ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

УДК 004.056

На правах рукописи

Викснин Илья Игоревич

МОДЕЛИ И МЕТОДЫ ОБНАРУЖЕНИЯ НАРУШЕНИЙ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ГРУППАХ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Специальность 05.13.19 – методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель:
к.ф.-м.н., доцент
Комаров Игорь Иванович

Санкт-Петербург – 2018

Оглавление

Введение

Актуальность работы. Концепция Индустрии 4.0, включающей в себя развитие понятия кибер-физические системы (КФС), усиливает тенденцию автоматизации различных сфер жизни общества. Одной из областей применения КФС является организация дорожного движения, что привело к появлению концепции беспилотных транспортных средств (БТС). Использование БТС для организации дорожного движения является актуальной задачей, решением которой занимаются как крупные промышленные компании, так и различные научно-исследовательские группы.

При этом остается недостаточно изученным аспект информационной безопасности (ИБ) взаимодействия групп БТС. Классический подход к обеспечению ИБ групп БТС позволяет противодействовать явному деструктивному информационному воздействию (ДИВ) - когда нарушения ИБ имеют выраженные признаки. Однако, функционирование группы БТС в условиях агрессивной окружающей среды обуславливает появление не только явного ДИВ, но и скрытого деструктивного информационного воздействия (СДИВ), под которым понимается такое ДИВ, которое не выводит отдельные БТС из штатного режима работы.

Текущий уровень развития научно-методического аппарата (НМА) не позволяет эффективно противодействовать СДИВ. Перспективным направлением является парадигма «мягкой ИБ» мультиагентных систем (МАС), определяющая понятие СДИВ и возможные способы противодействия ему. Одной из составляющей этой парадигмы является подход, основанный на репутационных моделях. Он базируется на функциях ретроспективной оценки качества информации, что позволяет говорить о существовании временн***о***й оценки качества информации в системе, выражаемой с помощью показателя репутации.

Степень разработанности темы. Вопрос обеспечения информационной безопасности целостности информации в группах БТС

рассматривается в работах таких исследователей как Зикратов И.А., Финько О.А., Лебедев И.С., Стахов А.П., Blum J., Paar C., Wolf M., Hubaux J., Capkun S., Luo J., Haas Z., Zhou L., Perrig A., Goel A., Zhang J., Dellarocas C., Reznik L., Srivastava M., Balzano L. и др. Существующие исследования в области обеспечения целостности информации направлены в первую очередь на верхние уровни модели OSI. При таком подходе, вопросы, связанные с обеспечением целостности на нижних уровнях модели OSI, противодействие различным помехам, работа с особенностями физической среды передачи данных, особенности адресации сообщений, не рассматриваются в большинстве исследований. Исследования в области обеспечения целостности информации групп БТС принимают за допущение, что целостность сообщений на нижних уровнях модели OSI обеспечивается путем применения традиционных методов и протоколов. Рассматриваются вопросы, связанные с дальнейшей обработкой сообщений, а в качестве основы группы БТС рассматриваются сети устойчивые к разрывам, что гарантирует не только доставку сообщений, но и отсутствие нарушений синтаксической целостности в них. Одной из основных задач является противодействие нарушениям семантической целостности информации. Существующий НМА в данной области не позволяет гарантировать отсутствие нарушений семантической целостности информации.

Таким образом, в процессе развития концепции БТС и возможностей их использования возникло объективное *противоречие* между *необходимостью* обеспечения безопасного функционирования этих систем и *недостаточным уровнем* развития НМА обеспечения ИБ, а также возможности разрешения этого противоречия за счёт использования репутационных моделей, что и определяет ***актуальность исследования***. То есть, исследования, направленные на решение задачи обеспечения ИБ группы БТС, *актуальны* и имеют *теоретическую* и *практическую* значимость.

Целью работы является повышение уровня безопасности информации в процессе информационного взаимодействия БТС.

Научной задачей исследования является разработка моделей, методов и прототипа программного комплекса обнаружения нарушений целостности информации в группах БТС за счет реализации возможности обнаружения СДИВ, обеспечивающих их безопасное информационное взаимодействие.

Достижение поставленной цели и решение научной задачи предполагает решение следующих **частных задач**:

— разработка модели функционирования и модели защищенного ИВ группы БТС на основе мультиагентного подхода;
— разработка метода организации защищенного ИВ группы БТС на основе вре́менной централизации;
— разработка метода обнаружения нарушений семантической целостности информации в группе БТС на основе репутационных механизмов;
— разработка прототипа программного комплекса обеспечения ИБ на основе разрабатываемых методов для физической модели группы БТС.

В соответствии с целью и задачами диссертационной работы, **объектом исследования** является процесс информационного взаимодействия (ИВ) группы БТС, а **предметом исследования** – модели и методы обеспечения ИБ в процессе ИВ группы БТС.

Научная новизна работы определяется разработкой новых *моделей* и *методов* и заключаются в следующем:

1. Разработанные модель функционирования и модель защищенного ИВ группы БТС *отличаются* от существующих моделей децентрализованным подходом к организации функционирования группы БТС с вре́менной коалицией на основе централизованной стратегии ИВ, а также обнаружением нарушений целостности информации на основе анализа и сопоставления данных БТС в ходе коммуникации. Разработанные модели *позволяют* исключить

постоянное наличие центрального управляющего элемента, а также обнаруживать и противодействовать нарушениям семантической целостности информации в группах аутентичных агентов;

2. Разработанный метод вре́менной централизации локальных коалиций групп БТС *отличается* от известных методов централизованного управления распределенными системами способом выбора локального элемента для диспетчеризации взаимодействия в локальной коалиции, что *обеспечивает* снижение размерности задачи управления в группировке, возможность применения адаптивных алгоритмов взаимодействия в коалиции и снижение риска использования центрального управляющего элемента;
3. Разработанный метод обнаружения нарушений семантической целостности информации на основе репутационных механизмов *отличается* от известных возможностью раздельного управления инерционностью и реактивностью ИВ элементов, что *обеспечивает* повышение вероятности достижения целей системы, *позволяет* обнаруживать нарушения семантической целостности информации.

Теоретическая и практическая значимость работы. Разработанные модели, методы и алгоритмы являются основой для организации защищенной коммуникации между БТС. Предложенный подход к обнаружению СДИВ в процессе ИВ групп БТС позволяет выявлять такое воздействие, что позволяет сохранить работоспособность группы на доступном уровне. Разработанный прототип программного комплекса подтверждает продуктивность предложенного подхода в реальных группах БТС. Результаты диссертационной работы могут быть использованы для дальнейшего развития подходов к обеспечению ИБ групп БТС.

Методология и методы диссертационного исследования составляют: методы теории систем и системного анализа, теории информационной безопасности, анализа данных, теории вероятности, комбинаторики и теории множеств.

Положения, выносимые на защиту:

— предложенные модель функционирования и модель защищенного ИВ группы БТС позволяют осуществлять защищенное ИВ БТС на основе децентрализованного подхода;

— предложенный метод временной централизации группы БТС в процессе защищенного ИВ позволяет повысить значения показателей качества функционирования группы БТС, за счет учета особенностей функционирования группы;

— предложенный метод обнаружения нарушений семантической целостности информации на основе репутационных механизмов позволяет осуществлять автоматическое обнаружение нарушений целостности информации в группах БТС элементами группы.

Обоснованность и достаточная степень достоверности полученных результатов **достигается** применением апробированных теоретических положений и математических методов исследований; системным анализом принятых допущений, ограничений, факторов и условий описания объекта исследования; использованием корректных исходных данных; учетом имеющегося опыта и практики в области ИБ; **подтверждается** непротиворечивостью полученных результатов моделирования и теоретических положений; сходимостью результатов с данными других исследователей; практической проверкой в деятельности научно-производственных организаций и одобрением на научно-технических конференциях.

Реализация результатов работы. Представленные в диссертационной работе исследования использовались в рамках следующих научно-исследовательских работ: проекта ААА-А-16-115043610017-8 – 2015 «Информационная безопасность технологий управления»; проекта ААА-А-16-116072710022-9 – 2016 «Противодействие угрозам информационной безопасности технологий управления»; проекта АААА-А17-117042410163-4 «Разработка экспериментального стенда для проверки алгоритмов движения

автономных транспортных средств». Результаты использовались при проектировании СППР управления беспилотными летательными аппаратами, выполняемого АО «НИИ Специальных проектов» в 2016-2017гг. Полученные результаты используются при подготовке бакалавров по специальности 10.03.01 «Информационная безопасность» по дисциплинам «Теория систем и системный анализ» и «Информационные технологии», а также при подготовке магистров по специальности 10.04.01 «Информационная безопасность» по дисциплинам «Обучение машин» и «Управление рисками информационной безопасности» факультетом Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики в учебном процессе. Полученные результаты также используются экономическим факультетом Санкт-Петербургского государственного университета в учебном процессе при подготовке бакалавров по специальности 38.04.01 «Экономика» по дисциплинам «Блокчейн», «Индустрия 4.0».

Апробация основных результатов проводилась на следующих конференциях и семинарах:

- International Seminar on Information Security and Protection of Information Technology 2015, 2017;
- 18th, 20th, 22th Conference of Open Innovations Association FRUCT and Seminar on Information Security and Protection of Information Technology – 2016, 2017, 2018;
- IX и X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2015)» - 2015, «Информационная безопасность регионов России (ИБРР-2017)» - 2017;
- XLV, XLVI, XLVII Научных и учебно-методических конференция Университета ИТМО – 2016, 2017, 2018;

- VI, VII, VIII Конгрессах молодых учёных (КМУ) - 2016, 2017, 2018;
- Digital Transformations & Global Society 2018; «РусКрипто» – 2018;
- «Интернет и современное общество» - 2018;
- Ural-PDC – 2016.

Публикации. Материалы диссертации опубликованы в 16 печатных работах, из них: 3 статьи в журналах, входящих в список ВАК, 6 статей в изданиях, входящих в базы цитирования Web of Science и Scopus.

Личный вклад. Все результаты, представленные в диссертационной работе, получены лично автором в процессе выполнения научно-исследовательской деятельности.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения и четырех приложений. Основной материал изложен на 158 страницах. Полный объем диссертации составляет 207 страниц с 39 рисунками и 3 таблицами. Список литературы содержит 177 наименований.

Краткое содержание работы. В первой главе рассмотрена организация движения на основе БТС и основные проблемы ИБ БТС, меры противодействия угрозам ИБ, поставлена задача исследования. **Во второй главе** предлагается модель функционирования группы БТС на основе децентрализованного мультиагентного подхода, класс мягких атак на БТС, модель защищенного ИВ группы БТС. **В третьей главе** предлагается метод проверки целостности данных на основе построения оценок доверия и репутации, метод вре́менной централизации, заключающегося в выборе вычислительного элемента, выполняющего роль центрального элемента на некоторой итерации. **В четвертой главе** представлены результаты экспериментов по использованию предложенных модели и методов, а также показана их продуктивности на примере группы БТС.

Глава 1. Постановка задачи обеспечения информационной безопасности группы беспилотных транспортных средств

1.1 Обзор концепции кибер-физических систем

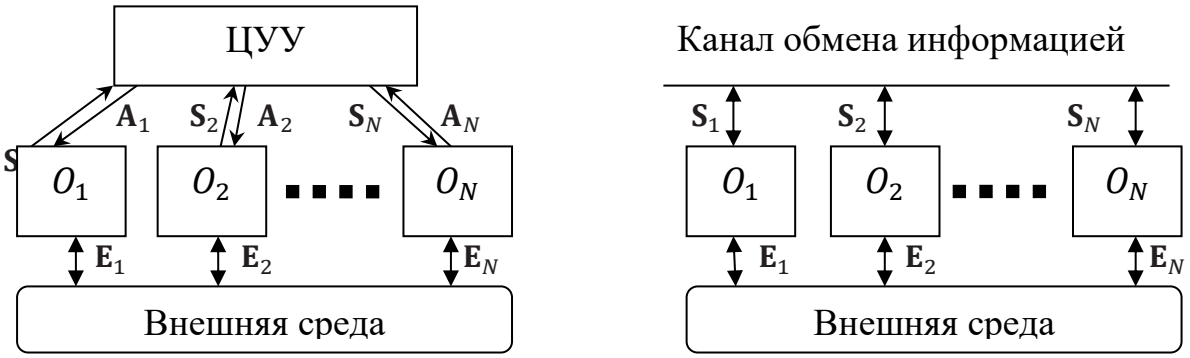
Активное использование термина «кибер-физическая система» началось относительно недавно. В 2006 году правительство Германии запустило программу поддержки развития высокотехнологичных технологий High-Tech Strategy [1], что стало предпосылкой развития новой парадигмы производственного процесса. Данная парадигма получила название Индустрия 4.0. Отличительной особенностью Индустрии 4.0 является отношение между элементами технологического процесс: в отличие от классического подхода, минимизируется участие человека, более того, участие человека в некоторых процессах может представлять опасность, как для успешного выполнения процесса, так и для самого человека.

В [1] утверждается, что «Индустрия 4.0» имеет четыре основания: совместимость, виртуализация, децентрализация и работа в режиме реального времени.

Совместимость подразумевает возможность взаимодействия человека и системы при помощи различных протоколов связи. В таком случае, все участвующие в производственном процессе объекты (станки, датчики, компьютеры, сети и т.д.) объединены в единую систему. Более того, подразумевается активное взаимодействие этой системы с человеком, который не оказывает воздействие на сам производственный процесс, но запускает его.

Для контроля функционирования предприятия в ходе осуществления технологического процесса используются информационные технологии, позволяющие создать *виртуальную* модель производства. В свою очередь, виртуальная модель позволяет контролировать функционирование системы в режиме реального времени. *Децентрализация* подразумевает отсутствие

центрального вычислительного устройства, что позволяет говорить об организации подобного рода систем как систем типа P2P [2-4]. Общий вид организации взаимодействия элементов представлен на рисунке 1.



а) Централизованная модель б) Децентрализованная модель

Рисунок 1. Централизованная и децентрализованная модели управления МРТС

Использование той или иной модели организации информационного взаимодействия обуславливает наличие различных преимуществ и недостатков у системы. Одним из преимуществ децентрализованной системы является отсутствие центрального вычислительного элемента, таким образом, потеря работоспособности одного элемента не влечет за собой потерю работоспособности всей системы [5].

Преимущества использования автоматизированного производства известны с момента создания АСУ ТП. Возможность и основные аспекты автоматизации систем управления (АСУ) ТП были сформулированы А.И. Китовым [6] в 1956 году, но разрабатываемые и применяемые АСУ являются составной частью парадигмы Индустрии 4.0. Реализуемые и используемые понятия, подходы и методы кибернетики при реализации АСУ предлагается масштабировать на весь спектр сфер жизни общества. При этом, базовые принципы Индустрии 4.0 и, как составной части Индустрии 4.0, кибер-физических систем имеют ряд значительных отличий от принципов АСУ ТП.

Одним из ключевых отличий является декларируемая пространственная распределённость систем. Использование распределённых систем позволяет решить проблему возможной параллельности ТП и

отсутствия способности современных вычислительных устройств работать в истинно параллельном режиме при централизованном управлении. И даже бóльшее распространение вычислительных устройств, значительное увеличение их мощностей и снижающиеся задержки между выполнением различных операций не способны в полной мере обеспечить корректное выполнение различных операций в процессе производства [7]. Следовательно, данное ограничение является одним из важнейших факторов замедления автоматизации различных аспектов жизни общества, в целом, и производственного процесса, в частности [8-11]. Однако, использование большего количества устройств, выполняющих роль вычислительных центров, позволяет нивелировать затруднения, возникающие из-за отсутствия возможности выполнения параллельных вычислений.

При использовании большого числа вычислительных устройств, принимающих решения, возникают проблемы, характерные для управления сложными системами [12, 13]. Подходы к реализации подобного рода систем при необходимости выполнения одной общей цели относятся к области теории систем, теории управления и кибернетики [14-18]. Кроме того, управление распределёнными интеллектуальными элементами системы является характерной задачей для раздела теории систем – мультиагентные системы. Применение мультиагентных систем позволяет решать задачи из различных областей жизнедеятельности человека [19-23], что позволяет рассчитывать на успешное применение существующих в рамках данного раздела науки подходов и методов к решению задач, сопутствующих внедрению Индустрии 4.0, а именно – управление кибер-физическими системами.

Кибер-физическая система (КФС) – система, объединяющая физические и информационные элементы [11, 24-27]. Кибер-компоненты системы включают компоненты, отвечающие за выполнение вычислений, реализацию алгоритмов и передачу данных по сети. Физическая составляющая такой системы определяется «аналоговыми» элементами,

другими физическими системами и самой окружающей средой. Разделение элементов по такому принципу позволяет утверждать, что элементы информационного уровня координируют общие принципы функционирования системы, определяют способ выполнения задач, согласно заложенным алгоритмам, контролируют функционирование элементов системы, в то время как элементы физического уровня выполняют действия, исходя из заранее определённого и присущего данным элементам набору действий. При этом набор действий необходимых к выполнению определяется элементами информационного уровня.

К КФС можно отнести любые физические системы, операции в которых контролируются и координируются коммуникационным ядром. Развитие КФС в современном мире обуславливается несколькими тенденциями, а именно:

- повышение доступности недорогих и доступных массовому потребителю сенсорных устройств, осуществляющих сбор информации;
- развитие научно-методического аппарата управления КФС;
- распространение беспроводных сетей, увеличением их пропускной способности и т.д. [28].

Рассматривая Индустрию 4.0 не только с точки зрения ТП, но и с других аспектов жизни общества, возможно говорить о постепенной автоматизации различных сфер деятельности человека, несвязанных напрямую с производством продукции. Предпосылками к этому стало развитие вычислительных устройств, применяемых человеком в повседневной деятельности.

Оценивая происходящее с точки зрения социологии и психологии, можно сделать вывод о том, что сегодня на компьютеры «перекладывается» все больше человеческих мыслительных функций и операций. В [29] прогнозируется, что к 2020 году общее количество устройств, обладающих возможностью коммуникации с другими устройствами, составит 21 млрд.

Таким образом, декларируется стратегия автоматизации не только технологических процессов (ТП), но и некоторых аспектов жизни общества [30]. Рассмотрение возможных сфер применения КФС позволит подтвердить актуальность изучения данной области.

Использование КФС можно разделить на несколько основных категорий, основываясь на области их применения:

- производство;
- услуги;
- здания и объекты инфраструктуры;
- транспорт;
- здравоохранение.

Использование КФС в *производственной сфере* позволяет повышать эффективность производственного процесса, благодаря полной интеграции вычислительных устройств с механизма предприятия [31]. Полная интеграция подразумевает не только управление оборудованием предприятия, но и проведение мониторинга рабочего процесса, управление цепями поставок и т.д. Применение КФС в *сфере здравоохранения* позволяет осуществлять дистанционный мониторинг состояния пациентов. Кроме того, использование подхода, основанного на КФС, позволит изучить функции организма человека [32].

Одной из самых актуальных сфер применения является *сфера энергетики*. КФС позволяют говорить об «умных» сетях, т.е. таких сетях, в которых присутствует информационное взаимодействие [33-35]. В таком случае, элементы сети сами могут контролировать расход энергии, определять надёжности других элементов и т.д. Использование «умных» сетей позволяет повышать экономическую выгоду, надёжность и эффективность сети. Кроме того, возможно изменение ролей элементов сети, когда устройство-потребитель передаёт часть энергии другому устройству при наличии избытков [36].

1.2 Концепция беспилотных транспортных средств

Важную роль КФС отводят в области *транспорта*. Помимо непосредственного использования КФС при разработке транспортных средств, обсуждается возможность их применения как элементов дорожной инфраструктуры. В таком случае, можно повысить эффективность использования дорожной сети – перераспределять потоки машин, минимизировать пробки, что приведёт к продолжительности использования дорожного полотна и уменьшению выбросов [37]. Работа в области создания беспилотных автомобилей ведётся многими крупными корпорациями и исследовательскими группами. Можно выделить ряд основных задач, которые стоят перед разработчиками АТС - выбор корректной траектории движения [38-40], предотвращение столкновения с препятствиями [41] и другими участниками дорожного движения [42], алгоритмы безопасного и быстрого разворота, проезда перекрёстка дорог [43-47], и т.д.

Устройство транспортных средств быстро изменяется. От сенсорных платформ, которые предоставляют информацию водителям и загружают данные в облако человечество перешло к сети автономных транспортных средств, которые обмениваются своими показателями датчиков друг с другом, чтобы оптимизировать работу системы, что позволяет обеспечивать быструю доставку пассажиров в пункт назначения с максимальной безопасностью и комфортом и минимальным воздействием на окружающую среду [48]. Другими словами, в транспортной среде происходит уход от Sensor Web к Internet of Things, теперь операторы играют роль наблюдателей, человеческий контроль удаляется, автономные транспортные средства должны эффективно сотрудничать для поддержания безопасного движения на дорогах. Такое устройство транспортной системы требует способности эффективно общаться друг с другом, а также обнаруживать, где находятся необходимые ресурсы (например, машины скорой помощи, информация об эвакуационных маршрутах и т.д.). Кроме того, обмен сообщениями должен

быть безопасным для предотвращения злонамеренных атак, которые в случае автономных транспортных средств могут быть смертельными, поскольку отсутствует резервный контроль. Для реализации модели транспортное средство использует растущие возможности обработки и хранения информации о других ТС и создает облако, к которому имеют доступ ТС, находящиеся в непосредственной близости к данному.

Другим направлением в разработке автономных транспортных средств является проектирование беспилотных летательных аппаратов. До недавнего времени БПЛА имели преимущественно военное назначение, однако сейчас ставятся новые задачи гражданского назначения, которые успешно могут решаться с помощью БПЛА. В автономных группах БПЛА решения о выполнении задач принимаются исходя из имеющихся данных [49]: появление новой выгодной информации, выход из строя части ресурсов, изменение критериев принятия решений; при этом считается, что группа БПЛА – мультиагентная система. Характерными особенностями интеллектуальных агентов являются: способность к коллективному целенаправленному поведению в интересах решения общей задачи; способность самостоятельно решать локальные задачи; способность активно перемещаться, целенаправленно искать и находить информацию; адаптивность в динамической среде. Автономные БПЛА имеют ряд преимуществ: взаимодействие между собой дает возможность корректировки плана и оптимизации маршрута полета, более эффективное решение задач, выигрыш при выполнении задачи, возможность постановки разных задач для разных участников группы БПЛА.

В статье [50] описывается моделирование поведения водителя в симуляторе вождения. Эта модель служит основой для проектирования автономных транспортных средств на основе моделей поведения человека. Эта структура состоит из четырех разделов: раздел восприятия, раздел эмоций, раздел принятия решений и раздел по применению решений. Раздел восприятия определяет, как модель воспринимает свою среду в локальных и

глобальных условиях. Раздел эмоций определяет, как следует реагировать на окружающую среду. Раздел принятия решений исследует среду для возможных действий, отвечающих запросам раздела эмоций. Конечная цель - найти действие, просмотрев все возможные пути, которые могут потенциально улучшить эмоциональный статус в зависимости от того, что более актуально для модели. Поскольку правила, составляющие раздел принятия решения, являются нечёткими правилами с нечётким выходом, при оценке текущих условий модели и трафика может выполняться более одного набора правил. Это приведёт к более чем одному решению, каждое из которых имеет разный вес, предлагаемый в качестве соответствующих кандидатов. Эти решения оцениваются, и решение с наивысшим весом выбирается и передаётся разделу применения решений для ее осуществления, когда это возможно. Разделение между принятием решения и фактическим его осуществлением связано с тем, что реальные водители обычно не принимают решения по мере их принятия. Раздел применения решений реализует принятое решение в условиях, когда это максимально безопасно, взаимодействует с динамической моделью с помощью трех входных сигналов: газа, тормоза и изменения угла поворота рулевого колеса, и получает два выходных сигнала от динамической модели: скорости и ориентации автомобиля. В дополнение к сигналам, переданным динамической модели, раздел посылает сигналы поворота влево и вправо, которые обновляют состояние транспортного средства и сообщают другим транспортным средствам на дороге о своём намерении менять полосы движения или совершать повороты. Каждый из этих блоков имеет свой собственный набор нечётких переменных и нечётких правил. Настоящая модель ограничена имитацией поведения человека при движении в двухполосной сельской местности.

В настоящее время уже доступна автоматизированная эксплуатация автомагистралей легковых автомобилей внутренними системами без необходимости постоянного активного управления водителем [51]. Такие

автоматизированные системы транспортных средств работают в автономном режиме. Имеющиеся автоматизированные системы помощи водителю ограничены: например, рулевое управление или торможение, или доступны в определённых условиях, например, шоссе с ограниченным доступом или медленное движение. Автономные транспортные средства, которые работают без вмешательства человека-водителя, станут составной частью более общей категории автономных транспортных средств, которая может охватывать широкую сферу применения: автономные транспортные средства могут использоваться для личной мобильности, коммерческой, военной или других целей при условии, что транспортное средство полностью управляется искусственным интеллектом. Автономный автомобиль объединяет в себе пять групп технологий: (1) интерфейс человек-транспортное средство; (2) датчики, которые предоставляют данные об эксплуатации транспортного средства и его частей; (3) датчики, которые предоставляют данные о внешней дорожной среде, источники динамических данных в реальном времени о зоне вокруг транспортного средства; (4) автоматическое управление работой и функциями транспортного средства; и (5) искусственный интеллект, который объединяет эксплуатационные данные в автомобиле с внешними данными о дорогах и использует его для активации автоматизированных средств управления транспортным средством. Автономный автомобиль будет опираться на высокотехнологичную компьютерную обработку, чтобы интегрировать и проанализировать внутренние эксплуатационные данные транспортного средства и данные датчика дорожного полотна, а затем определить, какие автоматизированные средства управления активировать и запускать их. Эта аналитическая функция возникает до включения автоматических средств управления транспортным средством, которые одновременно предоставляют данные обратной связи в систему. На данный момент достаточная вычислительная мощность для управления автономными интеграция, анализ и активация данных транспортных средств, как

представляется, доступны, но возможности для систем слияния и управления данными системы транспортного средства не являются неограниченными.

Интеграция коммуникационных технологий в современные автомобили началась несколько лет назад: популярными примерами являются мобильные телефоны и интернет-доступ на основе сотовых технологий, а также адаптеры Bluetooth для интеграции мобильных устройств. Современная наука позволяет разрабатывать целый ряд различных типов телекоммуникационных сетей, одной из которых стала Vehucular Ad-Hoc Network (Vanet). Она привлекла внимание учёных, которые прилагают усилия в области ее исследования, стандартизации и повышения безопасности ее использования для комфорта водителей и пассажиров. Основными задачами этого типа сетей являются повышение безопасности дорожного движения и эффективности перевозок, а также снижение воздействия транспорта на окружающую среду [52]. Многие работы, посвящённые исследованию VANET, рассматривали трансляцию данных, качество сервиса и безопасность.

Авторы статьи [53] изучили результаты некоторых исследований в данных областях и предоставили краткий обзор возможностей VANET. Потребность в таких сетях возросла из-за необходимости поддерживать большое число беспроводных устройств, которые могут использоваться в транспортных средствах, например, персональные цифровые помощники, ноутбуки, мобильные телефоны. К тому же, они могут использоваться для обеспечения безопасности транспортных средств, навигации, управления дорожным трафиком, оплаты дорожных сборов – и это далеко не все возможности применения VANET.

В интеллектуальных транспортных системах транспортное средство выполняет функции отправителя, получателя и маршрутизатора для передачи информации внутри транспортной сети или внутри одного транспортного средства, используя информацию для обеспечения безопасность и доступность трафика. Для коммуникации внутри транспортной системы ее

элементы должны быть оснащены радиоинтерфейсом и оборудованием для определения местоположения объекта (GPS или DGPS). Связь V2V (vehicle-to-vehicle) позволяет коммуницировать транспортным средствам между собой, передавая сообщения, содержащие данные о скорости автомобиля или предупреждения о смене местоположения. При взаимодействии транспортной системы с помощью связи V2R (vehicle-to-roadside) контроль над движением транспортных средств берет на себя придорожный блок, отправляющий широковещательное сообщение всем транспортным средствам поблизости. Например, придорожный блок будет периодически транслировать сообщение, содержащее ограничение скорости, и будет сравнивать любые географические данные с данными транспортного средства, чтобы определить, соответствует ли скорость транспортных средств ограничениям на данном участке пути.
Авторы [54] анализируют также результаты исследований проблем VANET, связанных с маршрутизацией, качеством обслуживания (QoS), радиовещания, атак и угроз безопасности, столкновения и помех, влияния мощности передачи на эффективность протокола и алгоритмы управления мощностью. Специфические проблемы, связанные с маршрутизацией в VANET - топология сети, демографические данные, различная плотность потока в разное время дня, быстрые изменения в транспортных средствах, прибывающих и покидающих VANET. В сетях VANET широковещательные пакеты передаются в зависимости от географической области, определённой пакетом, транспортные средства периодически транслируют короткие пакеты с их идентификаторами и текущим географическим положением. Таким образом, можно разработать систему совместного предотвращения столкновений, которая может помочь в предотвращении столкновений путём предоставления предупреждающих сообщений. Безопасность VANET имеет решающее значение, поскольку само их существование связано с критическими ситуациями, угрожающими жизни. Крайне важно, чтобы жизненно важная информация не могла быть изменена злоумышленником.

Система должна быть в состоянии определить ответственность водителей, сохраняя при этом их конфиденциальность. Эти проблемы трудно решить из-за размера сети, скорости передачи, их относительной географической позиции и случайности связей между ними.
Сети VANET имеют широкую область применения [55], первая из которых – приложения для создания комфорта пользователя: этот тип приложения улучшает эффективность движения пассажиров и оптимизирует маршрут до пункта назначения. Примерами для этой категории являются система информации о движении, информации о погоде, информации о заправочных станциях или ресторанах и ценах, а также интерактивная связь - доступ в Интернет или загрузка музыки. Вторая область применения — сфера безопасности. Использование VANET обеспечивает безопасность пассажиров путем обмена информацией, она предоставляется либо водителю, либо используется для активации привода активной системы безопасности. Примерами применения этого класса являются системы аварийного оповещения, помощники по смене полосы движения и по координации пересечения, системы предупреждения о дорожных знаках и об изменении скорости дорожного движении. Авторы [52] акцентируют внимание на различных аспектах безопасности сетей VANET. Надёжность системы, в которой информация собирается и распределяется между автономными объектами, вызывает обеспокоенность по поводу достоверности данных. Например, отправитель может искажать наблюдения для получения выгоды, по методу реализации такие атаки подобны bad-mouthing и ballot stuffing. Транспортные средства могут уменьшить эту угрозу, создав сети доверия и игнорируя или, по крайней мере, не доверяя информации от ненадёжных отправителей. Ключевой задачей обеспечения безопасности VANET является предоставление аутентификации отправителя в сценариях широковещательной связи, что обычно достигается за счёт использования подписей открытого ключа. Чтобы гарантировать, что открытый ключ принадлежит аутентифицированному узлу, обычно требуется структура,

называемая инфраструктурой открытого ключа, для экономии пропускной полосы верификаторы могут кэшировать сертификаты и открытые ключи подписывающего лица. Недавно была предложена синхронизированная эффективная потоковая аутентификация (TESLA), в ней отправитель подписывает сообщения с использованием алгоритма симметричной подписи, а затем передаёт это сообщение с сигнатурой. Спустя короткое время отправитель транслирует ключ и инструктирует всех, что этот раскрытый ключ не будет использоваться в будущем. Ресиверы кэшируют исходное сообщение до тех пор, пока ключ не будет принят, а затем проверяется подпись. Поскольку эта проверка использует симметричные криптографические примитивы, она требует примерно в 1000 раз меньше вычислительных ресурсов, чем предыдущий метод. Но вопрос конфиденциальности, по мнению авторов, все еще открыт.

