-

ностью киберфизической системы понимается обеспечение целостности, конфиденциальности и доступности обрабатываемых данных, а также инфраструктуры и связанных с ней физических процессов. Под информационной безопасностью киберфизической системы также можно понимать защищенность информации и информационных ресурсов этой системы от различного рода угроз (незаконного ознакомления, преобразования, уничтожения информации и нарушения работоспособности системы).

Точно также как при определении киберфизических систем, в научной литературе сложно обозначить единую их классификацию. В обобщенном виде основные атрибуты (признаки) классификации подобных систем можно представить следующим образом: *сложность* в соответствии с функциональными возможностями и используемыми компонентами; *связность* в соответствии с используемыми интерфейсами и протоколами передачи данных; *критичность* в соответствии с зависящими от системы бизнес-процессами; *социальный аспект* в соответствии с характером взаимодействия системы с пользователями и операторами. Понимание данных атрибутов позволяет получить представление о киберфизической системе, помогая определить, что является целью злоумышленника и какие возможности он использует при атаке на данную систему. Отметим, что учитывая множество способов оценки различных атрибутов киберфизических систем, в данном обзоре сделана попытка обобщить предлагаемые в научной и технической литературе решения и представить анализ в виде общего подхода. Рассмотрим каждый из представленных атрибутов более подробно.

Оценка сложности киберфизической системы может быть осуществлена в соответствии с функциональными возможностями данной системы и используемыми ей компонентами. Наиболее активно данные параметры киберфизических систем изучены в работах, связанных с их проектированием. При этом составляющие системы принято разделять на различные уровни в зависимости от функциональности элементов каждого слоя.

Например, авторы [11] предложили сервис-ориентированную архитектуру киберфизических систем, состоящую из таких уровней, как физический, сетевой и уровень сервисов. В исследовании [12] выделяют уровень восприятия, сетевой и прикладной. Задачей физического уровня, или уровня восприятия, является надежное считывание информации с датчиков. Сетевой уровень обеспечивает повсеместный доступ и передачу данных. На уровне сервисов, или прикладном уровне, выполняются функции по сбору, хранению, обработке и представлению данных.

В работах [13, 14] предложена архитектура киберфизической системы, состоящая из пяти уровней, которые содержат: *уровень соединения* – сбор всех видов данных от датчиков и контроллеров системы; *уровень преобразования данных* или *сетевой уровень* – анализ разнородных данных с целью определения значимой информации; *кибернетический уровень* или *уровень конвергенции* – центральный информационный узел в архитектуре, реализующий анализ данных и контроль работы системы; *уровень познания* – представление знаний пользователям, визуализация и принятие решений; *уровень конфигурации* – обратная связь между уровнями, выполнение функций центрального диспетчерского контроля.

Также распространенным представлением архитектуры киберфизических систем является структура из семи уровней модели ISO/OSI – от физического до прикладного уровня [15, 16]. Таким образом, элементы системы могут быть классифицированы по своей функциональности, то есть от места, занимаемого в общей архитектуре.

Киберфизические системы также могут быть классифицированы в зависимости от процессов, связанных с обработкой используемых ими данных. Например, в работе [17] предложен признак классификации данных систем по семантическому уровню используемых для работы данных: *уровень соединения* – использование данных, предоставляемых датчиками; *уровень преобразования* – использование данных от датчиков, после их предварительной обработки и агрегации; *уровень кибернетики* – использование данных от других систем; *уровень познания* – обработка данных датчиков на основе моделирования и дифференциального анализа для диагностики состояния системы; *уровень конфигурации* – использование поступающих данных для адаптации и реконфигурации.

Кроме того, согласно [18] оценку сложности можно также проводить на основе следующих структурных особенностей киберфизических систем: *количество контуров управления* – с одним контуром управления и множеством контуров управления; *структура контуров управления* – одноуровневые и иерархические; *количественный состав элементов* – фиксированный и переменный; *качественный состав элементов* – однородные и гетерогенные; *динамика поведения* – адаптивные и самоорганизующиеся. При этом под адаптацией и самоорганизацией подразумевается реакция на внешние воздействия, способность к прогнозированию предстоящих изменений во внешней среде, проведение внутреннего тестирования и совершенствование собственной организации не только под воздействием внешних факторов, но и в случае условно стабильной работы.

Отметим, что в области искусственных систем не существует четкой границы, разделяющей простые и сложные системы. При этом выделяют два основных способа оценки сложности систем [19]. Первый связан с количеством информации, необходимым для описания системы, и определяет ее дескриптивную сложность. Подобная оценка возможна на основе количественных параметров системы, например таких как число элементов, связей и иерархических уровней, а также непересекающихся системных функций [20]. Второй способ позволяет оценить сложность познания системы и связан с количеством информации, необходимым для уменьшения меры неопределенности системы. При этом дескриптивная сложность и сложность познания дополняют друг друга – возрастание одной сложности влечет за собой увеличение другой. Роль классификации киберфизических систем заключается в ограничении способов описания подобных систем, что задает основу для их оценки.

Оценка связности киберфизической системы может быть осуществлена в соответствии с используемыми в ней интерфейсами и протоколами передачи данных. Данная оценка затрагивает один из важнейших элементов любой системы – процесс организации надежного обмена данными между ее компонентами. При этом существующие телекоммуникационные технологии включают в себя как алгоритмы передачи данных, так и средства их реализации, вплоть до физических каналов связи.

В [18] для оценки связности киберфизических систем предлагается использовать такие признаки, как географическая распределенность и открытость системы. Относительно географической распределенности выделяют: централизованные системы, то есть системы, расположенные в границах одного физического объекта (предприятие, здание и т.п.), и распределенные системы, расположенные на нескольких связанных между собой объектах. Открытость системы определяет характер использования внутренних и внешних (глобальных) сетей и относит киберфизическую систему к системе закрытого типа, если для ее работы используется только внутренняя среда связи, и системе открытого типа, если для работы системы необходим доступ в глобальную сеть Интернет.

В исследовании [17] для оценки связности киберфизических систем предлагается использовать применяемые в них технологии и стандарты связи. При этом технологии характеризуют устройства, используемые системой для взаимодействия с физическими объектами или процессами, например датчики температуры и RFID-метки, в то время как стандарты характеризуют процесс взаимодействия элементов системы между собой, указывая на используемые протоколы и интерфейсы. Протоколы делят на высокоуровневые, низкоуровневые и межуровневые, а для классификации

интерфейсов предлагается использовать различные признаки, характеризующие топологию связи, формат и режим передачи данных, а также функциональное назначение сети.

Используемые протоколы и интерфейсы можно условно разделить на проводные и беспроводные. Беспроводные датчики и исполнительные механизмы играют центральную роль в разработке современных киберфизических систем. В таких сложных гетерогенных системах каналы связи должны отвечать строгим требованиям по пропускной способности, задержке и дальности, а также обладать низким энергопотреблением. В [21] рассматриваются наиболее актуальные стандарты беспроводной связи, такие как: NFC, UHF RFID, ZigBee, Z-Wave, EnOcean, Bluetooth, Wi-Fi, 3GPP, NB-IOT, LoRa и SigFox. При этом выделяют следующие топологии сети: звезда, древовидная, ячеистая и сотовая.

К наиболее распространенным проводным интерфейсам передачи данных между устройствами на основе микроконтроллеров относят UART, SPI, I2C, Ethernet, 1-Wire, Modbus и CAN [22, 23]. Каждый из перечисленных интерфейсов имеет ряд особенностей, влияющих на скорость передачи данных, потребление энергии и доступные дополнительные функции: например, функции адресации и идентификации подключаемых устройств. При этом для данных интерфейсов широко распространены их аппаратные реализации, что привело к их интеграции в большинство современных устройств на основе микроконтроллеров.

Отметим, что глобальная информатизация различных сфер жизнедеятельности человека способствует как развитию существующих спецификаций протоколов сетевого обмена, так и появлению новых протоколов. При этом для устройств киберфизических систем прослеживается тенденция к использованию проприетарных протоколов, то есть протоколов с нерегламентированными (по крайней мере, общедоступно) спецификациями. Подобная ситуация в основном связана со стремлением защитить интеллектуальную и коммерческую собственность компаний, а также усложнить условия анализа сетевых протоколов сторонними исследователями. Это означает, что зачастую трафик в киберфизических системах можно охарактеризовать как трафик большого объема, высокой гетерогенности и неопределенной структуры [24].

Оценка критичности киберфизической системы может быть осуществлена в соответствии с зависящими от нее бизнес-процессами. Для осуществления данной оценки зачастую используются модели бизнес-процессов, а также проводится анализ потенциальных угроз и уязвимостей для последующей оценки рисков и выбора контрмер. При этом риск определяется как способность конкретной угрозы использовать уязвимость

одного или нескольких активов для нанесения ущерба организации [25]. В свою очередь, активы могут представлять собой материальные активы, информацию, программное и аппаратное обеспечение, персонал и нематериальные ресурсы, имеющие ценность для организации.

По определению, критической информационной инфраструктурой является совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов, а также обеспечивающие их взаимодействие информационно-телекоммуникационные сети [26]. Таким образом, к данным объектам могут быть отнесены киберфизические системы, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, финансов, обороны и промышленности. Анализ области применения киберфизических систем представлен в работах [27–29]. Рассмотрим данные исследования более подробно.

В работе [27] выделяются следующие сферы применения киберфизических систем: общественная безопасность, розничная торговля, транспорт, промышленность, здравоохранение, «умный дом», строительство, энергетика. Для каждой сферы определяется конечный потребитель, и приводятся примеры устройств. Авторы [28] проводят обзор существующих решений в области проектирования киберфизических систем, что позволяет выделить следующие области применения: автомобильные системы и транспорт, медицинские системы, умные дома и здания, социальные сети и игровые системы, системы планирования, системы управления, системы питания, системы наблюдения, промышленные системы, авиационно-космические системы, поисковые системы, экологические системы, системы строительства, робототехнические системы и водораспределительные системы. В статье [29] рассматриваются основные составляющие современной интеллектуальной среды, а именно такие концепции как «умный дом», «умное здоровье», «умный город» и «умная фабрика». При этом данные концепции сопоставляются с текущими коммуникационными решениями в области киберфизических систем. Также в данной работе представлен обзор коммуникационных технологий и архитектур подобных систем, а в заключении обсуждаются проблемы, которые остаются открытыми для исследований.

Производственные киберфизические системы характеризуют как объединение автономных и согласованных элементов (от машин до логистических сетей), соединенных друг с другом в соответствии с поставленной целью на всех уровнях производства и способных принимать решения в режиме реального времени [30]. При этом преимущество от внедрения таких систем исследуются повсеместно. Так, в [31] показан процесс

внедрения принципов киберфизических систем в промышленный сектор путем организации работ предприятий в рамках таких технологий, как «умное производство» и «цифровая фабрика». В работах [32, 33] показаны преимущества взаимодействия человека и робототехнических систем в условиях опасной среды. Статья [34] описывает транспортные киберфизические системы, их основные принципы организации и функционирования. В работе [35] предложена парадигма киберфизической строительной системы, представляющая собой конечное множество функциональных компонентов, таких как строительные объекты и комплексы, а также вычислительные ресурсы, интегрированные во включенные физические процессы. В ряде работ [36, 37] приводятся исследования медицинских киберфизических систем для повышения эффективности и безопасности здравоохранения.

Отметим, что критичность киберфизической системы характеризуется последствиями полного или частичного отказа как всей системы, так и отдельных ее элементов. Данные последствия включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека. Одним из способов представления критичности является вектор из следующих составляющих: надежность, последствия отказа, возможность уменьшения вероятности возникновения и тяжести последствий [38]. При этом ранжирование элементов киберфизической системы по степени критичности зависит от типа системы, выбранных частных показателей, а также доступной экспертной информации.

Критичность информации, обрабатываемой в киберфизических системах, как правило, определяется владельцем системы и может зависеть от различных параметров. Например, на критичность информации может влиять ее необходимость для корректного функционирования системы, а также ущерб от потери, модификации или утечки информации. Критичность может вычисляться как с использованием качественных, так и количественных показателей [39].

В исследовании [40] предложена классификация информационных активов в соответствии с требованиями к конфиденциальности, целостности и доступности. Относительно конфиденциальности авторы выделяют информацию, ограниченную к распространению согласно требованиям законодательства; информацию, ограниченную к распространению согласно требованиям организации; и открытую информацию, обеспечение конфиденциальности которой не требуется. Относительно целостности выделяют информацию, нарушение целостности которой может привести к значительному, умеренному или незначительному ущербу, а также информацию, обеспечение целостности которой не требуется. Относительно

доступности выделяют информацию, доступную в любое время, а также информацию, доступную с задержкой до нескольких часов / дней / недель.

На основе предложенной авторами [40] классификации, информация может быть разделена на *критически важную* – конфиденциальность должна быть обеспечена в соответствии с требованиями законодательства, нарушение целостности может привести к значительному ущербу, информация доступна в любое время; *важную* – конфиденциальность должна быть обеспечена в соответствии с требованиями организации, нарушение целостности может привести к умеренному ущербу, информация доступна с задержкой до нескольких часов; и *обычную* – обеспечение конфиденциальности и целостности не требуется.

Оценка социального аспекта киберфизической системы может быть осуществлена в соответствии с характером взаимодействия системы с пользователями и операторами. При этом развитие данного направления исследований дало начало такому термину как социо-киберфизическая система. Важно отметить, что эффективность функционирования киберфизической системы зависит не только от аппаратного и программного обеспечения, но и от взаимодействующего с ней персонала и потребителя. Это означает, что интересы различных социальных групп должны учитываться как на уровне формирования внешнего облика системы, так и при разработке технического задания.

Так, в работе [41] данный факт позволил ввести признак социализации элементов киберфизической системы, который характеризует следующие виды взаимодействия системы с социумом: проектирование, производство, купля/продажа, хранение, выполнение работы (оператор), техническое обслуживание и утилизация. А в исследовании [17] был введен признак человеческого фактора, который описывает следующие типы взаимодействия киберфизических систем с оператором: *автономия* – система принимает все необходимые решения без какого-либо вмешательства оператора; *автоматизация* – система направляет оператора во время выполнения задач, принимая большинство решений; *инструмент* – оператор управляет системой и отвечает за большинство решений; *руководство* – система только предоставляет данные оператору, принимающему все решения.

Зачастую киберфизические системы моделируют интеллектуальные возможности человека в задачах поиска, анализа и синтеза информации об окружающем мире для получения новых знаний и решения поставленных задач. Так, в работе [18] для подобных систем вводится понятие интеллектуализации, описывающее способность системы к обучению, накоплению опыта и принятию решений. Кроме того, в данной работе

вводится понятие динамики реагирования на внешний мир, которое делится на динамику высокого, среднего и низкого уровней. Предполагается, что данный признак может быть использован для оценки способности киберфизических систем к работе с неопределенными и динамическими данными, а также к извлечению знаний из накопленного опыта. Также в данной работе вводится понятие модели восприятия внешнего мира, описывающее как объекты киберфизической системы воспринимают окружающий мир: без модели внешнего мира, с заданной моделью внешнего мира или с моделью внешнего мира, которая генерируется в процессе работы системы.

На основе анализа и систематизации современного состояния исследований авторами были выбраны в качестве основных такие атрибуты классификации, как сложность, связность, критичность и социальный аспект киберфизических систем. С использованием этих атрибутов была построена классификация, представленная на рисунке 2.

Рис. 2. Классификация киберфизических систем

Данная классификация позволяет оценить критичность системы или ее элементов в соответствии с зависящими от них бизнес-процессами, сложность в соответствии с функциональными возможностями и связность в соответствии с используемыми интерфейсами и протоколами передачи данных. Кроме того, данная классификация позволяет учесть социальный аспект работы системы в соответствии с задействованным персоналом и возможным пользователями. Достаточность классификации подтверждается анализом существующих научных и практических

работ, в которых для определения типа системы используются именно вышеперечисленные атрибуты.

Например, относительно сложности можно выделить децентрализованную одноуровневую самоорганизующуюся систему с переменным количеством элементов. Относительно связности – географически распределенную систему с наличием выхода в сеть Интернет, построенную на основе беспроводных и проводных технологий с использованием низкоуровневых и высокоуровневых протоколов. Относительно критичности – систему, используемую в критически важной инфраструктуре с участием человека, обрабатывающую критически важную информацию, отказ которой может повлечь финансовый ущерб. Относительно социального аспекта – автономную систему, выступающую в качестве источника данных, не способную к самообучению и накоплению знаний, имеющую низкую динамику реагирования на внешний мир. Каждая из полученных классификаций позволяет ограничить способ описания исследуемых систем и задает основу для оценки их сложности, связности, критичности и социального аспекта.

3. Анализ и классификация атакующих. Важным этапом в процессе определения угроз безопасности киберфизической системы является идентификация лиц, действия которых могут привести к нарушению конфиденциальности, целостности или доступности системы и возникновению ущерба. Согласно определению в ГОСТ Р. 53114-2008 [42] нарушителем информационной безопасности считается физическое лицо или логический объект, случайно или преднамеренно совершивший действие, которое повлекло негативные последствия. Модель, или профиль, атакующего характеризует возможные пути взаимодействия между атакующим и целевой системой, в частности определяет ограничения для атакующего. Результатом анализа модели атакующего является предположение о видах и потенциале нарушителей, которые могут реализовать угрозы безопасности для киберфизической системы с заданными характеристиками и особенностями функционирования.

Предполагается, что классификация атакующих позволит оценить их возможности в соответствии с типом доступа к системе, уровнем знаний, возможных намерений и доступных ресурсов. *Тип доступа* позволяет различать внешнего и внутреннего нарушителя, рядового пользователя и администратора. *Уровень знаний* является характеристикой атакующего, которая указывает на его технические навыки для инициирования и проведения атаки. Также данная характеристика описывает осведомленность нарушителя об архитектуре целевой системы и существующих мерах защиты. *Намерения* злоумышленника указывают на цель проведения

атаки на систему. Этот параметр трудно поддается количественной оценке и очень динамичен. *Доступные ресурсы* атакующего включают в себя аппаратные и программные ресурсы, которые могут быть использованы для развертывания определенного типа атаки.

Основными нормативными документами, определяющими модель атакующего в Российской Федерации, являются: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [43], «Методика определения угроз безопасности информации в информационных системах» [44] и «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» [45].

В нормативном документе [43] нарушители подразделяются на два типа: внешние и внутренние. При этом к внешним нарушителям относятся нарушители, не имеющие доступа к киберфизической системе, реализующие угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена. При этом внешними нарушителями могут быть разведывательные службы государств, криминальные структуры, конкурирующие организации, недобросовестные партнеры и физические лица. А к внутренним нарушителям относятся нарушители, имеющие доступ к киберфизической системе, включая пользователей и операторов системы, реализующие угрозы непосредственно в системе. При этом возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны организационно-технических мер защиты, в том числе по допуску физических лиц к данным системы и контролю порядка проведения работ.

Более того, внутренние нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа: *категория 1* – лица, имеющие санкционированный доступ к системе и обеспечивающие нормальное ее функционирование; *категория 2* – зарегистрированные пользователи системы, осуществляющие ограниченный доступ к ее ресурсам с рабочего места; *категория 3* – зарегистрированные пользователи системы, осуществляющие удаленный доступ к ее ресурсам; *категория 4* – зарегистрированные пользователи системы с полномочиями администратора безопасности отдельного сегмента системы; *категория 5* – зарегистрированные пользователи с полномочиями системного администратора системы; *категория 6* – зарегистрированные пользователи с полномочиями администратора безопасности системы;

категория 7 – разработчики программного обеспечения системы и лица, обеспечивающие его сопровождение; *категория 8* – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт оборудования системы.

В нормативном документе [44] вводится понятие потенциала нарушителя, который может быть низким, средним и высоким: *низкий потенциал* – нарушитель обладает информацией об уязвимостях отдельных элементов киберфизической системы, опубликованной в общедоступных источниках, при этом для проведения атак использует общедоступные инструменты или инструменты, созданные самостоятельно; *средний потенциал* – нарушитель обладает всеми возможностями нарушителей с низким потенциалом, а также имеет осведомленность о мерах защиты, применяемых в киберфизической системе; кроме того, нарушитель имеет информацию об уязвимостях отдельных элементов системы и применяет находящиеся в свободном доступе программные средства для проведения атак, а также имеет доступ к сведениям о характеристиках и особенностях функционирования киберфизической системы; *высокий потенциал* – нарушитель обладает всеми возможностями нарушителя со средним потенциалом, а также может получить несанкционированный доступ к киберфизической системе из выделенных сетей связи; кроме того, нарушитель данного типа имеет доступ к программному обеспечению и оборудованию системы, хорошо осведомлен о мерах защиты, применяемых в ней, а также обладает информацией об уязвимостях системы, проводит исследования атакуемой системы и использует узкоспециализированные инструменты для достижения своих целей.