В статье [55] предлагают различные схемы для обеспечения безопасности в VANET. Для обеспечения аутентификации могут использоваться центры сертификации (ЦС). Каждый блок транспортного средства и транспортного средства будет иметь уникальную идентификационную информацию, общедоступные и закрытые ключи и сертификат. Также будут проводиться перекрёстные сертификаты между ЦС. Предлагается использовать асимметричную криптографию для подписи сообщений о безопасности. Псевдонимы, которые могут использоваться для анонимного общения, были предложены как один из способов улучшения конфиденциальности в VANET авторами других статей. Вместо использования пары долгосрочных ключей узел подписывает исходящие сообщения с использованием закрытого ключа псевдонима и добавляет псевдоним в сообщения. Поскольку сообщения, подписанные под тем же псевдонимом, могут быть связаны друг с другом, узел должен периодически менять свой псевдоним. Конфиденциальность для одноадресного трафика может быть достигнута путем обмена симметричным ключом между

транспортными средствами с помощью криптографических алгоритмов с использованием открытого ключа.

Авторы [56] описывают технологию подключенных транспортных средств следующим образом. Связь V2V (vehicle-to-vehicle) используется как основа для обмена данными в режиме реального времени с малой дальностью между транспортными средствами, что обеспечивает значительные преимущества в области безопасности. Коммуникации V2V позволяют транспортному средству обнаруживать угрозы и опасности, определять местоположения других транспортных средств, а также об угрозе или опасности этих транспортных средств, рассчитать риски возникновения опасных ситуаций, выдавать рекомендации или предупреждения и предпринимать действия для предотвращения сбоев. В основе коммуникаций V2V лежит базовое приложение, известное как сообщение данных «Here I Am», оно может быть реализовано с использованием технологий GPS для определения местоположения и скорости транспортного средства или данных с датчиков транспортного средства, которые определяют местоположение и скорость транспортного средства и объединяют их с другими данными, такими как широта, долгота или угол, чтобы обеспечить детальную ситуационную осведомленность о позициях других транспортных средств. Видение V2V состоит в том, что в конечном итоге каждый автомобиль на дороге сможет общаться с другими транспортными средствами. Такая система коммуникации будет поддерживать новое поколение систем безопасности. По данным исследователей, коммуникации V2V позволят использовать активные системы безопасности, которые могут помочь водителям предотвратить 76 процентов аварий на дороге.

Технология подключенного транспорта фокусируется на режимах связи автомобиль-автомобиль, транспортное средство-инфраструктура, транспортное средство-девайсы для обеспечения безопасности, с помощью различных новых коммуникационных технологий, таких как специализированная коммуникация короткого диапазона (DSRC) или

беспроводной доступ для транспортных средств (WAVE) [57]. Данная технология определяет новые проблемы, такие как определение стандартов для взаимодействия, разработка новых схем обеспечения безопасности, идентификация и устранение технологических проблем, кластеризация движущихся транспортных средств для улучшения возможности подключения, стабильности кластеров, эффективности передачи обслуживания и устойчивости к ошибкам. В дальнейшем возможна интеграция облачных вычислений в систему подключенных транспортных средств и последующее ее внедрение в интернет вещей.

В условиях аварийной ситуации, после сбора необходимой информации интеллектуальная система управления транспортным средством информирует водителя о том, что он должен замедлиться и возможно сделать поворот, чтобы избежать каких-либо нежелательных последствий [58]. Интеллект ИТС проявляется в инициативном принятии решения относительно возможных альтернатив, что в противном случае было бы возможно только после того, как водитель мог попасть в чрезвычайную ситуацию. Однако, несмотря на создание ИТС, все еще существует путь для повышения эффективности и безопасности перевозок. Это оправдано следующим: условия трафика могут часто меняться внезапным или повторяющимся образом, поэтому его необходимо оценивать в режиме реального времени, но шаблоны ситуаций, полученные с помощью методов машинного обучения, могут повысить точность и правильность решений. Вторая проблема заключается в том, что устаревшие системы оценки и управления дорожным движением в основном централизованы, связь между управляющими устройствами и транспортными средствами осуществляется через интернет, спутниковые или сотовые системы, а реализация децентрализованной системы слишком сложна. Далее, концепция интернета автомобилей (IoV) описывает связанные между собой транспортные средства и объекты транспортной инфраструктуры на базе IP-адресов, способные обмениваться информацией прямо или косвенно; такая организация системы

подходит для решения проблем создания более эффективного и безопасного транспорта. Чтобы реализовать концепцию IoV, необходим анализ ряда аспектов системы: управление трафиком, управление безопасностью и аварийными ситуациями, энергоэффективность, оптимизация работы интернета транспортных средств и многие другие. Создание систем транспортных средств, подключенных к Интернету, которые управляются и координируются определенной транспортной инфраструктурой, автономными системами, приводит к улучшению транспортных услуг, а также более низким затратам.

В одном из разделов [59] схематично показана типичная архитектура существующих подключенных автомобилей, реализующая защиту от угроз транспортных средств. Транспортное средство имеет несколько электронных подсистем, таких как управление трансмиссией, управление комфортом, информационно-развлекательная система внутри транспортного средства, блок управления безопасностью транспортных средств и др. Каждая подсистема имеет набор модулей для управления ТС, антиблокировочной тормозной системой и расширенной системой помощи водителю. Многие модули имеют строго ограниченные ресурсы ЦП и памяти из-за жестких ограничений затрат. Различные электронные подсистемы традиционно используют физически разделенную сеть, специальные высокоскоростные шины используются для критически важных систем управления двигателем, силовой передачи и безопасности, а локальная сеть используется для менее чувствительных к времени подсистем управления. Отдельные сети и протоколы используются в подсистеме IVI для поддержки аудио и видео приложений и встроенных видеокамер. Различные сети внутри транспортного средства взаимосвязаны со шлюзами, которые контролируют, какие сообщения могут переходить из одной сети в другую. Сами шлюзы обычно соединяются с высокоскоростными CAN-шинами, которые в ближайшем будущем могут быть объединены с Ethernet. Сегодня каждая электронная подсистема обычно реализует свои собственные выделенные

коммуникационные модули для подключения к внешнему миру. Например, для поддержки мультимедийных и безопасных приложений, таких как громкая связь, экстренные вызовы и разрешить приложениям смартфона использовать звуковые и дисплейные системы автомобиля, а радиоприемники считаются включенными в оперативные системы, чтобы обеспечить безопасность транспортных средств. Каждый физически отдельный, взаимодействующий с окружающей средой, должен быть защищен отдельно, что приводит к дублированию функций безопасности на одном и том же транспортном средстве.

Подключенные транспортные средства являются хорошо проработанными и согласованными, они могут реализовывать функции обеспечения безопасности дорожного движения (например, обнаружение столкновения, предупреждение об изменении полосы движения и совместное слияние), интеллектуальную транспортировку (например, управление трафиком сигнала, интеллектуальное планирование трафика и диспетчерское управление), местоположение (например, оптимизация маршрута) и доступ к Интернету в автомобиле [60]. Рынок подключенных автомобилей находится на подъеме. Есть несколько аргументов в пользу обеспечения беспроводной связи с транспортными средствами. Первая из них - необходимость повышения эффективности и безопасности систем автомобильного транспорта. Растущие темпы урбанизации приводят к увеличению транспортных средств, которые отвечают требованиям безопасности и последствиям с точки зрения огромных экономических издержек и экологических проблем. Подключенные ТС относятся к автомобилям с поддержкой беспроводной связи, которые могут взаимодействовать со своей внутренней и внешней средой, то есть поддерживать взаимодействие между оборудованием (V2S), транспортным средством (V2V), инфраструктурой транспортного средства (V2R) и сетью Интернет (V2I). Эти взаимодействия образуют несколько уровней передачи данных в информационные системы для транспортных средств. Кроме того, связанные транспортные средства

рассматриваются как Интернет ТС, который обеспечивает сбор, совместное использование, обработку, вычисление и безопасную передачу информации и позволяет эволюционировать интеллектуальным транспортным системам следующего поколения. Разработка и развёртывание подключенных транспортных средств требует сочетание различных технологий.

Авторы [61] предлагают алгоритмы регулирования пассажиропотока в системах подключенных транспортных средств и оценивают их эффективность. Для обеспечения безопасности эксплуатации ТС необходимо контролировать поток на перекрестках, где взаимодействуют несколько автомобильных потоков. Это может быть достигнуто с помощью правил приоритета или светофоров. Недавние улучшения технологий в разработки подключенных транспортных средств (например, использование систем беспроводной связи) может помочь водителям, предоставляя подсказки по вождению или управляя транспортными средствами для повышения эффективности и безопасности движения. Наличие автономных технологий управления может допускать быстрые изменения в приоритете получения направления на перекрестках, что потребует быстрой реакции на новое распределение автомобильного потока, что трудно ожидать от водителей. Следовательно, доступность технологии может обеспечить гибкость в системе, которая в противном случае невозможна. С другой стороны, при наличии в реальном времени информации о местоположении и скорости автомобилей, возможно предлагать лучшие стратегии управления трафиком для оптимизации маршрутов и движения в целом.

Подключенные транспортные средства, общающиеся друг с другом по технологии V2V и с дорожной инфраструктурой по технологии V2I в настоящее время являются предметом обширных исследований, и ожидается, что в ближайшее время смогут улучшить эффективность транспортных систем. Авторы [62] разработали имитационную модель движения для таких транспортных средств и исследовали, может ли такая система эффективно улучшать качество поездок при одновременном снижении риска

столкновений. Каждому транспортному средству назначается фиксированный маршрут, ведущий к случайно выбранной точке назначения. Любые решения, принятые автономными машинами (относительно ускорения или поворота маневра), предшествуют этапам связи (получение необходимых данных, переговоры). В статье представлены фундаментальные концепции и предположения о модели. Возможно применение методов машинного обучения транспортных средств, для разработки лучших стратегий и повышения безопасности и эффективности движения в нетипичных случаях.

Таким образом, можно говорить о значительных перспективах в области применения БТС и КФС. Важным аспектом успешной реализации данных перспектив является обеспечение стабильной работы систем. Рассматривая КФС необходимо оценить защищенность системы с точки зрения информационного взаимодействия. В силу особенностей структуры подобного рода систем, атаки на них могут осуществляться как намеренно (кибер-преступниками), так и по неосторожности (сотрудниками, имеющими доступ к КФС). Следовательно, вред, наносимый системе, может быть как прямым (потеря информации, выведение из строя системы), так и косвенным (рассылка спама). Кроме того, возможно нарушение защищенности информации без участия человека, если реализация системы предполагает ее самостоятельное развитие. Для определения эффективных методов противодействия существующим угрозам требуется оценить существующие проблемы ИБ КФС.

1.3 Специфика обеспечения информационной безопасности кибер-физических систем

КФС основываются на обработке информации и коммуникации информационных и физических компонент. В ходе взаимодействия этих двух компонент, могут возникать уязвимости, влияющие на функционирование

системы [63]. Для уменьшения вероятности реализации угроз, использующих существующие уязвимости, необходимо обеспечение основных свойств безопасности КФС [64]:

- Конфиденциальность – гарантирует защиту системы от утечки информации. Для ее обеспечения необходимо предоставить безопасную передачу данных между элементами.
- Целостность – гарантирует, что данные не были модифицированы во время передачи. Для наибольшей защиты необходимо обеспечивать целостность всего потока сообщений.
- Доступность – гарантирует возможность получения информации элементом при наличии такого права. Ухудшение доступности информации может быть вызвано различными нападениями на систему.

Для обеспечения данных свойств применяются различные процедуры, методы и принципы защиты информации:

- Аутентификация – процедура проверки подлинности [65, 66]. Для ее обеспечения необходимо либо проверять, что сообщение отправлено доверенным источником, либо гарантировать, что в связь между элементами не может вмешаться третье лицо;
- Приватность – элементы, контактирующие с элементом, содержащим приватную информацию, должны быть не менее сильно защищены [67, 68];
- Идентификация – процедура присвоения идентификатора элементу системы [69]. Каждый элемент системы должен быть однозначно идентифицирован;
- Авторизация - процедура проверки прав на осуществление действий [70, 71]. В контексте КФС под действиями понимается отправка и получение информационных сообщений;
- Шифрование – преобразование информации в целях сокрытия информации от неавторизованных лиц [72]. Таким образом, гарантируется,

что даже при получении сообщения неавторизованным субъектом, информация из него не будет получена;

- и другие.

Рассматривая КФС как одну из областей применения мультиагентного подхода, необходимо рассмотреть проблемы информационной безопасности МАС и способы их решения. Проблемы ИБ МАС можно разделить на три группы [73]:

- Скрытые атаки вредоносных программ;
- Атаки агентов-нарушителей;
- Защита функционирования элемента.

Исходя из представленных проблем информационной безопасности, можно сформулировать основные угрозы [74]:

- несанкционированный пассивный перехват сообщений в процессе межагентных коммуникаций;
- нарушение целостности передаваемых по сети данных;
- несанкционированный доступ к данным;
- отказ в обслуживании;
- перехват запросов с последующей их модификацией и воспроизведением;
- отказ от факта получения или отправления данных и т.д.

Существует множество подходов, моделей и методов, позволяющих либо уменьшить ущерб от реализации угроз, либо уменьшить вероятность их реализации.

В работе [75] предлагается модель защищенных состояний агентов. Модель базируется на электронной подписи, шифровании с открытым ключом и изменении состояний агентов. Агенты согласно данной модели могут находиться в нескольких состояниях, изменяемых в зависимости от выполняемой задачи. Примерами состояний являются – состояние чтения данных, состояние модификации данных, состояние ограничения доступа и т.д.

Метод мобильной криптографии [76] позволяет обеспечить защищенность целостности программного кода агентов. Суть метода сводится к получению сведений об окружающей среде на основе вычисления значения некоторой шифрованной функции. В таком случае, агенты разделяются на клиент и сервер, где клиент шифрует функцию и передает программу для выполнения на сервер. Сервер исполняет программу на основе имеющихся у него данных, содержащих информацию об окружающей среде и других элементах системы. В условиях шифрования самой функции, сервер не имеет возможности получить информацию о результате выполнения функции. Результат ее работы может получить только клиент, отправивший функцию.

В работе [77] предлагается метод обеспечения информационной безопасности МАС на основе полицейских участков. При использовании данного метода, полигон функционирования МАС разделяется на области, и в каждой области появляется управляющий узел, который отвечает за безопасность соответствующей области.

В [78] предлагается «товарищеская» модель взаимной безопасности. В рамках данной системы безопасности, агенты путем взаимодействия друг с другом и с окружающей средой отслеживают происходящее в системе и отвечают, таким образом, за обеспечение безопасности друг друга. В рамках данной модели агенты являются равными по своему функционалу друг другу, кроме того, система является гомогенной.

Одним из частных случаев применения «товарищеской» модели взаимной безопасности является применение социальных механизмов. Суть подобного рода механизмов сводится к определению уровня доверия агента-субъекта к агенту-объекту. Различия между определением уровня доверия зависит от области применения МАС.

Поскольку КФС включает в себя, но не ограничивается концепцией АСУ ТП, требуется привести основные проблемы ИБ и подходы к решению

данных проблем, характерных для АСУ ТП. Особый интерес представляет обеспечение ИБ АСУ ТП с точки зрения законодательства.

К основным проблемам ИБ АСУ ТП можно отнести [79]:

- Взаимодействие операторов с системой: эксперты по ИБ должны обеспечивать соблюдение политики и стандартов безопасности для всех устройств, включенных в систему управления процессом. Подход подразумевает блокировку операторов только в крайнем случае и не допускает снижения производительности;
- Разработка нормативного внутреннего документа, в котором должна быть описана политика предприятия по информационной безопасности при разных ситуациях (технические, организационные, процедурные меры по обеспечению ИБ). Необходимо определить, кто будет заниматься восстановлением работоспособности системы в случае сбоя;
- Поддержка безопасности системы должна обеспечиваться на протяжении всего жизненного цикла, это подразумевает как обновление программных средств защиты системы, так и надежность поставщиков аппаратных средств;
- Даже если система не подключена к сети Интернет, многие специалисты пренебрегают косвенными связями системы. Таким образом, один из первых шагов в обеспечении процесса безопасности системы управления должна быть идентификацией всех взаимосвязей и коммуникационных сценарии;
- Необходимо постоянно отслеживать возникновение новых путей нелегального доступа к системе или возможного сбоя ее работы, при условии, что АСУ ТП рассчитана на длительное время работы.

Для предотвращения целенаправленной кибератаки на систему, необходимо предпринять ряд действий:

- Оценить последствия атаки и возможные риски;
- Разработать новые алгоритмы для обнаружения атак;

- Разработать архитектуру, устойчивую к атакам. Главная цель таких архитектур заключается в том, чтобы при обходе злоумышленниками некоторых механизмов безопасности, ущерб системе будет минимизирован.

Инфраструктуры АСУ часто связаны, поэтому незначительные сбои в одной системе, могут негативно отразиться на другой. Таким образом, кибератака на одну АСУ может привести к физическому сбою в другой. Инструменты визуализации системы позволят проанализировать и предотвратить подобный вариант развития событий.

Правильный подход к обеспечению безопасности АСУ подразумевает не только разработку новых архитектур, но и адаптацию, и обновление уже существующих решений устаревших систем. Методы защиты таких систем:

- Создание инкапсулированных зон – критическая система управления технологическим процессом должна находиться в самой защищенной зоне архитектуры. Несколько уровней систем обнаружения вторжений могут защитить систему от внешнего доступа к данным, но внутренняя передача информации должна также контролироваться, блокируя нелегитимные запросы, поступившие из внешней среды;
- Защита протоколов связи – защита целостности сообщений, шифрование, аутентификация и авторизация. Помимо этого, возможно использование виртуальных частных сетей;
- Контроль доступа к системе – только авторизованные пользователи имеют доступ к физической части системы;
- Приложения, не относящиеся напрямую к системе, следует размещать в отдельной сетевой зоне. Благодаря этому снижается риск целенаправленного заражения системы.

В настоящее время больше половины всех атак на АСУ ТП являются внешними, следовательно, защита сети является приоритетной задачей при разработке архитектуры системы [80]. Исходя из описаний основных проблем ИБ МАС и АСУ ТП, можно констатировать, что целостность информации является одним из важнейших аспектов обеспечения ИБ для

подобного рода систем. В общем случае целостность можно разделить на синтаксическую, семантическую и прагматическую составляющие, исходя из аспектов информации [81].

При децентрализованной организации сети каждый из существующих элементов отвечает за определенную часть системы и вносит собственный вклад в ее работу. Одна из основных составляющих такого вклада – передача информации об окружающей среде и о собственном состоянии элемента. Повышение информированности элемента приводит к выработке решения, наиболее приближенного к оптимальному. Следовательно, нарушение целостности может привести к потере работоспособности системы, т.к. информация, содержащая нарушения, не позволяет составить объективную (или приближенную к объективной) оценку текущей ситуации. При нарушении целостности сообщений на семантическом уровне невозможно оценить информацию с точки зрения наличия или отсутствия нарушений целостности в сообщении с точки зрения классических подходов к обеспечению ИБ.

Проблемы, затрагивающие обеспечение целостности информации, циркулирующей в системе, чаще всего порождаются неполадками в каком-либо отдельном элементе. Поражённый элемент способен максимизировать свои преимущества, нарушая работоспособность соседних элементов, либо нанести ущерб сетевой структуре [82].

Выполнение основных требований к обеспечению *синтаксической* целостности данных в КФС возможно с использованием различных методов, характерных для классического подхода к обеспечению ИБ. При этом классический подход к обеспечению ИБ не способен в полной мере гарантировать защищенность системы с точки зрения *семантической* целостности данных.

Для увеличения вероятности обнаружения нарушений целостности информации возможен анализ не только самой информации, но и поведения элемента системы в промежутке времени. Одним из возможных подходов

проверки целостности информации является использование модели репутации. При использовании такого подхода, представляется возможным провести анализ, как информации, так и поведения элемента. Использование подобного подхода является возможным в контексте КФС, исходя из утверждения о равных ролях элементов при функционировании системы.

В таком случае решение о взаимодействии с тем или иным элементом определяется на основе его репутации в системе. При контакте каждый элемент осуществляет операцию сбора информации и производит оценку элемента, с которым происходит взаимодействие. На основе полученных данных принимается решение о необходимости дальнейшего взаимодействия с элементом-соседом: если его репутация была определена как низкая, элемент, например, изолирует канал, по которому осуществляется контакт.

1.4 Специфика обеспечения информационной безопасности группы беспилотных транспортных средств

В области информационной безопасности разработаны зрелые технологии, которые могут защитить КФС и группы БТС [83]. Авторы делят инструменты ИБ на три категории: проактивные механизмы, реактивные механизмы, принципы проектирования и анализа. К проактивным инструментам относится аутентификация. Схемы аутентификации не позволяют людям и устройствам выдавать себя за другой объект в системе. Контроль доступа предотвращает несанкционированный доступ к системе: он предотвращает доступ к сети не прошедших аутентификацию. Подотчетность может обеспечиваться путем аудита действий аутентифицированных объектов. Безопасная связь между двумя объектами обеспечивается с помощью кодов аутентификации сообщений или цифровых подписей (с их помощью можно обнаружить факт подделки сообщения третьим лицом). Время создания сообщений также может быть обозначена временными метки (которые требуют защищенных протоколов

синхронизации времени) или механизмами реагирования. Кроме того, инструменты проверки безопасности программного обеспечения могут тестировать правильность работы системы, тем самым ограничивая количество уязвимостей. Основные результаты в области ИБ КФС включают эффективные алгоритмы для создания надежной инфраструктуры, безопасной связи и защищенных протоколов маршрутизации. В статье описаны наиболее эффективные методы: аутентификация серверов и клиентов, создание безопасных доменов, криптографическое разделение данных и авторизация на основе сертификатов.

В современных работах, связанных с осуществлением ИВ между элементами группы БТС, рассматривается организация ИВ на основе радиоканалов [84-86]. В контексте обеспечения целостности информации в системах управления групп БТС основные исследования на данный момент времени сосредоточены в области решения задач, связанных с сеансовым и прикладным уровнем, а также с уровнем представления модели OSI [87,88]. Таким образом, вопросы, связанные с физическими особенностями передачи данных (работа со средой, физическая и логическая адресации), получают решение схожее с уже существующими в других видах систем [86]. В существующих исследованиях рассматриваются системы, построенные с использованием технологии IEEE 802.11b [89-94] или технологии DSRC [95-99].

В работе [100] предлагается развитие технологии DSRC, в результате которого авторы предлагают базовый подход к организации защищенной коммуникации (с точки зрения нижних уровней модели OSI). В результате работы авторы предлагают подход к организации связи, устойчивый к различным нарушениям информационной безопасности. Однако должным образом не обеспечивается целостность сообщений с точки зрения верхних уровней модели OSI, что показано в работе [101]. В этой же работе авторы предлагают два возможных решения этой проблемы – использование доверительных центров и метода расширения спектра. Иными словами,

решение задачи обеспечения целостности информации в контексте развития задачи обеспечения переносится на изначальную технологию DSRC и не имеет собственного развития в рамках архитектуры CARAVAN.

В работе [102] проводится сравнения существующих подходов, основанных на традиционных системах ИВ, на примере организации коммуникации беспилотных автобусов. В работе рассматриваются основные системы коммуникации, исследуемые в этой области, а именно – LIN, CAN, FlexRay, MOST и Bluetooth. Рассматриваются вопросы, связанные с моделью угроз и нарушителя, устойчивость различных систем к угрозам и дополнительные методы обеспечения ИБ. Одним из ключевых методов обеспечения ИБ с точки зрения обеспечения целостности информации авторы работы называют различные криптографические системы.

Необходимо отметить, что множество работ, связанных с обеспечением ИБ групп БТС, рассматривают вопрос обеспечения целостности информации в контексте использования криптографических методов защиты [103-105]. Таким образом, целесообразно рассмотреть вопрос обеспечения целостности информации на основе криптографических методов.

Одним из основных методов является использование метода имитовставки [106]. Многие авторы рассматривают вопрос применения имитовставки в контексте различных приложений/реализаций беспроводных протоколов [107, 108]. Проведен ряд исследований, направленный на использование различных, направленный на повышение эффективности применения данного метода [109, 110]. Особый интерес представляет работа [110], т.к. ее авторы в дальнейшем использовали наработки для решения задачи обеспечения целостности информации в группах БПЛА [103]. В работе [103] предложен способ противодействия нарушениям целостности информации, в многоканальных системах однонаправленной радиосвязи. В отличие от существующих работ, авторы предлагают системное решение проблем, связанных с ошибками типа «вставка», «выпадение», «стирание», на основе математического аппарата модулярной арифметики. На базе этого

исследования предложена система ИВ БПЛА, позволяющая обеспечить целостность информации.

Существующие исследования в области обеспечения целостности информации направлены в первую очередь на верхние уровни модели OSI. При таком подходе, вопросы, связанные с обеспечением целостности на нижних уровнях модели OSI, противодействие различным помехам, работа с особенностями физической среды передачи данных, особенности адресации сообщений, не рассматриваются в большинстве исследований. Большинство исследований в области обеспечения целостности информации групп БТС принимают за допущение, что целостность сообщений на нижних уровнях модели OSI обеспечивается путем применения традиционных методов и протоколов. Можно говорить о том, что рассматриваются вопросы, связанные с дальнейшей обработкой сообщений, а в качестве основы группы БТС рассматриваются сети устойчивые к разрывам, что гарантирует не только доставку сообщений, но и отсутствие нарушений в них [111-116].

Таким образом, одной из основных задач является противодействие нарушениям семантической целостности информации, которые схожи с ложной информацией [117].

С точки зрения специфики обеспечения ИБ группы БТС можно выделить три основные атаки, относящиеся к нарушениям семантической целостности информации – on-off, bad mouthing, ballot stuffing.

Атака on-off. В данном случае атакующий стремится нарушить общую производительность системы, надеясь, что она не будет обнаружена или атакуемый узел не будет исключен из сети, в таком случае узел не будет помечен как обладающий низким статусом доверия. Противник чередует проявление ненормального поведения (реализация атаки) и нормального поведения, чтобы продлить время обнаружения, необходимое для распознавания его неправильного поведения. Атака on-off чередует on- и off-состояния: в состоянии on может нанести максимальный ущерб системе, но такую атаку проще обнаружить и предотвратить ее и такая атака,

находящаяся в on-состоянии, расходует заряд батареи с постоянной скоростью, ограничивающей время атаки, поэтому цикл атаки on-off состоит из on- и off-состояний. Цикл атаки on-off может быть постоянным или изменяться. On-off атаки, представленные в [118], происходят либо в состоянии on, когда нежелательное действие происходит, либо в состоянии off, когда действие не происходит, и сеть работает в обычном режиме. Предполагается, что такие атаки могут быть смоделированы с помощью DoS и RoQ атак.

Атака bad mouthing связана с обеспечением несправедливых отрицательных оценок для надежных узлов. Вредоносный узел может снизить уровень доверия хорошо организованного узла путем предоставления плохих рекомендаций против него, чтобы уменьшить вероятность того, что этот узел будет выбран для обслуживания. Данная форма атаки реализуется с помощью негативных рекомендаций, вредоносный узел может взаимодействовать с другими вредоносными узлами, чтобы разрушить доверие к хорошему узлу. После того, как противник скомпрометировал узел, он может использовать систему репутации, назначая ложноотрицательную обратную связь в качестве наблюдаемого узла с соседними узлами. Когда неверные прямые наблюдения контроля репутации распространяются на другие узлы, они будут рассматриваться соседними узлами, и уровень репутации узла будет вычислен неверно, если не будет проведена надлежащая проверка корректности оценок. Это приводит к неправильным значениям репутации для атакованного узла. Атака Bad Mouthing видна в сценариях, где рассматриваются косвенные наблюдения, и узлам разрешено делиться своей отрицательной обратной связью с узлами по соседству. Чтобы репутация узлов или агентов была значимой, любая практическая система репутации должна быть устойчивой к такому поведению. Авторы статей [119, 120] предлагают эффективный метод борьбы с данной атакой.

Атака ballot stuffing аналогична bad mouthing, но при реализации такой атаки противник пытается добиться противоположного эффекта, предоставляя несправедливо положительные оценки (ложная похвала) для выбранных узлов. Вредоносный узел может повысить доверие к другому вредоносному узлу, чтобы увеличить вероятность того, что этот вредоносный узел будет выбран как управляющий или ключевой. Высокий уровень доверия выбранных узлов является результатом ложной положительной обратной связи с вредоносными узлами. Эта атака видна в сценариях, где учитываются косвенные наблюдения, а сторонам разрешено делиться своими положительными отзывами с соседними узлами. Скомпрометированные узлы сговариваются друг с другом и присваивают более высокие значения репутации друг другу.

Существует достаточно большое количество методов защиты группы БТС от таких атак [121-143].

Поскольку маршрутизация является наиболее важным аспектом операций в VANET, некоторые доверительные решения строятся поверх протоколов маршрутизации. Одним из подходов к безопасной маршрутизации является протокол CONFIDANT [144], в котором авторы вводят механизмы watchdog и pathrater для маршрутизации в мобильных одноранговых сетях. Watchdog-это служба мониторинга, которая вычисляет репутацию каждого узла на основе его взаимодействия в маршрутизации. Pathrater является механизмом выбора маршрута, который использует репутацию как метрику в выборе маршрута, таким образом, только доверенные и сотрудничающие узлы будут использоваться для маршрутизации. Поскольку CONFIDANT был разработан для классических AD-hoc сетей, он имеет некоторые ограничения в применении к VANETs. Одно время он не масштабируется до очень крупной и динамично развивающейся сети как VANETs, и в нем не рассматриваются частые потери пакетов, вызванные изменениями в топологии как в VANETs.

SAODV другой защищенный протокол маршрутизации для AD hoc сетей [145, 146], он основан на AODV (AD-Hoc On demand Distance Vector). Этот протокол использует инфраструктуру открытых ключей и цифровых подписей для обеспечения целостности сообщения. Как AODV, SAODV страдает от большого избытка пакетов, значительно увеличивающихся из-за мобильности. Избыток также увеличиваются при использовании асимметричной криптографии, которая может привести к DoS-атакам на узлы с низким уровнем ресурсов [147]. Но, в виду того, что сила и хранение не главные задачи в VANETs, SAODV перспективнейшее решение доверия. Road Side Units (RSU) можно использовать как центральная доверенная система для ключевого управления. Тем не менее, это будет ограничено областями, в которых присутствует RSU. Другим недостатком инфраструктуры открытых ключей является то, что идентификация узлов больше не может быть закрытой.

Авторы статьи [124] предлагают использование в VANET две типичные модели доверия для противостояния атакам on-off, bad mouthing и ballot stuffing. Одна из данных моделей является централизованной, вторая - децентрализованной. В централизованной присутствует центр управления, который должен принимать во внимание расчет стоимости доверия всех транспортных средств, а в децентрализованной модели транспортное средство должно наблюдать поведение других транспортных средств и самостоятельно вычислять их показатели доверия. По мнению авторов, правильно спроектированные модели доверия могут выдержать указанные атаки и уменьшить число реализованных атак. Централизованные модели, как правило, включают три части: RMC (Центр управления репутацией), RSU (Road Side Units) и узлы транспортных средств. RMC отвечает за вычисление значений доверия всех транспортных средств в VANET. Каждое транспортное средство на дороге будет следить за поведением своих соседей и сообщает о своих наблюдениях в RMC. RMC обновляет информацию о доверии периодически в соответствии с полученными отчётами. Существует

также риск атаки, которая в данных моделях обозначается как bad mouthing. RMC может применять статистические методы для противодействия такой атаке. Если один автомобиль хочет опубликовать сообщение, он должен добавить свое доверительное значение, которое получено из RMC и зашифровано личным ключом RMC. Поскольку значение доверия зашифровывается, Алиса не имеет возможности изменять значение. Когда другое транспортное средство получило сообщение, оно может проанализировать значение доверия Алисы, используя открытый ключ RMC, а затем может решить, проявить доверие или недоверие к сообщению в соответствии с доверительным значением Алисы. RMC может рассматривать рекомендацию относительно транспортного средства как случайную величину, эти рекомендации должны соответствовать стандартным нормальным распределениям, тогда те рекомендации, которые находятся слишком далеко от центра распределения, будут считаться вредоносными, будут проигнорированы.