В нормативном документе [45] приводятся обобщенные возможности нарушителей, при этом основное внимание уделяется возможностям нарушителя по атакам на средства защиты системы и среду их функционирования: возможность атаковать киберфизическую систему только за пределами контролируемой зоны; возможность атаковать киберфизическую систему в пределах контролируемой зоны, но без физического доступа к ней; возможность атаковать киберфизическую систему в пределах контролируемой зоны с физическим доступом к ней; возможность привлекать специалистов, имеющих опыт разработки и анализа средств защиты, типичных для киберфизических систем.

Важно отметить, что помимо основных нормативных документов, различные классификации атакующих приведены в ряде исследований в области анализа угроз информационной безопасности. Рассмотрим данные работы более подробно.

Например, в работе [46] представлен обзор исследований в области атак на киберфизические системы, а также профилированию атакующих. В результате данного обзора делается вывод, что существующие исследования можно сгруппировать в две основные категории: (1) использующие различные модели атакующих с различными свойствами (например, одна модель для описания внутреннего нарушителя, другая – для описания разведывательной службы государства); (2) определяющие ряд параметров типа знаний, уровня или потенциала нарушителя для различения нарушителей в рамках единой модели. Кроме того, в данной работе предлагается обобщенная классификация атакующих, включающая следующие их виды: *любитель* – использует общедоступные инструменты для атаки на систему и имеет стандартный доступ к оборудованию, программному обеспечению и подключению к интернету; *внутренний нарушитель* – обладает системными привилегиями (например, пользователь, супервайзер, администратор); *хактивист* – использует свои способности для проявления политической активности; *кибертеррорист* – политически мотивированный злоумышленник, который использует свои способности для совершения правонарушений; *киберпреступник* – атакующий с обширными знаниями и навыками в области безопасности, цели которого могут варьироваться от шантажа до шпионажа и саботажа; *группировка* – группа людей, иногда финансируемая государством, целью которой часто является разведка и атаки на критически важные системы общественной инфраструктуры. Авторы также отмечают, что границы между видами атакующих в приведенной классификации достаточно размыты, а потому определение реального злоумышленника в качестве одного конкретного вида может быть затруднительно. Касательно целей атакующих, авторы выделяют: личные, экономические, криминалистические, террористические и политические.

В работе [47] приводится классификация атакующих на киберфизическую систему на примере системы управления водоснабжением. При этом злоумышленник классифицируются по типу доступа к системе и возможностям. Авторы выделяют следующие типы доступа к системе: *тип 0* – злоумышленник не имеет прямого доступа к инфраструктуре и сервисам системы, к применению доступны только методы социальной инженерии; *тип 1* – злоумышленник взаимодействует с инфраструктурой и сервисами системы опосредованно, осуществляя непрямой доступ к ним; *тип 2* – злоумышленник воздействует на инфраструктуру системы или ее сервисы напрямую, находясь при этом на некотором расстоянии от контролируемого периметра; *тип 3* – злоумышленник имеет физический доступ к инфраструктуре системы, но не имеет возможности исследовать

и модифицировать внутренние электронные компоненты; *тип 4* – нарушитель имеет полный доступ к инфраструктуре системы и всем внутренним элементам и интерфейсам.

Авторы выделяют следующие уровни возможностей атакующих: *уровень 1* – использование общедоступных инструментов и эксплуатация известных уязвимостей системы; *уровень 2* – способность выявлять и эксплуатировать ранее неизвестные уязвимости и разрабатывать новые инструменты для воздействия на целевую систему; *уровень 3* – возможности *уровня 2* и наличие почти неограниченных ресурсов для осуществления атак. Таким образом, предложенная авторами классификация позволяет рассматривать атакующих с точки зрения типа доступа, ресурсов и знаний, необходимых для успешной реализации атакующих действий.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации атакующих, как тип доступа, способ доступа, намерения, знания и ресурсы, была построена классификация, представленная на рисунке 3.

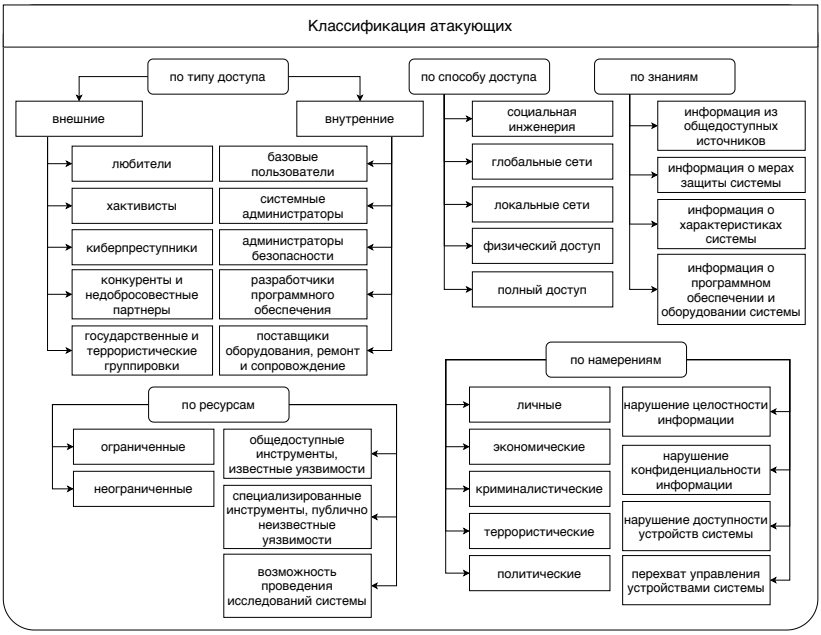


Рис. 3. Классификация атакующих

Данная классификация позволяет оценить возможности атакующих в соответствии с типом и способом доступа к системе, уровнем знаний и доступных ресурсов. Кроме того, данная классификация позволяет учесть возможные намерения атакующих, в том числе связанные с нарушением конфиденциальности и целостности информации, а также нарушением доступности устройств и перехватом управления ими.

4. Анализ и классификация атакующих действий. Не менее важным этапом в процессе определения угроз безопасности киберфизической системы является анализ действий, которые могут привести к нарушению конфиденциальности, целостности или доступности системы. Согласно определению в ГОСТ Р. ИСО/МЭК 27000–2012 [48] атакой является попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. При этом атаки могут происходить на разных уровнях системы, включать в себя множество этапов, быть растянутыми по времени и затрагивать собой различные ее элементы. И хотя многообразие атакующих действий активно исследуется в научном сообществе, на данный момент не существует единой их классификации. Рассмотрим существующие работы в данном направлении более подробно.

В [49] при классификации сетевых атакующих действий выделяют признаки классификации на основе ресурсов, топологии и трафика: *по влиянию на ресурсы* – направленные (отказ в обслуживании, переполнение таблицы маршрутизации) и ненаправленные (повышение привилегий); *по влиянию на топологию* – снижающие производительность (подмена таблицы маршрутизации, «воронка», «червоточина») и изолирующие («черная дыра»); *по влиянию на трафик* – подслушивающие (сниффинг и анализ трафика) и перехватывающие (понижение привилегий, спуфинг).

В работе [50] при классификации атакующих действий на SCADA-системы выделяют следующие типы атак: ослабление сетевого периметра с помощью бекдоров, эксплуатация уязвимостей в используемых протоколах, перехват управления отдельными устройствами системы, нарушение работы базы данных, перехват и модификация сетевых сообщений, модификация системного времени для прекращения работы средств защиты. В исследовании также предлагается разделить атакующие действия на атаки, направленные на модификацию, перехват или внедрение входных данных от датчиков системы; атаки, направленные на изменение процесса работы системы за счет модификации, перехвата или внедрения данных на уровне взаимодействия между контроллерами системы; атаки, направленные на модификацию логов системы; атаки, направленные на перехват управления отдельными устройствами или прекращение их работы.

В [51] авторы предлагают представлять атакующие действия следующим кортежем данных: субъект, объект, намерения, вектор и последствия. При этом субъектом атаки может быть злоумышленник, природная катастрофа, человеческий фактор, ошибки системы и поддерживающей инфраструктуры. Объектом атаки может быть любой элемент системы, среда передачи данных между ними, а также система в целом. Намерения могут быть криминальными, разведывательными, террористическими или политическими. Векторы атак разделены на перехват, модификацию и подделку данных, а также прекращение их передачи. Последствия атаки включают в себя компрометацию конфиденциальности, целостности, доступности, приватности и надежности системы.

В работе [52] представлена классификация атакующих действий на киберфизические системы. Авторы выделяют атаки на датчики, вычислительные процессы, обратную связь, среду передачи данных и исполнительные механизмы. Рассмотрим примеры для каждого из перечисленных видов атакующих действий более подробно: *атаки на датчики* – выведение оборудования из строя, прекращение подачи питания, использование физических процессов для некорректной работы датчиков; *атаки на вычислительные процессы* – удаление, модификация, подмена или подделка данных, черви, вирусы, трояны; *атаки на обратную связь* – нарушение целостности данных, перехват управления; *атаки на среду передачи данных* – удаление, модификация, подмена или подделка данных, потеря данных, сниффинг; *атаки на исполнительные механизмы* – удаление, модификация, подмена или подделка данных, прекращение подачи питания, модификация аппаратного и программного обеспечения.

В [53] при анализе безопасности киберфизических систем предлагается выделять атакующие действия в соответствии с уровнем киберфизической системы, на котором происходит атака, элементом системы, на который атака направлена, и намерениями злоумышленника. При этом для каждого уровня киберфизической системы авторы представили основные проблемы безопасности и возможные контрмеры. Авторы [54] также предлагают классифицировать атакующие действия на киберфизические системы в соответствии с уровнем системы: физическим, сетевым или приложений. При этом для каждого уровня авторы выделяют соответствующие атакующие действия: *физический уровень* – выведение из строя оборудования, прекращение работы оборудования, прекращение подачи питания, перехват электромагнитных сигналов, внесение помех, отказ в обслуживании, перехват и модификация данных, прекращение передачи данных, перехват управления, несанкционированный доступ; *сетевой уровень* – распределенный отказ в обслуживании, вмешательство

в процесс маршрутизации, прекращение передачи, перенаправление или потеря данных, переполнение буфера; *уровень приложений* – неавторизованный доступ, утечка данных, внедрение вредоносного кода, перехват управления, внедрение вирусов и троянов, инъекции в базу данных.

В работе [55] авторы предлагают разделять атакующие действия на киберфизические системы в соответствии с областью их воздействия: от взаимодействия с физическими устройствами до различных аспектов сетевого взаимодействия (сегментация, топология, используемые технологии и структура). При этом авторы приводят следующую обобщенную их классификацию: перехват и анализ трафика; утечка персональных данных; выведение из строя оборудования; удаленное выполнение вредоносного кода; нарушение целостности исходного кода приложений;эксплуатация уязвимостей сетевых протоколов; отказ в обслуживании.

В [56] предлагается классифицировать атакующие действия на киберфизические системы в соответствии с их причиной, следствием и выполненным действием. Для каждого действия выделяют метод и предусловия, а для причины и следствия – затронутый элемент и влияние на него. В работе [57] предложено классифицировать атакующие действия на киберфизические системы в соответствии с объектом атаки, влиянием на систему и влиянием на человека. Рассмотрим предложенную классификацию более подробно: *по объекту атаки* – сбор данных, среда передачи данных, система управления; *по влиянию на систему* – физическое (некорректная работа, отказ в обслуживание, медленная обработка данных) и кибернетическое (конфиденциальность, целостность, доступность, неаппелируемость); *по влиянию на человека* – эмоциональное воздействие, влияние на приобретенный опыт, причинение физического вреда.

В [58] атакующие действия разделяют на основе способа воздействия на объекты информационной безопасности и по аспекту безопасности, на нарушение которого они направлены. При этом по способу воздействия выделяют: *информационные* – несанкционированный доступ, копирование и хищение информации, нарушение технологии обработки информации; *программные* – использование ошибок и уязвимостей в программном обеспечении, распространение вредоносных программ, установка закладок; *физические* – уничтожение устройств системы, хищение носителей информации, хищение ключей и средств криптографической защиты данных; *радиоэлектронные* – внедрение устройств перехвата информации, перехват, расшифровка, подмена и уничтожение данных в каналах связи; *организационно-правовые* – нарушение законодательства, закупка устаревших программ и устройств. По аспекту безопасности

выделяют атакующие действия, направленные на нарушение *конфиденциальности*, *целостности* и *доступности*.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации атакующих действий, как субъект и объект, способ воздействия, предпосылки и последствия, была построена классификация, представленная на рисунке 4.

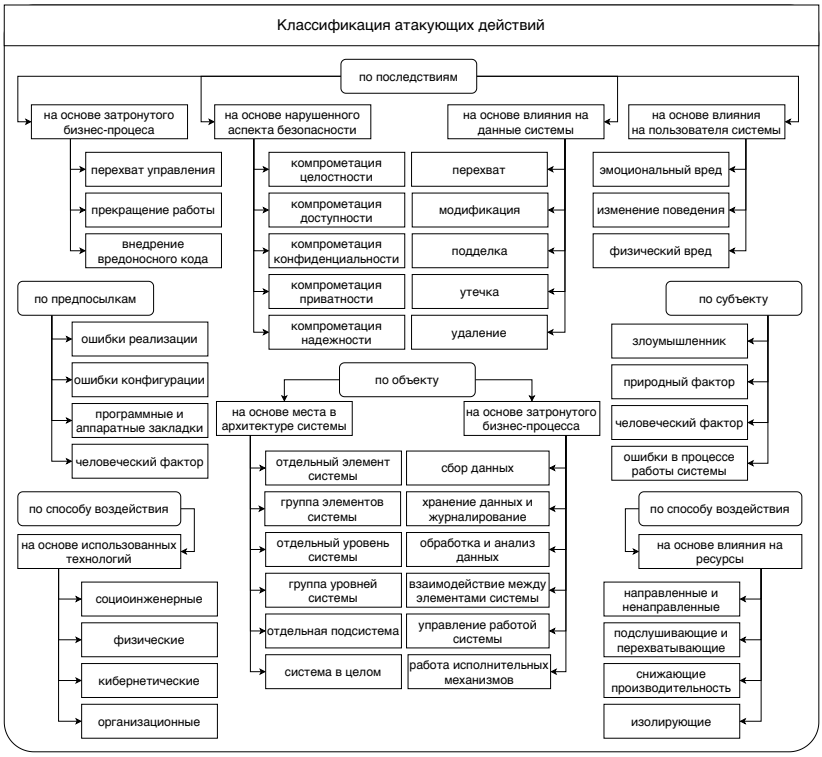


Рис. 4. Классификация атакующих действий

Данная классификация позволяет установить взаимосвязь между атакующим и атакующими действиями в соответствии со знаниями и ресурсами, необходимыми злоумышленнику для их реализации, а также целью, которой соответствует их применение. Кроме того, данная классификация устанавливает взаимосвязь между атакующими действиями и элементами киберфизической системы, в соответствии с которыми они могут быть реализованы.

5. Анализ и классификация методов и средств защиты. Поскольку одной из отличительных черт киберфизических систем является тесная интеграция физических процессов и информационных технологий, число проблем, которые необходимо учитывать при разработке механизмов безопасности для таких систем, значительно выше в сравнении с системами других типов. Кроме того, подобные системы часто обладают динамической инфраструктурой, гетерогенными источниками информации и разнородными хранилищами данных, что также увеличивает сложность требуемой защиты. При этом большинство исследований в данной области направлено на решение различных проблем безопасности на каждом отдельном уровне архитектуры киберфизической системы, а не системы в целом. Рассмотрим существующие работы в данном направлении более подробно.

В работах [12, 59] авторы предлагают определять необходимые методы и средства защиты на основе компонентного состава киберфизической системы. При этом в данных работах представлена классификация методов защиты в соответствии с уровнем системы, защиту которого они обеспечивают. Авторы выделяют следующие уровни: *уровень сбора данных* – сертификация, контроль доступа, аутентификация, легковесное шифрование данных, физическая безопасность устройств, мониторинг окружающей среды, доверительное управление; *уровень передачи данных* – надежная маршрутизация и шифрование данных, аутентификация и согласование ключей, контроль доступа к сети, механизм обнаружения атак; *уровень анализа и обработки данных* – сквозное шифрование, обнаружение вторжений, доверительное управление, аутентификация и авторизация, интеллектуальный анализ данных, форензика, защита персональных данных.

Отметим, что упомянутые выше методы и средства защиты в работе [12] авторы относят к информационному полю системы, помимо которого также выделяют управляющее поле и оценку рисков. Отмечается, что данные механизмы безопасности должны быть разработаны с учетом обеспечения безопасности системы в целом, а не только отдельного ее уровня. При этом данный процесс включает в себя разработку интегрированного межуровневого решения безопасности, которое способно к работе с различными методами и средствами защиты, а также надежно интегрирует данные из разных источников.

В работах [60, 61] представлена архитектура киберфизической системы, которая представляет собой комплексное решение по обеспечению безопасности подобных систем. Данное решение интегрирует в себе как решения по обеспечению физической, так и информационной

безопасности, и состоит из следующих основных частей: *источники данных* – включают в себя различные системы физической и кибернетической безопасности; *модуль сбора данных* – использует различные аппаратные и программные интерфейсы для подключения к источникам данных, при этом полученные данные подлежат процессам предобработки и нормализации; *модуль анализа данных* – включает в себя различные этапы процесса корреляции событий безопасности; *модуль представление данных* – включает в себя такие процессы, как оценка защищенности, выработка контрмер и генерация отчетов.

Отметим, что в соответствии с предложенной авторами архитектурой методы и средства защиты киберфизической системы могут быть классифицированы в соответствии с решаемой задачей.

В работах [7, 62] предлагается рассматривать методы и средства обеспечения безопасности киберфизических систем с точки зрения теории управления. При этом авторы выделяют следующие признаки, которые необходимо учитывать при проектировании защиты системы: наличие обратной связи, наличие контура адаптивного управления и возможность прогнозирования состояния системы. На основе данных признаков авторы предлагают следующую классификацию методов и средств защиты: *статические* – функция управления не изменяется со временем, выходное состояние объекта защиты зависит от постоянных значений управляющих воздействий; *активные* – результаты экспериментального тестирования объекта защиты используются для настройки параметров систем безопасности; *адаптивные* – параметры систем безопасности периодически изменяются для максимизации эффективности защиты на основе характеристик объекта в процессе мониторинга; *динамические* – присутствует динамическая компенсация нежелательных изменений состояния системы в процессе работы.

Отметим, что предложенный авторами подход позволяет сформулировать задачу обеспечения безопасности киберфизических систем как задачу автоматического управления в условиях целенаправленных киберугроз с целью обеспечения устойчивости функционирования.

Авторы [61] предлагают анализировать используемые в киберфизической системе сетевые интерфейсы и протоколы для определения необходимых средств и методов защиты среды передачи данных. При этом особое внимание уделяется процессу взаимодействия между контроллерами системы, где в приведенном эксперименте безопасность шины данных обеспечивается за счет взаимной аутентификация устройств и шифрования передаваемых данных, а надежность – за счет динамической адресации и мониторинга состояния подключаемых устройств, отсутствия

неконтролируемых потерь показаний датчиков и проверки целостности передаваемых данных.

В фреймворке безопасности, предложенном компанией «Cisco» [63] для киберфизических систем, выделяются четыре основных компонента: аутентификация и идентификация, контроль доступа, сетевая политика и аналитика безопасности. При этом базовое применение сетевой политики в первую очередь касается обеспечения соответствия поступающего в сеть трафика заданным правилам, в том числе допустимому диапазону IP-адресов и типам трафика. Пакеты трафика, не соответствующие заданным правилам, признаются в качестве аномальных и должны быть отброшены как можно ближе к границе сети, тем самым сводя к минимуму риск воздействия. Как правило, для обнаружения аномалий используются различные методы, обобщенная классификация которых может быть представлена следующим образом: поведенческие, статистические, интеллектуальный анализ данных, в том числе методы машинного обучения [64].

В работе [65] рассматриваются существующие методы оценки уязвимостей, их роль в процессе оценки рисков безопасности и способы применения. Выделяются три основные группы методов: количественные, качественные и качественно-количественные. Количественные методы оценки рисков позволяют оценить риск в денежных единицах и учитывают частоту нежелательных событий. Качественные методы ранжируют риски относительно друг друга на основе ценности активов, уязвимостей, угроз и защитных мер. При этом на практике в основном применяется качественно-количественный подход, в рамках которого любому качественному уровню сопоставляют определенные диапазоны количественных величин.