В [122] рассматриваются методы отражения атак ballot stuffing на примере систем репутации типа e-bay. Рассматривается бинарная модель репутации со шкалой {-1, 0, 1}, при том происходит взаимная оценка репутации, как покупателем продавца, так и продавцом – покупателя. По расчётам авторов, в предлагаемой ими модели риск реализации атаки ballot stuffing и bad mouthing значительно снижается. Они используем термин «вознаграждение за репутацию» для обозначения дополнительных затрат, которые покупатель готов заплатить за сделку с продавцом с более высокой репутацией, основной результат - представить ограничения на премию за репутацию, чтобы репутация была устойчивой к инфляции. Премия за *репутацию*, устойчивую к инфляции, гарантирует отсутствие стимулов для продавцов подделывать транзакции для повышения их репутации. Подобная модель может быть применима и в других системах, например, в VANET.

Авторы [123] предлагают несколько методов, которые помогут сохранять максимально честные значения репутации в различных системах,

использующих механизмы доверия и репутации, применимые не только к онлайн-сообществам, но и к робототехническим системам. Первый – использование контролируемой анонимности. Основное положение данного метода заключается в том, что режим анонимности онлайн-сообщества может влиять на возможность атак на системы репутации. Bad mouthing основан на способности выбирать несколько конкретных «жертв» и давать им несправедливо низкие оценки репутации. Есть возможность избежать данного неблагоприятного процесса отбора, если сообщество скрывает истинную идентичность покупателей и продавцов друг от друга. В такой схеме «контролируемой анонимности» рынок знает истинную идентичность всех участников рынка, применяя некоторый эффективный процесс аутентификации, прежде чем он разрешит доступ к любому агенту. Рынок публикует оценочную репутацию покупателей и продавцов, но сохраняет личности скрытыми от друг друга (или присваивает им псевдонимы, которые меняются от одной транзакции к другой, чтобы сделать идентификацию очень сложной). Таким образом, истинные значения доверия и репутации формируются на основе действительного функционирования агентов в системе. Ограничением метода является невозможность его применения к отражению атаки ballot stuffing.

Второй метод, предлагаемый авторами – Median Filtering. Предлагается вместо среднего значения выборки при расчёте коэффициента репутации будет использован образец медианы (Sample median). Злонамеренные оценщики стратегически распределяют несправедливые оценки, чтобы максимизировать предвзятость. Насколько известно автору, анализ, представленный в этом разделе, является новым. По мере увеличения размера n образца средняя медиана образца, взятого из нормального распределения, быстро сходится к нормальному распределению со средним значением, равным медиане родительского распределения. В нормальных распределениях медиана равна среднему. Поэтому в ситуациях, когда нет несправедливых оценщиков, использование образцового медианного

результата приводит к непредвзятым справедливым оценкам репутации. Такой подход эффективен как для отражения атак bad mouthing, так и ballot stuffing.

Авторы [124] обозревают возможные методы защиты от различных классов атак, включая ballot stuffing, on-off и bad mouthing. Один из них - Байесовский вывод, который рассматривает доверие как случайную величину, следуя распределению вероятности с обновляемыми параметрами модели при новых наблюдениях. Эта вычислительная модель доверия популярная из-за её простоты, предложена система бета-репутаций на основе байесовского вывода со значением доверия, моделируемым как случайная величина в диапазоне [0, 1] бета-распределения; суммы положительного и отрицательного опыта сопоставляются с параметрами (α, β) в бета-распределении, так что можно вычислить среднее значение доверия для оценки репутации узла. Дисконтирование убеждений применяется для защиты от атак bad mouthing и ballot stuffing.

В статье [125] в качестве одного из методов также предлагается использование контролируемой анонимности. Атака bad mouthing основана на способности выбирать несколько конкретных «жертв» и давать им несправедливо низкие рейтинги. Этого можно избежать, если скрываются идентичности объектов системы друг от друга. В такой схеме «контролируемой анонимности» только управляющий элемент знает личность всех участников системы. Кроме того, он отслеживает все транзакции и рейтинги. Рынок публикует оценочную репутацию покупателей и продавцов, но сохраняет свою личность скрытыми друг от друга (или присваивает им псевдонимы, которые меняются от одной транзакции к другой). Таким образом, покупатели и продавцы принимают свои решения исключительно на основе предлагаемых условий торговли, а также публикуемой репутации. Поскольку они больше не могут идентифицировать своих «жертв», можно избежать отрицательной дискриминации. Кроме того, предлагается использование кластерной фильтрации для снижения эффекта

несправедливо высоких оценок и положительной дискриминации, атак ballot stuffing. Даже когда скрываются личности покупателей и продавцов, покупатели и продавцы, у которых есть стимул сигнализировать о своей идентичности друг другу, всегда могут найти подходящие способы сделать это. Например, продавцы, участвующие в схеме «набивки бюллетеней», могут использовать определённый шаблон в суммах, которые они предлагают (например, суммы, заканчивающиеся на .33), чтобы сигнализировать о своём присутствии их заговорщикам. Кроме того, становится гораздо легче значительно снизить последствия несправедливых положительных оценок. Для этого предлагается следующий алгоритм: для вычисления несмещённой оценки персонализированной репутации сначала используются методы совместной фильтрации, чтобы идентифицировать набор покупателей и их ближайших соседей. После фильтрации рейтинги образуют два кластера: нижний кластер, состоящий из справедливых рейтингов и верхнего кластера, который состоит из несправедливых рейтингов. Чтобы устранить несправедливые рейтинги, применяется алгоритм делительной кластеризации, например, предложенный Макнаутоном и, наконец, вычисляется окончательная оценка репутации.

Авторы [148] представили доверительную версию протокола OLSR (Optimised Link State Routing Protocol). Они показали, как основанные на доверии рассуждения могут позволить каждому узлу оценить поведение других узлов и проверять согласованность информации о маршрутизации. Фактически, каждый узел использует ряд правил для проверки правильности топологии сети путем сопоставления всей полученной информации из сети. Этот протокол не создает дополнительных проблем для сети по сравнению с базовым протоколом OLSR, но применение правил доверия и проверка согласованности всех сообщений потребует больше времени от каждого узла, что может быть проблемой в VANETs. По сравнению с AODV, OLSR генерирует больше проблем, однако протокол OLSR имеет самую низкую

задержку при высокой мобильности, и это может быть объяснено фактом, что OLSR является проактивным протоколом [149, 150].

В целом, все модели доверия могут быть классифицированы на три крупные группы: авторы [151, 152] классифицировали модели доверия в литературе по трем основным категориям: объектно-ориентированные, ориентированные на данных и комбинированные или гибридные модели доверия. Доверие, объектно-ориентированное доверие, также называемое прямым доверием, основано на информации об идентификаторе узла. В то время как модели доверия, ориентированные на данные, больше фокусируются на оценке содержания сообщения, для принятия решения о доверии. Наконец, комбинированные модели доверия основаны на прямых наблюдениях и рекомендациях других узлов сети.

Объектно-ориентированные модели доверия: в этой категории доверие определяется как сочетание нескольких факторов объекта. Например, М. Герлах [153] предложил модель социального доверия, в которой используются расчеты, основанные на принципах доверия и доверительного тегирования, общее значение доверия для определенного узла вычисляется из имеющихся данных о текущей конкретной ситуации (ситуационное доверие) в сочетании с собственным мнением узла (диспозиционное доверие), и системы, в которой находятся два узла (системное доверие). Одним из недостатков является то, что автор не предоставил информацию о том, как различные типы доверия объединяются в архитектуре. Авторы [154] предложили другую расширенную модель доверия, основанную на ролях и репутации узла. По сути, их модель сочетает в себе ролевое доверие, опыт доверия, большинство на основе доверия и приоритета на основе доверия. Доверие на основе ролей извлекается из предопределенных ролей, а доверие на основе опыта вычисляется из прямых взаимодействий. Мнение большинства формируется на основе мнений выбранных консультантов. Приоритетное доверие – это значение, получаемое на основе источника информации о доверии. Один недостаток этой модели заключается в том, что

она использует криптографию с открытым ключом для определения доверия на основе ролей (т. е. роль узла берется из предоставленного сертификата). Для управления ключами и их проверки требуется центр сертификации. В то время как вышеупомянутые две модели имеют некоторые общие аспекты, модель в [155] более справедлива для VANET, поскольку она имеет возможность включать время и местоположение исходного узла и имеет согласованное большинство значений для каждого узла.

Модели доверия, ориентированные на данные: этот тип имеет дело больше с достоверностью данных, полученных от других узлов, а не с самими узлами. Два примера таких моделей можно найти в [156, 157]. Обе модели основаны на том факте, что ассоциации между узлами в VANETs ”недолговечны” и происходят в ”изменчивых” средах. Raya утверждал, что идентичность узла в VANETs не имеет значения по сравнению с полученной информацией, такой как обновления условий движения и предупреждения безопасности [158]. Модель использует Байесовский вывод (метод слияния данных) и теорию Демпстера-Шафера (оценка доказательств, вдохновленная человеческими рассуждениями) для оценки вероятности события, происходящего в определенное время и контексте. Модель использует различные доказательства для вычисления вероятности корректности события в конкретном времени, месте и контексте. Недостатком этого предложения является то, что доверие основано исключительно на событиях, и его необходимо устанавливать каждый раз, когда событие или сообщение получено от сущности, независимо от предыдущего взаимодействия с этой сущностью. Другим недостатком является то, что она требует оценки определенной информации (доказательств), которая может быть подделана или недоступна в случае необходимости.

В [159], автор использовал подход, дающий оценку каждой части данных на основе объяснений, собранных местным агентом. Локальный агент информации находится в каждом узле и содержит знание узла VANET. При получении информации агент оценивает ее по тому, что уже известно.

Агенты имеют датчики, которые применяют основные правила физики и статистические свойства событий. Например (два узла не могут занимать одно место в одно время) и (узлы редко ездят быстрее 100 миль в час). Эта модель также предоставляет методы обнаружения атак, особенно для сложных атак, таких как “Sybil attack”. Это дает модели преимущество перед моделью, предложенной [158]. Недостатком этой модели является предположение о том, что каждый узел обладает глобальными знаниями о сети, что на практике невозможно. Но если предположить, что придорожным подразделениям можно доверять этот тип знаний, то это решение будет очень применимо.

Комбинированные модели доверия: этот тип моделей доверия объединяет надежность узлов и надежность представленных данных. В [159] предложена модель репутации, вдохновленную идеей, что каждый узел добавляет свое собственное мнение о сообщении. Предложенный алгоритм позволяет узлам формировать собственное мнение о сообщении на основе собранных данных предыдущих скачков. Узел может иметь прямое доверие к другим узлам из предыдущих встреч или использовать мнения других для формулировки новых значений доверия. Когда новый узел впервые входит в сеть, он может оценить доверие на основе фактического сообщения, а не источника, который делает обратную связь от других полезной. Доверие является динамическим и использует геолокацию узла отчетов и отметку времени в сообщении. Модель также включает информацию об окружающей среде в сети и контексте, в котором было создано сообщение. Недостатком этого подхода является то, что он уязвим для столкновения между узлами, влияющего на систему репутации. В модели, представленной в [160] доверие вычисляется на основе репутации узла и проверки данных сообщения. Надежность ранее неизвестного узла основана на значении, предоставленном доверенными "якорными узлами", которые имеют хорошо установленные идентификаторы в сети. Эта модель имеет возможность проверить содержимое сообщения путем изучения нескольких факторов, таких как:

расположение источника сообщения и прокси-сервера, предоставляющего его. Для обнаружения вредоносных узлов используется алгоритм проверки сообщений. Одним из недостатков моделей, основанных на репутации, является то, что они полагаются на существование других узлов, которые обладают достаточными знаниями и которым можно доверять. VANETs может использовать RSU в качестве надежных якорных узлов. Но, если они не существуют, то становится труднее вычислить доверие, основанное только на содержании сообщения. Другая модель была предложена в [161] для безопасной VANETs маршрутизации основанной на примере Муравейника. В модели предложен алгоритм кластеризации узлов в VANETs и выбора главного кластера, облегчающий процесс маршрутизации. Когда исходный узел (S) хочет передать сообщение получателю (D) в кластере, то сначала идет связь с главным кластера (CH). Главный кластера вычисляет значение косвенного доверия, полученного из узлов в диапазоне, и добавляет его к прямому доверию или знанию источника. Недостатками этого предложения является то, что предполагается, что узлы должны перемещаться в одном направлении, чтобы сформировать кластер, и процесс выбора главного кластера занимает много времени.

1.5 Постановка задачи исследования

Пусть $E = \{e_1, \dots, e_n\}$ – группа БТС, которые способны осуществлять между собой ИВ. Пусть a – алгоритм, используемый группой БТС для достижения поставленных перед ними целей. Группа БТС переходит из начального состояния E в некоторое желаемое конечное состояние $\tilde{E}$.

Процесс перехода из состояния E в состояние $\tilde{E}$ не возможен без ИВ. Тогда, алгоритм a может быть представлен в следующем виде: $a = f(Env, E, Inf_{cm})$, где Env – окружающая среда, Inf_{cm} – множество информационных сообщений, передаваемых в процессе ИВ между БТС. Введем функцию для описания алгоритма, исполняемого БТС для перехода в

желаемое конечное состояние, при реализации угроз ИБ, связанных с семантической целостностью информации: $\tilde{a} = f(Env, E, \widetilde{Inf_{cm}})$, где $\widetilde{Inf_{cm}}$ – множество информационных сообщений, информация в которых представлена с нарушением семантической целостности.

В общем случае, при формировании планов действий, основанных на информации с нарушенной семантической целостностью, БТС не достигают желаемого конечного состояния $\tilde{E}$. Таким образом, можно говорить о потере работоспособности группы. При таком подходе, задача исследования может быть сформулирована следующим образом:

разработать модель защищённого ИВ БТС, в рамках которой должны быть предложен метод обнаружения нарушений семантической целостности информации.

Требуется разработать управляющее воздействие $Cntrl_{prt} = F_{imp}(M)$ такое, что $\left|\widetilde{Inf_{cm}^{det}}\right| = \left|\widetilde{Inf_{cm}}\right|$, где $\widetilde{Inf_{cm}^{det}}$ – множество обнаруженных информационных сообщений с нарушениями семантической целостности, M – разрабатываемые методы и модель, F_{imp} – имплементация разрабатываемых методов и модели в контексте существующего управляющего воздействия. В таком случае, алгоритм достижения целей БТС может быть представлен в виде функции – $\widetilde{a_{prt}} = f(Env, E, \widetilde{Inf_{cm}}, Cntrl_{prt})$

Допущением задачи является рассмотрение такой группы БТС, для которой выполняются методы обеспечения ИБ на всех уровнях модели OSI, что гарантирует доставку сообщений от источника до адресата, обеспечение целостности информации, а также позволяет пренебречь условиями физической среды и особенностей БТС.

Выводы по главе 1

В главе 1 решены следующие задачи:

1. Выполнен анализ существующих угроз и методов обеспечения информацинной безопасности. На основе проведенного анализа сделан вывод о недостаточночти НМА для обеспечения защищенности семантической целостности информации;
2. Проведен анализ основных атак на семантическую целостность информации в группе БТС. На основе анализа было выделено три основных типа атак, противодействие которым не может быть обеспечено существующими методами обеспечения ИБ в полной мере;
3. Выполнена постановка задачи диссертационного исследования, которая заключается в разработке методов и моделей для организации управляющего воздействия при функционировании группы БТС.

Глава 2. Модель защищённого информационного взаимодействия группы беспилотных транспортных средств

2.1 Обобщённая модель функционирования группы беспилотных транспортных средств

Рассмотрим группу БТС, состоящую из n элементов: $E = \{e_0, \dots, e_n\}$. $\forall e \in E$ характеризуется набором свойств $P = \{p_0, \dots, p_m\}$, при этом $P \neq \emptyset$. Соотношение свойств элементов позволяет говорить об однородности элементов. Пусть $e_i, e_j \in E, i \neq j$, тогда:

1. $P_i = P_j \Leftrightarrow e_i$ и e_j – гомогенны;
2. $P_i \subset P_j \Leftrightarrow e_j$ расширяет и дополняет свойства и функции, характеризующие элемент e_i;
3. $P_i \cap P_j = \emptyset \Leftrightarrow e_i$ и e_j – гетерогенны.

Соотношения свойств 1-3 верны тогда и только тогда, когда среди рассматриваемых свойств отсутствуют свойства пространственных характеристик.

Кроме того, с точки зрения ИВ, можно выделить базовые свойства связи (P_{con}), характерные для всех БТС:

— получение;

— преобразование;

— передача;

— хранение.

Исходя из существующих теоретических разработок [111-116], верно утверждение: $\forall e_i, e_j \in E, i \neq j \Rightarrow P_{con_i} = P_{con_j}$. Следовательно, соотношение 3 не выполняется, если рассматривать среди всех свойств свойства связи БТС. Кроме того, можно говорить о гомогенности БТС с точки зрения ИВ.

Каждое БТС выполняет две базовые функции:

— вычислительные функции;

— исполнительные функции.

Вычислительные функции – функции, позволяющие выработать план действий, необходимых для выполнения задач/перемещения в пространстве. Исполнительные функции – функции, позволяющие выполнить задачу, основываясь на ранее разработанном плане. Таким образом, вычислительное устройство каждого БТС вырабатывает план действий, который исполняется соответствующими физическими устройствами БТС (двигатель, оси и т.д.).

Можно представить БТС следующим образом – $e_i = e_i^{inf} \cup e_i^{phy}$, где e_i^{inf} - вычислительные устройства (ВУ) БТС e_i, e_i^{phy} – физические устройства (ФУ) БТС e_i. Стоит отметить, в зависимости от способа реализации БТС внутренние элементы могут быть представлены как одним устройством, так и множеством. В таком случае, графическое представление группы демонстрируется на рисунке 2.

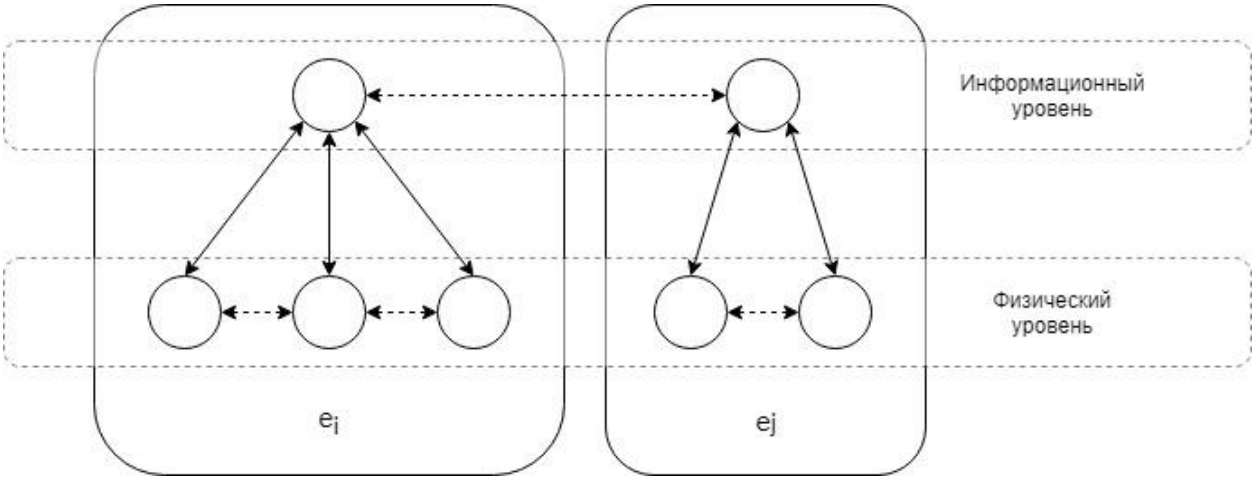


Рисунок 2. Графическое представление группы БТС с разделением каждого ТС на вычислительные и физические устройства. Пунктирные стрелки – ИВ устройств одного уровня, сплошные стрелки – ИВ элементов разных уровней

$\forall e_i, e_j \in E, i \neq j$ осуществляют ИВ $\Rightarrow \exists \, C_{i_j}$ – устойчивый канал связи. Необходимость существования устойчивого канала для осуществления ИВ является обязательным условием функционирования группы БТС

согласно работам [161-165]. При этом устойчивый канал связи должен существовать между ВУ различных БТС, а между ФУ канал передачи сообщений может не существовать. Кроме того, каждый ВУ имеет канал связи как минимум с одним ФУ.

Предположим, $e_i \in E$, тогда $\forall e_j \in E, i \neq j$ и $\exists\, C_{i_j} \Leftrightarrow e_j \in E_{nei_{e_i}}$, где $E_{nei_{e_i}}$ – множество БТС-соседей, имеющих возможность осуществлять непосредственное ИВ с БТС e_i. Тогда $E_{nei_{e_i}} \subseteq E$. Если $E_{nei_{e_i}} = E$, то e_i может осуществлять ИВ с любым БТС. Если группа БТС является полносвязной, то $|E| = \left|\bigcup_{i=0}^{n} E_{nei_{e_i}}\right|$, обратное – неверно. При этом рассматривается только взаимодействие между ВУ различных БТС.

Основываясь на вышеприведенных тезисах, можно представить группу БТС в виде графа *G(E)*, где

$\{e_i\} -$ множество вершин графа $(e_i \in E)$

$\left\{C_{i_j}\right\} -$ множество устойчивых каналов связи между $e_i, e_j \in E$.

Графическое представление графов приведено на рисунке 3.

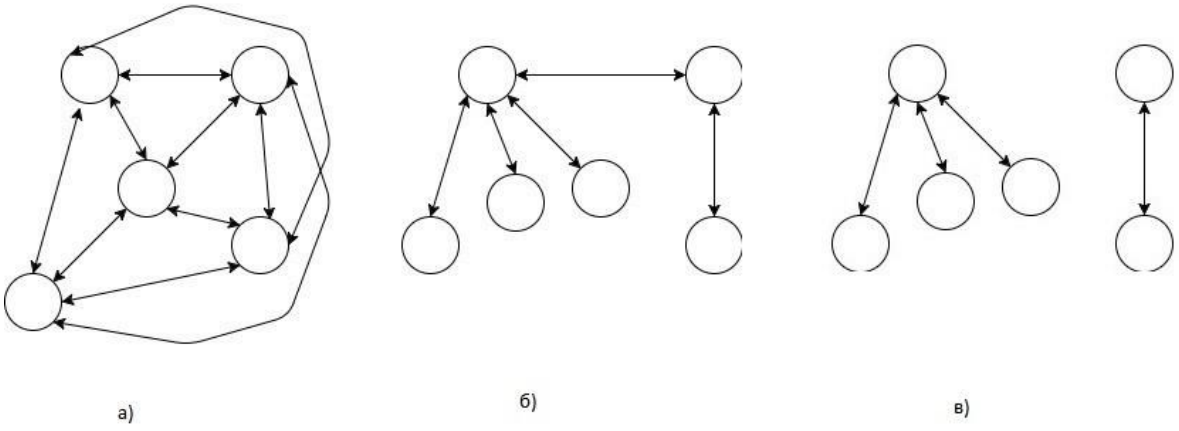


Рисунок 3. Граф на основе группы БТС. Стрелки – устойчивый канал связи между ВУ, круги – БТС. Рисунок а) и б) – графы на основе полносвязных групп БТС, в) – граф на основе групп БТС без полной связи

Таким образом, если группа БТС является полносвязной, то *G(E)* является связным, т.е. $\forall e_i, e_j \in E, i \neq j\ \exists \langle e_i, e_j \rangle$ – путь от вершины e_i до вершины e_j (рис. 1 а) и б)). Однако не каждая группа БТС является

полносвязной (рис. 1 в)), следовательно, между БТС не всегда существует возможность осуществить ИВ. Если не существует пути, связывающего любые два элемента системы, следует говорить о наличии подгрупп в рамках группы БТС, основанных на возможности ИВ.

$E_{sub} \subseteq E -$ подгруппа группы БТС $\Leftrightarrow E_{sub} \neq \emptyset$ и $\forall e_i, e_j \in E_{sub}, i \neq j \ \exists \langle e_i, e_j \rangle$, при этом $\nexists \langle e_i, e_k \rangle \ \forall e_k \in E$ и $e_k \notin E_{sub}$.

Следовательно, $E = \bigcup_{sub=1}^{k} E_{sub}$, где k – количество подгрупп группы БТС. Кроме того, полносвязная группа БТС имеет только одну подсистему, выделяемую по возможности ИВ. Для определения информационных потоков, существующих между БТС, необходимо дать определение понятия плана, применимое в контексте группы БТС.

Определение 1: План действий – набор действий, обязательных для выполнения всеми указанными элементами. Общий план действий группы БТС может быть представлен в виде множества планов для каждого БТС:

$$Pl_{all} = \{Pl_0, \dots, Pl_n\}$$

Под действием понимается некоторая операция, которую может выполнить БТС. БТС может выполнять различные действия:

$$Act_e = \{Act_{e_0}, \dots, Act_{e_l}\}$$

Определение 2: Действие называется элементарным тогда и только тогда, когда БТС не может выполнить меньшую операцию за такт времени. Таким образом, действие можно представить, как множество элементарных действий:

$$AS_{e_i} = \{as_{e_{i_0}}, \dots, as_{e_{i_m}}\}$$

где i – номер действия, представляемого в виде набора элементарных действий.

Основываясь на определениях 1 и 2, можно представить план следующими способами:

1. $Pl_e = \{\dots, Act_{tk_{e_i}}, \dots\}$, где tk – выполняемая задача, e – БТС, предпринимающий действие, i – действие БТС e;

2. $Pl_e = \{\dots, as_{tk_{e_{i_m}}}, \dots\}$, где tk – выполняемая задача, e – БТС, предпринимающий действие, i – действие БТС e, m – элементарное действие, входящее в действие i.

Пусть o_{i_j} – информационное сообщение, содержащее план действий, обязательный к исполнению для БТС j, и передаваемое от ВУ БТС j ФУ j. Тогда, O_j^t– множество информационных сообщений, содержащих планы, выработанные БТС j для всех ФУ, с которыми существует связь, в момент времени t. Множество всех информационных сообщений, передающихся в момент времени t от ВУ всех БТС на ФУ всех БТС, $O^t = \{O_o^t, \dots, O_{|E_{inf}|}^t\}$.

ВУ БТС не имеют собственные сенсорные устройства для оценки окружающей среды и выполнения поставленных задач перед ФУ [9]. Без знаний об окружающей среде и о текущем положении и состоянии ФУ БТС, не представляется возможным построить локально оптимальный план по выполнению поставленных задач. Таким образом, ФУ должны передавать на ВУ информационное сообщение, содержащее информацию об окружающей среде, выполнении плана и состоянии ФУ.

Пусть f_j^t- информационное сообщение, содержащее информацию об окружающей среде, выполнении плана и состоянии ФУ БТС j, передаваемое ВУ БТС j в момент времени t. Исходя из утверждения о наличии у ФУ только одного устойчивого канала связи с ВУ, в момент времени передаётся только одно сообщение от ФУ на ВУ. $F^t = \{\dots, f_j^t, \dots\}$ – множество всех информационных сообщений, передаваемых в момент времени t от ФУ всех БТС на ВУ всех БТС.

Информационные сообщения, циркулирующие в группе БТС, позволяют элементу получать, накапливать и применять знания о других БТС и об окружающей среде. Полученные знания KN позволяют выработать планы для выполнения поставленных задач. Можно говорить о локальной оптимальности вырабатываемых планов, т.к. знания БТС об окружающей среде и о других БТС ограничены физическими характеристиками сенсоров.

Однако в рамках имеющихся знаний разрабатываемый план будет оптимальным [166].

Под множеством всех знаний, имеющихся у всех БТС, понимается знания каждого БТС: $KN = \{KN_{e_0}, \dots, KN_{e_n}\}$. При этом, знания БТС также являются множеством знаний: $KN_{e_0} = \{kn_{e_0}, \dots, kn_{e_n}\}$. Стоит отметить, что знания могли быть произведены самим БТС, а могли быть получены в ходе ИВ от других БТС. Таким образом, возможно разделение знаний на активные и пассивные.

Определение 3: Пассивные знания ($KN_{e_{pas}}$) – знания, имеющиеся у БТС $e \in E$ и не являющиеся результатом активной работы группы БТС, непосредственно направленной на выполнение поставленных перед группой БТС задач.

Определение 4: Активные знания ($KN_{e_{act}}$) – знания, имеющиеся у БТС $e \in E$ и являющиеся результатом активной работы группы БТС, непосредственно направленной на выполнение поставленных перед группой БТС задач.

Основываясь на определениях 3 и 4, к пассивным знаниям можно отнести текущие знания об окружающей среде и о состоянии БТС, а к активным знаниям – план действий, сведения о предположительном состоянии БТС после выполнения плана и предположительное состояние окружающей среды после выполнения плана.

Принципы построения планов выполнения действий основываются на решение задачи поиска локально оптимального решения задачи максимального выполнения поставленных перед группой БТС задач.

Рассмотрим множество поставленных перед группой БТС задач $TK = \{tk_0, \dots, tk_k\}$. Любое БТС может построить вектор оценок, характеризующий некоторую стоимость выполнения поставленных задач:

$$\overline{cost_e} = \begin{pmatrix} cost_e(tk_0) \\ \dots \\ cost_e(tk_k) \end{pmatrix}$$

где $cost_e(tk_k)$ – функция оценки стоимости выполнения БТС *e* задачи tk_k.

В таком случае, решение задачи нахождения плана действий сводится к задаче следующего вида.

Задача 1:

$$\begin{cases} |TK_k| \to |TK| \ (1) \\ cost_e(tk_k) < cost_e \ (2) \end{cases}$$

где TK_k – выполняемые задачи, $cost_e$ – максимально допустимые затраты БТС *e*. Критерий (1) задачи 1 позволяет говорить о выполнении максимально возможного числа задач при условии выполнения ограничений (2). Ограничения (2) – набор ограничений, соответствующий по смыслу правилу «БТС *e* не может потратить на выполнение задачи больше ресурсов, чем он имеет». Таким образом, решение задачи 1 гарантирует максимальное покрытие целей, без учёта издержек (за исключением ограничения (2)). Следовательно, можно говорить о максимальном выполнении задач, что необходимо для решения критически важных задач. Решение задач, не имеющих критического значения, подразумевает возможное уменьшение издержек [167].

Задача 2:

$$\begin{cases} |TK_k| \to |TK| \ (1) \\ \dfrac{\sum_{i=1}^{|E_{phy}|} cost_{e_i}(tk_k)}{|TK_k|} \to min \ (2) \\ cost_e(tk_k) < cost_e \ (3) \end{cases}$$

Критерий (1) задачи 2 и ограничения (3) задачи 2 идентичны критерию и ограничением задачи 1. Критерий (2) задачи 2 выражает минимизацию средних затрат на выполнение задач. Также, можно использовать не средние издержки на одну задачу, а общие издержки $\sum_{i=1}^{|E_{phy}|} cost_{e_i}(tk_k) \to min.$

Задача 3:

$$\begin{cases} (|TK| - |TK_k|) \dfrac{\sum_{i=1}^{|E_{phy}|} cost_{e_i}(tk_k)}{|TK_k|} \to min \ (1) \\ cost_e(tk_k) < cost_e \ (2) \end{cases}$$

Решение задачи 3 позволяет выработать такие планы действий, что будет выполнен максимум задач при минимальных средних затратах на одну задачу. Таким образом, не будут выполнены задачи, чьё выполнение потребует слишком больших затрат.

Функция затрат на выполнение задачи может быть представлена как сумма затрат на выполнение элементарных действий, из которых состоит план выполнения задачи.