В работе [66] авторы рассматривают исследования по оценке уязвимостей киберфизических систем в академических и коммерческих сферах. При этом авторы отмечают, что для последней характерно многообразие подходов к выявлению уязвимостей, в то время как в академической среде подобного не наблюдается.

В [67] рассматриваются методики оценки рисков киберфизических систем с точки зрения экономического эффекта, который проявляет себя даже тогда, когда мотивация злоумышленника не является финансовой. Приводится анализ различных моделей и методик оценки рисков, а также систем оценки уязвимостей.

В работе [68] рассматриваются существующие подходы к оценке и управлению рисками с точки зрения безопасности, защиты и их интеграции. Методы оценки рисков безопасности для киберфизических систем включают в себя: *анализ дерева отказов* – представление, позво-

ляющее связать различные легитимные события и ошибки, возникновение которых может привести к нежелательному событию; *анализ отказов и их последствий* – структурированный метод анализа безопасности системы, позволяющий распознать ситуации, которые приводят к отказу системы или отдельных ее элементов, а также их последствия; *анализ критичности и надежности* – метод анализа безопасности системы, позволяющий оценить степень критичности и надежности процессов системы за счет изучения последствий возможных отклонений; *разработка в соответствии с моделью* – метод разработки имитационных моделей систем реального времени и анализа данных моделей для проверки соответствия требованиям безопасности; *анализ деревьев успеха и целей* – метод анализа безопасности системы, основанный на структурном анализе надежности и риска системы; *анализ аварийных процессов* – метод анализа безопасности, основанный на теоретико-множественной модели и анализе ситуаций, возникновение которых приводит к аварии.

Работа [69] посвящена исследованию основных подходов в области оценки рисков для потенциально опасных объектов. Методы оценки включают в себя количественную оценку с помощью применения математической статистики, экспертную оценку рисков, имитационное моделирование и их комбинации. При этом в исследовании уточняется, что оценка нарушения физической безопасности проводится для каждого конкретного объекта с использованием следующих методов: математическое моделирование распределения вероятности рискового события; экспертная оценка методами Дельфи и ранжирования; численное интегрирование функции риска во времени и пространстве. Это означает, что оценку безопасности киберфизической системы можно представить в виде процесса анализа накопленных данных, мнения экспертов или работы математического аппарата.

Социальный аспект киберфизических систем и, соответственно, возможные атаки социальной инженерии приводят к поиску методов и средств защиты от них. Например, в работе [70] изучаются явления агрессии в социо-киберфизической среде и их влияние на индивидуальное и групповое сознание пользователей. Полученные результаты предлагается использовать при разработке единой социо-киберфизической системы управления данными процессами. Авторы отмечают, что в социальной сети объединение источника с используемыми средствами и формами коммуникации позволяет учесть социальный эффект сообщения, который может быть использован для предсказания проявлений агрессии, давления и других деструктивных явлений.

В работе [71] авторами предложена классификация социоинженерных атак и возможный подход к оценке индекса защищенности корпоративных сетей с точки зрения поведения человека. Предлагаются следующие основные меры защиты от атак социальной инженерии: доступность политики информационной безопасности; проведение инструктажа; мониторинг соблюдения информационной безопасности; политика управления идентификацией; внедрение биометрических систем доступа.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации методов и средств защиты, как принцип работы, объект защиты и решаемая задача, была построена классификация, представленная на рисунке 5.

Рис. 5. Классификация методов и средств защиты

Данная классификация позволяет оценить возможность реализации атакующих действий в соответствии с используемыми методами и средствами защиты. Это возможно благодаря тому, что классификация методов и средств защиты по объекту защиты совпадает с классификацией атакующих действий по аналогичному атрибуту. Следовательно, при дальнейшем анализе знаний, ресурсов и возможностей злоумышленника можно будет сделать вывод о реализуемости тех или иных атакующих действий. При этом, классификация методов и средств защиты позволяет установить взаимосвязь между используемой системой защиты и возможностью реализации атакующих действий (рис. 6).

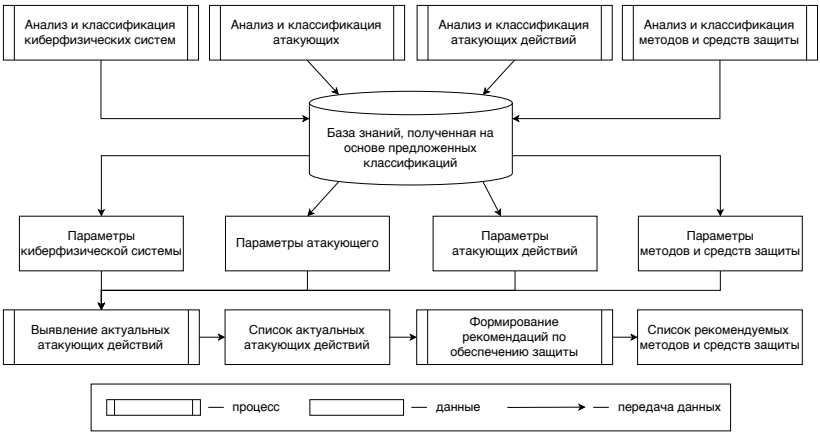


Рис. 6. Процесс выявления актуальных атакующих действий и рекомендации методов и средств защиты

Это означает, что имея информацию о компонентном составе киберфизической системы, можно определить перечень атакующих действий, которым данная система потенциально подвержена. Затем, имея представление об уровне знаний злоумышленника и доступных ему ресурсах, данный перечень атак может быть ограничен точно также как при наличии информации об используемых методах и средствах защиты. Все атакующие действия, оставшиеся после данных преобразований, представляют собой реальную угрозу и должны быть приняты во внимание.

6. Заключение. Проведены анализ и систематизация современных исследований в области обеспечения информационной безопасности киберфизических систем с точки зрения объекта атаки, злоумышленника, цели и мотива атаки, способа атаки, а также методов и средств защиты. Предложено определение киберфизических систем. Дана классификация киберфизических систем по таким атрибутам, как сложность, связность, критичность и социальный аспект. При этом по сложности киберфизические системы разделяют на централизованные и децентрализованные, иерархические и одноуровневые, с постоянным и переменным количеством элементов, адаптивные и неадаптивные, самоорганизующие и несамоорганизующиеся. По связности – географически распределенные и нераспределенные, с наличием и отсутствием выхода в Интернет, беспроводные, проводные и смешанные, с использованием низкоуровневых, высокоуровневых, межуровневых и проприетарных протоколов. По кри-

тичности – используемые в критической и некритической инфраструктуре, работающие с участием или без участия человека, с наличием или отсутствием потенциального ущерба финансам, репутации, пользователям и операторам при частичном и полном отказе, обрабатывающие данные, обладающие или не обладающие критической важностью. По социальному аспекту – автономные и автоматизированные, поддерживающие принятие решений и выступающие только в качестве источника данных, способные и не способные к самообучению и накоплению знаний, высокой, средней и низкой динамики реагирования на внешний мир.

Предложена классификация атакующих по таким атрибутам, как тип доступа, способ доступа, намерения, знания и ресурсы. При этом по типу доступа атакующих разделяют на внешних и внутренних. Внешние атакующие делятся на любителей, хактивистов, киберпреступников, конкурентов и недобросовестных партнеров, государственные и террористические группировки. Внутренние атакующие делятся на базовых пользователей, системных администраторов, администраторов безопасности, разработчиков программного обеспечения, поставщиков оборудования и сотрудников, осуществляющих ремонт и сопровождение системы. По способу доступа выделены – социальная инженерия, глобальные сети, локальные сети, физический и полный доступ. При этом такующий может обладать информацией как из общедоступных источников, так и о мерах защиты, характеристиках, программном обеспечении и оборудовании системы. Ресурсы атакующего могут быть ограничены и неограничены, а также задействованы на общедоступные и специализированные инструменты, известные и публично неизвестные уязвимости, проведение исследований системы. По намерениям выделены личные, экономические, криминалистические, террористические и политические. Кроме того, намерения связаны с нарушение целостности, конфиденциальности и доступности информации, перехватов управления устройствами системы.

Рассмотрена классификация атакующих действий по таким атрибутам, как субъект, объект, способ воздействия, предпосылки и последствия. Субъектом атакующего действия может быть злоумышленник, природный или человеческий фактор, ошибки в процессе работы системы. Объект атакующего действия может быть выделен на основе места в архитектуре системы и затронутого бизнес-процесса. На основе места в архитектуре системы – отдельный элемент, группа элементов, отдельный уровень, группа уровней, отдельная подсистема, система в целом. На основе затронутого бизнес-процесса – сбор данных, хранение данных и журналирование, обработка и анализ данных, взаимодействие между элементами системы, управление работой системы, работа исполнительных

механизмов. Способ воздействия может быть определен на основе использованных технологий и на основе влияния на ресурсы системы. На основе использованных технологий – социоинженерные, физические, кибернетические и организационно-правовые атакующие действия. На основе влияния на ресурсы – направленные и ненаправленные, подслушивающие и перехватывающие, снижающие производительность, изолирующие. По предпосылкам – ошибки реализации и конфигурации, программные и аппаратные закладки, человеческий фактор. Последствия атакующих действия могут быть определены на основе затронутого бизнес-процеса, нарушенного аспекта безопасности, влияния на данные и пользователя системы. На основе затронутого бизнес-процеса – перехват управления, прекращение работы, внедрение вредоносного кода. На основе нарушенного аспекта безопасности – компрометация целостности, доступности, конфиденциальности, приватности и надежности. На основе влияния на данные системы – перехват, модификация, подделка, утечка, удаление. На основе влияния на пользователя системы – эмоциональный вред, изменение поведения, физический вред.

Предложена классификация методов и средств защиты по таким атрибутам, как принцип работы, объект защиты и решаемая задача. По решаемой задаче методы и средства защиты разделяют на элементы сбора, обработки и хранения данных; анализа данных, обнаружения атак и аномалий; мониторинга безопасности и поддержки принятия решений; идентификации, аутентификации и контроля доступа; шифрования и предотвращения утечек данных; оценки рисков и расследования инцидентов; обучения персонала, подготовки инструкций и документов. Объект защиты определяется на основе места в архитектуре системы и затронутого бизнес-процесса. На основе места в архитектуре – отдельный элемент, группа элементов, отдельный уровень, группа уровней, отдельная подсистема и система в целом. На основе затронутого бизнес-процесса – сбор данных, хранение данных и журналирование, обработка и анализ данных, взаимодействие между элементами системы, управление работой системы, работа исполнительных механизмов. По принципу работы – статические, активные, адаптивные, динамические.

Предполагается, что данная статья будет полезна как разработчикам, позволяя ответить на ряд проблемных вопросов информационной безопасности киберфизических систем на этапе их проектирования и поддержки, так и системным администраторам, давая возможность получить представление о состоянии безопасности устройств, которые входят в зону их ответственности. Кроме того, работа будет полезна исследователям и студентам, изучающим проблемы информационной безопасности.

Литература

1. *Десницкий В.А. и др.* Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. Вып. 5. № 48. С. 5–31.
2. *Levshun D., Chechulin A., Kotenko I., Chevalier Y.* Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems // 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2019. pp. 1–5.
3. *Pressley A.* Securing connections in the cloud and across IoT devices // Intelligent CIO Europe, 2020.
4. *Baheti R., Gill H.* Cyber-physical systems // The impact of control technology. 2011. vol. 12. no. 1. pp. 161–166.
5. *Schwab K.* The fourth industrial revolution // Currency. 2017.
6. *Hehenberger P. et al.* Design, modelling, simulation and integration of cyber-physical systems: Methods and applications // Computers in Industry. 2016. vol. 82. pp. 273–289.
7. *Зегжда Д.П.* Устойчивость как критерий информационной безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы, 2016. Т. 2. С. 13–18.
8. *Broy M.* Engineering cyber-physical systems: Challenges and foundations // Complex Systems Design & Management. 2013. pp. 1–13.
9. *Li Y., Li X., Wang L., Li Y.* Limestone-gypsum wet flue gas desulfurization based on Cyber-Physical System // 2019 Chinese Control And Decision Conference (CCDC). 2019. pp. 473–477.
10. *Рогозинский Г.Г.* Мультидоменный подход и модели объектов киберфизического пространства в задачах отображения информации // Труды учебных заведений связи. 2017. Т. 3. №. 4. С. 88–93.
11. *Xiao-Le W., Hong-Bin H., Su D., Li-Na C.* A service-oriented architecture framework for cyber-physical systems // Recent Advances in Computer Science and Information Engineering. 2012. pp. 671–676.
12. *Dong P., Han Y., Guo X., Xie F.* A systematic review of studies on cyber physical system security // International Journal of Security and Its Applications. 2015. vol. 9. no. 1. pp. 155–164.
13. *Xia X., Liu C., Wang H., Han Z.* A Design of Cyber-Physical System Architecture for Smart City // Recent Trends in Intelligent Computing, Communication and Devices. 2020. pp. 967–973.
14. *Lee J., Bagheri B., Kao H.A.* A cyber-physical systems architecture for Industry 4.0-based manufacturing systems // Manufacturing letters. 2015. vol. 3. pp. 18–23.
15. *Rojas R.A., Rauch E., Vidoni R., Matt D.T.* Enabling connectivity of cyber-physical production systems: a conceptual framework // Procedia Manufacturing. 2017. vol. 11. pp. 822–829
16. *Alguliyev R., Imamverdiyev Y., Sukhostat L.* Cyber-physical systems and their security issues // Computers in Industry. 2018. vol. 100. pp. 212–223.
17. *Cardin O.* Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry. 2019. vol. 104. pp. 11–21.
18. *Zegzhda D.P., Poltavtseva M.A., Lavrova D.S.* Systematization and security assessment of cyber-physical systems // Automatic control and computer sciences. 2017. vol. 51. no. 8. pp. 835–843.
19. *Романов В.Н.* Техника анализа сложных систем // СПб: СЗТУ. 2011. 287 с.
20. *Кохановский В.А., Сергеева М.Х., Комахидзе М.Г.* Оценка сложности систем // Вестник Донского государственного технического университета. 2012. № 4(65). С. 22–26.

21. *Burg A., Chattopadhyay A., Lam K.Y.* Wireless communication and security issues for cyber–physical systems and the Internet-of-Things // Proceedings of the IEEE. 2017. vol. 106. no. 1. pp. 38–60.
22. *Mikhaylov K., Tervonen J.* Evaluation of power efficiency for digital serial interfaces of microcontrollers // 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). 2012. pp. 1–5.
23. *Avatefipour O., Hafeez A., Tayyab M., Malik H.* Linking received packet to the transmitter through physical-fingerprinting of controller area network // 2017 IEEE Workshop on Information Forensics and Security (WIFS). 2017. pp. 1–6.
24. *Гайфулина Д.А., Котенко И.В., Федорченко А.В.* Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности. 2019. № 4. С. 280–299.
25. *Дойникова Е.В.* Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов. // Диссертация на соискание ученой степени кандидата технических наук. 2017. 207 с.
26. Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017№ 187-ФЗ (последняя редакция) // АО «Консультант Плюс».
27. *Stallings W.* The internet of things: network and security architecture // Internet Protoc. J. 2015. vol. 18. no. 4. pp. 2–24.
28. *Khaitan S.K., McCalley J.D.* Design techniques and applications of cyberphysical systems: A survey // IEEE Systems Journal. 2014. vol. 9. no. 2. pp. 350–365.
29. *Gomez C. et al.* Internet of Things for enabling smart environments: A technology-centric perspective // Journal of Ambient Intelligence and Smart Environments. 2019. vol. 11. no. 1. pp. 23–43.
30. *Monostori L.* Cyber-physical production systems: Roots, expectations and R&D challenges // Procedia Cirp. 2014. vol. 17. pp. 9–13.
31. *Гурьянов А.В., Заколдаев Д.А., Жаринов И.О., Нечаев В.А.* Принципы организации цифровых проектных и производственных предприятий Индустрии 4.0 // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 3. С. 421–427.
32. *Nikolakis N., Maratos V., Makris S.* A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace // Robotics and Computer-Integrated Manufacturing. 2019. vol. 56. pp. 233–243.
33. *Liu H., Wang L.* Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment // Journal of Manufacturing Systems. 2020. vol. 54. pp. 24–34.
34. *Лёвин Б.А., Розенберг И.Н., Цветков В.Я.* Транспортные кибер-физические системы // Наука и технологии железных дорог. 2017. Т. 3. № 3. С. 3.
35. *Волков А.А.* Кибернетика строительных систем. Киберфизические строительные системы // Промышленное и гражданское строительство. 2017. №. 9. С. 4–7.
36. *Dey N. et al.* Medical cyber-physical systems: A survey // Journal of medical systems. 2018. vol. 42. no. 4. pp. 74.
37. *Shishvan O.R., Zois D.S., Soyata T.* Incorporating Artificial Intelligence into Medical Cyber-Physical Systems: A Survey // Connected Health in Smart Cities. Springer, Cham. 2020. pp. 153–178.
38. *Попов Д.С.* Информационное обеспечение технологической подготовки ремонтного производства на транспорте // Вестник Сибирского государственного университета путей сообщения. 2007. № 17. С. 163–168.

39. *Федорченко А.В., Дойникова Е.В., Котенко И.В.* Автоматизированное определение активов и оценка их критичности для анализа защищенности информационных систем // Труды СПИИРАН. 2019. Т. 18. № 5. С. 1182–1211.
40. *Коптенков М.М.* Категорирование информации –– первый шаг к обеспечению информационной безопасности организации // Безопасность информационных технологий. 2011. Т. 18. № 4. С. 117–119.
41. *Микони С.В.* Модель участников жизненного цикла социо-киберфизической системы // Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста. 2019. С. 341–347.
42. ГОСТ Р. 53114-2008 Защита информации // Обеспечение информационной безопасности в организации. Основные термины и определения. 2008.
43. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 15 февраля 2008 г.
44. Методика определения угроз безопасности информации в информационных системах // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), проект, 2015 г.
45. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности // Федеральная служба безопасности (ФСБ России), 31 марта 2015 года, № 149/7/2/6-432.
46. *Rocchetto M., Tippenhauer N.O.* On attacker models and profiles for cyber-physical systems // European Symposium on Research in Computer Security. 2016. pp. 427–449.
47. *Десницкий В. А.* Модель киберфизической системы управления водоснабжением для анализа инцидентов безопасности // Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. С. 93–102.
48. ГОСТ Р. ИСО/МЭК 27000–2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология // М.: ФГУП «СТАНДАРТИНФОРМ». 2014.
49. *Mayzaud A., Badonnel R., Chrisment I.* A Taxonomy of Attacks in RPL-based Internet of Things. 2016.
50. *Zhu B., Joseph A., Sastry S.* A taxonomy of cyber attacks on SCADA systems // 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. 2011. pp. 380–388.
51. *Humayed A., Lin J., Li F., Luo B.* Cyber-physical systems security – A survey // IEEE Internet of Things Journal. 2017. vol. 4. no. 6. pp. 1802–1831.
52. *Alguliyev R., Imamverdiyev Y., Sukhostat L.* Cyber-physical systems and their security issues // Computers in Industry. 2018. vol. 100. pp. 212–223.
53. *Ashibani Y., Mahmoud Q.H.* Cyber physical systems security: Analysis, challenges and solutions // Computers & Security. 2017. vol. 68. pp. 81–97.
54. *Gao Y. et al.* Analysis of security threats and vulnerability for cyber-physical systems // Proceedings of 2013 3rd International Conference on Computer Science and Network Technology. 2013. pp. 50–55.
55. *Makhdoom I. et al.* Anatomy of threats to the internet of things // IEEE Communications Surveys & Tutorials. 2018. vol. 21. no. 2. pp. 1636–1675.
56. *Yampolskiy M. et al.* A language for describing attacks on cyber-physical systems // International Journal of Critical Infrastructure Protection. 2015. vol. 8. pp. 40–52.
57. *Heartfield R. et al.* A taxonomy of cyber-physical threats and impact in the smart home // Computers & Security. 2018. vol. 78. pp. 398–428.