$Pl_{e_{tk}} = \{\dots, as_{e_m}, \dots\}$ – план выполнения задачи tk БТС e. В таком случае, $cost_e(tk) = \sum_{m=1}^{\left|Pl_{e_{tk}}\right|} cost_e(as_{e_m})$, где $cost_e(as_{e_m})$ – затраты на выполнение элементарного действия as_{e_m}.

Таким образом, модель ИВ группы БТС в процессе выполнения поставленных задач может быть представлена следующим образом.

Пусть $T = \{t_0, \dots, t_{end}\}$ – время функционирования группы БТС. Под временем функционирования группы БТС понимается либо максимально возможное время функционирования системы, либо выполнение всех поставленных перед группой задач. Выполнение задач БТС может быть как синхронным, так и асинхронным. Под синхронным выполнением задач понимается такое выполнение задач, при котором БТС, исполнившие разработанный план, не выполняют последующие задачи (не разрабатывают план по выполнению последующих задач) до момента завершения всеми БТС текущего плана. В таком случае, уместно говорить об итерации, представляющей из себя множество моментов времени, где первый момент – начало выработки плана, последний момент времени – передача информации от ФУ к ВУ на последнее БТС о выполнении плана. Под последним БТС подразумевается БТС, завершившее выполнение плана позже остальных БТС. ИВ БТС при синхронной и асинхронной модели функционирования группы БТС не отличается с точки зрения принципов и подходов, различаются число задействованных БТС и выполняющие задачи в текущий момент времени БТС. Далее будет рассмотрена одна итерация выполнения

задачи, т.к. принципы модели ИВ группы БТС не меняется от итерации к итерации.

В момент времени t_0 БТС (e) начинают выработку планов действий на достижение целей Tk. После разработки планов (момент времени $t_{pln\_cmpl\_f}$) происходит ИВ между ВУ всех БТС, в ходе которого все БТС получают K_{act} других БТС. После ИВ $\forall e_i \in E$ обладает $KN_{e_i} = \{KN_{act_{e_i}}, KN_{pas_{e_0}}, \dots, KN_{pas_{e_n}}\}$. $\{KN_{pas_{e_i}}\}$ представляет из себя активные данные, полученные от БТС i и используемые получившим их субъектом в качестве пассивных знаний. Пассивные знания выступают в качестве дополнительных ограничений, позволяющих выработать локально оптимальный план действий для БТС. Доработка планов завершается в момент времени t_{pln_cmpl}.

В момент времени $t_{pln\_cmpl}+1$ $e_i^{inf} \in e_i$ получают доступ к каналу связи, куда передают информационные сообщения для соответствующих ФУ, имеющих с ними устойчивый канал связи, O_e. Таким образом, $e_i^{inf} \in e_i$ отправляет информационные сообщения $\{o_{e_i}\}$, содержащие соответствующие планы действий Pl_{e_i} для ФУ $e_i^{phy} \in e_i$. Обязательным условием отправки планов является наличие устойчивого канала связи между устройствами. На рисунке 4 представлено схематичное отображение действий ВУ в модели функционирования БТС.

После обработки сообщения o_{e_i}ФУ $e_i^{phy} \in e_i$ выполняет действия согласно полученному плану. Момент окончания действий по плану – t_{tsk_cmpl}. В момент времени t_{tsk_cmpl} $+1$ e_i получает доступ к каналу связи, куда передает информационное сообщение f_{e_i}, содержащее отчет о выполнении плана. На рисунке 5 представлено схематичное отображение действий ФУ в модели функционирования БТС. После этого, ВУ $e_i^{inf} \in e_i$ получает доступ к каналу связи и обрабатывает полученное сообщение, в результате чего, у БТС появляются новые знания $kn_{pas_{e_j}}$.

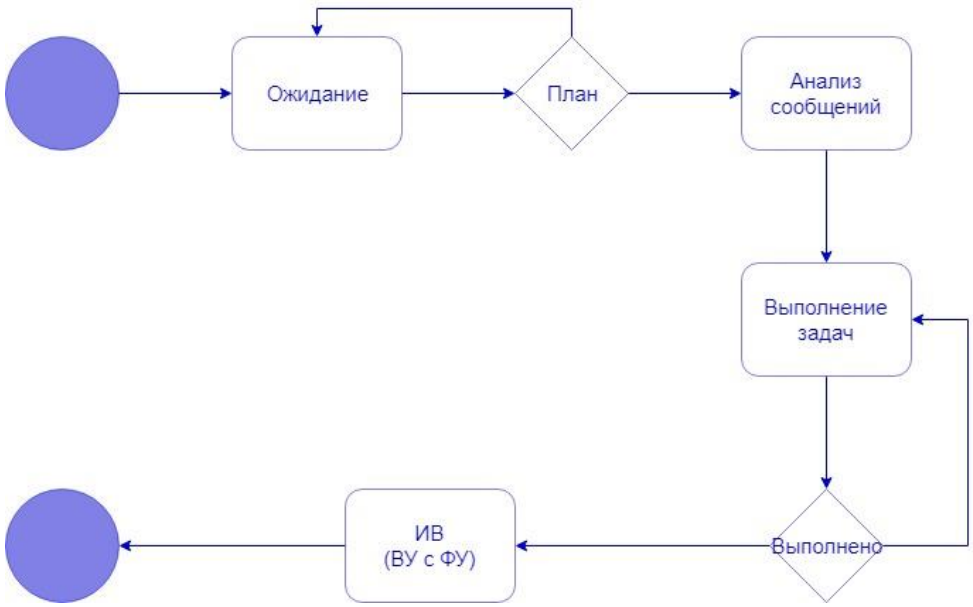


Рисунок 4. Действия ВУ БТС

Обработка множества сообщений, получаемых от ФУ БТС, позволяет ВУ БТС сформировать знания KN_{pas}, используемые для дальнейшего построения планов действий (при необходимости). Графическое представление модели ИВ группы БТС в процессе функционирования можно представить при помощи диаграмма последовательности UML стандарта. Кроме того, возможно представление внутреннего (между ВУ и ФУ одного БТС) и внешнего (между ВУ различных БТС) ИВ БТС. Диаграмма последовательности внутреннего ИВ группы БТС представлена на рисунке 6. Диаграмма последовательности внешнего ИВ группы БТС представлена на рисунке 7.

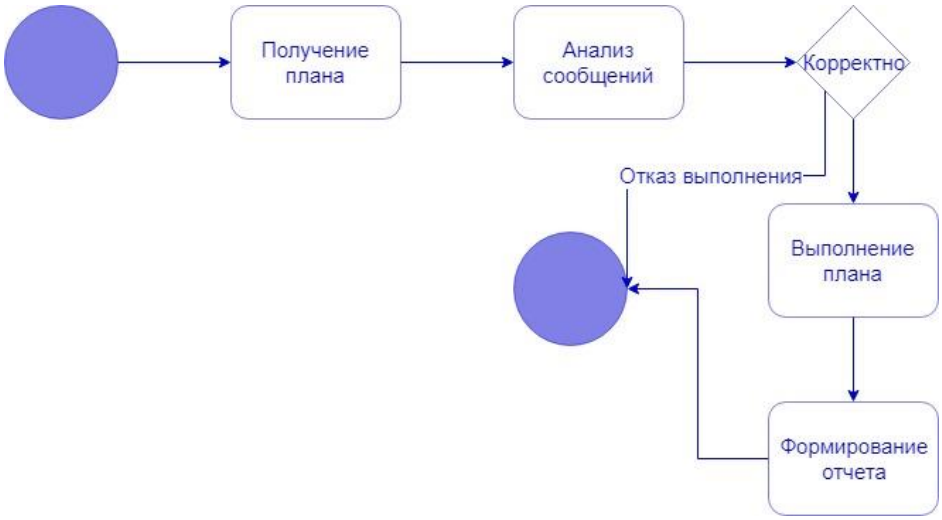


Рисунок 5. Действия ФУ БТС

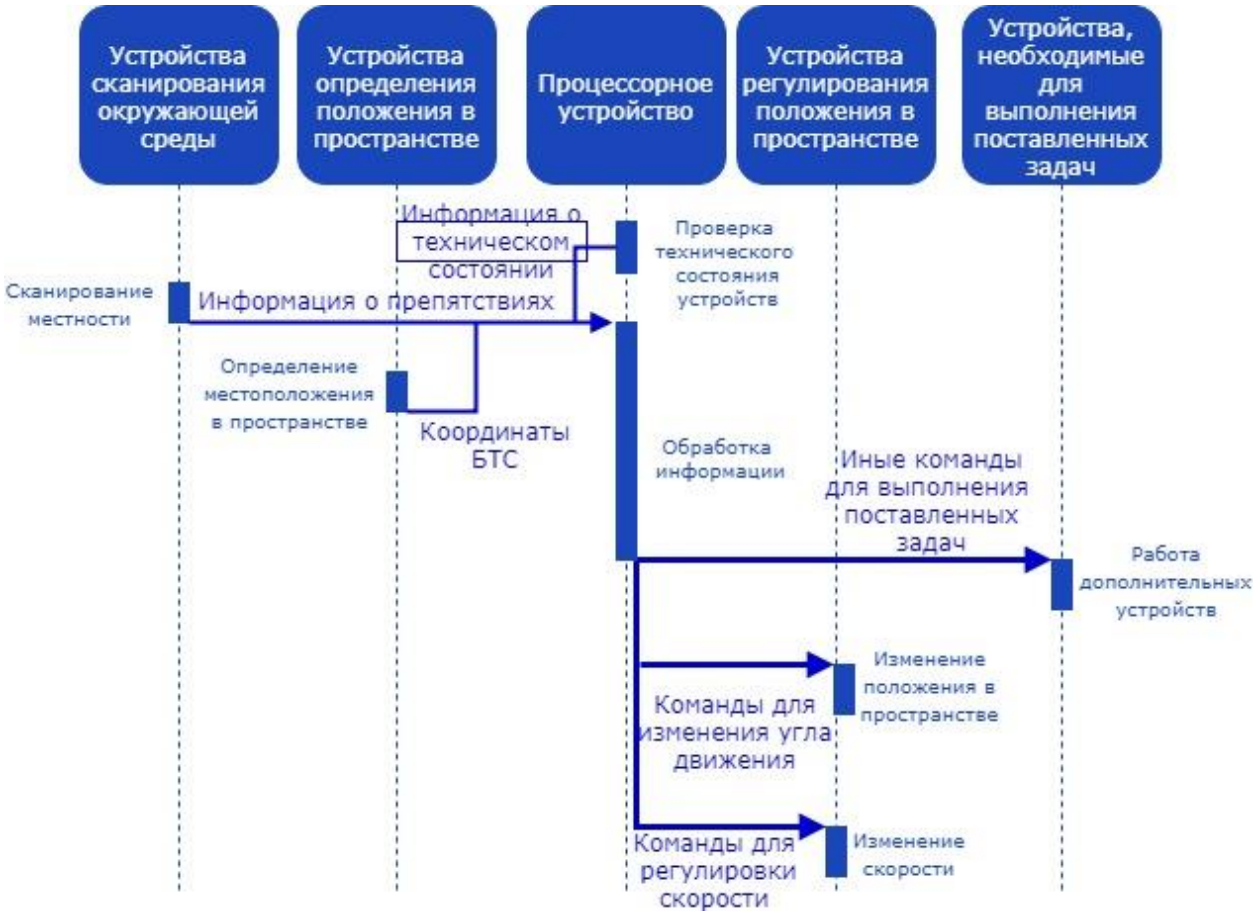


Рисунок 6. Диаграмма внутреннего ИВ БТС в процессе функционирования

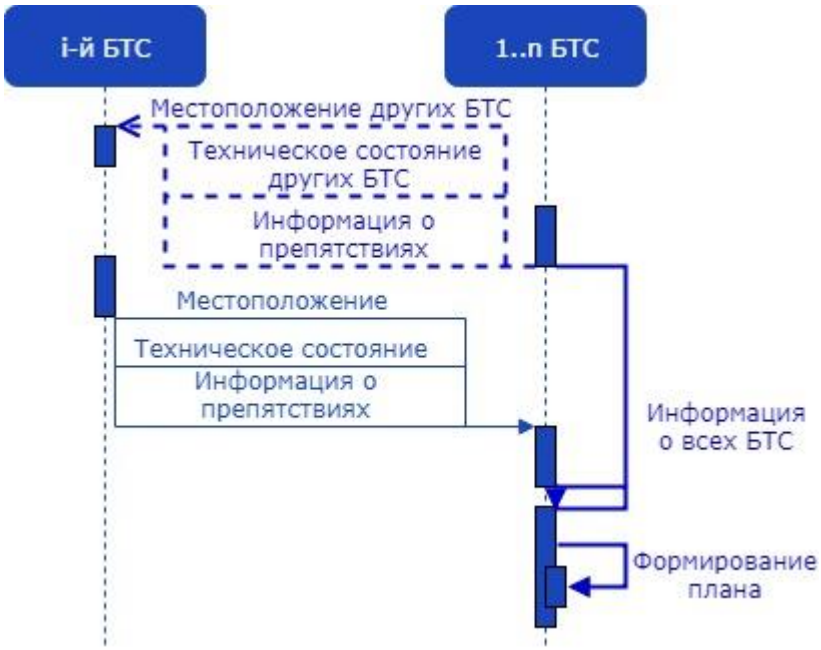


Рисунок 7. Диаграмма внешнего ИВ БТС в процессе функционирования

2.2 Определение класса мягких атак на информационную безопасность группы беспилотных транспортных средств

Основываясь на модели функционирования группы БТС, представленной в разделе 2.1, можно выделить три основных типа информационных сообщений, циркулирующих в системе:

1. Сообщения, содержащие планы действий для элементов физического уровня (O);
2. Сообщения, содержащие информацию о выполнении планов действий (F);
3. Сообщения, содержащие знания, выработанные при разработке планов действий (KN_{act}).

В разделе 1.5 представлена постановка задачи работы, согласно которой требуется разработать методы противодействия атакам, при которых БТС функционируют в штатном режиме. В дальнейшем, такой вид атак будет называться «мягкой атакой».

Определение 5: Мягкая атака – совокупность преднамеренных или непреднамеренных действий, в результате которой реализуются угрозы ИБ группы БТС, не нарушающие штатную работу как группы в целом, так и отдельных БТС, но нарушающие целостность информации, циркулирующей в группе.

Таким образом, определение 5 выделяет такой класс атак, при котором отсутствуют явные признаки нарушения ИБ, что не позволяет установить факт реализации угрозы. Как следствие, возможно снижение работоспособности группы БТС. Снижение работоспособности группы БТС подразумевает как уменьшение вероятности выполнения задач по сравнению с обычным функционированием группы, так и уменьшение эффективности функционирования.

Рассмотрим $e_i \in E_{inf}, e_j \in E_{phy}$. В таком случае, нарушение целостности информации подразумевает передачу модифицированного

сообщения. Тогда, согласно модели ИВ группы БТС, верны следующие утверждения:

1. Если ВУ БТС e_i передает $\widetilde{O_{i_j}}$ ФУ БТС, где $\widetilde{O_{i_j}}$ – сообщение, содержащее информацию с нарушением целостности, то ФУ БТС e_i будет выполнять план действий, не соответствующий верному. Верный план действий (Pl_{e_j}) – план действий, выработанный при решение одной из задач 1-3 и являющийся локально оптимальным. Верный план действий передается с сообщением O_{i_j}. Следовательно, в общем случае $Pl_{e_j} \neq \widetilde{Pl_{e_j}}$, где $\widetilde{Pl_{e_j}}$ – план действий, переданный в сообщении $\widetilde{O_{i_j}}$. В таком случае, снижается эффективность выполнения поставленных задач БТС, вплоть до их полного невыполнения;

2. Сообщение F_{j_i}, передаваемое от ФУ БТС e_i ВУ БТС e_i, содержит информацию об окружающей среде, состоянии ФУ и результате выполнения действий, исходя из полученного плана. В дальнейшем информация из этого сообщения используется ВУ БТС e_i в качестве пассивной информации $kn_{pas_{e_i}}$, с использованием которой вырабатывается план действий на следующей итерации для всех ФУ БТС. Тогда, если $\widetilde{F_{j_i}}$ – сообщение, содержащее информацию с нарушенной целостностью, в общем случае $kn_{pas_{e_i}} \neq \widetilde{kn_{pas_{e_i}}}$, где $\widetilde{kn_{pas_{e_i}}}$ – знания, полученные в результате обработки сообщения $\widetilde{F_{j_i}}$. В таком случае, вырабатываемые планы действий для ФУ БТС могут быть локально не оптимальными, что может привести к снижению эффективности выполнения поставленных задач;

3. Пусть $\{e_0, \dots, e_{n\_inf}\} \in E$. После выработки планов действий осуществляется обмен данными между БТС с содержанием выработанных планов и информацией о предполагаемом состоянии окружающей среды и БТС. В дальнейшем, данные знания используются получившими их БТС как пассивные знания при доработке ранее подготовленных планов действий БТС. В таком случае, нарушение целостности информации о выработанных

планах действий может привести к использованию в доработке планов ложной информации, что приведет в свою очередь к подготовке локально не оптимальных планов действий для ФУ БТС и, как следствие, к снижению эффективности выполнения поставленных задач.

Мягкие атаки осуществляются при использовании БТС-нарушителей.

Определение 6: БТС e_s является нарушителем, если выполняется хотя бы одно из следующих условий:

1. передает сообщения $\widetilde{F_{s_i}}$;
2. передает сообщения $\widetilde{O_{s_i}}$;
3. передает сообщения $\widetilde{KN_{act}}$.

Рассматривая свойства информационных сообщений ($P_{\inf\_m}$), можно выделить семантику сообщений ($p_{sem} \in P_{\inf\_m}$). Семантика сообщения – сведения, передаваемые в сообщении [168, 169]. В этом случае, информационные сообщения, содержащие информацию с нарушением целостности, могут быть представлены следующим образом:

1. $P_{\inf\_m}(\tilde{O}) = P_{\inf\_m}(O)$, но $p_{sem}(\tilde{O}) \neq p_{sem}(O)$
2. $P_{\inf\_m}(\tilde{F}) = P_{\inf\_m}(F)$, но $p_{sem}(\tilde{F}) \neq p_{sem}(F)$
3. $P_{\inf\_m}(\widetilde{KN_{act}}) = P_{\inf\_m}(KN_{act})$, но $p_{sem}(\widetilde{KN_{act}}) \neq p_{sem}(KN_{act})$

Тогда, методы обеспечения ИБ должны основываться на проверке семантики сообщений. При этом проверка семантики не является достаточным условием эффективности методов ИБ. Также необходима проверка источника информации, т.к. не всегда есть возможность оценить соответствие семантики сообщения текущим условиям функционирования [170]. Для разработки методов ИБ требуется сформулировать основные гипотезы, проверка которых позволит говорить о защищенности информации в системе.

С точки зрения внешнего ИВ основной интерес представляют такие атаки, при которых нарушается семантическая целостность сообщений, передаваемых между ВУ различных БТС. Внутреннее ИВ БТС, прежде всего,

основывается на надежности компонент БТС, для реализации защищенного внутреннего ИВ возможно применение методов контроля функционирования внутренних устройств. При внешнем ИВ и наличии нарушений в передаваемых сообщениях между БТС возможна ситуация, при которой группа не сможет выполнить задачи, стоящие перед ней, но нарушения семантической целостности невозможно будет обнаружить при использовании классических методов обеспечения ИБ. Таким образом, наибольший интерес представляет внешнее ИВ в группе БТС, т.к. возможно использовать механизмы обеспечения защиты на внешнем уровне также и на внутреннем.

2.3 Постановка задачи обеспечения семантической целостности информации в группе беспилотных транспортных средств

На основании сведений, изложенных в разделе 2.2, можно предположить, что частные гипотезы разделяются на три основные группы: проверка физическим элементом информационного, информационным элементом физического и информационным элементом информационного. Общий вид гипотез может быть представлен следующим образом:

1. $f_e\left(I_{get_{e_i}}, J_{have}\right) \geq \alpha_{self}$, где $I_{get_{e_i}}$ – информация, полученная от БТС e_i БТС e; I_{have} – информация, которой располагает БТС e, f_e – функция оценки полученной информации на основе имеющейся информации.

2. $f_{e_t}\left(I_{get\_e\_i\_t}, f_{e_t-1}\left(I_{get\_e\_i\_t-1}, J_{have\_t-1}\right)\right) \geq \alpha_{rep}$, где $I_{get\_e\_i\_t}$ – информация, полученная от БТС e_i БТС e в момент времени t; J_{have_t-1} – информация, которой располагает БТС e в моменты времени, предшествующие моменту времени t, f_{e_t-1}– функция оценки полученной информации на основе имеющейся информации в моменты времени, предшествующие моменту времени t.

3. $f_{e_{soc}}\left(I_{get_{e_i}},\ f_{e\_j\_inf}\left(I_{get_{e_i}}, J_{have\_e\_j}\right)\right) \geq \alpha_{soc}$, где $I_{get_{e_i}}$ – информация, полученная от БТС e_i БТС $e_j \in E, j \neq i, e_j \neq e$; $f_{e\_j\_inf}\left(I_{get_{e_i}}, J_{have\_e\_j}\right)$ – оценка информации, полученной от БТС e_i БТС-соседями БТС e.

Гипотезы первого и второго вида оценивают информацию, передаваемую от БТС на основе имеющейся информации. Таким образом, данная оценка информации может производиться без осуществления ИВ с другими БТС группы. Гипотезы третьего вида позволяют оценить целостность получаемой информации на основе ИВ, т.е. на основе оценки целостности информации, полученной другими БТС группы, принимается решение о целостности информации БТС-субъектом. Для разработки методов обеспечения ИБ группы БТС требуется конкретизировать гипотезы на основе положений, изложенных в предыдущих разделах, а также на основе общего вида гипотез.

Гипотезы проверки целостности информации, передаваемой от ВУ одного БТС на ВУ других БТС, принимают следующий вид:

Гипотеза 1:

$$f_{KN\_act\_e}\left(KN_{act\_e\_j}, KN_{pas\_e}\right) \geq \alpha_{KN_{act}}$$

БТС e оценивает активные знания, выработанные БТС e_j, на основе имеющихся пассивных знаний, включающих в себя, но не ограничивающиеся активными знаниями, полученными от других элементов информационного уровня.

Гипотеза 2:

$$f_{e_{rep}}\left(\left\{f_{KN\_act\_e}\right\}\right) \geq \alpha_{e_{rep}}$$

Гипотеза 2 заключается в оценке качества передаваемых активных знаний на основе оценки информации, полученной при проверке гипотезы 1 на предыдущих итерациях.

Гипотеза 3:

$$f_{e_{soc}}(\{f_{KN\_act\_e\_j}\}) \geq \alpha_{e_{soc}}$$

Гипотеза 3 основывается на проверке поведения БТС другими БТС. Таким образом, данная гипотеза позволяет говорить об оценке поведения БТС на основе его поведения по оценкам других БТС. Следовательно, БТС-субъект оценки может оценить БТС даже при отсутствии необходимого количества наблюдений для выполнения гипотезы 2.

Таким образом, представленные гипотезы являются частным случаем гипотез проверки семантической целостности информации общего вида, применимые для групп БТС. Однако предложенные гипотезы не позволяют в полной мере обеспечить ИБ группы БТС, т.к. методы защиты ИБ, основанные на проверке представленных выше гипотез, позволяют обеспечить только защищенное ИВ. Для комплексного обеспечения ИБ группы БТС требуется разработать модели угроз и нарушителя, привести основные субъекты и объекты ИБ, описать основные этапы жизненного цикла группы БТС и этапы разработки БТС.

2.4 Модель обеспечения информационной безопасности группы беспилотных транспортных средств

Наличие уязвимостей ИБ группы БТС, организация работы которой основывается на децентрализованном мультиагентном подходе, обусловлено особенностями знаний и действий, характерных БТС. На основе ранее изложенной в работе информации, к таким причинам можно отнести:

1. итерационность выполнения задач;
2. ограниченность знаний об окружающей среде;
3. ограниченность знаний о свойствах других БТС группы;
4. субъективность знаний об окружающей среде и группе;
5. автономность функционирования группы;
6. ограниченность возможности ИВ;
7. недостаточность средств обнаружения аномального поведения.

Анализ существующих угроз ИБ группы БТС может быть проведен при помощи стандарта моделирования процессов UML. На рисунке 8 представлено ИВ внутри БТС в процессе выполнения задач.

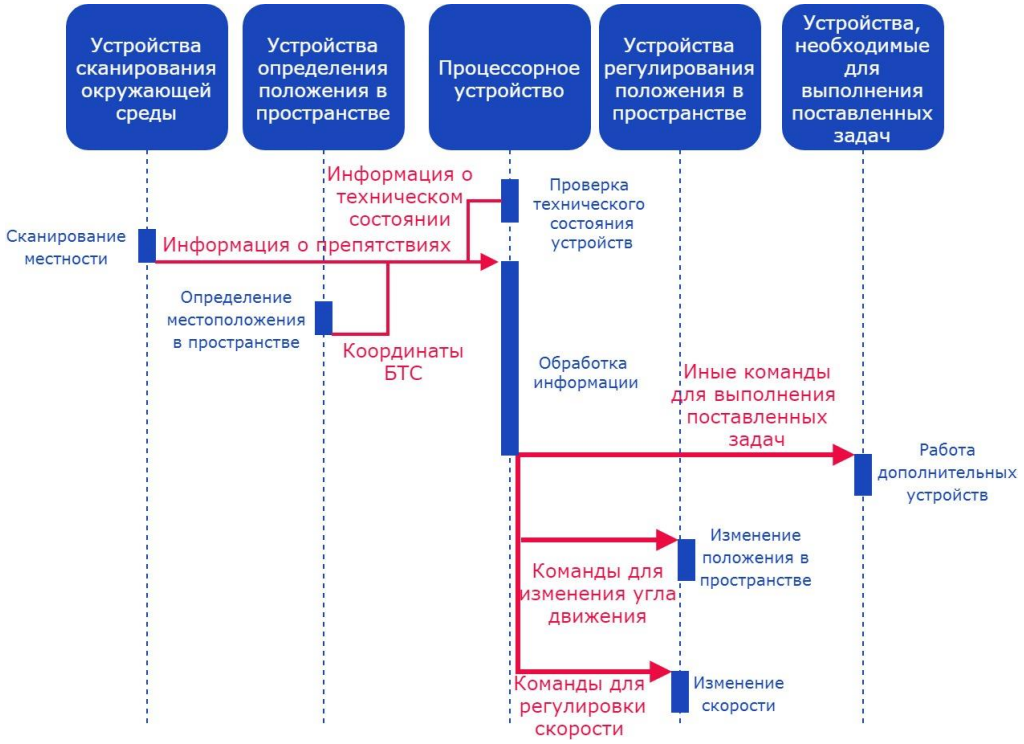


Рисунок 8. Диаграмма последовательности внутреннего ИВ БТС в процессе функционирования. Красным выделены процессы с возможным нарушением целостности информации

На рисунке 9 представлены основные процессы, наиболее уязвимые к реализации угроз ИБ. Все угрозы ИБ можно разделить на аппаратные и программные угрозы. Под аппаратными угрозами понимаются угрозы ИБ, реализация которых возможна при возникновении сбоев, нарушений или отказов в аппаратной части БТС. Таким образом, данный вид угроз обусловлен физическими особенностями реализации БТС. Под информационными угрозами понимаются угрозы ИБ, возникающие в результате сбоев, нарушений или отказов в программной части БТС.

К аппаратным угрозам можно отнести:

1. сбой работы модуля связи;
2. сбой работы модуля функционирования БТС;
3. нарушения работы каналов связи;

4. отказ функционирования БТС по естественным причинам.

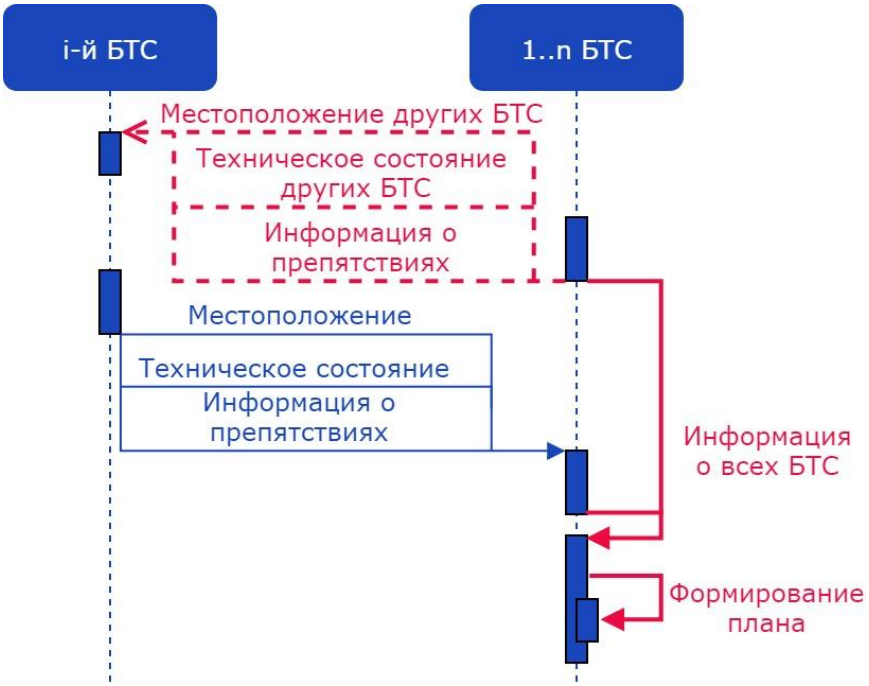


Рисунок 9. Диаграмма последовательности внешнего ИВ группы БТС в процессе функционирования. Красным пунктиром выделены процессы с возможным нарушением целостности информации, красные линии – процессы, которые не могут быть корректно выполнены после процессов с нарушением целостности информации

К программным угрозам относятся:

1. нарушения обработки информации физических устройств;
2. нарушения обработки информационных сообщений;
3. нарушения принципов функционирования группы;
4. нарушения при генерации информационных сообщений.

Для разработки модели нарушителя необходимо описать модель жизненного цикла БТС. На основе модели жизненного цикла БТС возможно определить список основных физических лиц, имеющих доступ к БТС на различных этапах жизненного цикла системы. Жизненный цикл БТС от момента разработки до ее применения для решения задач представлен на рисунке 10.

На основе проведенного анализа жизненного цикла БТС выделим две группы нарушителей по возможности доступа к группе БТС и БТС:

1. не допущенные к работе с БТС/группе БТС;
2. имеющие доступ к БТС/группе БТС.