58. *Алексеев Д.М., Иваненко К.Н., Убирайло В.Н.* Классификация угроз информационной безопасности // Символ науки. 2016. № 9-1. С. 18–20.
59. *Ashibani Y., Mahmoud Q. H.* Cyber-physical systems security: Analysis, challenges and solutions // Computers & Security. 2017. vol. 68. pp. 81–97.
60. *Desnitsky V., Levshun D., Chechulin A., Kotenko I.* Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System // JoWUA. 2016. vol. 7. no. 2. pp. 60–80.
61. *Котенко И. В. и др.* Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3(27). С. 29–38.
62. *Зегжда Д.П. и др.* Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасностию 2018. № 2(26). С. 2–14.
63. *Frahim J.* Securing the Internet of Things: A Proposed Framework // Cisco White Paper, March 2015.
64. *Гайфулина Д.А.* Аналитический обзор методов обнаружения аномалий сетевого уровня киберфизических систем // Альманах научных работ молодых ученых Уни-верситета ИТМО. 2018. Т. 1. С. 4–5.
65. *Котенко И.В., Дойникова Е.В.* Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. 2011. № 4. С. 74–81.
66. *Desmit Z., Elhabashy A.E., Wells L.J., Camelio J.A.* An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems // Journal of Manufacturing Systems. 2017. vol. 43. pp. 339–351.
67. *Radanliev P. et al.* Future developments in cyber risk assessment for the internet of things // Computers in Industry. 2018. vol. 102. pp. 14–22.
68. *Lyu X., Ding Y., Yang S.H.* Safety and security risk assessment in cyber-physical systems // IET Cyber-Physical Systems: Theory & Applications. 2019. vol. 4. no. 3. pp. 221–232.
69. *Телегина М.В., Янников И.М., Куделькин В.А., Ушаков И.С.* Модели и методы оценки безопасности критически важных и потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15. № 1. С. 118–121.
70. *Кулагина И.В., Исхакова А.О., Галин Р.Р.* Моделирование практик агрессии в социо-киберфизической среде // Вестник Томского государственного университета. Философия. Социология. Политология. 2019. № 52. С. 147–161.
71. *Гарате В.Г.* Анализ уровня защищенности корпоративных компьютерных сетей в контексте социоинженерных атак // Известия СПбГЭТУ «ЛЭТИ». 2017. Т. 3. С. 12–15.

Левшун Дмитрий Сергеевич — младший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: безопасность в соответствии с проектом, проектирование, моделирование и верификация киберфизических систем. Число научных публикаций – 47. levshun@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-26-42; факс: +7(812)328-44-50.

Гайфулина Диана Альбертовна — младший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПб ФИЦ РАН). Область научных интересов: неструктурированных данных, обнаружение

атак и аномалий. Число научных публикаций – 19. gaifulina@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-26-42; факс: +7(812)328-44-50.

Чечулин Андрей Алексеевич — канд. техн. наук, доцент, ведущий научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: безопас-ность компьютерных сетей, обнаружение вторжений, анализ уязвимостей, визуализация, безопасность встроенных устройств, анализ социальных сетей. Число научных публикаций – 100. chechulin@comsec.spb.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-71-81; факс: +7(812)328-44-50.

Котенко Игорь Витальевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: информационная безопасность, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, ложные информационные системы, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибертерроризму; искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений; телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций – 450. ivkote@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-71-81; факс: +7(812)328-44-50.

Поддержка исследований. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-17-50205.

DOI 10.15622/ia.2020.19.5.6

D. Levshun, D. Gaifulina, A. Chechulin, I. Kotenko

PROBLEMATIC ISSUES OF INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS

Levshun D., Gaifulina D., Chechulin A., Kotenko I. **Problematic Issues of Information Security of Cyber-Physical Systems.**

Abstract. This paper is an analysis and systematization of modern research in the field of cyber-physical system information security. The problematic issues of information security of such systems are considered: «what is being attacked?», «who is attacking?», «why is someone attacking?», «how is someone attacking?» and «how to protect the system?». As an answer to the first question, the paper proposes a definition and classification of cyber-physical systems according to such criteria as complexity, connectivity, criticality and social aspect. As an answer to the second and the third questions, the paper describes a classification of attacker according to such criteria as type of access, method of access, intentions, knowledge and resources. As an answer to the fourth question, the paper contains a classification of attack actions according to such criteria as subject and object, method of influence, prerequisites and consequences. As an answer to the fifth question, the paper proposes a classification of protection methods and security tools according to such criteria as principle of operation, object of protection and task to be solved. The scientific significance of the paper is systematization of a current state of the art in the subject area. The practical value of the paper is providing information about security issues that are specific to cyber-physical systems, which will allow one to develop, manage and use such systems in a more secure way.

Keywords: information security, cyber-physical system, target of the attacker, model of the attacker, model of attack actions, protection method, security tool.

Levshun Dmitry — Junior Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: security by design, design, modeling and verification of cyber-physical systems. The number of publications – 47. levshun@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-26-42; fax: +7(812)328-44-50.

Gaifulina Diana — Junior Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: data mining, analysis of unstructured data, detection of attacks and anomalies. The number of publications – 19. gaifulina@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-26-42; fax: +7(812)328-44-50.

Chechulin Andrey — Ph.D., Associate Professor, Leading Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: computer network security, intrusion detection, vulnerability analysis, visualization, IoT security, social networks analysis. The number of publications – 100. chechulin@comsec.spb.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-71-81; fax: +7(812)328-44-50.

Kotenko Igor — Ph.D., Dr.Sci., Professor, Chief Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: : information security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; artificial intelligence, including

multi-agent frameworks and systems, agent-based modeling and simulation, soft and evolutionary computing, machine learning, data mining, data and information fusion; telecommunications, including decision making and planning for telecommunication systems. The number of publications – 450. ivkote@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-71-81; fax: +7(812)328-44-50.

Acknowledgements. The reported study was funded by RFBR, project number 19-17-50205.

References

1. Desnitsky V.A. et al. [Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2016. vol. 5. no. 48. pp. 5–31. (In Russ.).
2. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems. 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2019. pp. 1–5.
3. Pressley A. Securing connections in the cloud and across IoT devices // Intelligent CIO Europe, 2020.
4. Baheti R., Gill H. Cyber-physical systems. *The impact of control technology*. 2011. vol. 12. no. 1. pp. 161–166.
5. Schwab K. The fourth industrial revolution. Currency. 2017.
6. Hehenberger P. et al. Design, modelling, simulation and integration of cyber-physical systems: Methods and applications. *Computers in Industry*. 2016. vol. 82. pp. 273–289.
7. Zegzhda D.P. [Stability as information security criteria for cyber-physical systems]. *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy — Information Security Problems. Computer Systems*. 2016. Issue 2. pp. 13–18. (In Russ.).
8. Broy M. Engineering cyber-physical systems: Challenges and foundations. Complex Systems Design & Management. 2013. pp. 1–13.
9. Li Y., Li X., Wang L., Li Y. Limestone-gypsum wet flue gas desulfurization based on Cyber-Physical System. 2019 Chinese Control And Decision Conference (CCDC). 2019. pp. 473–477.
10. Rogozinsky G.G. [Multi-domain approach and models of cyber-physical objects in information representation systems]. *Trudy uchebnyh zavedenij svyazi -– Proceedings of Telecommunication Universities*. 2017. Issue 3. vol. 4. pp. 88–93. (In Russ.).
11. Xiao-Le W., Hong-Bin H., Su D., Li-Na C. A service-oriented architecture framework for cyber-physical systems. Recent Advances in Computer Science and Information Engineering. 2012. pp. 671–676.
12. Dong P., Han Y., Guo X., Xie F. A systematic review of studies on cyber physical system security. *International Journal of Security and Its Applications*. 2015. vol. 9. no. 1. pp. 155–164.
13. Xia X., Liu C., Wang H., Han Z. A Design of Cyber-Physical System Architecture for Smart City. Recent Trends in Intelligent Computing, Communication and Devices. 2020. pp. 967–973.
14. Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing letters*. 2015. vol. 3. pp. 18–23.
15. Rojas R. A., Rauch E., Vidoni R., Matt D.T. Enabling connectivity of cyber-physical production systems: a conceptual framework. *Procedia Manufacturing*. 2017. vol. 11. pp. 822–829.
16. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. 2018. vol. 100. pp. 212–223.
17. Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework. *Computers in Industry*. 2019. vol. 104. pp. 11–21.

18. Zegzhda D.P., Poltavtseva M.A., Lavrova D.S. Systematization and security assessment of cyber-physical systems. *Automatic control and computer sciences*. 2017. vol. 51. no. 8. pp. 835–843.
19. Romanov V.N. [Approach for complex systems analysis]. SPb: SZTU. 2011. 287 p. (In Russ.).
20. Kohanovskiy V.A., Sergeyeva M.H., Komakhidze M.G. [System complexity index]. *Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta – Advanced Engineering Research*. 2012. vol. 4(65). pp. 22–26. (In Russ.).
21. Burg A., Chattopadhyay A., Lam K.Y. Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *Proceedings of the IEEE*. 2017. vol. 106. no. 1. pp. 38–60.
22. Mikhaylov K., Tervonen J. Evaluation of power efficiency for digital serial interfaces of microcontrollers. 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). 2012. pp. 1–5.
23. Avatefipour O., Hafeez A., Tayyab M., Malik H. Linking received packet to the transmitter through physical-fingerprinting of controller area network. 2017 IEEE Workshop on Information Forensics and Security (WIFS). 2017. pp. 1–6.
24. Gaifulina D.A., Kotenko I.V., Fedorchenko A.V. [A Technique for Lexical Markup of Structured Binary Data for Problems of Protocols Analysis in Uncertainty Conditions]. *Sistemy upravleniya, svyazi i bezopasnosti -– Systems of Control, Communication and Security*. 2019. vol. 4. pp. 280–299. (In Russ.).
25. Doynikova E.V. [Security assessment and selection of protective measures in computer networks based on attack graphs and service dependencies]. *Dissertaciya na soiskanie uchenoj stepeni kandidata tekhnicheskih nauk – Dissertation for the degree of candidate of technical sciences*. 2017. 207 p. (In Russ.).
26. Federal'nyj zakon «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» ot 26.07.2017 № 187-FZ (poslednyaya redakciya) – Federal Law «On the Security of the Critical Information Infrastructure of the Russian Federation» dated July 26, 2017 No. 187-FZ (last edition)]. Consultant Plus. (In Russ.).
27. Stallings W. The internet of things: network and security architecture. *Internet Protoc. J*. 2015. vol. 18. no. 4. pp. 2–24.
28. Khaitan S.K., McCalley J.D. Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*. 2014. vol. 9. no. 2. pp. 350–365.
29. Gomez C. et al. Internet of Things for enabling smart environments: A technology-centric perspective. *Journal of Ambient Intelligence and Smart Environments*. 2019. vol. 11. no. 1. pp. 23–43.
30. Monostori L. Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia Cirp*. 2014. vol. 17. pp. 9–13.
31. Gurjanov A.V., Zakoldaev D.A., Zharinov I.O., Nechaev V.A. [Design concepts for digital project and production companies of Industry 4.0 standard]. *Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki -– Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2018. Issue 18. vol. 3. pp. 421-427. (In Russ.).
32. Nikolakis N., Maratos V., Makris S. A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace. *Robotics and Computer-Integrated Manufacturing*. 2019. vol. 56. pp. 233–243.
33. Liu H., Wang L. Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment. *Journal of Manufacturing Systems*. 2020. vol. 54. pp. 24–34.
34. Levin B.A., Rosenberg I.N., Tsvetkov V.Y. [Transport cyber-physical systems]. *Nauka i tekhnologii zheleznyh dorog — Science and technology of railways*. 2017. Issue 3. vol. 3. pp. 3. (In Russ.).

35. Volkov A A. [Cybernetics of construction systems]. *Promyshlennoe i grazhdanskoe stroitel'stvo — Cyber-physical construction systems*. 2017. vol. 9. pp. 4–7. (In Russ.).
36. Dey N. et al. Medical cyber-physical systems: A survey. *Journal of medical systems*. 2018. vol. 42. no. 4. pp. 74.
37. Shishvan O.R., Zois D.S., Soyata T. Incorporating Artificial Intelligence into Medical Cyber-Physical Systems: A Survey. *Connected Health in Smart Cities*. 2020. pp. 153–178.
38. Popov D.S. [Information support for technological preparation of repair production in transport]. *Vestnik Sibirskogo gosudarstvennogo universiteta putej soobshcheniya -– Journal of the Siberian State Transport University*. 2007. vol. 17. pp. 163–168. (In Russ.).
39. Fedorchenko A.V., Doynikova E.V., Kotenko I.V. [Automated detection of assets and calculation of their criticality for the analysis of information system security]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2019. Issue 18(5). pp. 1182–1211. (In Russ.).
40. Koptenkov M.M. [Information categorization is the first step to ensuring the information security of an organization]. *Bezopasnost Informatsionnykh Tekhnologiy — IT Security*. 2011. Issue 18. vol. 4. pp. 117–119.
41. Mikoni S.V. [Model of the participants in the life cycle of a socio-cyber-physical system]. *Tekhnologicheskaya perspektiva v ramkah evrazijskogo prostranstva: novye rynki i tochki ekonomicheskogo rosta – Technological perspective within the Eurasian space: new markets and points of economic growth*. 2019. pp. 341–347. (In Russ.).
42. GOST R. 53114-2008 Information security. Ensuring information security in the organization. Basic terms and definitions. 2008. (In Russ.).
43. The basic model of threats to the security of personal data during their processing in personal data information systems. Federal Service for Technical and Export Control (FSTEC of Russia), February 15, 2008. (In Russ.).
44. Metodika opredeleniya ugroz bezopasnosti informacii v informacionnyh sistemah [Methodology for determining threats to information security in information systems]. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii), proekt, 2015. (In Russ.).
45. Methodological recommendations for the development of regulatory legal acts that determine threats to the security of personal data, relevant when processing personal data in information systems of personal data used in the implementation of relevant activities. Federal Security Service (FSB of Russia), March 31, 2015, No. 149/7/2/6-432. (In Russ.).
46. Rocchetto M., Tippenhauer N.O. On attacker models and profiles for cyber-physical systems. European Symposium on Research in Computer Security. 2016. pp. 427–449.
47. Desnitsky V.A. [A Modeling and Analysis of Security Incidents in a Cyber-Physical System for Water Supply Management]. *Informacionnye tekhnologii i telekommunikacii – Telecom IT*. 2017. vol. 5. no. 3. pp. 93–102. (In Russ.).
48. GOST R. ISO/IEC 27000–2012 Information technology. Security methods and means. Information security management systems. General overview and terminology. Moscow: FGUP STANDARTINFORM. 2014. (In Russ.).
49. Mayzaud A., Badonnel R., Chrisment I. A Taxonomy of Attacks in RPL-based Internet of Things. 2016.
50. Zhu B., Joseph A., Sastry S. . A taxonomy of cyber attacks on SCADA systems. 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. 2011. pp. 380–388.
51. Humayed A., Lin J., Li F., Luo B. Cyber-physical systems security – A survey. *IEEE Internet of Things Journal*. 2017. vol. 4. no. 6. pp. 1802–1831.
52. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. 2018. vol. 100. pp. 212–223.
53. Ashibani Y., Mahmoud Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017. vol. 68. pp. 81–97.

54. Gao Y. et al. Analysis of security threats and vulnerability for cyber-physical systems. Proceedings of 2013 3rd International Conference on Computer Science and Network Technology. 2013. pp. 50–55.
55. Makhdoom et al. Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials*. 2018. vol. 21. no. 2. pp. 1636–1675.
56. Yampolskiy et al. A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*. 2015. vol. 8. pp. 40–52.
57. Heartfield et al. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*. 2018. vol. 78. pp. 398–428.
58. Alekseev D.M., Ivanenko K.N., Ubirailo V.N. [Classification of threats to information security]. *Simvol nauki -– Science symbol*. 2016. vol. 9-1. pp. 18–20. (In Russ.).
59. Ashibani Y., Mahmoud Q.H. Cyber-physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017. vol. 68. pp. 81–97.
60. Desnitsky V., Levshun D., Chechulin A., Kotenko I.V. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. *JoWUA*. 2016. vol. 7. no. 2. pp. 60–80.
61. Kotenko I.V. et al. [Integrated approach to provide security of cyber-physical systems based on microcontrollers]. *Voprosy Kiberbezopasnosti -– Voprosy Kiberbezopasnosti*. 2018. vol. 3(27). pp. 29-38. (In Russ.).
62. Zegzhda D.P. et al. [Advanced production technologies security in the era of digital transformation]. *Voprosy Kiberbezopasnosti – Voprosy Kiberbezopasnosti*. 2018. vol. 2(26). pp. 2–14. (In Russ.).
63. Frahim J. Securing the Internet of Things: A Proposed Framework. Cisco White Paper, March 2015.
64. Gaifulina D.A. [Analytical review of methods for detecting network layer anomalies in cyber-physical systems]. *Al'manah nauchnyh rabot molodyh uchenyh Universiteta ITMO — Almanac of scientific works of young scientists of ITMO University*. 2018. Issue 1. pp. 4–5. (In Russ.).
65. Kotenko I.V., Doynikova E.V. [Vulnerabilities assessment techniques: use for the computer systems security analysis]. *Zashchita informacii. Insajd -– Information Security*. Inside. 2011. vol. 4. pp. 74–81. (In Russ.).
66. Desmit Z., Elhabashy A.E., Wells L.J., Camelio J.A. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal of Manufacturing Systems*. 2017. vol. 43. pp. 339–351.
67. Radanliev P. et al. Future developments in cyber risk assessment for the internet of things. *Computers in Industry*. 2018. vol. 102. pp. 14–22.
68. Lyu X., Ding Y., Yang S.H. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*. 2019. vol. 4. no. 3. pp. 221–232.
69. Telegina M.V., Yannikov I.M., Kudelkin V.A., Ushakov I.S. [Models and methods for safety assessment of potentially dangerous objects]. *Intellektual'nye sistemy v proizvodstve — Intelligent systems in production*. 2017. Issue 15. vol. 1. pp. 118–121. (In Russ.).
70. Kulagina I.V., Iskhakova A.O., Galin R.R. [Modeling the practice of aggression in the socio-cyber-physical environment]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya — Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2019. vol. 52. pp. 147–161. (In Russ.).
71. Garate V.G. Analysis of security level of corporate networks in the context of socioengineering attacks. *Izvestiya SPbGETU «LETI» – Izvestiya ETU LETI*. 2017. Issue 3. pp. 12–15. (In Russ.).

УДК 004.065 **DOI** 10.15622/ia.2020.19.5.7

Р.В. Мещеряков, А.Ю. Исхаков, О.О. Евсютин

СОВРЕМЕННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В ПРОТОКОЛАХ УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Мещеряков Р.В., Исхаков А.Ю., Евсютин О.О. **Современные методы обеспечения целостности данных в протоколах управления киберфизических систем.**

Аннотация. В настоящее время остро стоит проблема создания методологического обеспечения безопасности киберфизических систем, в частности проектирования и реализации подсистем информационной безопасности. При этом ландшафт угроз и уязвимостей, характерных для применяемого в киберфизических системах широкого спектра аппаратных и программных технологий, чрезвычайно широк и сложен. В этом контексте безопасность протоколов прикладного уровня имеет первостепенное значение, поскольку эти протоколы лежат в основе взаимодействия между приложениями и службами, работающими на различных устройствах, а также в облачных инфраструктурах. В условиях постоянного взаимодействия исследуемых систем с реальной физической инфраструктурой актуальна проблема определения эффективных мер по обеспечению целостности передаваемых команд управления, поскольку нарушение выполняемых критически важных процессов может затрагивать жизнь и здоровье людей. Представлен обзор основных методов обеспечения целостности данных в протоколах управления киберфизических систем, а также обзор уязвимостей протоколов прикладного уровня, широко используемых в различных киберфизических системах. Рассмотрены классические методы обеспечения целостности и новые методы, в частности блокчейн, а также основные направления повышения эффективности протоколов обеспечения целостности данных в киберфизических системах. Анализ уязвимостей прикладного уровня проведен на примере наиболее популярных спецификаций MQTT, CoAP, AMQP, DDS, XMPP, а также их реализаций. Установлено, что несмотря на наличие во всех перечисленных протоколах базовых механизмов обеспечения безопасности, исследователи продолжают регулярно выявлять уязвимости в популярных реализациях, что зачастую ставит под угрозу сервисы критической инфраструктуры. В ходе подготовки обзора существующих методов обеспечения целостности данных для исследуемого класса систем были определены ключевые проблемы интеграции этих методов и способы их решения.

Ключевые слова: киберфизическая система, интернет вещей, протокол, блокчейн, цифровые водяные знаки, аутентификация

1. Введение. Исследование методов и подходов к обеспечению информационной безопасности в киберфизических системах является важной задачей на пути формирования единой методологии развития средств автоматизации и управления в сложных гетерогенных системах, переход к которым позволит человечеству выйти на более высокий уровень индустриализации, снизить количество и уровень последствий техногенных производственных катастроф и повысить качество жизни.

Актуальность задач обеспечения комплексной безопасности киберфизических систем за счет специализированных научно обоснован-

ных методов организации защищенного взаимодействия компонентов обусловлена стремительным ростом кибератак по всему миру – сложных, многошаговых и зачастую адаптированных под целевую инфраструктуру. Так, после нашумевшей Mirai [1] двумя другими крупными ботнет-атаками стали Hajime и Reaper, которые направлены на большое количество умных устройств. В апреле 2020 года исследователи в области кибербезопасности зафиксировали множественные атаки ботнета «Dark Nexus», использующего уязвимые гаджеты Интернета вещей для выполнения распределенных атак «отказ в обслуживании». На данный момент атака включает более 1400 ботов, функционирующих в режиме обратного прокси-сервера, и направлена на критически важные объекты Китая, Таиланда, Бразилии, Южной Кореи и России [2].

Подобные вторжения в киберфизические системы производственных процессов, запущенных в критической инфраструктуре, недопустимы. Именно поэтому обсуждению данной проблемы и выдвижению собственных подходов и методов посвящено множество публикаций российских и зарубежных авторов, а также материалов докладов профильных конференций. Такая активность показывает заинтересованность мирового научного сообщества в создании комплексных решений в данной области.

К числу отличительных особенностей подавляющего большинства решений для киберфизических систем являются высокие требования к уровню функционирования, безопасности и надежности протоколов управления, а также необходимость сочетания многопрофильных задач в рамках одного производственного процесса, ведения непрерывного мониторинга и анализа состояния системы. Наряду с этим не менее важной отличительной особенностью является проблема применимости современных средств и методов обеспечения безопасности. Перспективные направления адаптации методов и алгоритмов защиты информации для их использования в киберфизических системах зачастую обусловлено низкой вычислительной способностью компонентов таких комплексов.

Результаты исследований [3-5] говорят о том, что наибольшей популярностью у злоумышленников пользуются именно протоколы прикладного уровня (Application layer), в рамках которых разработчики реализуют проприетарные правила и механизмы (форматы запросов и ответов, программные интерфейсы приложений (application programming interface, API), запросы к уровню представления, обработчики ошибок и т.д.). Это связано с высокой вероятностью наличия уязвимостей нулевого дня, что обусловлено низкой степенью защиты применяемых методов вследствие игнорирования разработчиками не-

обходимого анализа со стороны научного сообщества и исследователей в сфере информационной и кибернетической безопасности. В [6] представлено исследование типовых протоколов безопасности DTLS и IPSec, применяемых в контексте защиты рассматриваемых инфраструктур. Приведенный в вышеуказанной работе анализ подчеркивает, что эти протоколы не отвечают некоторым требованиям безопасности, кроме того, существует проблема высокой нагрузки и масштабирования, когда речь заходит о применении протоколов DTLS и IPSec в устройствах инфраструктуры Интернета вещей (Internet of Things, IoT) с низкими вычислительными способностями. Указанные обстоятельства вынуждают разработчиков еще раз задуматься об обеспечении безопасности непосредственно на уровне приложений. В этой связи в рамках данной статьи обзор будет ориентирован на методы защиты, предназначенные для применения на прикладном уровне модели OSI (The Open Systems Interconnection model). В качестве перспективных мер по нейтрализации угроз нарушения целостности данных приводится анализ мирового опыта по применению технологии блокчейн и цифровых водяных знаков в качестве механизмов обеспечения информационной безопасности киберфизических систем.

Статья организована следующим образом. В разделе 2 представлена общая характеристика рассматриваемых протоколов прикладного уровня, которые применяются для управления объектами киберфизических систем и элементами инфраструктуры Интернета вещей. В разделе 3 рассматриваются потенциальные риски безопасности, основанные на консолидации записей из баз данных Common Vulnerabilities and Exposures (CVE) и банка данных угроз ФСТЭК России, характерных для исследуемых протоколов, а также мировых практик и научных исследований. В разделе 4 представлен обзор современных научных публикаций в контексте обеспечения целостности данных для выбранной предметной области, в том числе приводится обзор научных публикаций, рассматривающих интеграцию технологии блокчейн в киберфизические системы, а также обзор методов встраивания цифровых водяных знаков в качестве механизма обеспечения целостности и аутентификации данных. В разделе 5 обсуждаются основные результаты анализа актуальных методов противодействия угрозам обеспечения целостности данных, передаваемых в протоколах управления киберфизических систем.

2. Краткий обзор исследуемых протоколов. Необходимо отметить, что рассматриваемые в статье протоколы зачастую относят и к протоколам Интернета вещей. Это связано с тем, что в научной среде инфраструктуры IoT и киберфизических систем имеют схожие опре-

деления. Оба понятия соответствуют тенденции интеграции цифровых возможностей, подразумевающей тесное взаимодействие между физическими и вычислительными процессами, в том числе с применением соответствующих систем и сетевой инфраструктуры. При этом в ходе анализа публикаций по соответствующей тематике у разных исследователей прослеживаются разногласия в архитектуре представления данных концепций. Так различные эксперты используют противоречивые определения о разного рода перекрытии понятий «Интернет вещей» и «киберфизические системы» – частичное или полное включение одного множества в другое, обратные включения, эквивалентность. Тем не менее наблюдается тенденция сближения этих терминов [7] – несмотря на различие в происхождении, современные системы, рассматриваемые с точки зрения функциональности, попадают под формальное определение обоих понятий.

Исследования, направленные на систематизацию различных категорий киберфизических систем [8, 9], применяют разнообразные подходы к их классификации:

– по уровням интеграции (connection, conversion, cyber и т.д.);

– по доменам применения (энергетика, робототехника, транспортные задачи, военные объекты, системы здравоохранения и т.д.);

– по степени взаимодействия с человеком.

Очевидно, что многообразие и гетерогенность используемого оборудования в той или иной области применения, а также различные архитектурные модели киберфизических и социокиберфизических систем требуют дифференцированного подхода в подборе оптимального перечня методов и средств обеспечения информационной безопасности. В данной статье обзор протоколов ограничивается наиболее популярными стандартами и реализациями [10], применяемыми при разработке киберфизических систем и IoT-решений:

– CoAP;
– MQTT;
– DTLS;
– Eddystone;
– HTTP2;
– iBeacon;
– PJON;
– STOMP;
– Websocket;
– XMPP.

Как было отмечено ранее, протоколы связи на прикладном уровне являются фундаментальным элементом киберфизической эко-

системы, поскольку они лежат в основе всех взаимодействий между элементами IoT, а также между устройствами и облачной инфраструктурой [11-12]. Типичные функции, реализованные этими протоколами, связаны с обменом сообщениями и обнаружением сервисов. В частности, обмен сообщениями относится к передаче информации (данных и управляющих воздействий) между устройствами, а обнаружение – к детектированию предлагаемых устройств и сервисов. В таблице 1 приведены основные характеристики наиболее популярных протоколов обмена сообщениями, а именно: MQTT, CoAP, AMQP, DDS и XMPP. Протоколы обнаружения служб (такие как mDNS и SSDP) не предоставляют функционал передачи команд управления, поэтому не являются предметом настоящего исследования.

Таблица 1. Основные характеристики протоколов прикладного уровня

Протокол	MQTT	CoAP	AMQP	DDS	XMPP
Стандарт	OASIS	IETF	OASIS	OMG	IETF
Архитектура	Централизованная	Централизованная	Централизованная	Децентрализованная	Централизованная
Модель взаимодействия	Pub/Sub	Req/Resp	Pub/Sub	Pub/Sub	Pub/Sub, Req/Resp
Транспорт	TCP	UDP	TCP	TCP / UDP	TCP
Обеспечение конфиденциальности	TLS	DTLS	TLS	TLS/ DTLS	TLS
Аутентификация	Проприетарная	Проприетарная	SASL	Проприетарная	SASL
Авторизация	-	-	-	Проприетарная	Проприетарная

Содержимое таблицы 1 демонстрирует, что протоколы различаются по многим аспектам, таким как архитектурные модели и модели взаимодействия, режимы транспорта данных и встроенные механизмы обеспечения безопасности. Некоторые протоколы используют централизованные, то есть клиент-серверные архитектуры, в то время как другие основаны на полностью распределенных архитектурах. Например, для таких протоколов, как MQTT и AMQP, брокер играет роль сервера и взаимодействует с клиентами, получая и пересылая сообщения. Обмен сообщениями, как правило, осуществляется в соответствии с моделями публикации/подписки или запроса/ответа. Несмотря на то, что все рассмотренные протоколы предназначены для

подключения устройств в распределенной сети, выбор того или иного протокола определяется исходя из необходимости выполнения конкретных операционных сценариев и архитектуры внедрения, особенно когда приняты во внимание ключевые системные требования, такие как производительность, качество обслуживания, интероперабельность, обеспечение отказоустойчивости и безопасности [13].

3. Анализ уязвимостей. Несмотря на то, что во всех перечисленных протоколах в той или иной степени предусмотрены базовые механизмы обеспечения безопасности, исследователи регулярно находят уязвимости, которые ставят под угрозы сервисы критической инфраструктуры. На рисунке 1 представлена статистика национальной базы данных уязвимостей США (National vulnerability database, NVD) за последние 2,5 года по указанным протоколам.

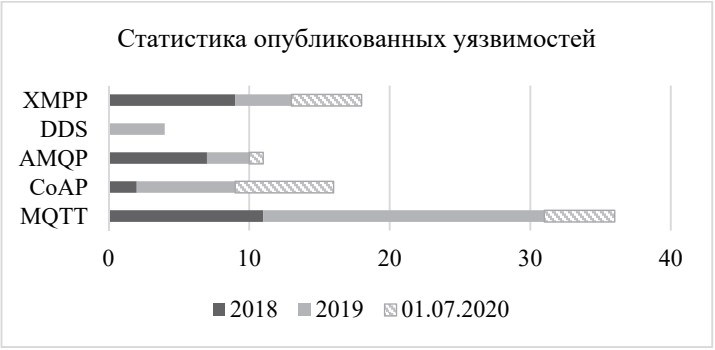


Рис. 1. Статистика по количеству уязвимостей протоколов (реализаций), опубликованных в базе NVD с 2018 года

Проведенный авторами анализ CVE, связанных с сервисами и системами, которые используют протокол MQTT, позволяет судить не только о характере выявленных угроз безопасности [14] в конкретных инфраструктурах, но и выявить общую тенденцию уязвимых точек данного стандарта. Так, в ходе анализа поисковой выдачи специализированной системы vulners.com было найдено более 70 записей (в том числе эксплойты, бюллетени безопасности и другие публикации), прямо или косвенно связанные с исследуемым протоколом. Поиск по NVD показал, что из более 36 тематических записей, опубликованных начиная с 2018 года, большинство уязвимостей связано с недостаточной проверкой сообщений сервисами и службами. Например, «ошибка неучтенной единицы» (CVE-2020-10070) в декодере длины пакета MQTT проекта Zephyr может привести к повреждению памяти и возможному удаленному выполнению кода. Уязвимость (CVE-2019-

11779) характеризует возможность вредоносного клиента MQTT вызвать переполнение стека, просто отправив *subscribe*-пакет, содержащий тему из не менее 65400 «/» символов. Аналогично пакет *connect* в сочетании с вредоносным пакетом запроса *unsubscribe* может быть использован для того, чтобы вызвать атаку типа «отказ в обслуживании» (DoS) на брокера (CVE-2019-6241). Другие вопросы безопасности относятся к категориям аутентификации и авторизации. Широко известен яркий пример (CVE-2017-7650), когда клиенты, определяющие имя пользователя как «#», полностью игнорируют механизмы контроля доступа и подписываются на все темы MQTT. В публикации [15] обсуждается несколько причин того, почему существует множество систем IoT на основе MQTT, в которых не реализованы адекватные механизмы безопасности, а также представлены демонстрационные сценарии типовых атак. Интерес представляет исследование [16], в рамках которого авторы провели оценку атак отказа в обслуживании, нацеленных на брокеров различных реализаций данного протокола, а также представили консолидированную модель угроз MQTT. Стоит отметить обзор популярной среди злоумышленников схемы DoS-атаки посредством отправки брокеру сообщений с высоким уровнем QoS.

Обзор публикаций, обобщающих уязвимости CoAP [17-19], а также БДУ ФСТЭК (BDU:2019-00925, BDU:2020-02424) и NVD (CVE-2020-12884, CVE-2020-10063, CVE-2019-17212, CVE-2018-12679, CVE-2018-12680) позволяет утверждать, что наиболее частая проблема безопасности в реализациях связана с некорректной проверкой объема подаваемых данных и содержимого сообщений. Использование этих уязвимостей может привести к таким последствиям, как утечка памяти и удаленное выполнение кода, что ставит под угрозу работоспособность всей киберфизической системы, использующей CoAP. Также известны уязвимости популярных библиотек CoAP, позволяющие в результате подмены адреса источника и некорректной обработки ответных сообщений (CVE-2019-9750) выполнять распределенную атаку типа «отказ в обслуживании».

Согласно базе данных NVD и научного сообщества [5, 20] сервисы киберфизических систем, использующие AMQP, неоднократно подвергались критике со стороны исследователей в области информационной безопасности. Так в ходе изучения практических исследований безопасности протокола AMQP было выявлено множество фактов некорректной настройки брокера, что зачастую приводит к серьезным угрозам для объекта. Кроме того, сам пользовательский веб-интерфейс управления зачастую становится источником критических

угроз (например, CVE-2015-0862, CVE-2016-0734, CVE-2017-4965). Безусловно, в отличие от MQTT и CoAP такие защитные механизмы, как TLS и SASL, как правило, включены по умолчанию, что снижает потенциальные риски безопасности. Тем не менее последствия уязвимостей (в большинстве случаев, связанных с компонентом брокера) позволяют злоумышленникам использовать повышение привилегий, выполнять перехват трафика в обход аутентификации и выполнять атаки типа «отказ в обслуживании» (CVE-2015-7559, CVE-2017-15699, CVE-2015-0224, CVE-2015-1499) и MiTM. В частности, некоторые уязвимости (CVE-2018-11087, CVE-2018-8119, CVE-2016-4467, CVE-2019-3845), связанные с отсутствием процедур проверки имени хоста и сертификатов, а также контролем доступа в очередях сообщений, позволяют злоумышленникам подделывать идентификационные данные и перехватывать команды управления.

DDS протокол поддерживает TLS, DTLS и другие механизмы безопасности. Последняя спецификация безопасности DDS OMG определяет архитектуру, основанную на наборе встроенных плагинов. Так плагины предлагают механизмы аутентификации и авторизации DataWriters и DataReaders, что позволяет избежать несанкционированной публикации и подписки. Тем не менее как спецификация, так и плагины подвержены уязвимостям. В частности, протокол рукопожатия, используемый для авторизации, как представлено в [21], может позволить злоумышленникам обнаружить потенциально конфиденциальную информацию о доступности в сети DDS (CVE-2019-15135). На практике [22] далеко не все продукты и сервисы DDS соответствуют спецификации безопасности, и даже совместимые реализации могут быть подвержены уязвимостям.

Протокол XMPP включает поддержку TLS для обеспечения конфиденциальности и целостности данных, а также обеспечивает поддержку SASL для процесса аутентификации. Подобные механизмы встроены в основные спецификации протокола и включены по умолчанию. Тем не менее отсутствие сквозной поддержки шифрования делает протокол уязвимым для различных типов угроз. В дополнение к этому за последние 5 лет было обнаружено более 90 CVE, которые в основном относятся к процессам аутентификации и проверки сообщений в тех или иных сервисах (например, CVE-2019-1845, CVE-2019-12855, CVE-2014-3451, CVE-2018-15720, CVE-2016-1307). В [23] рассматриваются уязвимости, связанные не с XMPP напрямую, а с пользовательскими функциями, встраиваемыми разработчиками поверх протокола, а также проведено моделирование атак типа «отказ в обслуживании» на сервер XMPP.

4. Методы защиты данных в протоколах киберфизических систем.

4.1. Классические методы обеспечения контроля целостности данных. Существует два больших научных направления, занимающихся целостностью данных в телекоммуникационных системах: теория кодирования и криптография. Одной из ключевых задач теории кодирования является обнаружение и исправление ошибок в передаваемых и хранимых данных. Обнаружение ошибок обеспечивает контроль целостности данных, в то время как исправление ошибок обеспечивает саму целостность. Во втором случае речь идет о так называемом помехоустойчивом кодировании.

Помехоустойчивое кодирование представляет собой метод, вводящий избыточность в передаваемую информацию для последующего восстановления ее целостности [24]. Кроме того, идеи, лежащие в основе помехоустойчивого кодирования, позволяют строить на его основе криптографические системы, устойчивые к атакам с использованием квантового компьютера [25]. Помехоустойчивые коды можно разделить на две основные группы: блоковые (блочные) коды [26] и сверточные коды [27]. Основное отличие блочных кодов от сверточных заключается в том, что блочные коды оперируют информационными последовательностями конечной длины, в то время как длина информационной последовательности для сверточного кода не ограничена. На практике широко используют следующие классы блочных кодов: коды Галлагера с малой плотностью проверок на четность (англ. LDPC), основным свойством которых является разреженная структура их порождающей матрицы, что оптимизирует процедуру их декодирования [28]; турбо-коды, объединяющие в себе идеи сверточного и блочного кодирования [29]; полярные коды, предложенные Ариканом в 2008 году и достигающие пропускной способности двоичного канала без памяти [30]. Также известны каскадные коды, позволяющие комбинировать различные методы конструирования блочных кодов с целью построения мощных кодов с хорошей корректирующей способностью [31].

Криптография представляет собой науку, занимающуюся поиском и исследованием математических методов преобразования информации с целью ее защиты. В отличие от теории кодирования криптография не позволяет обеспечивать целостности данных, а позволяет лишь ее контролировать. Другим отличием криптографических методов от методов теории кодирования является ориентированность на защиту от целенаправленных вредоносных действий, в то время как помехоустойчивое кодирование предназначено для защиты от естественных помех, присущих каналам передачи данных.

Выделяют три группы методов, предназначенных для обеспечения контроля целостности:

– хеширование;

– коды аутентичности сообщений (MAC);

– электронная подпись.

Поскольку область криптографических методов защиты информации на практике достаточно жестко ограничивается немногочисленным перечнем государственных стандартов, дадим определения перечисленным методам и приведем соответствующие стандарты.

Хешированием называется преобразование входной битовой строки произвольной длины в выходную битовую строку фиксированной длины. Функция, реализующая данное преобразование, называется хеш-функцией. Значение хеш-функции называют хеш-значением, хеш-кодом. Хеш-код является своего рода характеристическим признаком входной последовательности данных, по которому эти данные можно впоследствии идентифицировать, а также установить факт их изменения. Для этого хеш-код добавляется к передаваемым или хранимым данным и при необходимости рассчитывается повторно. Действующим отечественным стандартом хеширования является ГОСТ Р 34.11–2012 [32].

Кодом аутентичности сообщения (имитовставкой) называется контрольная комбинация, зависящая от открытого текста и секретного ключа, и использующаяся для обнаружения всех случайных или преднамеренных изменений в открытом тексте. Отличие от хеш-кода заключается в том, что в выработке имитовставки участвует секретный ключ. Поэтому рассчитать имитовставку может лишь законный пользователь, знающий этот ключ. Основные современные схемы выработки имитовставки строятся на основе симметричных блочных шифров при использовании последних в специальном режиме. Такой режим описан в отечественном стандарте ГОСТ Р 34.13–2015 [33].

Наконец, электронной подписью сообщения называется некоторая битовая строка, зависящая от самого сообщения и секретного ключа, известного только автору подписи. При возникновении спорной ситуации, связанной с отказом подписывающего от факта подписи им некоторого сообщения либо с попыткой подделки подписи, третья сторона (арбитр) должна иметь возможность разрешить спор. Существуют две основные схемы построения электронной цифровой подписи: на основе симметричных криптосистем и на основе криптографии с открытым ключом. На практике обычно используется вторая схема. Отечественный стандарт электронной подписи ГОСТ Р 34.10–2012 построен на математическом аппарате эллиптических кривых [34].