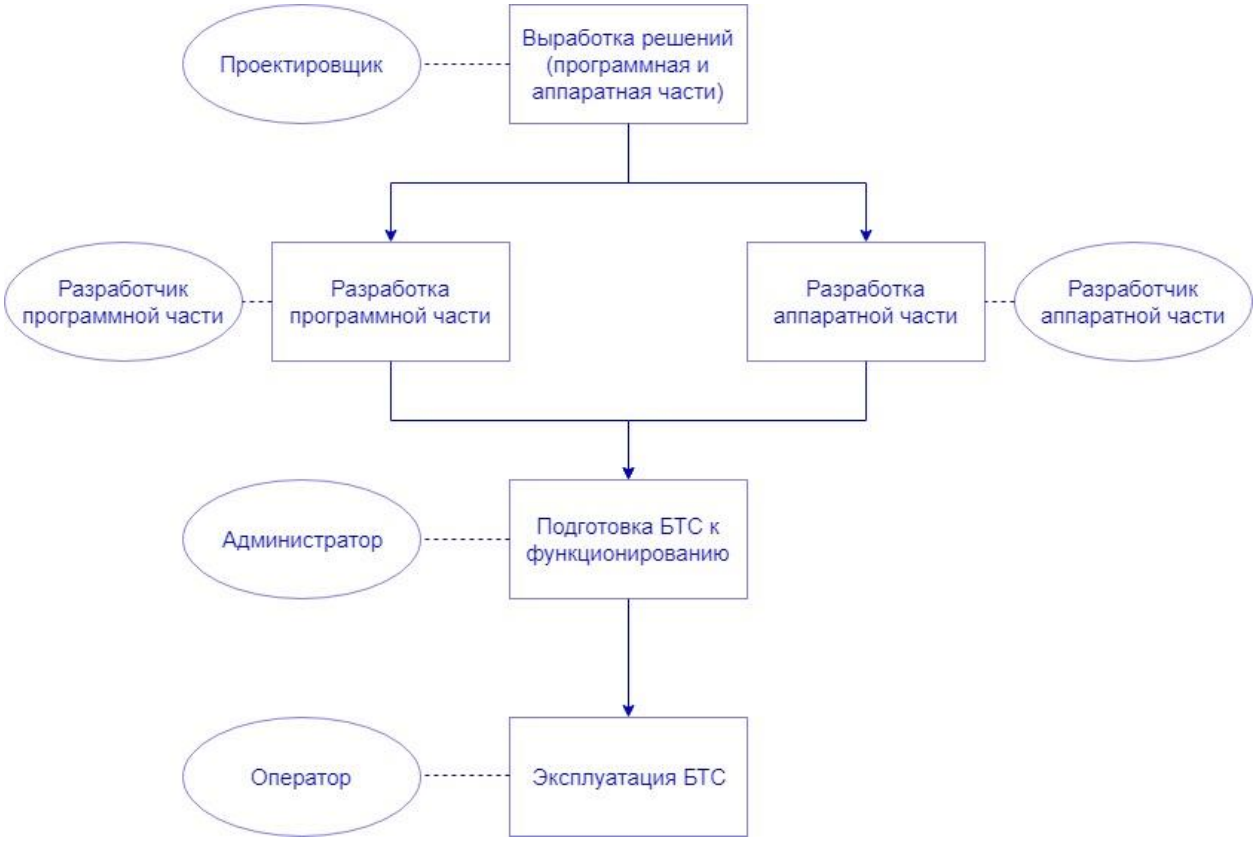


Рисунок 10. Жизненный цикл БТС от момента разработки системы до ее применения для решения задач. Пунктирные линии связывают этап разработки и исполнителя этапа

Лица первой группы можно отнести к внешним нарушителям, т.е. к таким нарушителям, которые не имеют прав на работу с БТС. Лица второй группы – нарушители, осуществляющие атаку с использованием имеющихся прав на работу с БТС, или внутренние нарушители. Предложенные модель угроз и модель нарушителей позволяют выявить присущие обеим группам нарушителей угрозы. Внешние нарушители способны оказать воздействие на аппаратную составляющую БТС, т.к. не имеют прямого доступа к программному обеспечению, использующемуся в БТС. Следовательно, основными угрозами, характерными для данной группы нарушителей, являются следующие угрозы:

1. сбой работы модуля связи;
2. сбой работы модуля функционирования БТС;
3. нарушения работы каналов связи.

Внутренние нарушители могут оказывать влияние как на аппаратную часть БТС, так и на программную. Тогда угрозы, исходящие от данной группы нарушителей, совпадают со списком всех возможных угроз БТС. К нарушителям данной группы можно отнести участников жизненного цикла БТС, представленных на рисунке 9:

1. проектировщик;
2. разработчик программной части;
3. разработчик аппаратной части;
4. администратор;
5. оператор.

Проанализировав модели угроз, нарушителей и основные уязвимости БТС/группы БТС, можно предложить схему взаимодействия основных элементов модели обеспечения ИБ. Графическое представление схемы продемонстрировано на рисунке 11.

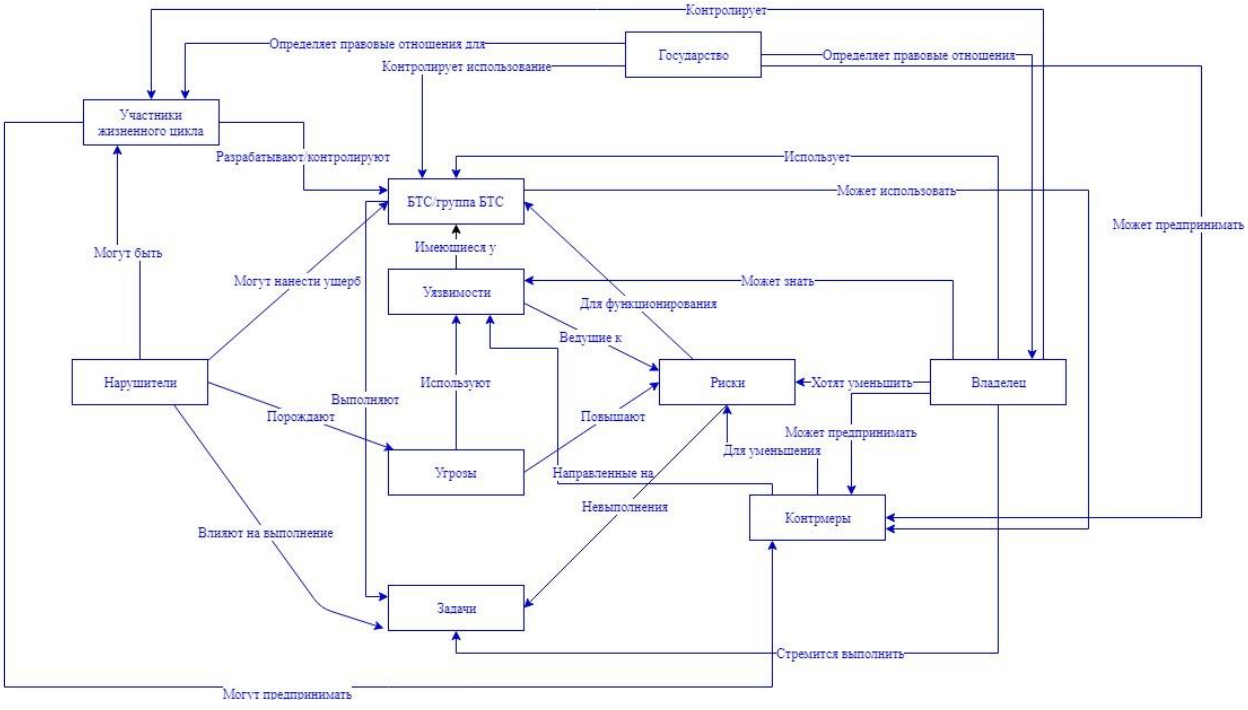


Рисунок 11. Схема взаимодействия элементов модели обеспечения ИБ группы БТС

На основе представленной схемы можно выделить субъекты обеспечения ИБ: государство, владелец, участники жизненного цикла, сама группа. Стоит отметить, что владелец не будет выделяться в дальнейшем в качестве отдельного субъекта обеспечения ИБ, а будет входить в число участников жизненного цикла, которому присущи свойства контроля, как за остальными участниками жизненного цикла, так и за самой группой БТС. К объектам обеспечения ИБ относится БТС/группа БТС. Государство стремится обеспечить ИБ БТС/группы БТС путем разработки законодательных и правовых документов, направленных на контроль работы участников жизненного цикла, регулирование их взаимоотношений с владельцем БТС и разработки контрмер для устранения уязвимостей БТС. Участники жизненного цикла предпринимают контрмеры для минимизации рисков и устранения уязвимостей при помощи разработки аппаратных и программных решений, при этом, владелец БТС разрабатывает организационные контрмеры, исходя из предположения о его контролирующих функциях. На основе предложенной схемы взаимодействия элементов модели обеспечения ИБ, можно представить обобщенную модель обеспечения ИБ БТС/группы БТС. Графическое отображение предлагаемой модели представлено на рисунке 12.

В рамках обобщенной модели обеспечения ИБ группы БТС требуется реализовать модель защищенного ИВ группы БТС, как одну из возможных реализаций программных мер по обеспечению ИБ группы БТС. Под программными мерами понимается разработанные методы, подходы и механизмы, позволяющие уменьшить риск и/или избавиться от уязвимости и реализуемые при помощи программных инструментов. Таким образом, модель защищенного ИВ группы БТС подразумевает разработку подхода к обеспечению ИВ группы БТС с разработанными методами защиты от нарушений целостности, доступности и конфиденциальности информации. В рамках данной работы рассматриваются методы защиты ИВ для контроля целостности информации, передаваемой при ИВ БТС.

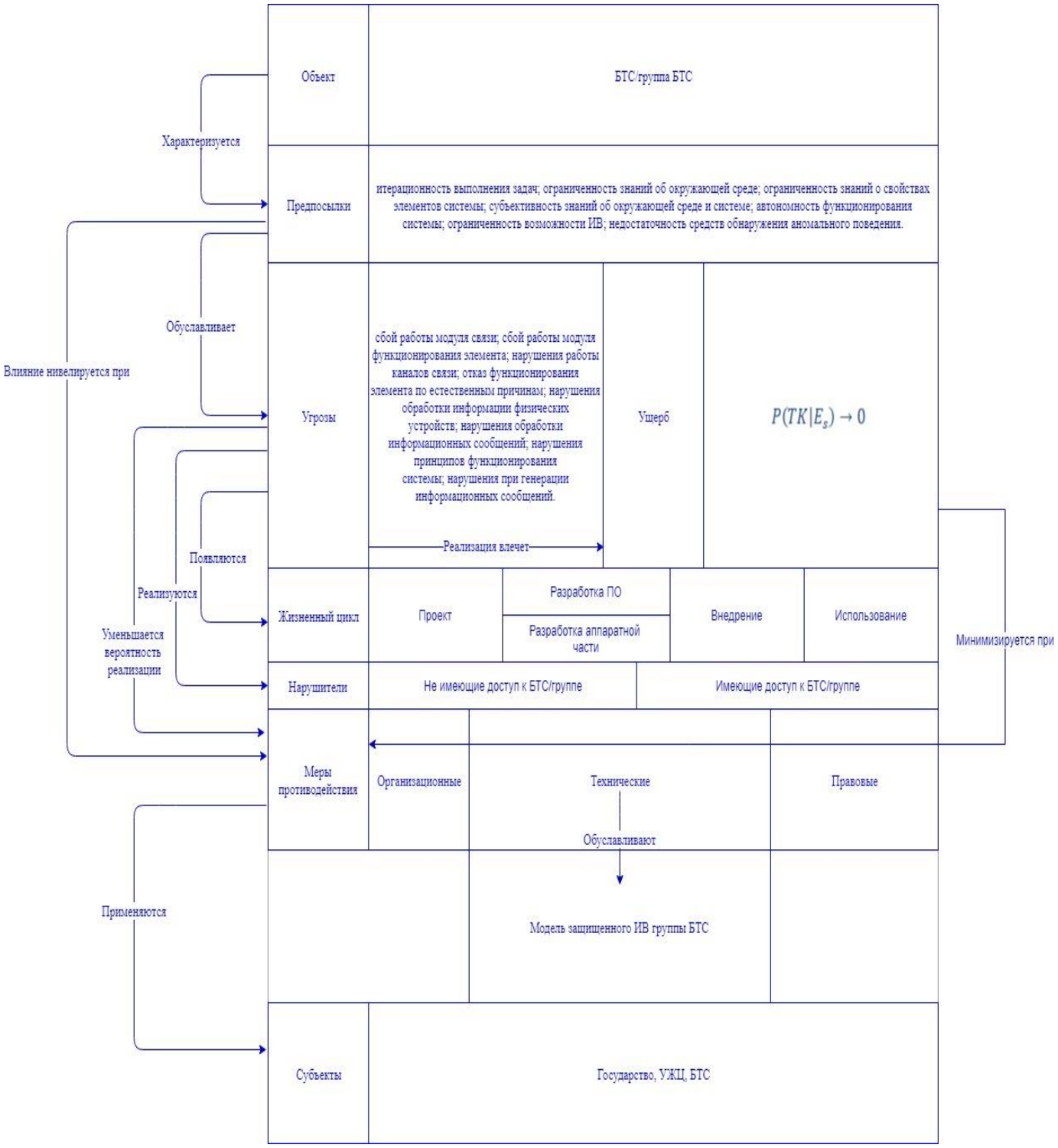


Рисунок 12. Обобщенная модель обеспечения ИБ группы БТС

2.5 Модель защищенного информационного взаимодействия

Рассмотрим модель организации защищенного ИВ группы БТС на основе товарищеской модели безопасности [170, 171]. В данном разделе

будет рассматриваться организация защищенного ИВ на основе одной итерации, т.к. другие итерации выполнения модели совпадают.

Пусть $T = \{t_0, \dots, t_{end}\}$ – время функционирования группы БТС. В момент времени t_0 все БТС начинают выработку планов действий на достижение целей Tk. После разработки планов (момент времени $t_{pln\_cmpl\_f}$) происходит ИВ БТС, в ходе которого все БТС получают KN_{act} других БТС.

В момент времени $t_{pln\_cmpl\_f}$ + 1 ВУ начинают выполнение методов для проверки целостности информации либо путем сбора недостающей информации об окружающей среде, либо на основе имеющихся пассивных знаний, либо на основе оценки поведения элемента в предыдущие моменты времени. Под недостающими знаниями понимаются знания, без которых ВУ не может оценить информацию, получаемую от другого устройства. В случае если доверие к БТС-объекту оценки превышает некоторое пороговое значение, полученные от него знания принимаются БТС-субъектом оценки для дальнейшего использования. Если ВУ не может определить качество (корректность) получаемой информации, т.е. отсутствует возможность оценить показатель истинности, БТС начинает ИВ с другими БТС, чей предыдущий уровень доверия позволяет оценить их поведение как корректное, в результате которого происходит получение информации о значении показателя истинности для БТС-объекта. Момент начала ИВ с целью получения показателя истинности других БТС t_{com_truth} начинается после ИВ с целью обмена планами, а также после проведения оценки показателя истинности БТС, для которых получение данной оценки представляется возможной. Следовательно, $t_{com\_truth} > t_{pln\_cmpl\_f}$. Момент завершения данного этапа ИВ $t_{com\_truth\_compl}$ будет различен для всех БТС, однако, разработка новых планов выполнения действий подразумевает выработку последовательного плана действий. Таким образом, время начала выполнения действий БТС должно быть синхронизировано, либо разработано так, что будет учтена разница во времени начала выполнения плана. В общем случае, будем понимать под временем завершения этапа ИВ

с целью обмена информацией о значении показателя истинности такой момент времени, в который все БТС группы завершат данный этап ИВ.$\forall e \in E \; \exists \left\{t_{e_{com_{truth}}}, t_{e_{com_{truth_{compl}}}}\right\}: t_{com_{truth_{compl}}} = \sup\{t_{e_{com_{truth_{compl}}}}\}$

После ИВ и проведения оценки показателя доверия БТС (в момент времени $t_{com_{truth_{compl}}} + 1$) каждое БТС e_i обладает $KN_{e_i} = \{KN_{act_{e_i}}, KN_{pas_{e_0}}, \dots, KN_{pas_{e_n}}\}$. $\{KN_{pas_{e_i}}\}$ представляет собой активные данные, полученные от БТС e_i, прошедшего проверку на основе метода доверия, и используемые получившим их субъектом в качестве пассивных знаний. Пассивные знания выступают в качестве дополнительных ограничений, позволяющих выработать локально оптимальный план действий для всех БТС. Однако во множество пассивной информации входит только информация, целостность которой была проверена согласно предложенному методу доверия. Доработка планов завершается в момент времени t_{pln_cmpl}.

В момент времени $t_{pln\_cmpl}+1$ ВУ получают доступ к каналу связи, куда передают информационные сообщения для ФУ, имеющих с ними устойчивый канал связи, O_e. Таким образом, ВУ отправляет информационные сообщения $\{o_{e_{e_j}}\}$, содержащие соответствующие планы действий Pl_{e_j} для всех связанных ФУ. В момент времени $t_{com_{phy_{end}}}$ все ФУ завершают оценку целостности полученной информации.

В момент времени $t_{com_{phy_{end}}}$ + 1 ФУ выполняет действия согласно полученному плану, полученному в сообщении $o_{e_{e_j}}$. Момент окончания действий по плану – t_{tsk_cmpl}. В момент времени t_{tsk_cmpl} +1 e_j получает доступ к каналу связи, куда передает информационное сообщение $f_{e_{j_e}}$, содержащее отчет о выполнении плана.

После этого, ВУ получает доступ к каналу связи и обрабатывает полученное сообщение, в результате чего, у БТС появляются новые знания

$kn_{pas_{e_j}}$. Обработка множества сообщений, получаемых от ФУ, имеющих устойчивый канал связи с ВУ БТС *e*, позволяет БТС *e* сформировать знания KN_{pas}, используемые для дальнейшего построения планов действий (при необходимости). Диаграмма последовательности действий БТС при подобной организации ИВ представлена на рисунке 13 при помощи стандарта UML.

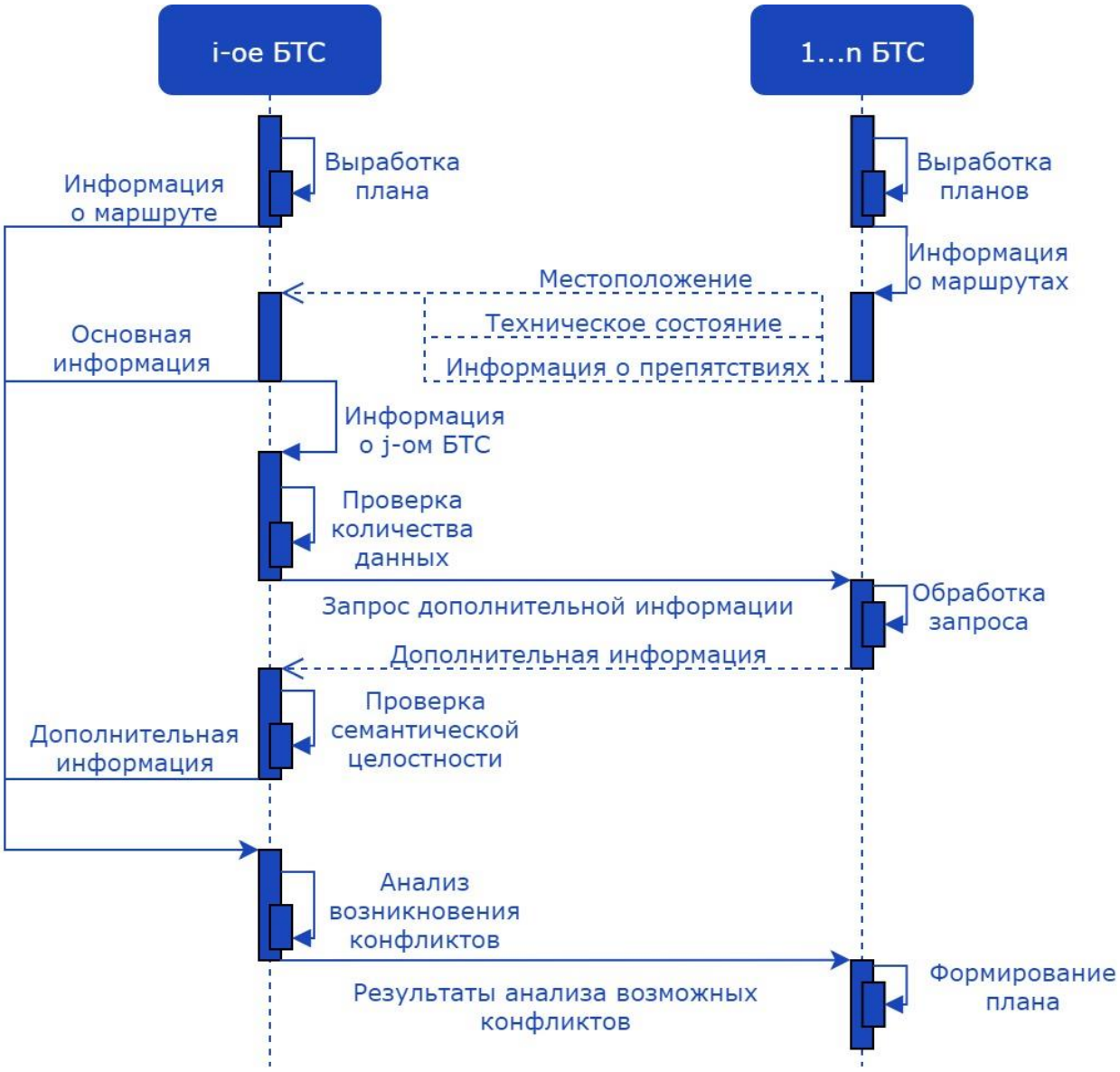


Рисунок 13. Диаграмма последовательности ИВ БТС в процессе функционирования с выполнением метода доверия и репутации

Модель защищенного ИВ, в основе которой находится не только методы проверки семантической целостности данных, но и методы

организации ИВ на основе централизованных стратегий управления. Стоит отметить, что первая итерация проходит так же, как и итерация при использовании модели защищенного ИВ, основанного только на методе проверки семантической целостности данных. Такое ограничение позволяет оценить корректность поведения БТС до выделения одного из них в ЦВЭ. В противном случае, может возникнуть ситуация, когда БТС, выбранный в качестве ЦВЭ, функционирует не в штатном режиме, что может привести к полной потери работоспособности подгруппы БТС.

Как было указано выше, группу БТС можно разделить на подгруппы, исходя из субъективных требований владельца, оператора и/или администратора группы. Иными словами, естественное разделение группы БТС на подгруппы зависит от физических особенностей аппаратной составляющей БТС. В формализованном виде, можно представить естественное разделение группы БТС на подгруппы следующим образом:

$$E = \bigcup_{sub=1}^{m} E_{sub}\text{, где } E_{sub} = \{e_k \in E : \forall e_l \in E_{sub},\ \exists C_{e_{k e_l}}\}$$

При такой организации процесса функционирования ИВ, ЦВЭ используется для оценки целостности информации, получаемой от других БТС подгруппы. Таким образом, после выработки планов действий в момент времени $t_{pln\_cmpl\_f}$ + 1 БТС подгруппы передают разработанные планы БТС, значения функции принадлежности которого больше, чем у других элементов: $e \in E_{sub} - \text{ЦВЭ} \Leftrightarrow \forall e_i : \overline{\mu_{E_{sub}}(e)} > \overline{\mu_{E_{sub}}(e_i)}$, а показатель доверия позволяет отнести поведение БТС к корректному. После получения выработанных планов от других БТС, ЦВЭ начинает проводить оценку целостности информации на основе методов проверки целостности. В случае необходимости, ЦВЭ начинает ИВ с другими БТС с целью сбора информации для проведения оценки БТС-объекта. Таким образом, t_{com_truth} – начало ИВ ЦВЭ с другими БТС, $t_{com\_truth\_compl}$ – окончание. После этого, делается вывод о целостности полученной информации, если информация не прошла такую проверку (полученный план некорректен), данная информация

не принимается для доработки планов. Планы дорабатываются либо ЦВЭ, либо БТС, разработавшими изначальные планы и оцененными положительно. С точки зрения загрузки вычислительных ресурсов, предпочтительнее использовать второй подход, однако, с точки зрения организации ИВ на основе метода временной централизации после доработки БТС опять должны будут передать информацию ЦВЭ, который, в свою очередь, должен будет оценить показатель доверия для этих БТС и переслать планы действий ФУ. Момент окончания доработки планов и получения новых планов действий ЦВЭ, а также проведения проверки показателя доверия - t_{pln_cmpl}.

Тогда t_{pln_cmpl} + 1 – момент начала ИВ с БТС, когда e (ЦВЭ) передает информацию ЦВЭ другой подгруппы e_j. БТС e_j проводит проверку полученной информации на основании имеющегося у него или у БТС его подгруппы знаний. Для получения знаний подгруппы ЦВЭ проводит ИВ с БТС, доверие к которым в предыдущие моменты было выше порогового значения. После проверки целостности полученной информации ЦВЭ e_j пересылает соответствующий план действий каждому БТС подгруппы, если полученный план был признан корректным. В момент времени $t_{com_{phy}}$ ЦВЭ начинает оценку информации, полученной от ЦВЭ другой подгруппы, во время которой осуществляет ИВ с другими БТС своей подгруппы, тогда $t_{com_{phy_{end}}}$ – момент времени, в который ЦВЭ завершает оценку информации и завершает ее передачу соответствующим БТС. После этого каждый ВУ БТС передает планы действий собственным ФУ.

Момент окончания действий по плану – t_{tsk_cmpl}. В момент времени t_{tsk_cmpl} *+1* начинается передача информация о выполнении полученных планов ФУ. После чего происходит оценка полученной информации по методу доверия. Оценка показателя доверия происходит аналогично предыдущему этапу оценки данного показателя. После этого, ВУ БТС передает собранные данные ЦВЭ e_j, далее ЦВЭ подгруппы осуществляет ИВ

с ЦВЭ других подгрупп и передает собранную информацию. ЦВЭ *е* также осуществляет проверку полученных данных и передает ее соответствующим БТС.

Стоит отметить, что при подобной организации ИВ группы БТС требуется оценивать не полный набор информации, а делать это по блокам, т.к. при нарушении целостности нескольких блоков могут быть отвергнуты для дальнейшего использования блоки информации, прошедшие проверку целостности. Также стоит отметить, что ЦВЭ различных подгрупп должны обладать устойчивым каналом связи между собой. В противном случае, невозможно обеспечить ИВ БТС двух подгрупп, что приведет к потери работоспособности группы в целом. Схема ИВ приведена на рисунке 14.

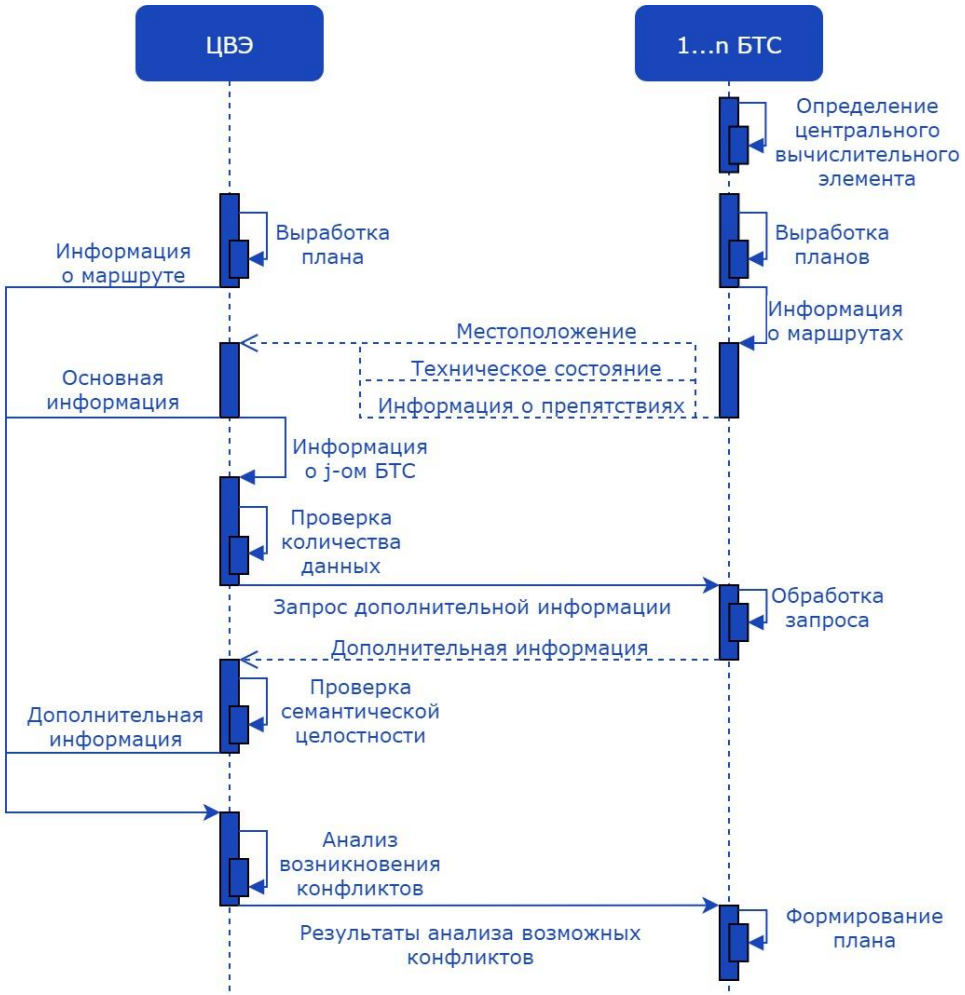


Рисунок 14. Диаграмма последовательности ИВ группы БТС в процессе функционирования с выполнением метода доверия и метода временной централизации

Вышеописанная модель защищенного ИВ элементов группы БТС, включающая методы оценки доверия и репутации, обеспечивает защищенность ИВ элементов от воздействия деструктивного характера, направленного на нарушение семантики передаваемой информации. Защищенность группы БТС, основанной на данной модели, может быть повышена за счет внедрения методов аутентификации элементов в группе, построенной на основе Police Office Model (POM) и мобильной криптографии, а также шифрования любой передаваемой информации с использованием открытого ключа. На рисунке 15 при помощи стандарта UML представлена улучшенная модель защищенного ИВ элементов группы БТС.

Будем рассматривать последовательность действий БТС группы в контексте единичной итерации. Все БТС группы владеют некой “секретной” информацией, присущей только им, также все БТС группы имеют секретную информацию обо всех других БТС. Данная информация необходима для процессов аутентификации на протяжении всего времени функционирования агентов. Данная информация будет использоваться для регистрации агентов при миграции между областями, за безопасность которых ответственны соответствующие Police Office (PO) – локальные центральные элементы, ответственные за соответствующую область. Для обеспечения безопасности ИВ в группе необходимо назначить PO, ответственные элементов, мигрирующих в их области.

При миграции элемента e_j в новую область функционирования, PO_i, отвечающий за безопасность данной области, обязан зарегистрировать данный элемент, при условии, что он является доверенным (доверенный элемент – элемент, удовлетворяющий правилам безопасности, не являющийся угрозой для функционирования других элементов). Для установления доверенности e_i, PO_i посылает ему информационное сообщение, которое содержит функцию f, которую необходимо вычислить, основываясь на данных, хранящихся у e_j.