4.2. Основные направления развития и оптимизации методов защиты данных в M2M протоколах. Можно выделить большое количество исследований, посвященных различным вариантам модернизациям TLS и разработке решений, адаптированных для интеграции в ресурсы киберфизических систем с поддержкой MQTT [35-41]. Например, в [38] предлагают подход, основанный на алгоритме Blake2 [42], который позволяет обеспечить целостность и конфиденциальность передаваемых сообщений. Этот подход очень перспективный с точки зрения производительности на устройствах с ограниченными возможностями, особенно подходит для промышленных условий, в которых датчики и контроллеры обмениваются заранее определенными объемами данных. Авторы [37] предлагают безопасную версию MQTT, которая использует новый пакет управления, называемый Spublish, для публикации зашифрованных данных с помощью легковесной криптографии на основе эллиптических кривых [43, 44]. Для внедрения усовершенствованного механизма контроля доступа на устройствах с ограниченным доступом, где применение TLS ограничено, авторы [35] разработали облегченный механизм аутентификации. Аналогичным образом в [39] предлагают архитектуру MQTT, основанную на модифицированной версии OAuth framework [45], в которой два набора учетных данных используются устройствами для доступа к брокеру. С целью внедрения правил политик безопасности в работе [46] предлагается реализация специального коннектора, который перехватывает сообщения от брокера. Это позволяет не только генерировать соответствующие уведомления безопасности, но и способствует выполнению определенных контрмер. В основе коннектора лежит применение технологии прокси-сервера, отслеживающего обмен данными между клиентами и серверами.

Исследование [47] посвящено вопросам аутентификации, целостности, конфиденциальности, неотказуемости и контроля доступа для применения протокола XMPP в рамках передачи данных по сенсорным сетям. Связь на основе XMPP в сенсорных сетях ISO/IEC/IEEE 21451 использует маркер безопасности имени пользователя и пароля, а также интегрированные технологии публикации/подписки (pub/sub) и управления доступом на основе ролей. С использованием предложенного механизма обмен сообщениями ISO/IEC/IEEE 21451 осуществляется на основе модели pub/sub с использованием расширенного протокола доступа к простому объекту безопасности через XMPP.

Интерес вызывает работа [48], где авторы сравнивают библиотеки DTLS, поддерживаемые реализациями CoAP, которые наиболее часто встречаются в промышленных средах IoT. В работе [49] сравнивают сервисы безопасности, предоставляемые IPSec, TLS и DTLS.

Данное исследование показывает, что несмотря на популярность и признание мировым сообществом алгоритмов, заложенных в IPSEC и TLS, их реализации в киберфизических системах зачастую приводят к существенным нагрузкам, что может значительно снизить вычислительные ресурсы устройств. В нескольких работах эти проблемы были решены путем сосредоточения внимания на разработке легких решений для обеспечения безопасности канала связи между клиентами и серверами. В частности, в [50] представлена архитектура FDTLS, которая сочетает в себе безопасность на уровне хранилища и сети/связи для устройств с ограниченными ресурсами при использовании DTLS. Отмечено, что применяемая схема FDTLS решает проблемы избыточных операций за счет использования генерации асимметричных ключей, виртуального однорангового узла и оптимизации хранения на основе сокращения заголовков. Полученные авторами результаты с использованием реализации на основе Contiki на платформах OpenMote показывают, что по сравнению с использованием хранилища и сетевой безопасности отдельно FDTLS может уменьшить задержку ответов при передаче пакетов, а также способствовать экономии энергии. Усовершенствование протокола DTLS с точки зрения модернизации непосредственно криптографических алгоритмов является актуальной научной задачей. В частности, в работе [51] предлагается схема уменьшения числа рукопожатий для DTLS. Как показано в [52, 53], интеграция DTLS поверх CoAP на основе криптографии эллиптических кривых помогает свести к минимуму нагрузку на вычислительные ресурсы при преобразованиях данных. Задачи оптимизации протокола коснулись и вопросов энергоэффективности вычислительных аппаратных устройств [54]. По заявлению авторов, их аппаратная реализация протокола DTLS 1.3 повышает энергоэффективность в 438 раз по сравнению с программным обеспечением, наряду с размером кода и использованием памяти данных всего 8 КБ и 3 КБ соответственно. Криптографические ускорители соединены с процессором RISC-V с низким энергопотреблением на кристалле для тестирования приложений, выходящих за рамки DTLS, с экономией энергии до двух порядков. Тестовый чип, изготовленный на 65-нм CMOS, демонстрирует сеансы DTLS с аппаратным ускорением при потреблении 44,08 мкДж на квитирование и 0,89 нДж на байт зашифрованных данных при 16 МГц и 0,8 В.

4.3. Применение технологии блокчейн для подтверждения достоверности транзакций в киберфизических системах. Относительно новым направлением в кибербезопасности является направление, связанное с созданием механизмов и систем защиты на основе технологии блокчейн.

Блокчейн представляет собой децентрализованную технологию, которая обеспечивает целостность транзакций без участия доверенного центра. Под транзакциями понимаются некоторые действия из заранее определенного перечня, производимые над материальными или нематериальными активами, которыми владеют пользователи системы. Информация о произведенных транзакциях объединяется в блоки, которые, в свою очередь, связываются друг с другом через хеширование. Для распространения одинаковых копий блоков между всеми участниками системы используется некоторый специальный алгоритм, называемый алгоритмом достижения консенсуса и направленный на то, чтобы компрометация цепочек блоков была сложной для потенциального злоумышленника задачей.

Основное преимущество блокчейна, которое делает технологию привлекательной для разнообразных приложений защиты данных, состоит в сложности нарушения целостности сохраненных транзакций. Целенаправленное изменение блока скомпрометирует все другие блоки в цепочке, после чего всю цепочку нужно будет построить заново. Однако вычислительная сложность данной задачи минимизирует вероятность взлома блокчейна [55].

В настоящее время технология блокчейн стала активно применяться в киберфизических системах различного назначения. Как уже было отмечено, главная ценность данной технологии заключается в том, что она позволяет обеспечить подтверждение разного рода транзакций, производимых в недоверенной среде. Многочисленные исследования обосновывают важность технологии блокчейн для четвертой промышленной революции (Industry 4.0), например [56, 57].

Кроме того, в рамках Индустрии 4.0 блокчейн продвигается совместно с иными перспективными технологиями нашего времени [58]. К ним относятся Интернет вещей [59], большие данные [60], туманные вычисления [61], дополненная реальность [56]. В целом блокчейн рассматривается как одна из ключевых технологий индустриального Интернета вещей, способствующая модернизации традиционных фабрик в современные интеллектуальные фабрики, использующие последние достижения в области цифровых технологий.

Отметим некоторые примеры современных исследований, предлагающих конкретные научно-технические решения, связанные с применением технологии блокчейн для решения задач безопасности в киберфизических системах.

Существенная часть известных работ связана с проблемой безопасного управления различными активами, в том числе в киберфизических системах. Это следует из того факта, что первое применение

технологии блокчейн было связано с криптовалютой биткоин. Дальнейшее развитие технологии блокчейна также шло в этом направлении, сформировался рынок криптовалют, который сейчас играет заметную роль в жизни общества.

С течением времени количество приложений технологии блокчейн значительно расширилось. Так недавняя работа [62] анализирует полезность блокчейна в решении проблем безопасности «умного города», который является примером масштабной киберфизической системы. Авторы рассматривают такие составляющие функционирования «умного города», как здравоохранение, транспорт, интеллектуальные сети, управление цепочками поставок, финансовые системы и сети центров обработки данных, обсуждают возможности технологии блокчейн применительно к каждой из перечисленных составляющих и выделяют направления будущих исследований.

В целом исследования, посвященные приложениям технологии блокчейн, можно разделить на несколько обширных групп.

Первая группа исследований связана с управлением цепочками поставок с использованием технологии блокчейн. К данной группе, прежде всего, относятся исследования общего характера, которые не выделяют какую-то конкретную область или конкретный класс киберфизических систем, а предлагают общее решение по безопасному управлению поставками с использованием блокчейна и обсуждают некоторые аспекты данной проблемы. В некоторых случаях предлагаемые решения рассчитаны на применение в киберфизических системах различного назначения, в некоторых – явно не оговариваются такой сферой использования.

Так, в работе [63] представлена классификация барьеров, ограничивающих внедрение технологии блокчейн в управление цепочками поставок. Некоторые вопросы преодоления таких барьеров представлены в [64]. В обоих случаях конкретный актив не уточняется. К этой же группе можно отнести исследования, в которых рассматривается очень широкий перечень услуг и товаров в цепочках поставок. Статья [65] описывает реальные случаи применения блокчейна для отслеживания сырьевых ресурсов, ингредиентов или запасных комплектующих в различных отраслях промышленности. Акцент делается на использовании технологии блокчейн совместно с технологиями Интернета вещей, лежащими в основе многих киберфизических систем.

К первой группе, если не вводить более подробную классификацию, можно отнести исследования, посвященные смежным задачам, возникающим в сфере организации и управления производством. В качестве примера отметим работу [66], в которой представ-

лено архитектурное решение по защите целостности данных в киберфизических производственных системах, используемых в сфере совместного производства.

Вторая группа исследований направлена на решение задачи безопасного управления конкретной разновидностью активов или видом услуг, в том числе управление соответствующими цепочками поставок. В настоящее время перечень подобных приложений стал весьма широк. Блокчейн применяют для контроля за продажами или распределением электроэнергии [67, 68], топлива [69, 70], вычислительных ресурсов [71], программного обеспечения [72].

Все перечисленные исследования объединяет то, что в них присутствует товарно-денежный обмен. Поэтому предлагаемые блокчейн-решения во многом наследуют идеи криптовалют.

К следующей группе можно отнести исследования, посвященные проблеме организации доверенного взаимодействия между множеством некоторых устройств. Конкретные задачи, связанные с обеспечением целостности тех или иных данных, которыми оперируют такие устройства, могут различаться.

Во многих работах идет речь о взаимодействии произвольных устройств Интернета вещей без привязки к конкретным типам киберфизических систем. В качестве некоторых примеров последних работ в данном направлении можно отметить [73-76].

В большинстве таких работ делается акцент на энергоэффективности архитектурных решений, предназначенных для использования в системах Интернета вещей, и предлагаются различные способы достижения этого свойства.

В части решаемых задач рассматриваемые работы можно разделить на те, в которых речь идет только об обеспечении целостности транзакций, и те, в которых помимо этого обеспечивается конфиденциальность данных, содержащихся в транзакциях. Так, в исследовании [77] в качестве объекта защиты рассматриваются данные о местоположении устройств Интернета вещей. Авторы указывают на необходимость обеспечения конфиденциальности этих данных, поэтому в предлагаемой ими схеме блокчейн объединяется с шифрованием.

Переходя от общих решений по применению технологии блокчейн для защиты данных в киберфизических системах, которые построены на основе технологии Интернета вещей, к частным случаям, необходимо отметить такой класс киберфизических систем, как подключенные транспортные средства, в том числе беспилотные [78-80]. В 2019–2020 годах наблюдается «взрывной» рост числа журнальных публикаций, посвященных соответствующим исследованиям, поэто-

му можно сказать, что обеспечение безопасности данного класса киберфизических систем с помощью технологии блокчейн представляет собой пример перспективного направления в рассматриваемой проблемной области.

4.4. Аутентификация данных в киберфизических системах с помощью цифровых водяных знаков. Эксплуатация киберфизических систем, включающих в себя автономные устройства интернета вещей, сопряжена с необходимостью экономии расхода энергии, в том числе при выборе защитных механизмов. В частности, это является одной из основных причин существования так называемой «легковесной криптографии».

Альтернативой криптографии являются методы цифровой стеганографии и цифровых водяных знаков. Указанные методы позволяют скрывать дополнительную информацию различного назначения в цифровых объектах. Обычно целью применения стеганографического сокрытия является обеспечение конфиденциальности данных, а внедрение цифровых водяных знаков в цифровые объекты в большинстве случаев применяется с целью их аутентификации.

Целесообразность использования методов встраивания информации в киберфизических системах, требовательных к энергопотреблению, объясняется следующими особенностями этих методов: низкой вычислительной сложностью в общем случае и направленностью на работу с избыточными данными.

Применение методов встраивания информации в цифровые данные в киберфизических системах является предметом исследований многих ученых, что подчеркивает актуальность данного направления. Соответствующие работы можно разделить на два больших класса:

– встраивание информации в мультимедиа-данные (цифровые изображения, аудио- и видеопоследовательности), вырабатываемые и передаваемые в киберфизических системах;

– встраивание информации в данные иной природы, не относящиеся к мультимедиа (сенсорные данные, информационные и управляющие сигналы в киберфизических системах).

Очевидно, что первый случай применим не ко всем киберфизическим системам, а только к тем, которые оперируют информацией подобного типа. Тем не менее такие системы не являются редкостью и подобные исследования представлены в достаточно большом количестве. Во многом это обусловлено тем фактом, что область сокрытия информации в мультимедиа имеет достаточно богатую историю и дает хорошую базу для новых направлений исследований.

В свою очередь, встраивание информации в произвольные данные в киберфизических системах представляет собой более широкий

случай, однако это направление представлено существенно меньшим количеством исследований.

В [81] приводится обзор методов встраивания информации в цифровые данные в Интернете вещей, актуальный на конец 2018 года. Поэтому в настоящем обзоре сосредоточимся на новых исследованиях, появившихся за последние несколько лет. При этом отметим, что в рамках настоящего обзора будут рассмотрены только методы встраивания цифровых водяных знаков, поскольку методы цифровой стеганографии в общем случае не связаны с задачей обеспечения целостности данных.

Прежде всего, следует выделить достаточно широкий класс исследований, которые посвящены разработке методов и алгоритмов сокрытия информации в цифровых изображениях (и иных цифровых объектах), предназначенных для защиты данных в киберфизических системах, но не обладающих какими-либо специфическими особенностями, которые связаны с заявленной областью применения. К данному классу относятся, например, работы [82-84]. Их авторы утверждают, что предлагаемые ими решения предназначены для защиты данных в Интернете вещей, однако не указывают какие-либо специфичные для данной области сценарии использования своих алгоритмов. Многие работы, которые можно отнести к данной группе, посвящены вопросам безопасности в телемедицинских системах.

Поскольку такие исследования представлены достаточно широко, их следует отметить как отдельный класс. Однако работы указанного класса фактически не выходят за пределы классического встраивания в мультимедиа-данные и далее рассматриваться не будут.

Следующая группа работ также охватывает классическое встраивание данных в мультимедиа-объекты. Отличие заключается в том, что авторы, заявляя применимость своих решений в киберфизических системах, определяют некоторые специфические сценарии передачи данных, характерные для таких систем, и указывают связанные с ними ограничения.

Работы указанной группы представлены не столь широко, но тем не менее их следует отделить от работ, составляющих первую группу.

В [85] также предлагается схема защищенной передачи изображений в телемедицинских системах. Зашифрованные конфиденциальные изображения встраиваются в изображения, содержимое которых не является конфиденциальным. Дополнительно в изображение-контейнер встраивается отпечаток (перцептивный хеш) конфиденциального изображения с целью его последующей аутентификации. Отличительной особенностью данной схемы является отслеживание порядка передачи изображений. Для этого авторы вводят понятие цепоч-

ки отпечатков изображений (image fingerprint) по аналогии с понятием цепочек блоков, лежащих в основе технологии блокчейн.

Исследование [86] носит несколько специфичный характер, поскольку в нем идет речь о встраивании скрытых вложений в изображения, используемые в печатной продукции. Однако в этой работе достаточно ясно определены приложения предлагаемого подхода в системах Интернета вещей и соответствующие сценарии применения, в частности для обеспечения аутентификации данных с целью защиты продукции от подделки, поэтому она соответствует теме настоящего обзора. Здесь также нужно отметить, что авторы работы говорят о стеганографическом встраивании, однако делают акцент на свойстве робастности, что характерно для встраивания цифровых водяных знаков.

Следующая группа работ посвящена встраиванию цифровых водяных знаков в данные, вырабатываемых и передаваемых в киберфизических системах и не относящихся к мультимедиа. В существенной части работ, относящихся к этой группе, речь идет о встраивании цифровых водяных знаков в данные беспроводных сенсорных сетей для обеспечения контроля целостности.

Подобный алгоритм предлагается в том числе и в одной из работ авторов настоящего обзора [87]. Отличительной особенностью данного алгоритма является возможность управлять уровнем искажений, вносимых в результате встраивания. Это делает его применимым к сенсорным данным различной физической природы.

В [88] представлен алгоритм встраивания цифровых водяных знаков в данные беспроводных сенсорных сетей, основное назначение которого заключается в обеспечении защиты от атаки, направленной на клонирование сенсорных узлов. Встраивание основано на преобразовании, схожем с гаммированием над двоичным алфавитом. В качестве преимущества алгоритма заявлена легковесность.

Алгоритмы встраивают элементы цифрового водяного знака в сенсорные данные последовательным и независимым образом, поскольку он не зависит от значений этих сенсорных данных или некоторых их характеристик. Идея формировать цифровой водяной знак в зависимости от самих защищаемых данных является достаточно распространенной как для классических методов и алгоритмов цифровых водяных знаков, так и для рассматриваемой проблемной области защиты данных беспроводных сенсорных сетей и интернета вещей.

В более простом случае элементы цифрового водяного знака вырабатываются только на основании значений элементов сенсорных данных. Примером является схема встраивания, представленная в [89]. В соответствии с данной схемой бит цифрового водяного знака, встра-

иваемый в очередное сенсорное значение, вырабатывается на основе нескольких предыдущих сенсорных значений.

Такой подход обладает определенными преимуществами по сравнению с независимым встраиванием элементов цифрового водяного знака, однако приводит к появлению проблемы синхронизации. Если при получении сообщения порядок элементов данных будет нарушен, это приведет к ошибкам при извлечении цифрового водяного знака даже при отсутствии на канале связи активного злоумышленника. Некоторый способ решения данной проблемы представлен в [90]. Авторы предлагают схему цифровых водяных знаков с двумя цепочками, в соответствии с которой сенсорные данные разделяются на группы переменной длины, зависящей от ключа. Выработка и встраивание цепочек цифровых водяных знаков осуществляется для пар смежных групп. Одна цепочка цифровых водяных знаков служит для аутентификации самих сенсорных данных. Вторая цепочка цифровых водяных знаков кодирует разделители между группами и обеспечивает синхронизацию между отправителем и получателем данных.

В более сложном случае в формировании цифрового водяного знака участвуют не только значения сенсорных величин, но и некоторые их характеристики. Так работа [91] посвящена проблеме аутентификации данных, поступающих от устройств Интернета вещей. Для этого предлагается извлекать стохастические характеристики потоков данных и формировать на их основе цифровые водяные знаки. В качестве метода встраивания цифровых водяных знаков в поток данных используется метод расширения спектра. В работе [92] также идет речь о том, чтобы использовать при формировании цифрового водяного знака различные характеристики захваченных данных: длину данных, частоту появления и время захвата. В [93] цифровой водяной знак формируется на основе информации о коллизиях протокола CSMA/CA и служит для отражения атаки клонирования сенсорных узлов. Кроме того, отличительной особенностью работы является способ представления сенсорных данных. Из них формируется матрица, подобная цифровому изображению. В общем случае такое решение позволяет использовать при работе с сенсорными данными подходы, которые успешно зарекомендовали себя применительно к цифровым изображениям.

Алгоритмы, представленные во всех отмеченных исследованиях, работают с цифровыми водяными знаками, представляющими собой двоичные последовательности. Кроме того, существует класс работ, посвященных встраиванию водяных знаков в аналоговые сигналы (в частности, в модулированные сигналы) для решения задач

аутентификации сигналов или их источника. Решения, которые можно найти в данных работах, идейно схожи с решениями по встраиванию цифровых водяных знаков. Отличие заключается лишь в форме представления сигнала и, как следствие, в способах его обработки.

Исследование [94] посвящено задаче аутентификации отправителя в системах, соответствующих стандарту NB-IoT (Narrow Band Internet of Things). В исследовании используется понятие радиочастотного водяного знака. Изначально водяной знак формируется как цифровой, однако далее встраивание осуществляется не уровне двоичных последовательностей, а на уровне модулированных сигналов. Основным преимуществом предлагаемой схемы называется повышенная надежность за счет устранения взаимной помехи между полезным сигналом и сигналом водяного знака.

В определенных случаях водяные знаки служат для отражения конкретных видов атак. Работа [95] посвящена идентификации кибератак воспроизведения, направленных на сетевые промышленные системы управления (networked control industrial systems). Под этим подразумевается попытка злоумышленника вмешаться в управление системой посредством воспроизведения ранее перехваченных последовательностей данных. Основным вкладом данной работы является не алгоритм встраивания, который взят из предшествующих работ, а стратегия применения данного алгоритма для защиты от злоумышленника.

В работе [96] представлен алгоритм встраивания обратимых водяных знаков в сигналы, передаваемые в промышленных системах управления с «жестким» реальным временем. В качестве приоритетной области применения авторы указывают судовые системы управления. Встраивание является аддитивным и осуществляется под управлением секретного ключа, который предварительно должен быть передан по защищенному каналу связи. Предлагаемый алгоритм позволяет выявлять атаки, направленные на задержку и искажение сигнала.