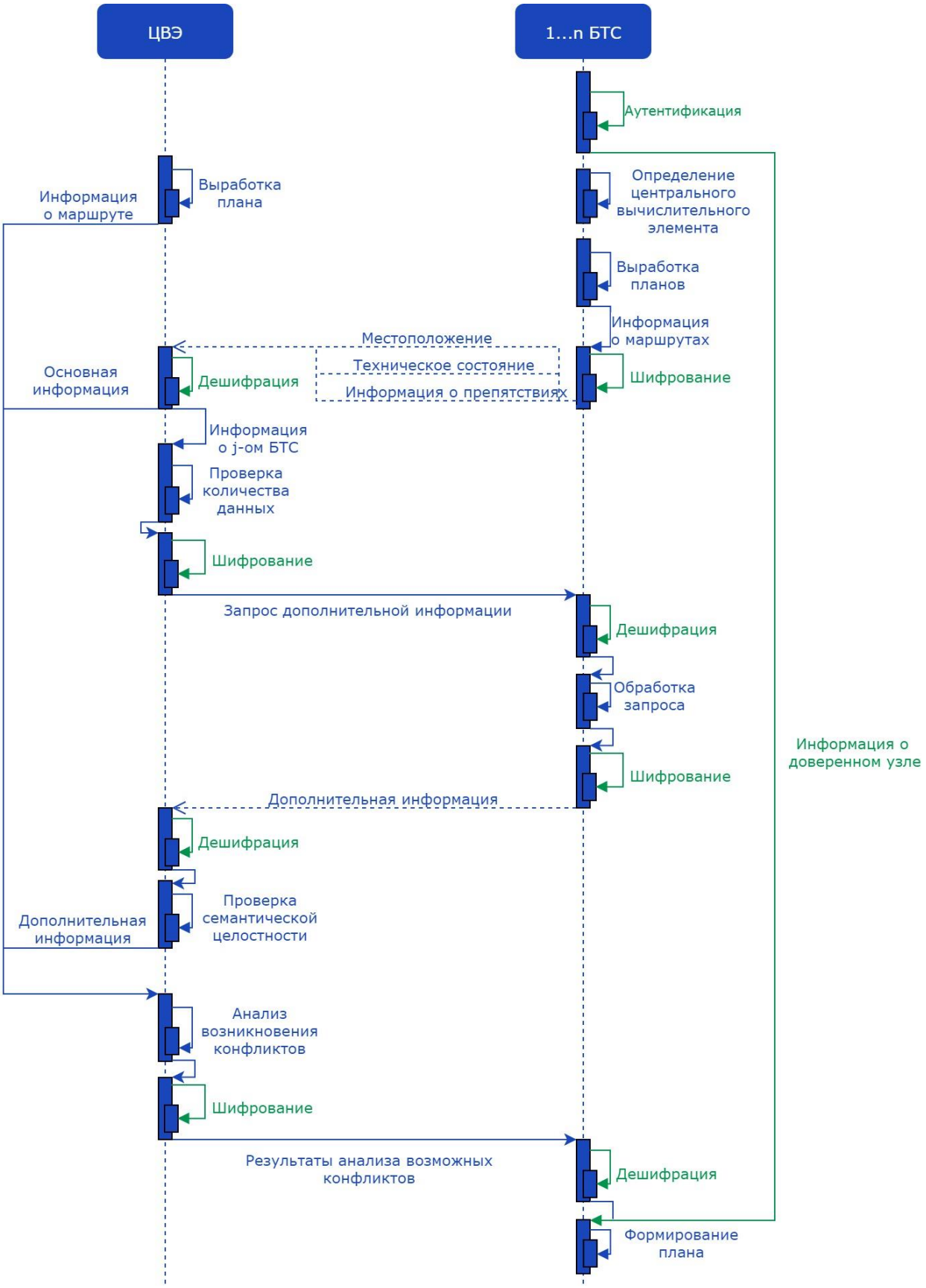


Рисунок 15. Диаграмма последовательности ИВ группы БТС в процессе функционирования с выполнением методов проверки семантической целостности информации, аутентификации и шифрования

Для обеспечения семантической целостности передаваемой функции, используется метод мобильной криптографии. Таким образом, происходит процесс шифрации функции – $E(f)$, после чего выполняется программа $P\big(E(f)\big)$, которую PO_i передает e_j.

Учитывая, что каждый элемент группы хранит “секретную” информацию x, присущую только ему и данной информацией владеют все остальные элементы группы, элемент, внедренный в группу БТС с целью деструктивного воздействия на ИВ элементов, не сможет реализовать деструктивные воздействия, поскольку не будет обладать данной информацией. e_j, получая информационное сообщение от PO_i, выполняет программу $P\left(E\big(f(x_j)\big)\right)$, используя свою “секретную” информацию и передает выполненную программу PO_i. Получив выполненную программу и произведя процесс дешифрации, PO_i имеет информацию $f(x_j)$, после чего извлекает “секретную” информацию x_j. В случае, если полученная от e_j информация совпадает с имеющейся у PO_i, элемент e_j считается доверенным. В случае, если полученная от e_j информация не совпадает с имеющейся у PO_i, агент e_j не считается доверенным, и PO_i оповещает всех доверенных элементов своего пространства об угрозе со стороны элементов e_j. Несовпадение полученных данных от e_j с имеющимися у PO_i может быть обусловлено несколькими факторами: была предпринята попытка нарушить семантическую целостность информационного сообщения или использована неверная “секретная” информация. Данные факторы приводят к неверному вычислению исходной функции f, в связи с чем элемент e_j не удовлетворяет заявленным правилам безопасности.

После процесса аутентификации БТС, как было описано в ранее введенной модели, выявляется ЦВЭ. Улучшенная модель защищенного ИВ группы БТС сохраняет процессы передачи информации, проверки и семантической целостности сообщений. Для ликвидации уязвимостей при

передаче информационных сообщений, предполагается использование криптосистемы с открытым ключом. При передаче информации между двумя БТС, используются открытый ключ x, который передается между БТС по незащищенному каналу, и зашифрованное информационное сообщение. При генерации ключа x, используются функции $y = f(id; s)$ и $y' = f(id'; s')$, где id и id' – идентификаторы БТС-отправителя и БТС-получателя соответственно. При отправке информационного сообщения, информация шифруется с помощью ключа x, который содержит электронную подпись (ЭП) отправителя – y. ЭП необходима для сравнения y и $f(id; s)$, что позволяет верифицировать отправителя. При получении информационного сообщения БТС-получателем, дешифрация происходит с использованием ключей x и s'. По аналогии с отправителем, высчитывается $f(id'; s')$ и сравнивается с y', что позволяет верифицировать получателя.

Выводы по главе 2

В главе 2 решены следующие задачи:

1. Предложена модель функционирования группы БТС на основе децентрализованной мультиагентной системы. В рамках предложенной модели группа БТС рассматривается как одноранговая сеть с точки зрения ИВ;
2. Определен класс мягких атак. Предложенное определение позволяет формализовать атаки на семантическую целостность информации в группе БТС;
3. Предложена модель обеспечения информационной безопасности. В контексте модели обеспечения информационной безопасности задача исследования сводится к разработке технических мер противодействия угрозам ИБ;
4. Сформулирована задача обеспечения семантической целостности инфомрации в группе БТС. Постановка задачи позволяет описать

гипотезы для проверки семантической целостности информации в группе БТС;

5. Предложена модель защищенного ИВ в группе БТС. Модель защищенного ИВ позволяет обеспечить ИБ в группе БТС.

Глава 3. Методы обеспечения информационной безопасности группы беспилотных транспортных средств

3.1 Метод обнаружения нарушений целостности информации на основе репутационных механизмов

Современные работы в области защиты информации от СДИВ, построенные на моделях репутации и доверия, рассматривают два показателя – доверие и репутация [121-143]. В общем случае, репутация является функцией, зависящей от доверия, вычисляемого в предыдущие моменты времени. В таком случае, обобщенный подход принятия решения о поведении БТС принимается на основе вычисления репутации. Следовательно, показатель доверия оказывает косвенное влияние на принятие решения относительно поведения БТС. При линейной функции оценки репутации поведение БТС может быть оценено неверно в некоторый момент времени, т.к. при продолжительном периоде наблюдений уровень репутации будет изменяться не достаточно быстро при резком изменении уровня доверия.

Одним из возможных подходов к решению данной проблемы является использование модифицированной системы показателей, также базирующейся на показателях доверия и репутации, к которым добавляется показатель оценки корректности информации в момент времени. При такой системе показателей требуется уточнить значения терминов. В работе предлагаются следующие определения приведенных показателей.

Определение 7: Истинность (*Truth*) – показатель, характеризующий субъективную оценку информации, предоставляемую объектом наблюдения субъекту, на основе сенсорных устройств.

Определение 8: Репутация (R) – показатель, сформировавшийся во времени и в процессе оценки $Truth$ агентом-субъектом агента-объекта.

Определение 9: Доверие (*Trust*) – показатель, основанный на оценке R и $Truth$ $f(R_{t-1}, Truth_t)$ и характеризующий субъективную оценку поведения агента-объекта агентом-субъектом.

Формализуя приведенные определения, можно представить их следующим образом:

$Truth_t = f_{tr_t}(information)$, где $Truth_t$ – показатель истинности в момент времени *t*, *information* – оцениваемая информация, f_{tr_t} – функция оценки истинности уровня доверия в момент времени *t*.

$R_t = f_{r_t}(Truth_t) = f_{r_t}\left(f_{tr_t}(information)\right)$, где R_t – показатель репутации в момент времени *t*, f_{r_t} – функция оценки значения уровня репутации в момент времени *t*.

$Trust_t = f_{trust_t}(R_{t-1}, Truth_t) =$

$f_{trust_t}\left(f_{r_{t-1}}\left(f_{tr_{t-1}}(information)\right), f_{tr_t}(information)\right)$, где $Trust_t$ – показатель доверия в момент времени *t*, f_{trust_t} – функция оценки значения уровня доверия в момент времени *t*.

В работе вводится ряд допущений, ограничивающих значения показателей истинности, репутации и доверия. Наивное предположение о возможных значениях приведенных показателей заключается в том, что каждый из представленных показателей может принимать два противоположных значения, условно выражаемых как «корректный» и «некорректный». Под «корректный» можно понимать такое значение показателя, при котором БТС-субъект оценки однозначно классифицирует действия БТС-объекта как корректное. При этом «некорректный» - такое значение показателя, при котором БТС-субъект оценки однозначно классифицирует действия БТС-объекта как некорректное. Таким образом, каждый показатель может принимать значения в диапазоне [0,1]. При этом значение показателей может не быть ни 0, ни 1. В таком случае, следует рассматривать поведение БТС в контексте поведения других БТС группы.

Допущение 1.1: $Truth \in [0,1]$

Допущение 1.2: $R \in [0,1]$

Допущение 1.3: $Trust \in [0,1]$

Предложенная модель ИВ БТС вовремя функционирования группы позволяет адаптировать описанную выше систему показателей для разработки модели защищенного ИВ группы БТС.

Предположим, $e \in E$, E_{nei_e} – множество БТС, взаимодействующих с БТС e. Тогда, предлагаемый метод доверия и репутации сводится к формированию векторов значений показателей истинности, доверии и репутации:

$\overline{Truth_e} = \begin{pmatrix} \dots \\ Truth_{e_i} \\ \dots \end{pmatrix}$, где $Truth_{e_i}$ – истинность информации, полученной от БТС e_i БТС e, $e_i \in E, e_i \neq e, i = 1 \dots |E|$;

$\overline{R_e} = \begin{pmatrix} \dots \\ R_{e_i} \\ \dots \end{pmatrix}$, где R_{e_i} – репутация БТС-объекта e_i, рассчитанная БТС $e, e_i \in E, e_i \neq e, i = 1 \dots |E|$;

$\overline{Trust_e} = \begin{pmatrix} \dots \\ Trust_{e_i} \\ \dots \end{pmatrix}$, где $Trust_{e_i}$ – доверие к БТС-объекту оценки e_i БТС $e, e_i \in E, e_i \neq e, i = 1 \dots |E|$.

Рассмотрим способы оценки показателей в рамках предложенных определений и допущений. Согласно допущению 1.1, показатель репутации может принимать значения от 0 до 1. Оценка истинности информации, передаваемой от БТС-объекта БТС-субъекту, основывается на пассивных знаниях, имеющихся у БТС-субъекта. Из ранее сказанного следует, что к пассивным знаниям может относиться информация, собранная при помощи сенсорных устройств БТС-субъекта или при помощи информации, переданной от других БТС, но также собранной при помощи сенсорных устройств. Кроме того, информация может быть проверена на основе других блоков информации, входящих во множество пассивных знаний. Проверка в данном случае будет заключаться в проверке соответствия полученной информации представлениям БТС-субъекта об окружающей среде. В таком

случае, БТС e может оценить показатель *Truth* как среднее значение показателей истинности для каждого блока информации, оцениваемой по различным блокам пассивных знаний, имеющихся у БТС e. В формализованном виде можно представить расчет данного показателя для БТС-объекта e_i БТС-субъектом e следующим образом:

$$\overline{\overline{Truth_e^s}} = \begin{pmatrix} Truth_{e_i}^{s_o} \\ \cdots \\ Truth_{e_i}^{s_{bl}} \end{pmatrix}$$

где bl – количество блоков информации, по которым производится оценка истинности информации. В таком случае, вектор оценок показателя истинности для всех БТС может быть представлен следующим образом:

$$\overline{\overline{Truth_e}} = \begin{pmatrix} \cdots \\ \frac{\sum_{j=1}^{bl} Truth_{e_i}^{s_j}}{bl} \\ \cdots \end{pmatrix}$$

где $Truth_{e_i}^{s_j}$ – оценка значения показателя истинности для БТС-объекта оценки e_i по блоку информации s_j. В общем случае, каждый блок информации оценивается как корректный или некорректный. Таким образом:

$$Truth_{e_i}^{s_j} = \begin{cases} 0\text{, если информация некорректная} \\ 1\text{, если информация корректная} \end{cases}$$

При такой оценке показателя истинности по блокам информации, показатель истинности для БТС-объекта будет принимать значения от 0 до 1. Однако когда БТС-субъект не имеет возможности оценить информацию, получаемую от БТС-объекта, либо не имеет устойчивого канала связи с ним, то оценка показателя истинности производится по усредненной оценке показателей, полученных от других БТС, проведших оценку БТС-объекта: $Truth_{e_{e_i}} = \frac{\sum Truth_{e_{j e_i}}}{n_{truth}}$, где $e \in E$ и $e_i \in E, n_{truth}$ - количество БТС, имеющих оценку истинности информации для БТС e_i. Если таких БТС нет, показатель истинности оценивается как 0.5, т.е. среднее значение, при котором информация не оценивается ни как корректная, ни как некорректная.

Гипотеза 1 (раздел 2.3) проверяется на основе показателя истинности. Гипотеза 2, представленная в разделе 2.3 может быть проверена при помощи показателя репутации. Линейная функция оценки репутации не позволяет корректно оценить поведение БТС, как было сказано ранее. При этом линейный рост показателя репутации корректен при увеличении показателя репутации БТС-объекта у БТС-субъекта. Рост показателя репутации означает, что показатель истинности получаемой информации от БТС-объекта оценивался положительно в каждый момент времени, предшествующий моменту расчета показателя репутации. Однако, при изменении оценки целостности информации, полученной от БТС-объекта, требуется значительно снизить показатель репутации. В качестве возможного способа расчета репутации в данном случае предлагается использовать функцию, основанную на функции распределения Вейбулла [165]. В таком случае, показатель репутации будет рассчитываться следующим образом:

$$R^{S}_{e_{e_{i_t}}} = \begin{cases} \sum_{k=1}^{t} R_{t-k} + Truth_t & , Truth_{e_{e_{i_t}}} \geq \alpha \\ \sum_{j=1}^{t-1} R_j - \left(\frac{\sum_{j=1}^{t-1} R_j}{t-1} - e^{-(1-Truth_t)t} \right) & , Truth_{e_{e_{i_t}}} < \alpha \end{cases}$$

где $Truth_{e_{e_{i_t}}}$ – показатель истинности информации, получаемой от БТС e_i БТС e в момент времени t, R_j – показатель репутации БТС-объекта в момент времени j.

В таком случае, показатель репутации не удовлетворяет допущению 1.2. Исходя из этого, $R^{S}_{e_{e_{i_t}}}$ рассматривается как промежуточный этап расчета показателя репутации. Для расчета показателя репутации требуется нормировать значение $R^{S}_{e_{e_{i_t}}}$ по времени. В таком случае, значение показателя репутации будет находиться в рамках допущения 1.2. В начальный момент времени функционирования группы БТС показатель репутации можно принимать равным показателю истинности, т.е. при $t = 0$, $R_{e_{e_{i_t}}} = Truth_{e_{e_{i_t}}}$.

Значение α, при котором уровень истинности является корректным, выбирается эмпирически. В общем случае, $\alpha = 0.5$.

Для проверки гипотезы 3 раздела 2.3 требуется провести ИВ с остальными БТС. Уровень репутации может быть рассчитан любым БТС для любого другого БТС, т.к. показатель истинности рассчитывается даже при отсутствии непосредственного взаимодействия с БТС-объектом оценки. Для проверки гипотез требуется получить информацию о значении показателя репутации оцениваемого БТС-объекта у других БТС-субъектов:

$$R_{e_{e_{i_t}}} = \frac{\sum_{t=1}^{|E|-1} R_{e_{j_{e_{i_t}}}}}{|E|}$$

где $e_j \in E, e_j \neq e_i$. В таком случае, показатель репутации будет строиться не только на основе собственных оценок БТС-субъекта, но и на основе оценок других БТС. Стоит отметить, что при отсутствии непосредственного взаимодействия БТС процесса оценки, данный подход позволяет уточнить значение показателя для БТС-объекта на основе вычисленных значений показателя репутации от других БТС, предположительно обладающих возможностью непосредственного взаимодействия с БТС-объектом. Однако, при расчете показателя репутации БТС-субъектом, обладающим возможностью непосредственного взаимодействия с БТС-объектом данный подход может быть излишним и использоваться для уточнения и проверки рассчитанного показателя репутации, но не оказывать непосредственного влияния на его расчет.

Однако самостоятельная проверка ни одной из гипотезы не может дать корректного результата оценки целостности информации. Для этого требуется использовать показатель доверия, являющийся функцией от двух других показателей, т.е. данный показатель должен быть способен оценить целостность информации при верности одних гипотез и ошибочности других. В таком случае, можно уменьшить вероятность ошибок первого и второго рода, т.к. количество критериев оценки возрастает.

Как было сказано ранее, функция оценки показателя доверия является функцией от двух параметров – значению показателя репутации за моменты время, предшествующие текущему моменту времени и значению показателя истинности в текущий момент времени:

$$Trust_{e_{e_{i_t}}} = f(R_{e_{e_{i_{t-1}}}}, Truth_{e_{e_{i_t}}})$$

Общая задача проверки доверия элемента-объекта сводится к проверке значения показателя относительно некоторого порогового значения:

$$Trust_{e_{e_{i_t}}} \geq \alpha_{trust}$$

Если данное условие выполняется, поведение БТС оценивается как корректное (без нарушений ИБ). В таком случае, информация, получаемая от БТС-объекта, оценивается БТС-субъектом как верная, без нарушений целостности. Функция расчета показателя репутации может быть представлена как функция, построенная на весовых коэффициентах. В таком случае, значение показателя истинности и показателя репутации учитываются при расчете показателя доверия с некоторыми коэффициентами, характеризующими влияние на рассчитываемое значение каждого из показателя. В обобщенном виде, данная функция может быть представлена следующим образом:

$$Trust_{e_{e_{i_t}}} = \gamma Truth_{e_{e_{i_t}}} + (1-\gamma) R_{e_{e_{i_{t-1}}}}, \text{где } \gamma \in [0,1], \text{где } \gamma -$$

коэффициент реактивности системы.

Однако, вычисление точных значений коэффициентов возможно при сборе множественной статистики, что позволит эмпирически установить такие значения коэффициентов, при которых результат расчета показателя доверия сможет корректно охарактеризовать поведение БТС-объекта. В работе рассматривается еще один способ оценки показателя доверия, основанный на относительном расположении элемента на плоскости с измерениями – истинность и репутация.

$$Trust_{e_{e_{i_t}}} = \sqrt{(R_{min} - R)^2 + (T_{min} - Truth)^2} - \sqrt{(R_{max} - R)^2 + (T_{max} - Truth)^2}$$

В качестве значения показателей R_{min} и T_{min} принимается 0, т.к. БТС, находящийся на плоскости истинность/репутация в точке (0,0) однозначно может быть классифицирован как БТС с некорректным поведением. БТС, находящееся в точке (1,1), однозначно классифицируется как БТС с корректным поведением, тогда R_{max} и T_{max} равняются 1. В таком случае, поведение БТС будет считаться корректным, если значение показателя доверия больше 0.

Подход, основанный на расчете показателя доверия, как расстоянии на плоскости, позволяет строить универсальный показатель без наличия значительного массива информации, т.е. данный подход позволяет рассчитывать показатель доверия в любой момент времени без предварительного поиска оптимальных значений коэффициентов.

Ранее говорилось о том, что показатель доверия позволяет сократить вероятность ошибок первого и второго рода. Однако свести данную вероятность к нулю не представляется возможным, если рассматривать одноранговую сеть, когда все элементы имеют равные права и обязанности, а также оценки, определенные каждым элементом, являются равными. В таком случае, можно искусственно изменить структуру сети с целью выделения элементов, чьи оценки обладают повышенным весом при оценке других элементов. Такой подход схож с моделью полицейских участков, когда некоторые элементы находятся выше в иерархии элементов системы и именно их оценки определяют корректность или некорректность поведения других элементов системы, т.е. на основе их наблюдений и вычислений определяются возможные нарушения ИБ [171, 172].

3.2 Метод временной централизации

Временное изменение иерархии группы БТС позволяет использовать преимущества централизованных систем [173], но минимизировать

присущие им риски. Такой эффект достигается за счет ограничения времени, когда один из элементов системы является ЦВЭ.

Организация функционирования группы БТС, разработка планов действий и организация ИВ БТС может быть осуществлена на основе трех различных подходов, основывающихся на принципах децентрализации системы. К таким подходам относятся: децентрализованный подход, централизованный подход и подход на основе временной централизации. Основываясь на модели функционирования группы БТС, представленной в разделе 2.1, данные подходы можно также называть:

1. ИВ без посредников;
2. ИВ при помощи заранее определенных посредников;
3. ИВ при помощи посредников, определяемых на основе состояния группы.

Подобные названия подходов более полно характеризуют отличия подходов друг от друга. Подходы основываются на возможности естественной или искусственной декомпозиции группы БТС на подгруппы. Естественная декомпозиция группы БТС на подгруппы подразумевает разделение группы на подгруппы, исходя из принципов, изложенных в разделе 2.1. Однако, возможна ситуация, при которой принципы, изложенные в разделе 2.1, не позволяют разделить группу на подгруппы, но количество БТС группы не позволяет должным образом оценить поведение БТС одним БТС, т.е. невозможно однозначно определить нарушение ИБ из-за значительных вычислительных требований, либо данная процедура занимает значительное время, что также нарушает работоспособность системы. В таком случае, можно говорить об искусственной декомпозиции, когда БТС выделяются в подгруппу не только на основе принципов ИВ, но и на основе введенной функции принадлежности БТС подгруппе. В таком случае, количество подгрупп определяется на основе количества БТС в группе, доступных вычислительных мощностей, типа системы, однородности БТС и т.д. Функция принадлежности также определяется на основе приведенных

выше факторов. Таким образом, принадлежность БТС некоторой подгруппе может быть выражена следующим образом:

$$E_i = \{(e, \mu_{E_i}(e)) | e \in E\}$$

Предположим, что требуется выделить две подгруппы $E_i, E_j \in E$. В таком случае, $\mu_{E_i}(e) = 0, \mu_{E_j}(e) = 1 \Leftrightarrow \left(e, \overline{\mu_{E_i}(e)}\right), \left(e, \overline{\mu_{E_j}(e)}\right)$ и $\overline{\mu_{E_i}(e)} < \overline{\mu_{E_j}(e)}$. Такой подход позволяет однозначно отнести БТС к той или иной подгруппе. Необходимо рассмотреть принципы подходов на основе ранее введенных обозначений, ограничений и определений.

Рассмотрим группу БТС, декомпозированную на две подгруппы $E_i, E_j \in E$. Пусть $e_l \in E_i, e_k \in E_j$. Предположим, БТС e_l не имеет устойчивого канала связи ни с одним из БТС подгруппы E_j.

При ИВ без посредников, БТС e_l пытается самостоятельно установить канал связи с подгруппой E_j. Рассмотрим группу E, в которой каждый БТС составляет отдельную подгруппу. На рисунке 16 представлен общий вид группы и существующих каналов связи в момент начала функционирования.

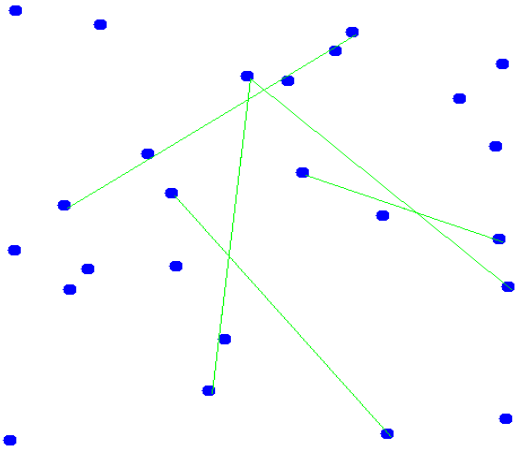


Рисунок 16. Возможное представление группы БТС и существующих каналов связи в момент начала функционирования. БТС представлены точками, существующие каналы связи – зелеными линиями

В таком случае, БТС e_l опрашивает все БТС группы, с которыми возможно ИВ. В случае если опрашиваемый БТС e_k относится к подгруппе, с БТС которой необходимо установить устойчивый канал связи, e_l может

начать ИВ с этим БТС, что позволит получить все знания, имеющиеся у БТС подгруппы E_j. ИВ БТС в процессе функционирования представлено на рисунке 17.

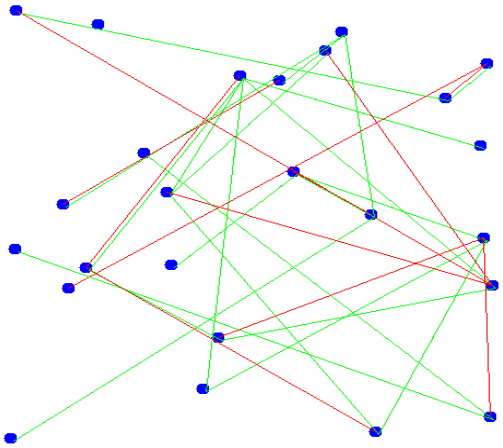


Рисунок 17. Возможное представление группы БТС и существующих каналов связи во время функционирования. Красные линии – передача информационных сообщений по существующим каналам связи

Последнее утверждение верно, если БТС подгруппы E_j осуществляют ИВ между собой. На следующих итерациях, БТС e_l знает о принадлежности всех БТС, входящих в другие подгруппы и опрошенных вовремя предыдущих итераций. На рисунке 18 представлена схема существующих каналов связи после нескольких итераций.

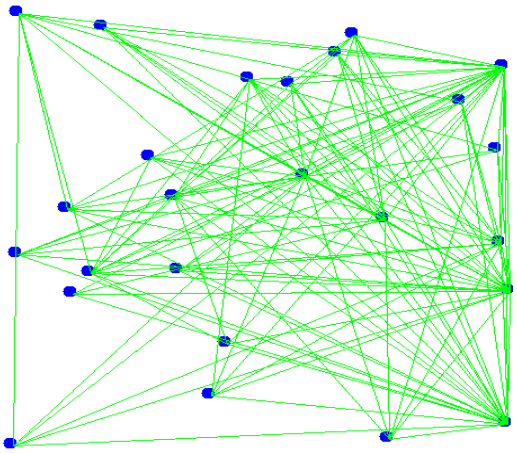


Рисунок 18. Возможное представление группы БТС и существующих каналов связи после нескольких итераций

ИВ при помощи заранее определенных посредников подразумевает централизацию системы на основе функции принадлежности. Пусть $\forall e_o \in$

E_i: $\overline{\mu_{E_i}(e_l)} > \overline{\mu_{E_i}(e_o)}$, где $e_l \in E_i$. В таком случае, можно говорить о том, что БТС e_l является ЦВЭ подгруппы, т.е. таким элементом, который осуществляет выработку планов действий других БТС, проверяет состояние ИБ подгруппы и является посредником при осуществлении ИВ между БТС, как различных подгруппы, так и БТС одной подгруппы. Рассмотрим данный подход на основе группы БТС с четырьмя выделяемыми подгруппами. На рисунке 19 представлена группа БТС и возможное расположение БТС.

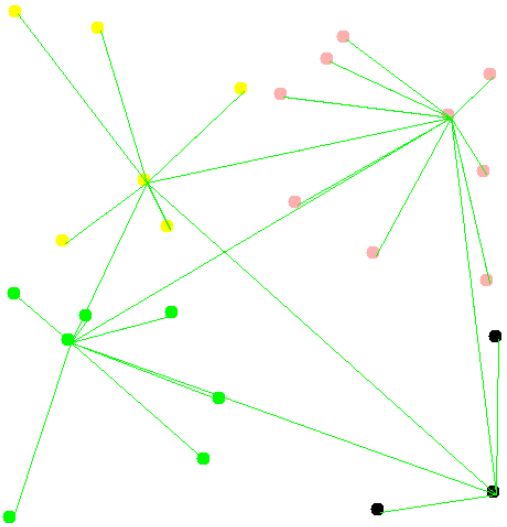


Рисунок 19. Возможное представление группы БТС и существующих каналов связи в момент начала функционирования. БТС представлены точками различных цветов (БТС одного цвета относятся к элементам одной подсистемы), существующие каналы связи – зелеными линиями

В данном примере, значение функции принадлежности определяется на основе расположения БТС подгруппы – ближайший к центру подгруппы БТС является ЦВЭ подгруппы. На рисунке 20 представлена схема конфигурации группы БТС после нескольких итераций.

Таким образом, структура и количество каналов связи, характеризующих группу БТС, не меняется с течением времени. Можно говорить об устойчивой иерархии БТС при отсутствии изменений в организационной структуре группы. Такой подход является частным случаем подхода, основанного на посредниках, определяемых на основе свойств группы. Если функция принадлежности при данном подходе выбрана таким

образом, что она не изменяется при изменениях группы, происходящих в процессе функционирования, принцип организации ИВ БТС не отличается от принципа организации ИВ БТС при помощи заранее определенных посредников.

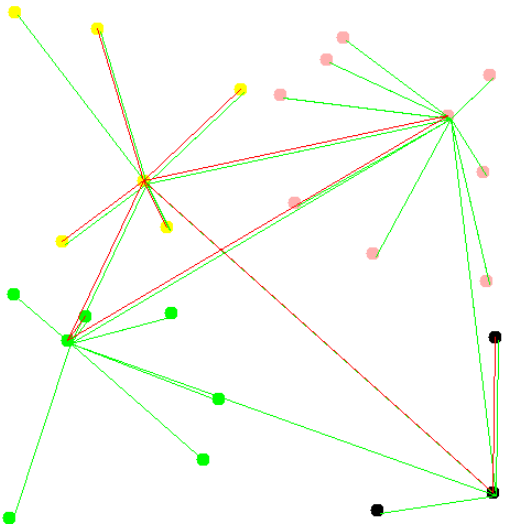


Рисунок 20. Возможное представление группы БТС и существующих каналов связи после нескольких итераций при организации функционирования на основе ИВ при помощи заранее определенных посредников

Однако, при определении функции принадлежности на основе факторов, меняющих ее значение при изменении свойств группы БТС, можно говорить о том, что подход с использованием посредников, определяемых на основе свойств группы, будет иметь ряд отличий от централизованного подхода. Далее рассматривается пример на основе группы с тремя выделяемыми подгруппами. Схема такой группы представлена на рисунке 21.

Таким образом, все БТС подгруппы могут осуществлять ИВ с другими БТС подгруппы без посредников. В таком случае, каждую итерацию определяется новый ЦВЭ подгруппы. Такое БТС определяется на основе расчета функции принадлежности, которая зависит от заранее определенных факторов. Выбранные факторы для расчета функции принадлежности должны определяться таким образом, чтобы функция принадлежности

изменяла свое значение при изменении характеристик группы в процессе функционирования.

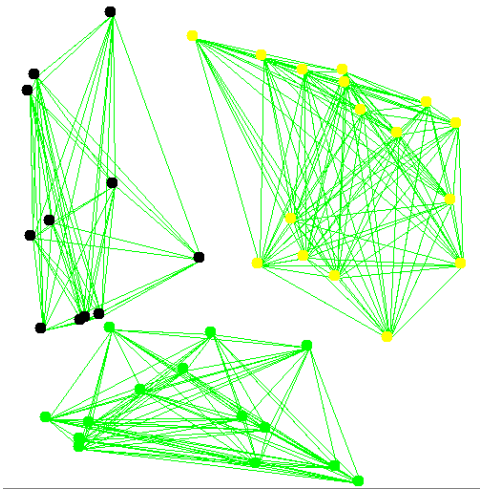


Рисунок 21. Возможное представление группы БТС и существующих каналов связи в момент начала функционирования. БТС представлены точками различных цветов (БТС одного цвета относятся к одной подгруппе), существующие каналы связи – зелеными линиями

В таком случае, каждую итерацию будет определяться новый посредник, при помощи которого осуществляется ИВ как в рамках одной подгруппы, так и между подгруппами. Каждую итерацию выбранный посредник будет осуществлять ИВ с теми подгруппами, с которыми требуется осуществить ИВ другим БТС подгруппы. Если у выбранного БТС имеется устойчивый канал связи, он сразу осуществляет ИВ с подгруппой. Если канал связи отсутствует, посредник выполняет ИВ способом, аналогичным способу ИВ без посредников. Рисунок 22 демонстрирует каналы связи и группу после нескольких итераций при использовании описанного подхода.