В завершение отметим, что стали появляться исследования, объединяющие рассмотренную в предыдущей секции технологию блокчейн и технологию цифровых водяных знаков. Блокчейн и цифровые водяные знаки направлены на решение разных задач безопасности в киберфизических системах. Их совместное использование потенциально позволит добиться большего уровня безопасности, чем при использовании данных технологий по отдельности. Эта идея уже нашла отражение в предшествующих исследованиях, однако преимущественно только в одном направлении, связанном с проблемой управления цифровыми правами [97-99]. Совместное применение данных технологий в иных приложениях [100-103] является перспективным

направлением исследований, развитие которого позволит внести вклад в область кибербезопасности.

5. Заключение. Стремительный прогресс в области вычислительных и коммуникационных технологий обуславливает интерес научного сообщества и промышленности к киберфизическим системам [100-103]. Используя сенсорные, вычислительные и сетевые возможности, киберфизические системы способствуют становлению нового поколения научно-технических решений, обеспечивающих автоматические процессы принятия решений в различных областях – от автоматизации мелких бытовых процессов до транспортировки материалов, фабрик будущего и критически важных производств. Интеграция методов информационных технологий с физической системой, такой как электросеть, транспортная система и цепочка поставок, для формирования «умной» инфраструктуры – это залог большей эффективности, надежности и устойчивости.

Представлен обзор основных методов обеспечения целостности данных в протоколах управления киберфизических систем, а также обзор уязвимостей протоколов прикладного уровня, широко используемых в киберфизических системах различной природы. Рассмотрены классические методы обеспечения целостности, новые методы, в частности блокчейн, а также направления развития и оптимизации методов защиты в M2M протоколах. Масштаб представленных сведений об уязвимостях и угрозах безопасности для протоколов киберфизических систем наилучшим образом подчеркивает потребность в новых методах и механизмах обеспечения безопасности, адаптированных для предотвращения таких угроз без препятствий в работе подобных инфраструктур.

Дальнейшие направления исследований будут связаны с повышением эффективности методов обеспечения целостности данных в киберфизических системах. В частности, интерес представляет гибридизация технологий блокчейн и цифровых водяных знаков для построения эффективных методов аутентификации данных и источников данных в мультимедиа-системах.

Литература

1. *Suastegui Jaramillo L.E.* Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack // Journal of Information Systems Engineering & Management. 2018. vol. 3(3). no. 19. pp. 1–6.
2. *Mahbub M.* Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics // Journal of Network and Computer Applications. 2020. vol. 168. no. 102761. pp. 1–26.
3. *Luo J.-Z., Shan C., Cai J., Liu Y.* IoT Application-Layer Protocol Vulnerability Detection using Reverse Engineering // Symmetry. 2018. vol. 10. no. 561. pp. 1–13.
4. *Johnson D., Ketel M.* IoT: Application Protocols and Security // International Journal of Computer Network and Information Security. 2019. vol. no. 11. pp. 1–8.

5. *Nebbione G. Calzarossa M.C.* Security of IoT Application Layer Protocols: Challenges and Findings // Future Internet. 2020. vol. 12. no. 55. pp. 1–20.
6. *Alghamdi T., Lasebae A., Aiash M.* Security Analysis of the Constrained Application Protocol in the Internet of Things // Second International Conference on Future Generation Communication Technologies (FGCT 2013). 2013. pp. 163–168.
7. *Ватаманюк И.В., Яковлев Р.Н.* Обобщенные теоретические модели киберфизических систем // Известия Юго-Западного государственного университета. 2019. № 23(6). С. 161–175.
8. *Korzun D. et al.* Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities // IGI Global. 2019.
9. *Zavyalova Y.V., Korzun D.G., Meigal A.Y., Borodin A.V.* Towards the Development of Smart Spaces-Based Socio-Cyber-Medicine Systems // International Journal of Embedded and Real-Time Communication Systems (IJERTCS). 2017. pp. 45–63
10. *Kayal P. Perros H.* A comparison of IoT application layer protocols through a smart parking implementation // 2017 20th Conference on Innovations in Clouds, Internet and Networks. 2017. pp. 331–336.
11. *Dizdarevic J., Carpio F., Jukan A., Masip X.* A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration // ACM Computing Surveys. 2019. vol. 51. no. 6. pp. 1–29.
12. *Naik N.* Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP // Proceedings of the 2017 IEEE International Systems Engineering Symposium. 2017. pp. 1–7.
13. *Селезнёв С.П., Яковлев В.В.* Архитектура промышленных приложений IoT и протоколы AMQP, MQTT, JMS, REST, COAP, XMPP, DDS // International Journal of Open Information Technologies. 2019. № 5. С. 17–28.
14. *Dinculean D.* Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices // Applied Sciences. 2019. vol. 9. no. 848. pp. 1–10.
15. *Andy S., Rahardjo B., Hanindhito B.* Attack scenarios and security analysis of MQTT communication protocol in IoT system // 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics. 2017. pp. 1–6.
16. *Firdous S.N., Baig Z., Valli C., Ibrahim A.* Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol // Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2017. pp. 748–755.
17. *Jarvinen I., Raitahila I., Cao Z., Kojo M.* Is CoAP Congestion Safe? // ANRW '18: Proceedings of the Applied Networking Research Workshop. 2018. pp. 43–49.
18. *Roselin A.G. et al.* Exploiting the Remote Server Access Support of CoAP Protocol // IEEE Internet of Things Journal. 2019. pp. 9338–9349.
19. *Park C.* Security Architecture for Secure Multicast CoAP Applications // IEEE Internet of Things Journal. 2020. vol. 7. no. 4. pp. 3441–3452.
20. *Wani S.Y.* Internet of Things(IoT) Security and Vulnerability // Research proposal. 2018. pp. 1–9.
21. *White R. et al.* Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems // Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops. 2019. pp. 57–66.
22. *Michaud M., Dean T., Leblanc S.* Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems // Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software. 2018. pp. 68–77.
23. *Malik I. et al.* XMPP architecture and security challenges in an IoT ecosystem // Proceedings of the 16th Australian Information Security Management Conference. 2019. pp. 62–73.

24. *Blahut R.E.* Principles and practice of information theory. Part 1 // Addison-Wesley. 1987. 458 p.
25. *Ivanov F., Kabatiansky G., Krouk E., Rumenko N.* A New Code-Based Cryptosystem // Code-Based Cryptography Workshop. 2020. pp. 41–49.
26. *Bahl L., Cocke J., Jelinek F., Raviv J.* Optimal decoding of linear codes for minimizing symbol error rate (Corresp.) // IEEE Transactions on Information Theory. 1974. vol. 20. no. 2. pp. 284–287.
27. *Ivanov F., Kreshchuk A., Zyablov V.* On the Local Erasure Correction Capacity of Convolutional Codes // 2018 International Symposium on Information Theory and Its Applications. 2018. pp. 296–300.
28. *Zyablov V.V., Ivanov F.I., Potapov V.G.* Comparison of various constructions of binary LDPC codes based on permutation matrices // Journal of Communications Technology and Electronics. 2012. vol. 57. pp. 932–945.
29. *Berrou C. et al.* An overview of turbo codes and their applications // The European Conference on Wireless Technology. 2005. pp. 1–9.
30. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Transactions on Information Theory. vol. 55. no. 7. pp. 3051–3073.
31. *Zhilin I., Ivanov F., Zyablov V.* Generalized Error Locating Codes with Soft Decoding of Inner Codes // Proceedings of European Wireless 2015; 21th European Wireless Conference. 2015. pp. 1–5.
32. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования // М.: Госстандарт России. 2012.
33. ГОСТ Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // М.: Госстандарт России. 2015.
34. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи // М.: Госстандарт России. 2012.
35. *Bali R.S., Jaafar F., Zavarasky P.* Lightweight Authentication for MQTT to Improve the Security of IoT Communication // Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019. pp. 6–12.
36. *Malina L. et al.* A Secure Publish/Subscribe Protocol for Internet of Things // Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10.
37. *Singh M., Rajan M.A., Shivraj V.L., Balamuralidhar P.* Secure MQTT for Internet of Things (IoT) // Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies. 2015. pp. 746–751.
38. *Dinculeana D., Cheng X.* Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices // Applied Sciences. 2019. vol. 9. no. 848. pp. 1–10.
39. *Niruntasukrat A. et al.* Authorization mechanism for MQTT-based Internet of Things // Proceedings of the 2016 IEEE International Conference on Communications Workshops. 2016. pp. 290–295.
40. *Calabretta M., Pecori R., Veltri L.* A Token-based Protocol for Securing MQTT Communications // Proceedings of the 2018 26th International Conference on Software, Telecommunications and Computer Networks. 2018. pp. 1–6.
41. *Bisne L., Parmar M.* Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES // Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies. 2017. pp. 1–5.
42. *Aumasson J.P., Neves S., Wilcox-O'Hearn Z., Winnerlein C.* BLAKE2: Simpler, Smaller, Fast as MD5 // Proceedings of the Applied Cryptography and Network Security. 2013. pp. 119–135.
43. *Kuchta V., Sharma G.* Lattice - Based Cryptography and Internet of Things // IoT Security: Advances in Authentication. 2020. pp. 101–118.

44. *Porambage P., Braeken A., Schmitt C.* Public Key Based Protocols – EC Crypto // IoT Security: Advances in Authentication. 2020. pp. 85–99.
45. *Hardt D.* The OAuth 2.0 Authorization Framework. URL: https://tools.ietf.org/html/rfc6749 (дата обращения: 15.03.2020).
46. *Colombo P., Ferrari E.* Access Control Enforcement Within MQTT-based Internet of Things Ecosystems // Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. 2018. pp. 223–234.
47. *Guo L., Wu J., Xia Z., Li J.* Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks // IEEE Sensors Journal. vol. 15. no. 5. pp. 2577–2586.
48. *Iglesias-Urkia M., Orive A., Urbieta A., Casado-Mansilla D.* Analysis of CoAP implementations for industrial Internet of Things: A survey // Procedia Computer Science. 2017. vol. 109. pp. 188–195.
49. *Hussein A. Elhajj I., Chehab A., Kayssi A.* Securing Diameter: Comparing TLS, DTLS, and IPSec // 2016 IEEE International Multidisciplinary Conference on Engineering Technology. 2016. pp. 1–8.
50. *Boo E., Raza S, Höglund J., Ko J.* Towards Supporting IoT Device Storage and Network Security Using DTLS // MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. 2019. pp. 570–571.
51. *Shah V.* Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT // International Journal for Research in Applied Science and Engineering Technology. 2020. vol. 8. pp. 216–221.
52. *Albalas F., Al-Soud M., Almomani O., Almomani A.* Security-aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography // International Arab Journal of Information Technology. 2018. vol. 15. no. 3A. pp. 550–558.
53. *Capossele A., Cervo V., Cicco G.D., Petrioli C.* Security as a CoAP resource: An optimized DTLS implementation for the IoT // Proceedings of the 2015 IEEE International Conference on Communications. 2015. pp. 549–554.
54. *Banerjee U. et al.* An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications // IEEE Journal of Solid-State Circuits. 2019. vol. 54. no. 8. pp. 2339–2352.
55. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 15.05.2020).
56. *Fernández-Caramés T.M., Fraga-Lamas P.* A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories // IEEE Access. 2019. vol. 7. pp. 45201–45218.
57. *Alladi T., Chamola V., Parizi R.M., Choo K.-K.R.* Blockchain Applications for Industry 4.0 and Industrial IoT: A Review // IEEE Access. 2019. vol. 7. pp. 176935–176951.
58. *Aceto G., Persico V., Pescapé A.* A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges // IEEE Communications Surveys & Tutorials. 2019. vol. 21. no. 4. pp. 3467–3501.
59. *Fernández-Caramés T.M., Fraga-Lamas P.* A Review on the Use of Blockchain for the Internet of Things // IEEE Access. 2018. vol. 6. pp. 32979–33001.
60. *Zhaofeng M. et al.* Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data // IEEE Internet of Things Journal. 2020. vol. 7. no. 5. pp. 4000–4015.
61. *Baniata H., Kertesz A.* A Survey on Blockchain-Fog Integration Approaches // IEEE Access. 2020. vol. 8. pp. 102657–102668.
62. *Bhushan B. et al.* Blockchain for smart cities: A review of architectures, integration trends and future research directions // Sustainable Cities and Society. 2020. vol. 61. pp. 1–27.
63. *Saberi S., Kouhizadeh M., Sarkis J., Shen L.* Blockchain technology and its relationships to sustainable supply chain management // International Journal of Production Research. 2019. vol. 57. no. 7. pp. 2117–2135.

64. *Fu Y., Zhu J.* Big production enterprise supply chain endogenous risk management based on blockchain // IEEE Access. 2019. vol. 7. pp. 15310–15319.
65. *Kshetri N.* 1 Blockchain's roles in meeting key supply chain management objectives // International Journal of Information Management. 2018. vol. 39. pp. 80–89.
66. *Yu C., Jiang X., Yu S., Yang C.* Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation // Robotics and Computer-Integrated Manufacturing. 2020. vol. 64. pp. 1–15.
67. *Li M. et al.* Blockchain-enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things // IEEE Transactions on Industrial Informatics. 2020. vol. 16. no. 10. pp. 6564–6574.
68. *Han D., Zhang C., Ping J., Yan Z.* Smart contract architecture for decentralized energy trading and management based on blockchains // Energy. 2020. vol. 199. pp. 1–14.
69. *Lu H., Huang K., Azimi M., Guo L.* Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks // IEEE Access. 2019. vol. 7. pp. 41426–41444.
70. *Anwar H., Arasu M., Ahmed Q.* Ensuring fuel economy performance of commercial vehicle fleets using blockchain technology // Proceedings of SAE World Congress Experience (WCX 2019). 2019. pp. 1510–1516.
71. *Pan J. et al.* EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts // IEEE Internet of Things Journal. 2018. vol. 6. no. 3. pp. 4719–4732.
72. *Seitz A. et al.* Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study // Proceedings of the 2018 Fifth international conference on internet of things: systems, management and security. 2018. pp. 182–188.
73. *Koshy P., Babu S., Manoj B.S.* Sliding Window Blockchain Architecture for Internet of Things // IEEE Internet of Things Journal. 2020. vol. 7. no. 4. pp. 3338–3348.
74. *Luo J., Chen Q., Yu F.R., Tang L.* Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning // IEEE Internet of Things Journal. 2020. vol. 7. no. 6. pp. 5466–5480.
75. *Ge C., Liu Z., Fang L.* A blockchain based decentralized data security mechanism for the Internet of Things // Journal of Parallel and Distributed Computing. 2020. vol. 141. pp. 1–9.
76. *Chi J. et al.* A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things // Journal of Network and Computer Applications. 2020. vol. 167. pp. 1–10.
77. *Li D., Hu Y., Lan M.* IoT device location information storage system based on blockchain // Future Generation Computer Systems. 2020. vol. 109. pp. 95–102.
78. *Cebe M. et al.* Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles // IEEE Communications Magazine. 2018. vol. 56. no. 10. pp. 50–57.
79. *Rathee G. et al.* A blockchain framework for securing connected and autonomous vehicles // Sensors. 2019. vol. 19. no. 14. pp. 1–15.
80. *Qian Y. et al.* Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles // IEEE Network. 2020. vol. 34. no. 2. pp. 46–51.
81. *Евсютин О.О., Кокурина А.С., Мещеряков Р.В.* Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. 2019. Т. 43. № 1. С. 137–154.
82. *Al-Shayea T.K., Mavromoustakis C.X., Batalla J.M., Mastorakis G.* A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure // Measurement. 2019. vol. 148. pp. 1–14.
83. *Prasetyo H., Hsia C.-H., Liu C.-H.* Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment // IEEE Access. 2020. vol. 8. pp. 69919–69936.

84. *Liu J. et al.* Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things // IEEE Access. 2020. vol. 8. pp. 93939–93961.
85. *Peng H., Yang B., Li L., Yang Y.* Secure and Traceable Image Transmission Scheme Based on Semitensor Product Compressed Sensing in Telemedicine System // IEEE Internet of Things Journal. 2020. vol. 7. no. 3. pp. 2432–2451.
86. *Pu Y.-F., Zhang N., Wang H.* Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things // IEEE Internet of Things Journal. 2019. vol. 6. no. 4. pp. 6368–6383.
87. *Evsutin O. et al.* Algorithm for Embedding Digital Watermarks in Wireless Sensor Networks Data with Control of Embedding Distortions // Proceedings of the 2nd International Conference on Distributed and Computer and Communication Networks (DCCN 2019). 2019. pp. 574–585.
88. *Hoang T.-M., Bui V.-H., Vu N.-L., Hoang D.-H.* A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks // Proceedings of the 34th International Conference on Information Networking (ICOIN 2020). 2020. pp. 649–653.
89. *Xiao X., Gao G.* Digital Watermark-Based Independent Individual Certification Scheme in WSNs // EEE Access. 2019. vol. 7. pp. 145516–145523.
90. *Wang B., Kong W., Li W., Xiong N.N.* A dual-chaining watermark scheme for data integrity protection in internet of things // Computers, Materials and Continua. 2019. vol. 58. no. 3. pp. 679–695.
91. *Ferdowsi A., Saad W.* Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems // IEEE Transactions on Communications. 2018. vol. 67. no. 2. pp. 1371–1387.
92. *Hameed K. et al.* Towards a for-mally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks // Future Generation Computer Systems. 2018. vol. 82. pp. 274–289.
93. *Nguyen V.-T. et al.* A lightweight watermark scheme utilizing MAC layer behaviors for wireless sensor networks // Proceedings of the 3rd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom 2019). 2019. pp. 176–180.
94. *Huang H., Zhang L.* Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems // IEEE Communications Letters. 2019. vol. 23. no. 12. pp. 2262–2265.
95. *Rubio-Hernan J., De Cicco L., Garcia-Alfaro J.* Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems // Transactions on Emerging Telecommunications Technologies. 2018. vol. 29. no. 7. pp. 1–17.
96. *Song Z., Skuric A., Ji K.* A Recursive Watermark Method for Hard Real-Time Industrial Control System Cyber-Resilience Enhancement // IEEE Transactions on Automation Science and Engineering. 2020. vol. 17. no. 2. pp. 1030–1043.
97. *Zhao B. et al.* Y-DWMS: A Digital Watermark Management System Based on Smart Contracts // Sensors. 2019. vol. 19. no. 14. pp. 1–17.
98. *Qian Y. et al.* Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles // IEEE Network. 2020. vol. 34. no. 2. pp. 46–51.
99. *Zhang C. et al.* Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services // IEEE Transactions on Network Science and Engineering. 2020.
100. *Chen J., Gupta V., Quevedo D., Tesi P.* Privacy and security of cyberphysical systems // International Journal of Robust and Nonlinear Control. 2020. vol. 30. pp. 4165–4167.
101. *Lin H., Alemzadeh H., Iyer R.* Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks // Computer. 2020. vol. 53. no. 3. pp. 26–37.

102. *Iskhakov A., Meshcheryakov R.* Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors // 2019 International Siberian Conference on Control and Communications. 2019. pp. 1–5.
103. *Iskhakov A., Iskhakova A., Meshcheryakov R.* Dynamic Container Virtualization as a Method of IoT Infrastructure Security Provision. Cyber-Physical Systems and Control. Lecture Notes in Networks and Systems. 2020. vol. 95. pp. 482–490.

Мещеряков Роман Валерьевич – д-р техн. наук, доцент, заведующий лабораторией, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, системный анализ, робототехника. Число научных публикаций – 500. mrv@ieee.org; ул. Профсоюзная, 65, 117997, Москва, Россия; р.т.: +7(495)334-89-10.

Исхаков Андрей Юнусович – канд. техн. наук, старший научный сотрудник, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, аутентификация, вычислительные сети. Число научных публикаций – 55. iskhakovandrey@gmail.com; ул. Профсоюзная, 65, 117997, Москва, Россия; р.т.: +7(923)421-58-28.

Евсютин Олег Олегович – канд. техн. наук, доцент, заведующий кафедрой, кафедра информационной безопасности киберфизических систем, Московский институт электроники и математики (МИЭМ НИУ ВШЭ); старший научный сотрудник, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, цифровая обработка изображений, цифровая стеганография, цифровые водяные знаки. Число научных публикаций – 70. evsutin.oo@gmail.com; ул. Таллинская, 34, 123458, Москва, Россия; р.т.: +7(495)772-9590*12675.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 19-17-50248).