Различные подходы к организации ИВ группы БТС определяют порядок применения ранее представленного метода доверия и репутации. При использовании посредников для осуществления ИВ, посредник должен контролировать целостность циркулирующей в группе информации. Таким образом, система становится централизованной с точки зрения обеспечения

ИБ. При использовании децентрализованного подхода каждое БТС отвечает за проверку целостности информации, получаемой от других БТС.

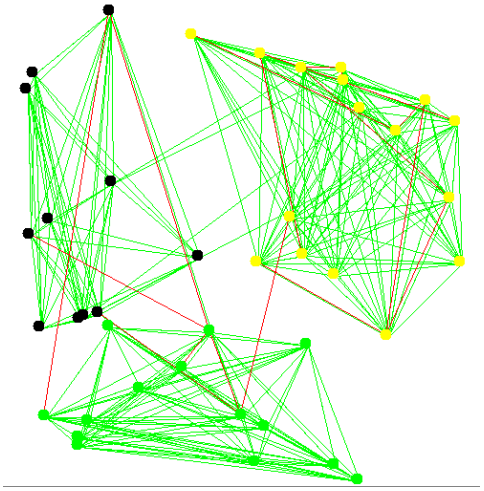


Рисунок 22. Возможное представление группы БТС и существующих каналов связи после нескольких итераций при организации функционирования на основе ИВ при помощи посредников, определяемых на основе свойств группы

Для выбора подхода к организации ИВ группы требуется оценить затраты вычислительных ресурсов при использовании того или иного подхода, а также оценить вероятность ошибок при оценке защищенности группы с точки зрения ИБ.

Выводы по главе 3

В главе 3 решены следующие задачи:

1. Предложен метод обнаружения нарушений семантической целостности на основе репутационных механизмов. Предложенный метод основан на трех показателях – истинности, репутации и доверия. Показатель доверия является показателем, на основе значения которого принимается решение относительно семантической целостности информации;

2. Предложен метод временной централизации группы БТС. Метод централизации позволяет использовать централизованное управление группой БТС для повышения продуктивности методов обеспечения ИБ.

Глава 4. Проверка продуктивности методов обеспечения информационной безопасности и моделей защищённого информационного взаимодействия группы беспилотных транспортных средств

4.1 Проверка продуктивности метода доверия и репутации

К свойствам, характеризующим БТС, можно отнести такие свойства, как:

1. скорость движения;
2. запас энергии;
3. расход энергии;
4. дальность действия сенсорных устройств;
5. дальность действия модулей связи и т.д.

Перечисленные выше свойства можно отнести к базовым свойствам для любых БТС. Основной особенностью БТС, присущей каждому БТС, является возможность менять свое положение в пространстве путем выполнения элементарных действий при помощи ФУ. В таком случае, простейшая задача, исполняемая БТС, является достижение некоторой определённой области пространства группой БТС. Для проверки предложенных в разделе 3.1 и 3.2 методов будет рассматриваться выполнение БТС задачи достижения области местности без дополнительных ограничений, накладываемых на перемещение в пространстве.

Необходимо отметить, для проверки продуктивности предложенных ранее методов особые требования к выполняемым задачам отсутствуют, т.к. тип выполняемых задач не накладывает ограничения на их выполнение. Однако тип задач может изменить способ проверки истинности информации, т.е. сравнение получаемой информации от других БТС зависит от типа задач, т.к. в зависимости от области применения БТС могут разниться свойства

БТС, следовательно, проверка данных может осуществляться на основе различных информационных блоков.

Рассматривая БТС с задачей достижения участка местности, проверка истинности будет заключаться в анализе местоположения других БТС. Кроме того, может быть осуществлена проверка согласно имеющимся у БТС знаниям. К таким знаниям можно отнести информацию, связанную с запасом энергии других БТС, рассчитываемым на основе предыдущих шагов. Для упрощения необходимых расчетов, будет рассматриваться гомогенная группа, т.е. такая группа, БТС которой будут обладать одинаковыми физическими характеристиками (скорость движения, радиус действия сенсорных устройств и т.д.). Дополнительным ограничением для проведения рассматриваемых экспериментов будет равный запас энергии БТС в момент инициализации эксперимента. Также, метод доверия будет применяться только для проверки целостности информации при ИВ БТС информационного уровня. Такой подход позволит оценить продуктивность предложенного метода без дополнительных условий, накладываемых на алгоритм расчета показателя доверия, из-за различных информационных блоков, имеющихся у БТС на данном уровне.

Для проведения эксперимента было разработано специализированное инструментальное средство, позволяющее провести имитационное моделирование функционирования БТС [174-177]. Разработанное инструментальное средство предоставляет возможность варьировать количество БТС системы, создавать задачи для БТС, изменять параметры БТС и некоторые условия окружающей среды, а именно – размер полигона, количество и тип препятствий. Под параметрами БТС понимаются:

1. затраты на прохождение единицы расстояния;
2. запас энергии;
3. радиус работы модулей связи;
4. дистанция работы сенсорных устройств.

Проведение анализа продуктивности метода доверия основывается на серии эмпирических наблюдений, собранных при проведении экспериментов в следующих условиях:

1. общее число БТС – 1000 элементов;
2. общий процент нарушителей – от 0% до 40% от общего числа БТС;
3. количество уровней задач – от 1 до 100;
4. количество задач на одном уровне – от 2 до 10;
5. необходимое количество элементов для выполнения одной цели – от 1% до 10% на одну цель.

Под нарушителем понимается такое БТС, поведение которого отличается от поведения других БТС группы только целостностью передаваемой информации, т.е. семантическая целостность передаваемых данных будет нарушена. Основная информация, циркулирующая в данной группе, представляет собой собственную оценку затрат БТС на выполнение задачи (прибытия в определённую область). Таким образом, БТС-нарушитель нарушает целостность информации о предполагаемых затратах на выполнение задач. Исходя из упрощения о гомогенности группы, каждый БТС (БТС-субъект) может определить затраты другого БТС (БТС-объекта) на выполнение задачи. Если БТС-объект находится в зоне действия сенсорных устройств БТС-субъекта, возможно проведение оценки стоимости выполнения задач без непосредственного ИВ с БТС-объектом. В таком случае, объект может быть отнесён к нарушителям или обычным БТС.

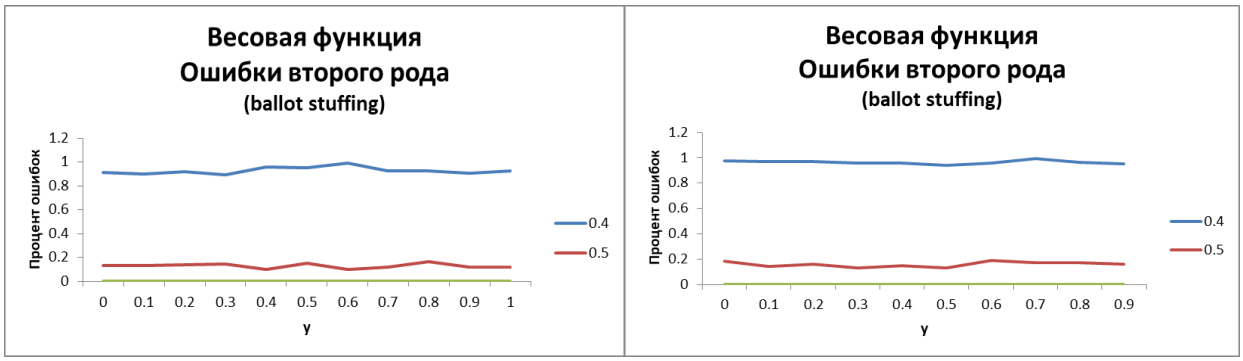
Возможность непосредственной оценки не всегда имеется у БТС. Более того, не всегда имеется возможность провести оценку показателя истинности на основе значения данного показателя у других БТС. В результате, возможна ситуация, при которой корректно действующий БТС считается нарушителем. В таком случае, можно говорить об ошибке первого рода, когда гипотеза об отсутствии нарушения целостности информации ошибочно отвергается, т.е. обычное БТС не участвует в выполнении задач. Таким

образом, уменьшается работоспособность группы, т.е. может быть выполнено меньшее количество задач. Однако, в общем случае, возможно оценить количество задач, которые будут выполнены. При возникновении ошибок второго рода невозможно однозначно утверждать о гарантированном выполнении задач. Под ошибками второго рода понимается ошибочное принятие гипотезы, т.е. поведение нарушителя классифицируется как корректное поведение (целостность передаваемой информации считается не нарушенной). Наличие ошибок второго рода подразумевает, что за выполнение задачи будет отвечать такое БТС, который может ее не выполнить (нарушитель). Однако нарушитель может выполнить цель, но затратить большее количество энергии. Следовательно, точно определить количество задач, которые будут выполнены, не представляется возможным. Таким образом, повышение вероятности выполнения задач в случае СДИВ может трактоваться как уменьшение вероятности ошибок второго рода при проверке гипотезы о целостности информации, передаваемой БТС.

Таким образом, под продуктивностью предложенных методов понимается вероятность появления ошибок первого и второго рода. В разделе 3.1 было предложено два возможных подхода к расчёту показателя доверия БТС-объекта. Для сравнения их продуктивности были проведены эксперименты при помощи описанного выше инструментального средства и определены вероятности возникновения ошибок первого и второго рода.

В качестве первой группы экспериментов предлагается оценить пороговое значение показателя доверия, при котором БТС-субъект оценивает БТС-объект как надежный. Рассматриваться будет три типа основных атак – bad mouth, ballot stuffing и on_off.

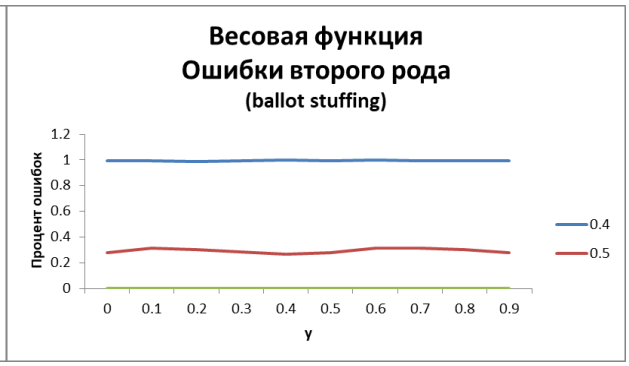
Результаты экспериментов, проведенных в приведенных выше условиях, представлены на рисунке 23.



а)

б)

в)



г)

д)

Рисунок 23. Ошибки второго рода для различных пороговых значений показателя доверия. а – процент диверсантов 5%, б – процент диверсантов 10%, в – процент диверсантов 20%, г – процент диверсантов 30%, д – процент диверсантов 40%

В рамках оценки функционирования метода доверия и репутации при использовании весовой функции не рассматриваются значения пороговых значений для показателя доверия больше 0,5 и меньше 0,4, т.к. в рамках данных значений процент ошибок равен 0% и 100% соответственно. Таким образом, в рамках противодействию атакам типа ballot stuffing

представляется верным использовать коэффициент не менее 0,5. При использовании коэффициента 0,6 и более, значительно растет процент ошибок первого рода, что показано на рисунке 24.

Для определения унифицированных значений параметров функционирования метода доверия требуется проанализировать процент ошибок второго и первого рода для различных атак. В таком случае, возможно определить такие параметры функционирования, при которых параметры функционирования позволят противодействовать различным атакам. На рисунке 25 представлены проценты ошибок второго рода для различных процентов нарушителей, действующих в рамках сценария атак on-off. На рисунке 26 представлены проценты ошибок второго рода для различных процентов нарушителей, использующих атаку bad mouth.

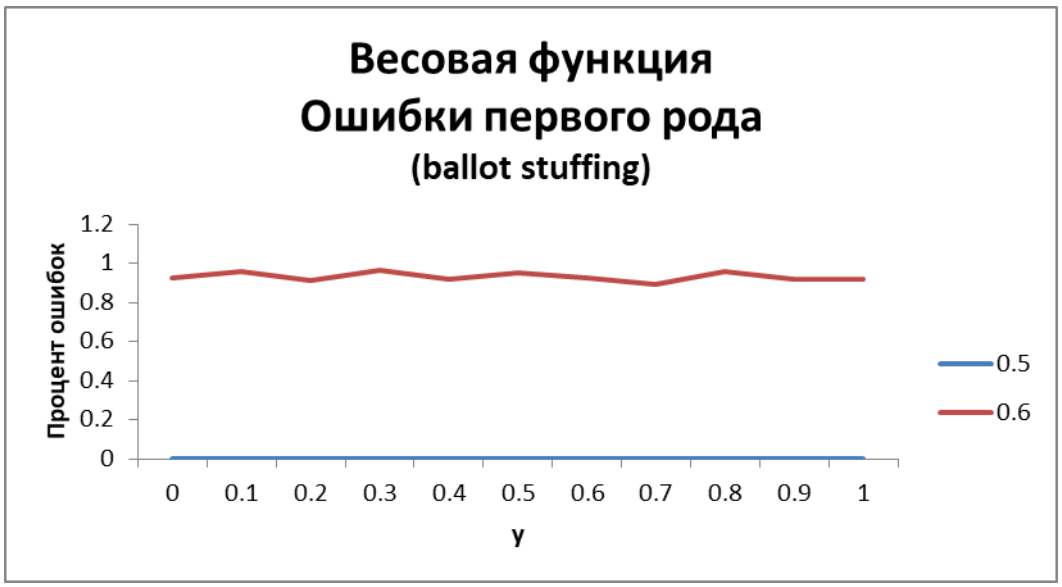
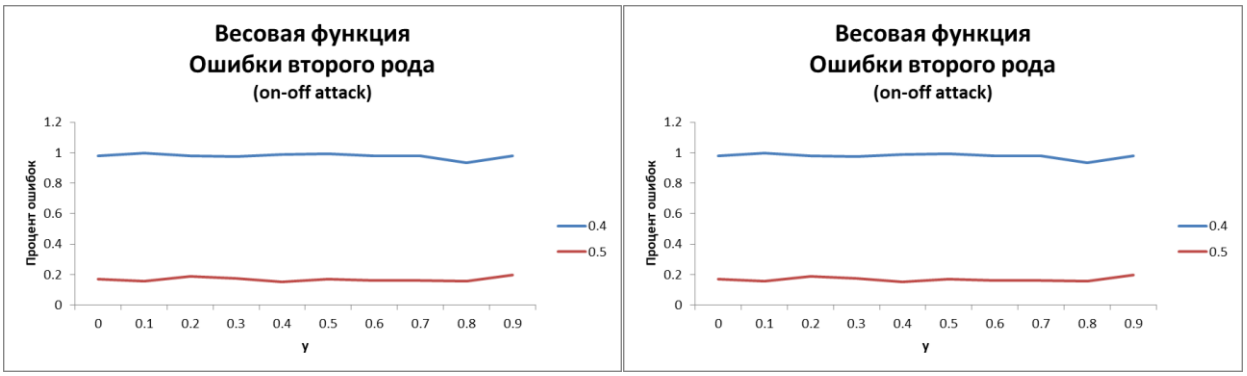
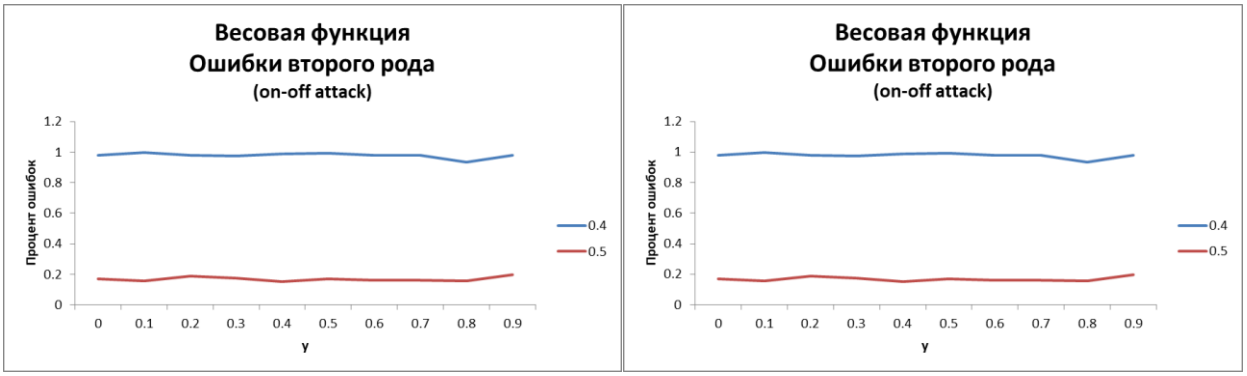


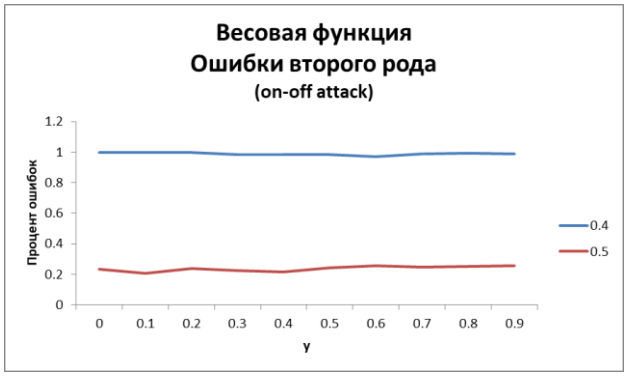
Рисунок 24. Ошибки первого рода для различных пороговых значений показателя доверия



а) б)

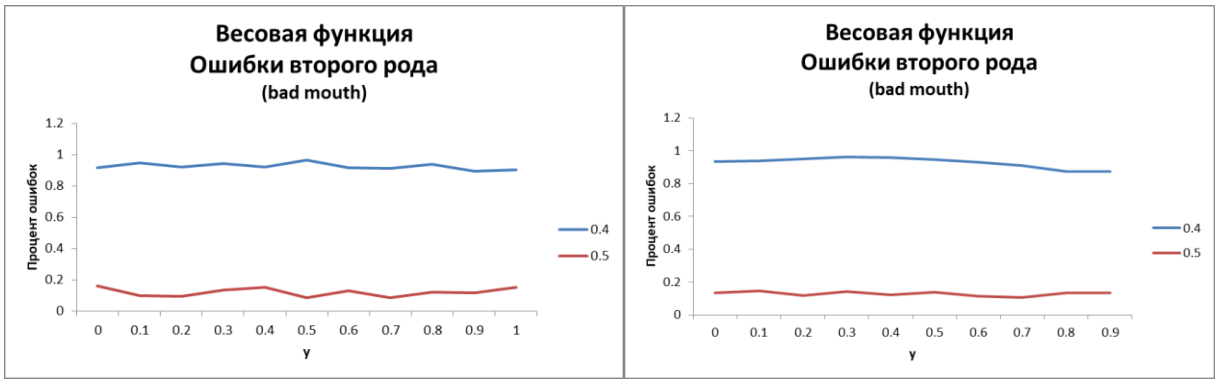


в) г)

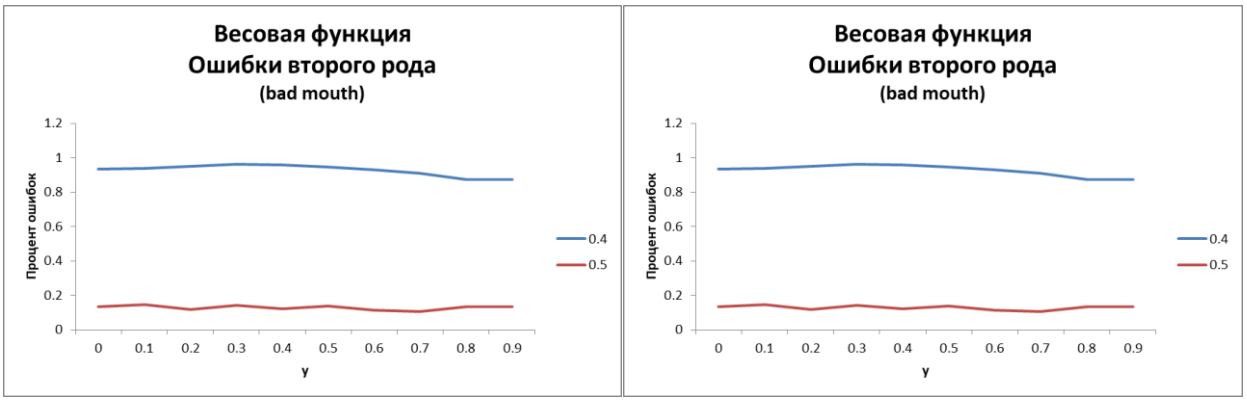


д)

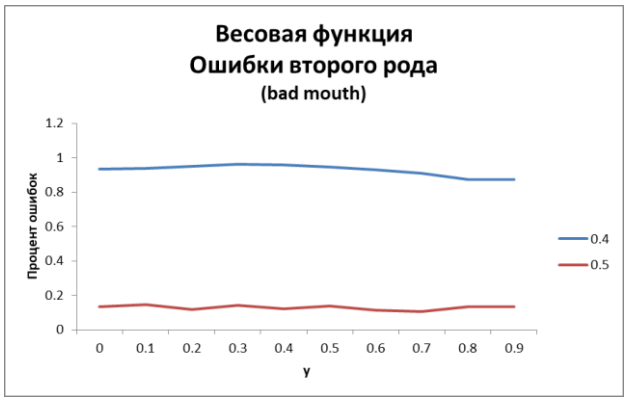
Рисунок 25. Ошибки второго рода для различных пороговых значений показателя доверия при атаках on-off. а – процент диверсантов 5%, б – процент диверсантов 10%, в – процент диверсантов 20%, г – процент диверсантов 30%, д – процент диверсантов 40%



а) б)



в) г)



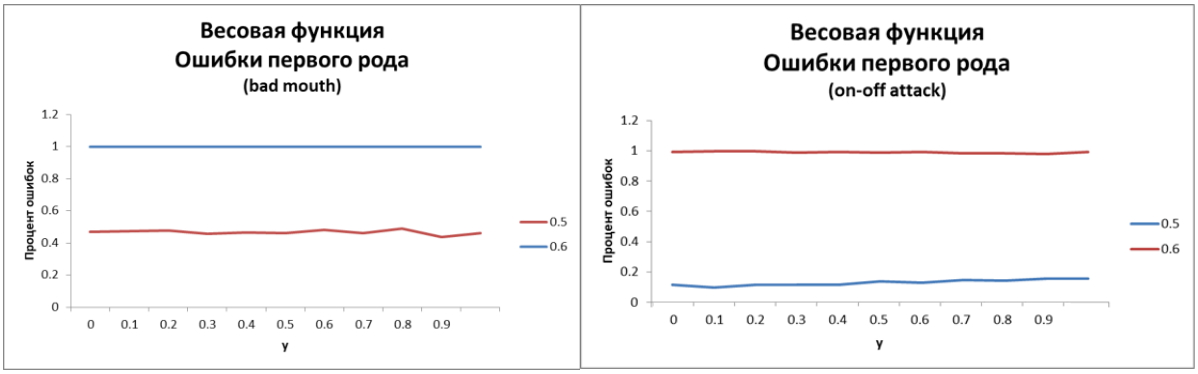
д)

Рисунок 26. Ошибки второго рода для различных пороговых значений показателя доверия при атаках bad mouth. а – процент диверсантов 5%, б – процент диверсантов 10%, в – процент диверсантов 20%, г – процент диверсантов 30%, д – процент диверсантов 40%

Исходя из выше представленных графиков, пороговое значение должно быть выше 0,5. Для уточнения верхней границы значения показателя порогового значения требуется провести анализ ошибок первого рода. На

рисунке 27 представлены проценты ошибок первого рода для атак bad mouth и on-off.

На основе продемонстрированных графиков можно сделать вывод, что в рамках весовой функции для метода доверия и репутации требуется использовать пороговое значение не менее 0,5 и не более 0,6.



а) б)

Рисунок 27. Ошибки первого рода для различных пороговых значений показателя доверия, а – для атак bad mouth, б – для атак on-off

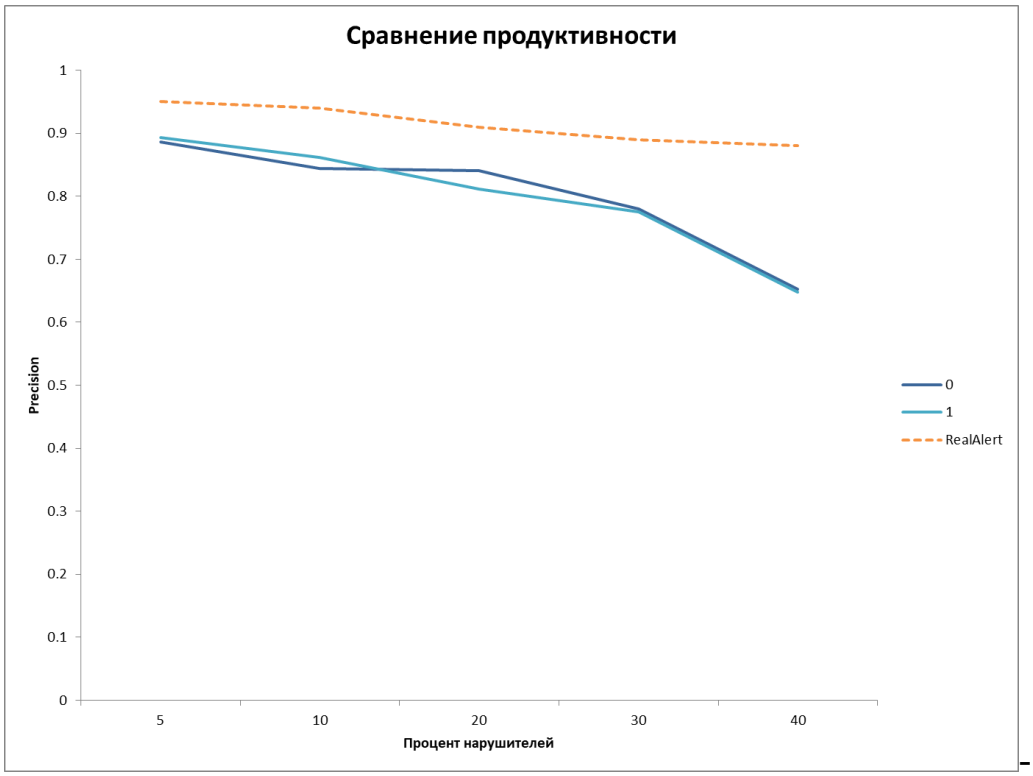
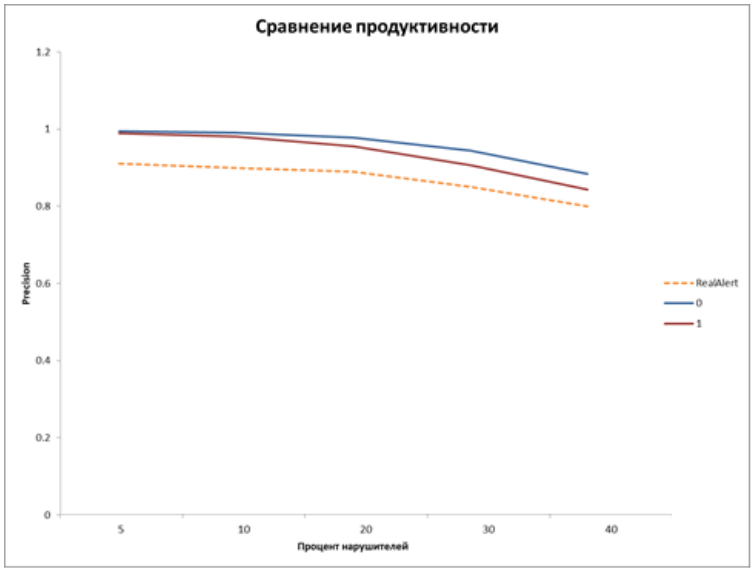
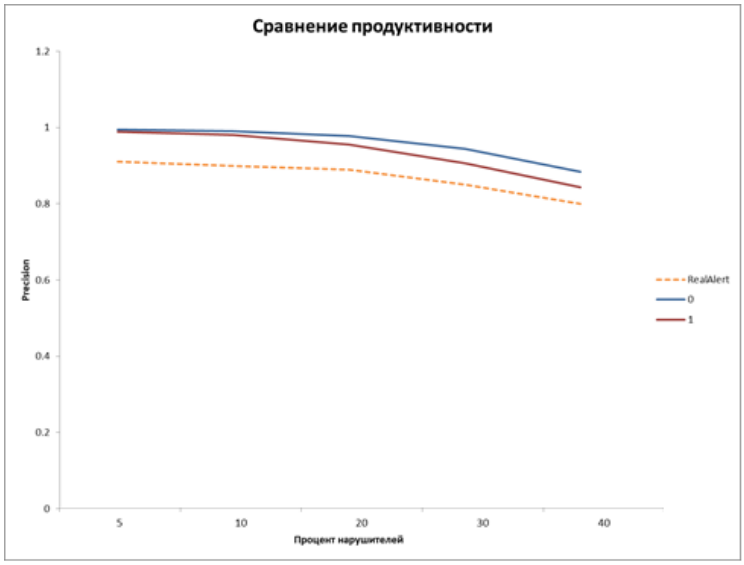


Рисунок 28. Сравнение с результатом применения метода RealAlert для атак ballot stuffing

Сравнение результатов функционирования (рисунок 28) метода весовой функции с методом RealAlert позволяет говорить о том, что показатель precision для разработанного метода и значения пороговой функции равным 0,5 меньше, чем у сравниваемого метода. Однако показатель recall демонстрирует лучший результат, т.к. для предлагаемого метода доверия он равен 1, а для метода RealAlert – менее 0,9.



а)



б)

Рисунок 29. Сравнение с результатом применения метода RealAlert для атак: а – on-off, б – bad mouth

На рисунке 29 представлены результаты функционирования метода доверия и репутации при проведении атак on-off и bad mouth соответственно. Исходя из этих данных, можно говорить о продуктивности предложенного метода по сравнению с существующими методами.

Приведенные эксперименты определяют продуктивность метода доверия и репутации только при применении весовой функции. Для оценки метода на основе метрической функции, требуется провести эксперименты на основе метрической функции. На рисунке 30 представлено схематичное отображение расположения БТС по показателю доверия в пространстве истинность/репутация.

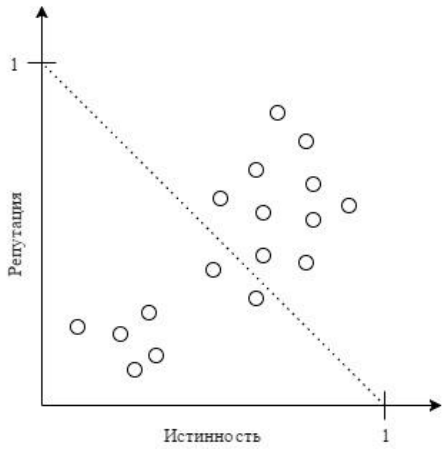


Рисунок 30. Возможное расположение БТС в пространстве истинность/репутация

В таком случае, нарушителями являются те БТС, значения доверия которых будет ниже диагонали, изображенной пунктирной линией на рисунке 30. Одним из вариантов расчета данного показателя является расчет расстояния от текущего положения БТС в пространстве до максимальных/минимальных значений. Под максимальным значением понимается положение БТС, при котором значение показателя репутации равняется 1 и значение показателя истинности равняется 1. На рисунке 31 представлено расположение БТС, обладающих максимальным/минимальным значением.