DOI 10.15622/ia.2020.19.5.7

R. MESHCHERYAKOV, A. ISKHAKOV, O. EVSUTIN

ANALYSIS OF MODERN METHODS TO ENSURE DATA INTEGRITY IN CYBER-PHYSICAL SYSTEM MANAGEMENT PROTOCOLS

Meshcheryakov R., Iskhakov A., Evsutin O. **Analysis of Modern Methods to Ensure Data Integrity in Cyber-Physical System Management Protocols.**

Abstract. At present, the problem of creating methodological security of cyberphysical systems, in particular, the design and implementation of information security subsystems is acute. At the same time, the landscape of threats and vulnerabilities typical for a wide range of hardware and software technologies used in cyberphysical systems is extremely wide and complex. In this context, the security of application layer protocols is of paramount importance, as these protocols are the basis for interaction between applications and services running on different devices, as well as in cloud infrastructures. With the constant interaction of the systems under study with the real physical infrastructure, the challenge is to determine effective measures to ensure the integrity of the transferred control commands, as disruption of the performed critical processes can affect human life and health. The paper provides an analytical review of the main methods of data integrity assurance in management protocol of cyberphysical systems, as well as an overview of application layer protocols vulnerabilities widely used in cyberphysical systems of different types. Classical methods of data integrity assurance, new methods, in particular, blockchain, as well as the main directions of increasing the efficiency of data integrity protocols in cyberphysical systems are considered. Analysis of application layer vulnerabilities is carried out on the example of the most popular MQTT, CoAP, AMQP, DDS, XMPP specifications and their implementations. It is established that despite the presence of basic security mechanisms in all these protocols, researchers continue to regularly identify vulnerabilities in popular implementations, that often endangers critical infrastructure services. In the course of preparing the review of the existing methods of data integrity assurance for the examined class of systems, the key problems of these methods integration and ways of their solution were defined.

Keywords: Cyberphysical System, Internet of Things, Protocol, Blockchain, Watermarking, Authentication

Meshcheryakov Roman – Ph.D., Dr.Sci., Associate Professor, Head of Laboratory, Laboratory of Cyberphysical Systems, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, system analysis, robotics. The number of publications – 500. mrv@ieee.org; 65, Profsoyuznaya str., 117997, Moscow, Russia; office phone: +7(495)334-89-10.

Iskhakov Andrey – Ph.D., Senior Researcher, Laboratory of Cyberphysical Systems, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, authentication, computer networks. The number of publications – 55. iskhakovandrey@gmail.com; 65, Profsoyuznaya str., 117997, Moscow, Russia; office phone: +7 923 421-58-28.

Evsutin Oleg – Ph.D., Associate Professor, Head of Department, Department of Cyber-Physical Systems Information Security, Moscow Institute of Electronics and Mathematics (MIEM HSE); Senior Researcher, Laboratory of Cyberphysical Systems, V.A. Trapeznikov

Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, digital image processing, digital steganography, digital watermarking. The number of publications – 70. evsutin.oo@gmail.com; 34, Tallinskaya str., 123458, Moscow, Russia; office phone: +7(495)772-9590*12675.

Acknowledgements. This research is supported by RFBR (19-17-50248).

References

1. Suastegui Jaramillo L.E. Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack. *Journal of Information Systems Engineering & Management*. 2018. vol. 3(3). no. 19. pp. 1–6.
2. Mahbub M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*. 2020. vol. 168. no. 102761. pp. 1–26.
3. Luo J.-Z., Shan C., Cai J., Liu Y. IoT Application-Layer Protocol Vulnerability Detection using Reverse Engineering. *Symmetry.* 2018. vol. 10. no. 561. pp. 1–13.
4. Johnson D., Ketel M. IoT: Application Protocols and Security. *International Journal of Computer Network and Information Security.* 2019. vol. no. 11. pp. 1–8.
5. Nebbione G. Calzarossa M.C. Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet.* 2020. vol. 12. no. 55. pp. 1–20.
6. Alghamdi T., Lasebae A., Aiash M. Security Analysis of the Constrained Application Protocol in the Internet of Things. Second International Conference on Future Generation Communication Technologies (FGCT 2013). 2013. pp. 163–168.
7. Vatamaniuk I.V., Iakovlev R.N. [Generalized Theoretical Models of Cyberphysical Systems]. *Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta – Proceedings of the Southwest State University*. 2019. vol. 23(6). pp. 161–175. (In Russ.).
8. Korzun D. et al. Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities. IGI Global. 2019.
9. Zavyalova Y.V., Korzun D.G., Meigal A.Y., Borodin A.V. Towards the Development of Smart Spaces-Based Socio-Cyber-Medicine Systems. *International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*. 2017. pp. 45–63
10. Kayal P. Perros H. A comparison of IoT application layer protocols through a smart parking implementation. 2017 20th Conference on Innovations in Clouds, Internet and Networks. 2017. pp. 331–336.
11. Dizdarevic J., Carpio F., Jukan A., Masip X. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *ACM Computing Surveys.* 2019. vol. 51. no. 6. pp. 1–29.
12. Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. Proceedings of the 2017 IEEE International Systems Engineering Symposium. 2017. pp. 1–7.
13. Seleznev S., Yakovlev V. [Industrial Application Architecture IoT and protocols AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS]. *International Journal of Open Information Technologies*. 2019. vol. 7. no. 5. pp. 17–28. (In Russ.).
14. Dinculean D. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences.* 2019. vol. 9. no. 848. pp. 1–10.
15. Andy S., Rahardjo B., Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics. 2017. pp. 1–6.
16. Firdous S.N., Baig Z., Valli C., Ibrahim A. Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol. Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Commu-

nications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2017. pp. 748–755.
17. Jarvinen I., Raitahila I., Cao Z., Kojo M. Is CoAP Congestion Safe?. ANRW '18: Proceedings of the Applied Networking Research Workshop. 2018. pp. 43–49.
18. Roselin A.G. et al. Exploiting the Remote Server Access Support of CoAP Protocol. *IEEE Internet of Things Journal.* 2019. pp. 9338–9349.
19. Park C. Security Architecture for Secure Multicast CoAP Applications. *IEEE Internet of Things Journal.* 2020. vol. 7. no. 4. pp. 3441–3452.
20. Wani S.Y. Internet of Things(IoT) Security and Vulnerability // Research proposal. 2018. pp. 1–9.
21. White R. et al. Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems. Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops. 2019. pp. 57–66.
22. Michaud M., Dean T., Leblanc S. Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems. Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software. 2018. pp. 68–77.
23. Malik I. et al. XMPP architecture and security challenges in an IoT ecosystem. Proceedings of the 16th Australian Information Security Management Conference. 2019. pp. 62–73.
24. Blahut R.E. Principles and practice of information theory. Part 1. Addison-Wesley. 1987. 458 p.
25. Ivanov F., Kabatiansky G., Krouk E., Rumenko N. A New Code-Based Cryptosystem. Code-Based Cryptography Workshop. 2020. pp. 41–49.
26. Bahl L., Cocke J., Jelinek F., Raviv J. Optimal decoding of linear codes for minimizing symbol error rate (Corresp.). *IEEE Transactions on Information Theory.* 1974. vol. 20. no. 2. pp. 284–287.
27. Ivanov F., Kreshchuk A., Zyablov V. On the Local Erasure Correction Capacity of Convolutional Codes. 2018 International Symposium on Information Theory and Its Applications. 2018. pp. 296–300.
28. Zyablov V.V., Ivanov F.I., Potapov V.G. Comparison of various constructions of binary LDPC codes based on permutation matrices. *Journal of Communications Technology and Electronics.* 2012. vol. 57. pp. 932–945.
29. Berrou C. et al. An overview of turbo codes and their applications. The European Conference on Wireless Technology. 2005. pp. 1–9.
30. Arikan E. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory.* vol. 55. no. 7. pp. 3051–3073.
31. Zhilin I., Ivanov F., Zyablov V. Generalized Error Locating Codes with Soft Decoding of Inner Codes. Proceedings of European Wireless 2015; 21th European Wireless Conference. 2015. pp. 1–5.
32. GOST R 34.11–2012. [Information technology. Cryptographic data security. Hash function]. M.: Gosstandart Rossii. 2012. (In Russ.).
33. GOST R 34.13–2015. [Information technology. Cryptographic data security. Block ciphers operation modes]. M.: Gosstandart Rossii. 2015.
34. GOST R 34.10–2012. [Information technology. Cryptographic data security. Signature and verification processes of (electronic) digital signature]. M.: Gosstandart Rossii. 2012.
35. Bali R.S., Jaafar F., Zavarasky P. Lightweight Authentication for MQTT to Improve the Security of IoT Communication. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019. pp. 6–12.
36. Malina L. et al. A Secure Publish/Subscribe Protocol for Internet of Things. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10.

37. Singh M., Rajan M.A., Shivraj V.L., Balamuralidhar P. Secure MQTT for Internet of Things (IoT). Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies. 2015. pp. 746–751.
38. Dinculeana D., Cheng X. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences.* 2019. vol. 9. no. 848. pp. 1–10.
39. Niruntasukrat A. et al. Authorization mechanism for MQTT-based Internet of Things. Proceedings of the 2016 IEEE International Conference on Communications Workshops. 2016. pp. 290–295.
40. Calabretta M., Pecori R., Veltri L. A Token-based Protocol for Securing MQTT Communications. Proceedings of the 2018 26th International Conference on Software, Telecommunications and Computer Networks. 2018. pp. 1–6.
41. Bisne L., Parmar M. Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES. Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies. 2017. pp. 1–5.
42. Aumasson J.P., Neves S., Wilcox-O'Hearn Z., Winnerlein C. BLAKE2: Simpler, Smaller, Fast as MD5. Proceedings of the Applied Cryptography and Network Security. 2013. pp. 119–135.
43. Kuchta V., Sharma G. Lattice ‐ Based Cryptography and Internet of Things. IoT Security: Advances in Authentication. 2020. pp. 101–118.
44. Porambage P., Braeken A., Schmitt C. Public Key Based Protocols – EC Crypto. IoT Security: Advances in Authentication. 2020. pp. 85–99.
45. Hardt D. The OAuth 2.0 Authorization Framework. Available at: https://tools.ietf.org/html/rfc6749 (accessed: 15.03.2020).
46. Colombo P., Ferrari E. Access Control Enforcement Within MQTT-based Internet of Things Ecosystems. Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. 2018. pp. 223–234.
47. Guo L., Wu J., Xia Z., Li J. Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks. *IEEE Sensors Journal.* vol. 15. no. 5. pp. 2577–2586.
48. Iglesias-Urkia M., Orive A., Urbieta A., Casado-Mansilla D. Analysis of CoAP implementations for industrial Internet of Things: A survey. *Procedia Computer Science.* 2017. vol. 109. pp. 188–195.
49. Hussein A. Elhajj I., Chehab A., Kayssi A. Securing Diameter: Comparing TLS, DTLS, and IPSec. 2016 IEEE International Multidisciplinary Conference on Engineering Technology. 2016. pp. 1–8.
50. Boo E., Raza S, Höglund J., Ko J. Towards Supporting IoT Device Storage and Network Security Using DTLS. MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. 2019. pp. 570–571.
51. Shah V. Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT. *International Journal for Research in Applied Science and Engineering Technology.* 2020. vol. 8. pp. 216–221.
52. Albalas F., Al-Soud M., Almomani O., Almomani A. Security-aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography. *International Arab Journal of Information Technology.* 2018. vol. 15. no. 3A. pp. 550–558.
53. Capossele A., Cervo V., Cicco G.D., Petrioli C. Security as a CoAP resource: An optimized DTLS implementation for the IoT. Proceedings of the 2015 IEEE International Conference on Communications. 2015. pp. 549–554.
54. Banerjee U. et al. An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications. *IEEE Journal of Solid-State Circuits.* 2019. vol. 54. no. 8. pp. 2339–2352.
55. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 15.05.2020).

56. Fernández-Caramés T.M., Fraga-Lamas P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access*. 2019. vol. 7. pp. 45201–45218.
57. Alladi T., Chamola V., Parizi R.M., Choo K.-K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access*. 2019. vol. 7. pp. 176935–176951.
58. Aceto G., Persico V., Pescapé A. A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges. *IEEE Communications Surveys & Tutorials*. 2019. vol. 21. no. 4. pp. 3467–3501.
59. Fernández-Caramés T.M., Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*. 2018. vol. 6. pp. 32979–33001.
60. Zhaofeng M. et al. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 5. pp. 4000–4015.
61. Baniata H., Kertesz A. A Survey on Blockchain-Fog Integration Approaches. *IEEE Access*. 2020. vol. 8. pp. 102657–102668.
62. Bhushan B. et al. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*. 2020. vol. 61. pp. 1–27.
63. Saberi S., Kouhizadeh M., Sarkis J., Shen L. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*. 2019. vol. 57. no. 7. pp. 2117–2135.
64. Fu Y., Zhu J. Big production enterprise supply chain endogenous risk management based on blockchain. *IEEE Access*. 2019. vol. 7. pp. 15310–15319.
65. Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*. 2018. vol. 39. pp. 80–89.
66. Yu C., Jiang X., Yu S., Yang C. Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. *Robotics and Computer-Integrated Manufacturing*. 2020. vol. 64. pp. 1–15.
67. Li M. et al. Blockchain-enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*. 2020. vol. 16. no. 10. pp. 6564–6574.
68. Han D., Zhang C., Ping J., Yan Z. Smart contract architecture for decentralized energy trading and management based on blockchains. *Energy*. 2020. vol. 199. pp. 1–14.
69. Lu H., Huang K., Azimi M., Guo L. Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access*. 2019. vol. 7. pp. 41426–41444.
70. Anwar H., Arasu M., Ahmed Q. Ensuring fuel economy performance of commercial vehicle fleets using blockchain technology. Proceedings of SAE World Congress Experience (WCX 2019). 2019. pp. 1510–1516.
71. Pan J. et al. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*. 2018. vol. 6. no. 3. pp. 4719–4732.
72. Seitz, A.; Henze, D.; Miehle, D.; Bruegge, B.; Nickles, J.; Sauer, M. Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study. Proceedings of the 2018 Fifth international conference on internet of things: systems, management and security. 2018. pp. 182–188.
73. Koshy P., Babu S., Manoj B.S. Sliding Window Blockchain Architecture for Internet of Things. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 4. pp. 3338–3348.
74. Luo J., Chen Q., Yu F.R., Tang L. Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 6. pp. 5466-=–5480.
75. Ge C., Liu Z., Fang L. A blockchain based decentralized data security mechanism for the Internet of Things. *Journal of Parallel and Distributed Computing*. 2020. vol. 141. pp. 1–9.

76. Chi J. et al. A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. *Journal of Network and Computer Applications*. 2020. vol. 167. pp. 1–10.
77. Li D., Hu Y., Lan M. IoT device location information storage system based on blockchain. *Future Generation Computer Systems*. 2020. vol. 109. pp. 95–102.
78. Cebe M., Erdin E., Akkaya K., Aksu H., Uluagac S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Communications Magazine*. 2018. vol. 56. no. 10. pp. 50–57.
79. Rathee G. et al. A blockchain framework for securing connected and autonomous vehicles. *Sensors*. 2019. vol. 19. no. 14. pp. 1–15.
80. Qian Y. et al. Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles. *IEEE Network*. 2020. vol. 34. no. 2. pp. 46–51.
81. Evsutin O.O., Kokurina A.S., Meshcheryakov R.V. A review of methods of embedding information in digital objects for security in the internet of things. *Computer optics*. 2019. vol. 43. no. 1. pp. 137–154.
82. Al-Shayea T.K., Mavromoustakis C.X., Batalla J.M., Mastorakis G. A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure. *Measurement*. 2019. vol. 148. pp. 1–14.
83. Prasetyo H., Hsia C.-H., Liu C.-H. Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment. *IEEE Access*. 2020. vol. 8. pp. 69919–69936.
84. Liu J. et al. Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things. *IEEE Access*. 2020. vol. 8. pp. 93939–93961.
85. Peng H., Yang B., Li L., Yang Y. Secure and Traceable Image Transmission Scheme Based on Semitensor Product Compressed Sensing in Telemedicine System. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 3. pp. 2432–2451.
86. Pu Y.-F., Zhang N., Wang H. Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things. *IEEE Internet of Things Journal*. 2019. vol. 6. no. 4. pp. 6368–6383.
87. Evsutin O. et al. Algorithm for Embedding Digital Watermarks in Wireless Sensor Networks Data with Control of Embedding Distortions. Proceedings of the 2nd International Conference on Distributed and Computer and Communication Networks (DCCN 2019). 2019. pp. 574–585.
88. Hoang T.-M., Bui V.-H., Vu N.-L., Hoang D.-H. A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks. Proceedings of the 34th International Conference on Information Networking (ICOIN 2020). 2020. pp. 649–653.
89. Xiao X., Gao G. Digital Watermark-Based Independent Individual Certification Scheme in WSNs. *EEE Access*. 2019. vol. 7. pp. 145516–145523.
90. Wang B., Kong W., Li W., Xiong N.N. A dual-chaining watermark scheme for data in-tegrity protection in internet of things. *Computers, Materials and Continua*. 2019. vol. 58. no. 3. pp. 679–695.
91. Ferdowsi A., Saad W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. *IEEE Transactions on Communications*. 2018. vol. 67. no. 2. pp. 1371–1387.
92. Hameed K. et al. Towards a for-mally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Future Generation Computer Systems*. 2018. vol. 82. pp. 274–289.
93. Nguyen V.-T. et al. A lightweight watermark scheme utilizing MAC layer behaviors for wireless sensor networks. Proceedings of the 3rd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom 2019). 2019. pp. 176–180.
94. Huang H., Zhang L. Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems. *IEEE Communications Letters*. 2019. vol. 23. no. 12. pp. 2262–2265.

95. Rubio-Hernan J., De Cicco L., Garcia-Alfaro J. Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. *Transactions on Emerging Telecommunications Technologies*. 2018. vol. 29. no. 7. pp. 1–17.
96. Song Z., Skuric A., Ji K. A Recursive Watermark Method for Hard Real-Time Industrial Control System Cyber-Resilience Enhancement. *IEEE Transactions on Automation Science and Engineering*. 2020. vol. 17. no. 2. pp. 1030–1043.
97. Zhao B. et al. Y-DWMS: A Digital Watermark Management System Based on Smart Contracts. *Sensors*. 2019. vol. 19. no. 14. pp. 1–17.
98. Qian Y. et al. Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles. *IEEE Network*. 2020. vol. 34. no. 2. pp. 46–51.
99. Zhang C. et al. Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services. *IEEE Transactions on Network Science and Engineering*. 2020.
100. Chen J., Gupta V., Quevedo D., Tesi P. Privacy and security of cyberphysical systems. *International Journal of Robust and Nonlinear Control.* 2020. vol. 30. pp. 4165–4167.
101. Lin H., Alemzadeh H., Iyer R. Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks. *Computer.* 2020. vol. 53. no. 3. pp. 26–37.
102. Iskhakov A., Meshcheryakov R. Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors. 2019 International Siberian Conference on Control and Communications. 2019. pp. 1–5.
103. Iskhakov A., Iskhakova A., Meshcheryakov R. Dynamic Container Virtualization as a Method of IoT Infrastructure Security Provision. Cyber-Physical Systems and Control. Lecture Notes in Networks and Systems. 2020. vol. 95. pp. 482–490.

Руководство для авторов

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Информатика и автоматизация» http://ia.spcras.ru/. При регистрации авторам рекомендуется заполнить все предложенные поля данных. Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше или LaTex. Объем основного текста (до раздела Литература) - от 20 до 30 страниц включительно. Переносы разрешены. Номера страниц не проставляются. Основная часть текста статьи разбивается на разделы, среди которых являются обязательными: введение, хотя бы один «содержательный» раздел и заключение. Допускается также мотивированное содержанием и структурой материал а выделение подразделов. В основную часть опускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

Author guidelines

Interaction between each potential author and the Editorial board is realized through the pesoal account on the website of the journal "Informatics and Automation" http://ia.spcras.ru/. At the registration the authors are requested to fill out all data fields in the proposed form. The submissions should be prepared using MS Word 2007, LaTex. The text of the paper in the main part should not exceed 30 pages. Pages are not numbered; hyphenations are allowed. Certain figures, tables, listings and formulas are allowed in the main section, and their typography is considered in more detail at the journal web.

Signed to print 25.09.2020
Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in the Federal Service for Supervision of Communications, Information Technology and Mass Media,
certificate ПИ № ФС77-79228 dated September 25, 2020
Subscription Index П5513, Russian Post Catalog

Подписано к печати 25.09.2020. Формат 60×90 1/16. Усл. печ. л. 12,49. Заказ № 391.
Тираж 300 экз., цена свободная.
Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ПИ № ФС77-79228 от 25 сентября 2020 г.

Подписной индекс П5513 по каталогу «Почта России»

ISSN 2713-3192