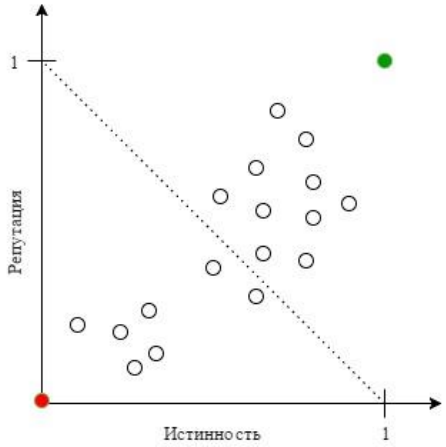
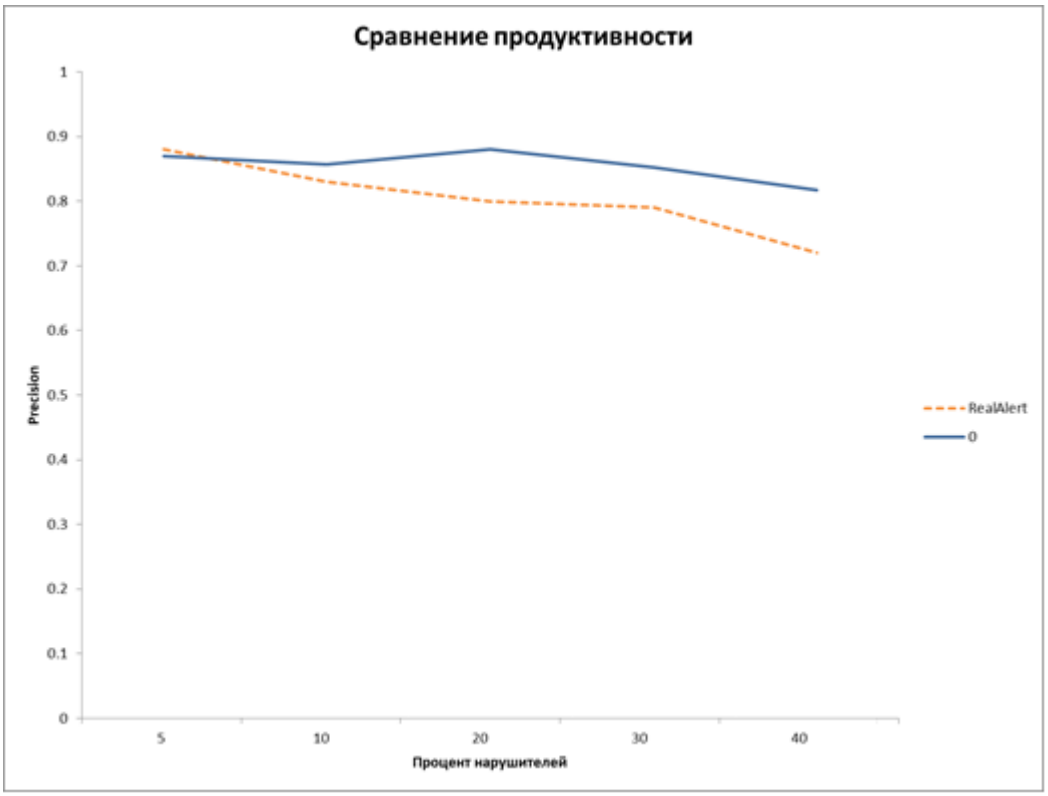


Рисунок 31. Возможное расположение БТС в пространстве истинность/репутация. Зеленым выделен БТС, имеющий значения репутации и истинности, равные 1; красным выделен БТС, имеющий значения репутации и истинности, равные 0

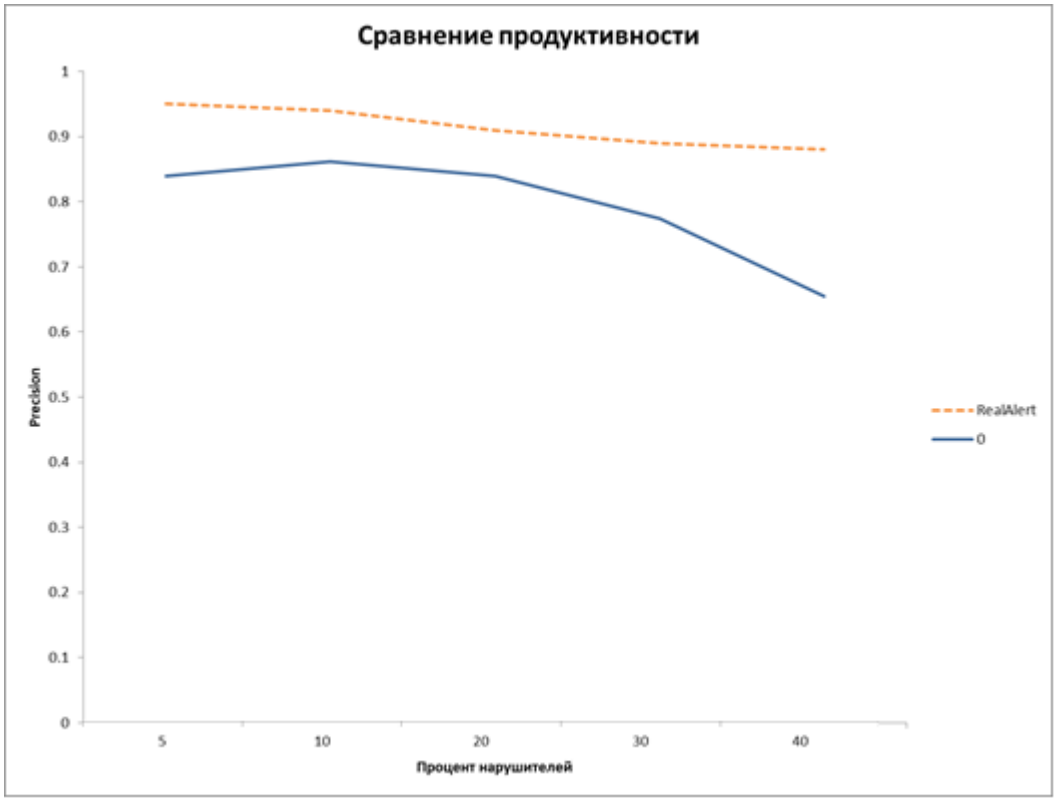
В таком случае, в формуле (2) минимальные и максимальные значения заменяются на 0 и 1 соответственно. Тогда формула (2) приобретает вид:

$$Trust_{e_{e_{i_t}}} = \sqrt{(0-R)^2 + (0-Truth)^2} - \sqrt{(1-R)^2 + (1-Truth)^2}$$

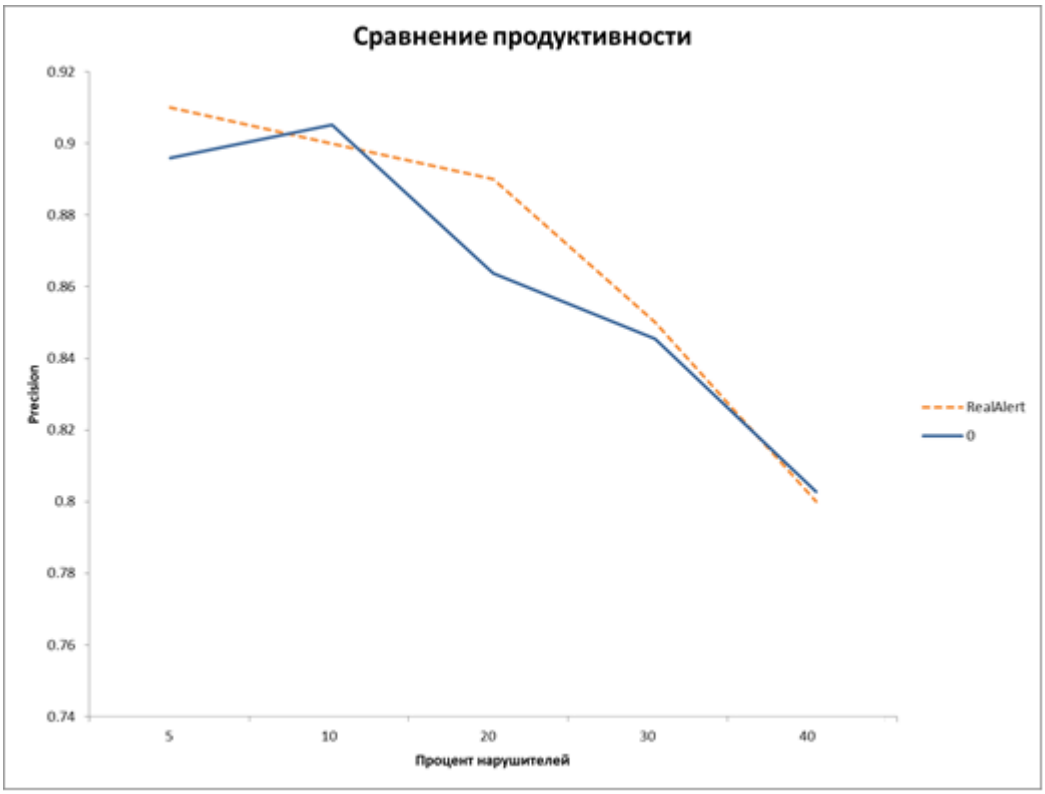
При таком подходе к определению показателя доверия, ошибкой второго рода является классификация поведения БТС как корректная при нахождении БТС ниже диагонали. Ошибка первого рода – классификация поведения БТС как некорректная при нахождении БТС выше диагонали. В разделе 3.1 говорилось о том, что показатель доверия должен быть больше 0, чтобы классифицировать поведение БТС как корректное. Однако, возможно изменение данного значения: при снижении порогового значения (показатель доверия может быть меньше 0, но информация, получаемая от БТС, будет признана целостной) снижается вероятность ошибки первого рода, но повышается вероятность ошибки второго рода. При увеличении порогового значения – повышается вероятность ошибки первого рода, но снижается вероятность ошибки второго рода. На рисунке 32 представлено изменение вероятности ошибки первого и второго рода при изменении порогового значения для показателя доверия.


Сравнение продуктивности
Precision
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
5
10
20
30
40
Процент нарушителей
RealAlert
0

а)


Сравнение продуктивности
Precision
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
5
10
20
30
40
Процент нарушителей
RealAlert
0

б)



в)

Рисунок 32. Сравнение с результатом применения метода RealAlert для атак: а – bad mouth, б – ballot stuffing, в – on-off

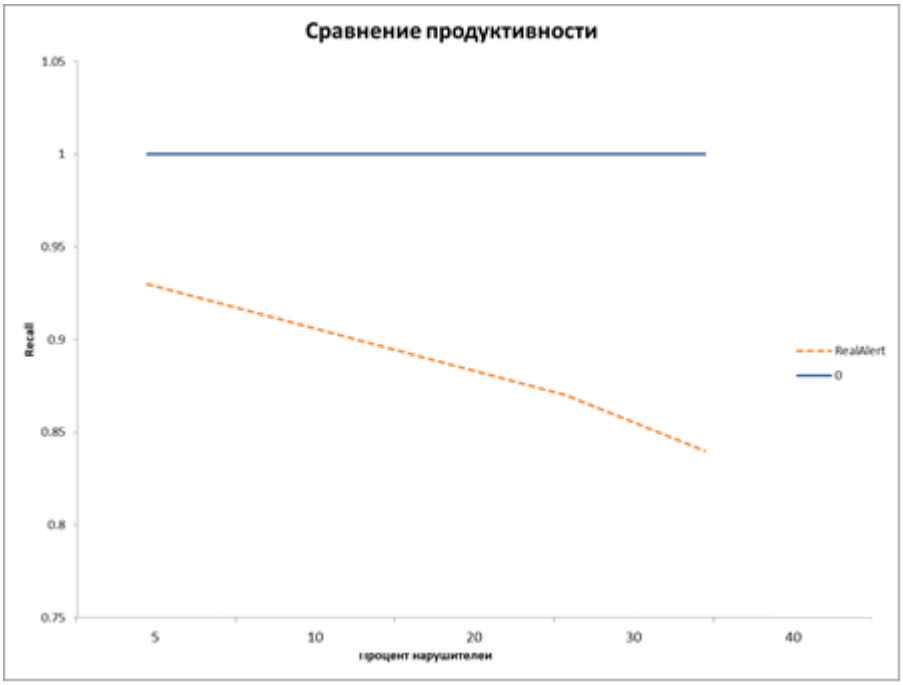


Рисунок 33. Сравнение показателя recall с результатом применения метода RealAlert для атак ballot stuffing

Исходя из представленных графиков, можно говорить о том, что для атак типа ballot stuffing результаты применения предлагаемого метода хуже, чем для метода RealAlert. Однако сравнение результатов показателя recall позволяет говорить о том, что предложенный метод корректнее оценивает поведение обычных БТС. Результаты представлены на рисунке 33.

4.2 Проверка продуктивности метода временной централизации

Зона ИВ позволяет оценить количество БТС, взаимодействующих друг с другом. Таким образом, предложенный метод позволяет повысить вероятность обнаружения нарушений семантической целостности информации при равных зонах покрытия.

Рассмотрим реализацию метода доверия при условии физической распределенности БТС. В таком случае, можно говорить о том, что группа не является полносвязной. В качестве примера будет рассматриваться группа БТС, состоящая из двух изолированных подгрупп. Ход эксперимента можно представить следующим образом:

В момент инициализации эксперимента создается две группы таким образом, что зоны их связи не пересекаются, следовательно, можно говорить о двух изолированных подгруппах. Каждая группа знает о наличии двух целей, которых следует достигнуть.

Между БТС проводится аукцион, в ходе которого определяется список БТС, перемещающихся к целям. Исходя из постулата об изолированности БТС, можно утверждать, что количество БТС, достигших целей, будет больше, чем требовалось.

Для сравнения подходов на устойчивость к возникновению СДИВ часть БТС будет заменена на нарушителей – БТС, ведущих себя как нормальные БТС, но передающих ложную информацию о себе или об окружающей среде.

Предположим, что каждый нарушитель фальсифицирует либо информацию о расстоянии до цели, либо меняет траекторию движения после выбора цели. Остальные члены группы могут обнаружить нарушение при помощи сенсорных устройств. Если нарушение заключается в предоставлении ложной информации о расстоянии до цели, то рейтинг репутации/доверия снижается. Следовательно, БТС не будет направлен к цели. Другой тип нарушителей, который предоставляет ложную информацию о траектории движения, может быть обнаружен только при движении БТС до цели. В таком случае, может не быть возможности сообщить оставшимся членам группы о необходимости направления другого БТС к цели.

Для сравнения адекватности применения глобальных и локальных показателей доверия/репутации введем дополнительные условия проведения эксперимента. Предположим, что после достижения первых целей перед группами, располагающимися в местах выполнения целей, ставятся две новые цели (цели второго уровня).

В рамках первой серии экспериментов рассмотрим ситуацию, при которой БТС-нарушитель предоставляет неверную информацию относительно стоимости достижения им цели. Таким образом, нарушитель может получить возможность отправиться к цели, не имея для этого объективных предпосылок. Также предположим, что БТС-нарушитель осуществляет движение до цели даже без назначения его на эту цель. Исходя из этого предположения и факта определения двух новых целей после достижения начальных, можно говорить о потенциальной успешности выполнения атаки на цели второго уровня. Расположение БТС-нарушителя в области цели не учитывается при определении выполнения цели на основе количества числа БТС.

На основе проведенных экспериментов были получены результаты, представленные в таблице 1.

Как видно из таблицы 1, цели второго уровня остаются невыполненными в большинстве случаев, т.к. дошедшие до целей первого

уровня БТС не позволяют провести адекватную оценку своих действий при помощи показателей доверия и репутации. Неверное представление об уровнях доверия и репутации приводит к тому, что около 70% БТС-нарушителей остаются не идентифицированными.

Таблица 1. Результаты проведения первой серии экспериментов

Показатель	**Цели первого уровня**	**Цели второго уровня (без метода плавающего центра)**
	Значение (%)	Значение (%)
Средняя потребность цели в роботах	5	5
Процент обнаруженных нарушителей	100	30,4
Процент экспериментов с целями, где процент роботов был недостаточен	0	75,3
Процент недостающих для достижения целей роботов	0	69,3

Для решения этой проблемы используем понятие полицейских участков. В предлагаемых экспериментах полицейские используются в качестве элементов, определяющих значения доверия и репутации для каждого БТС, находящегося в их зоне ответственности. После определения плана выполнения цели и обнаружения нарушителей, БТС начинают движения, в ходе которого меняют свою принадлежность к тому или иному полицейскому участку. Полицейский, в зону ответственности которого вошел БТС запрашивает информацию о его доверии и репутации у полицейского, осуществившего расчет этих данных на первом этапе. Даже при условии предоставления верной информации БТС-нарушителем на втором этапе выполнения эксперимента, полицейский не будет учитывать его

при определении планов по выполнению целей. Результаты проведения второй серии экспериментов представлены в таблице 2.

Таблица 2. Результаты проведения второй серии экспериментов

Показатель	**Цели первого уровня**	**Цели второго уровня (с методом плавающего центра)**
	Значение (%)	Значение (%)
Средняя потребность цели в роботах	5	5
Процент обнаруженных нарушителей	100	100
Процент экспериментов с целями, где процент роботов был недостаточен	0	0
Процент недостающих для достижения целей роботов	0	0

По результатам второй серии экспериментов можно говорить о том, что угроза участия в планах по выполнению целей роботов-нарушителей нейтрализована. Следовательно, будут выполнены все цели, при использовании полицейских.

Исходя из проведенных экспериментов, можно говорить об успешности применения подхода, основанного на полицейских участках для реализации межзональной политики ИБ. При его использовании можно не только минимизировать ущерб от реализации угрозы, но и полностью нейтрализовать возможную угрозу. Кроме того, возможно использование полицейских не только в качестве элементов, обеспечивающих ИБ, но и в качестве элементов, согласующих планы по выполнению целей, что приведет к уменьшению суммарных затрат роботов на выполнение поставленных целей.

Таким образом, ЦВЭ (полицейские) позволяют увеличить продуктивность применения метода доверия. Кроме того, данный подход

позволяет продемонстрировать продуктивность применения централизованного подхода к организации системы. Однако в таком случае появляется риск возникновения нарушений ИБ в критическом элементе системы – полицейском. Метод временной централизации позволяет минимизировать риск проведения атаки через ЦВЭ. Проверка продуктивности применения метода временной централизации предлагается провести на основе эмпирических экспериментов. Его отличительной особенностью от модели полицейских участков является отсутствие необходимости создания дополнительной инфраструктуры (полицейских) для функционирования метода.

На рисунке 34 представлены результаты сравнения процента ложных действий от типа атаки ballot stuffing при использовании постоянного ЦВЭ и при использовании временного ЦВЭ.

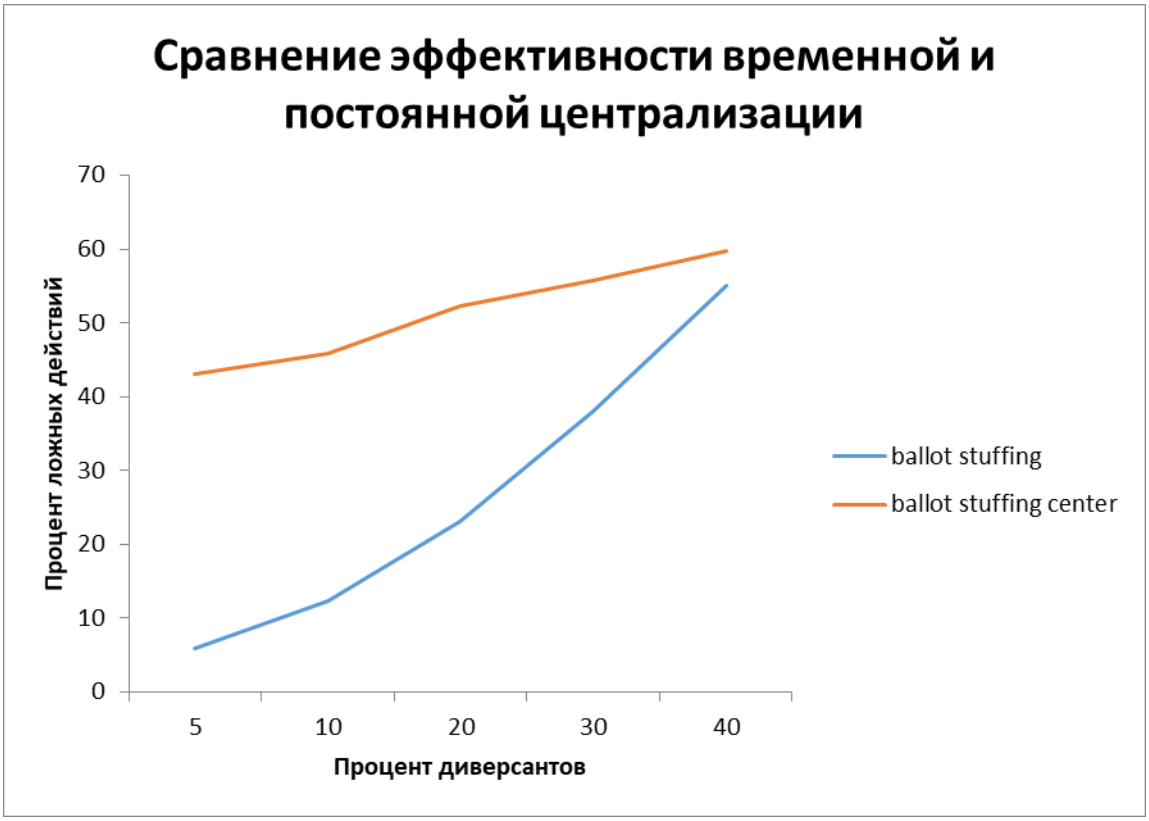


Рисунок 34. Сравнение процента ложных действий группы БТС при временном и постоянном ЦВЭ

Таким образом, в контексте атак ballot stuffing была показана продуктивность предложенного метода в сочетании с предложенным

методом доверия и репутации. Для оценки продуктивности метода временной централизации при проведении различных атак проводятся аналогичные эксперименты по начальным условиям, но с разным поведением диверсантов.

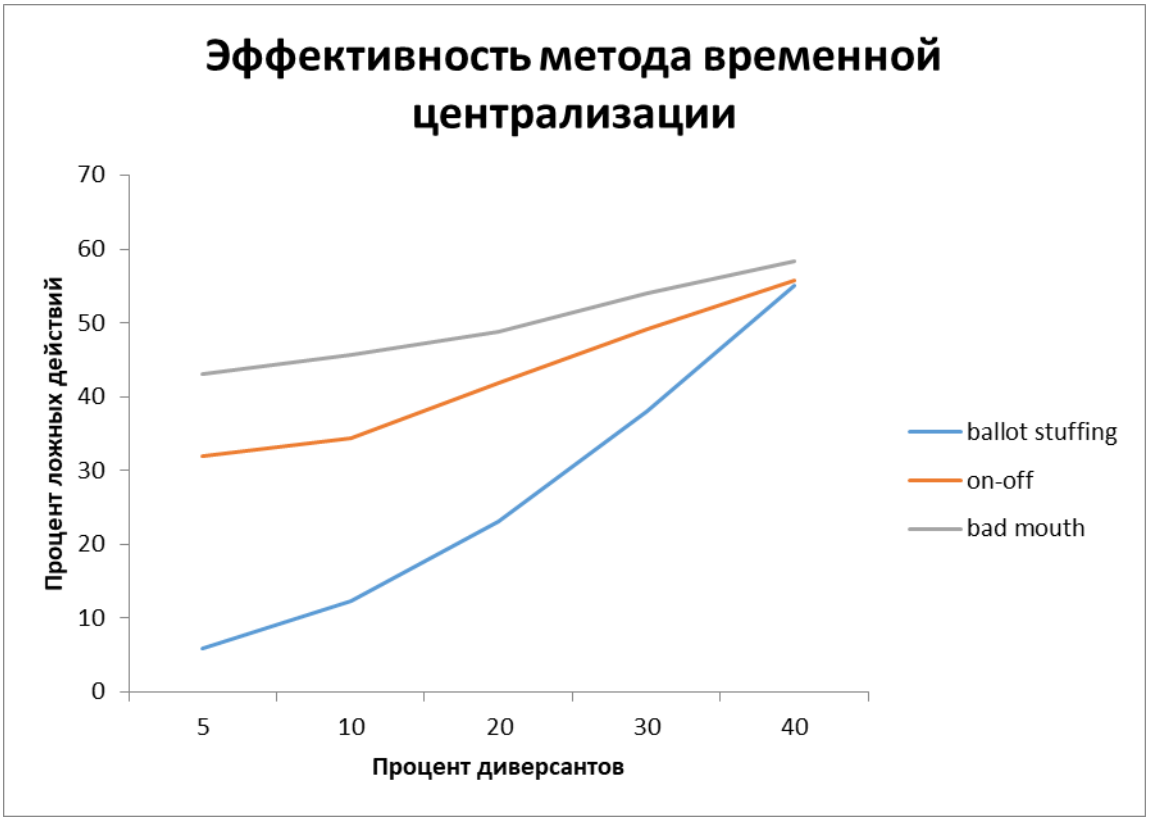


Рисунок 35. Сравнение процента ложных действий группы БТС при различных атаках

На рисунке 35 продемонстрированы результаты анализа продуктивности метода доверия и репутации. Проведение имитационного моделирования позволяет оценить алгоритмическую разрешимость и продуктивность предложенных методов. Однако требуется показать разрешимость и применимость данных методов и моделей в рамках физических условий.

4.3 Реализация модели защищенного информационного взаимодействия группы беспилотных транспортных средств

Группа БТС в контексте задачи пересечения перекрестка отличается от обычного применения БТС накладываемыми правилами. К таким правилам

можно отнести: действия по различным сигналам светофора, движения согласно знакам приоритета и т.д. В общем случае, такую систему можно представить как $E_{av} = \{e_0, \dots, e_n | R\}$, где $R = \{r_0, \dots, r_w\}$ – множество правил, устанавливаемых окружающей средой.

Для более полного представления об управлении пересечением перекрестков автомобилями следует описать общую схему организации взаимодействия участников движения. Рассмотрим следующую ситуацию: имеется перекресток двух дорог, на каждой из которой возможно движение в обе стороны (встречное и попутное). Схема такого участка дороги представлена на рисунке 36.

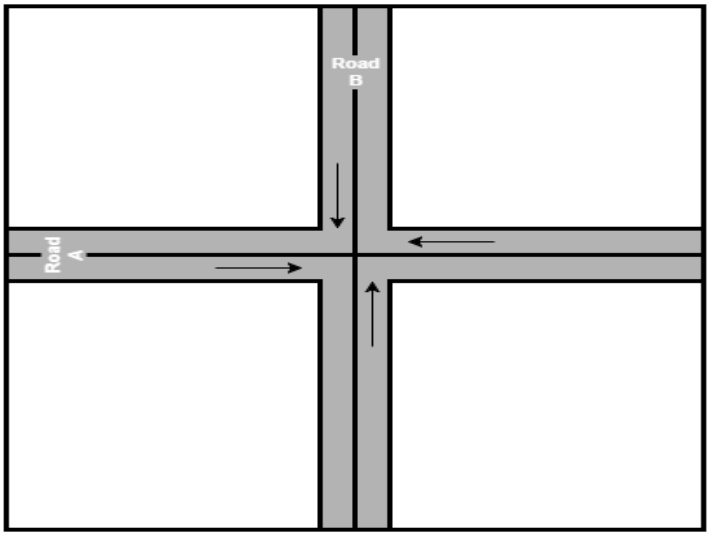


Рисунок 36.Схема организации движения на перекрестке

В ходе движения от начала дороги А к ее концу, автомобили, выбравшие подобный маршрут движения, будут пересекать перекресток с дорогой В. При распределенном управлении пересечением перекрестков автомобили будут объединяться в некоторую коллаборацию в определенный момент времени. Предположим, что дорога А является набором элементарных участков местности (ЭУМ) $\{p_0, \dots, p_{ra}\}$. Перекресток с дорогой находится на участке местности $p_i, 0 < i < n$. Максимально допустимая скорость на дороге А равняется s. Для возможности безопасного снижения скорости вплоть до полной остановки автомобиля, движущегося с максимальной скоростью, необходимо устанавливать взаимодействие с

другими автомобилями с того момента времени, когда автомобиль находится на достаточном расстоянии для безопасного торможения. Предположим, что на каждом следующем шаге автомобиль может снижать скорость на 1 единицу. Подобный подход является эквивалентом плавного торможения. Таким образом, необходимо *s+1* шагов для полной остановки автомобиля. Полный путь торможения займет в таком случае $\frac{s(s+1)}{2}+1$ элементарных участков местности. В приведенном на рисунке 31 примере автомобили должны начинать процесс взаимодействия с другими автомобилями в тот момент, когда они находятся на участке местности $p_i - \frac{s(s+1)}{2}+1$. В качестве допущения предполагается, что каждый автомобиль начинает контакт с другими в этот момент времени, не смотря на свою скорость движения. Кроме того, каждый БТС, снизивший скорость по каким-либо причинам, старается увеличить скорость до максимально разрешенного значения при отсутствии объективных обстоятельств, мешающих этому. Одним из ограничений является прохождение поворота. Движение при повороте осуществляется согласно рисунку 37.

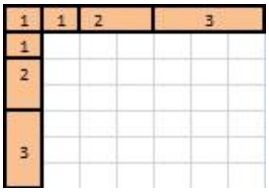


Рисунок 37. Схема выполнения поворота и допустимых скоростей при движении БТС

Таким образом, скорость на участках местности, входящих в траекторию выполнения поворота, равняется 1. Исходя из рисунка 35, скорость БТС в момент времени *t* не может отличаться от скорости БТС в момент времени *t-1* более, чем на один ЭУМ за дискрету времени. На основе представленных принципов, каждое БТС определяет желаемый маршрут следования, где начальный ЭУМ – место выезда автомобиля в зону перекрестка, а конечный – желаемое конечное положение БТС в зоне перекрестка.

Когда в зоне перекрестка находится несколько БТС, требуется определить такие маршруты следования каждого БТС, при котором не произойдет столкновение транспортных средств. Тогда, после построения желаемых маршрутов для всех транспортных средств, происходит определение конфликтных ситуаций – моментов времени, когда два или более автомобилей занимают один и тот же участок местности. Алгоритм определения конфликтных ситуаций происходит следующим образом: случайным образом выбирается один из маршрутов автомобилей коллаборации, происходит поэтапное сравнение выбранного маршрута со всеми остальными, если на каком-то шаге участки местности совпадают, данный участок записывается как конфликтный, а время наступления запоминается, при этом, дальнейший поиск конфликтов для данной пары автомобилей прекращается. Аналогичным образом происходит сравнение и поиск конфликтов для всех оставшихся участников. При нахождении конфликта, возникающего в более ранний момент времени, данный конфликт является приоритетным для решения, а остальные конфликты не решаются до момента решения первого возникшего. После этого повторяется алгоритм поиска конфликтных ситуаций до момента полного отсутствия таких ситуаций.

Алгоритм разрешения конфликтных ситуаций представляется интуитивно понятным – в общем случае, каждый из автомобилей должен перестроить свой маршрут, исходя из снижения скорости движения. В результате применения такого подхода получается два возможных варианта проезда. После этого каждый из полученных вариантов проверяется на наличие конфликтов, и подобная задача решается для всех. Стоит отметить, что данный вариант является общим, т.к. возможна ситуация, при которой один из автомобилей движется впереди другого, но с меньшей скоростью, тогда единственным вариантом решения задачи является снижение скорости второго автомобиля до скорости первого.

Нахождение оптимальных маршрутов (маршрутов без конфликтов) может быть представлено в виде ориентированного дерева, где каждая вершина является набором маршрутов всех участников системы на каждом шаге выполнения алгоритма по нахождению бесконфликтных путей. Концевые вершины такого дерева содержат бесконфликтный план пересечения перекрестка всеми участниками. Общий вид подобного дерева представлен на рисунке 38.

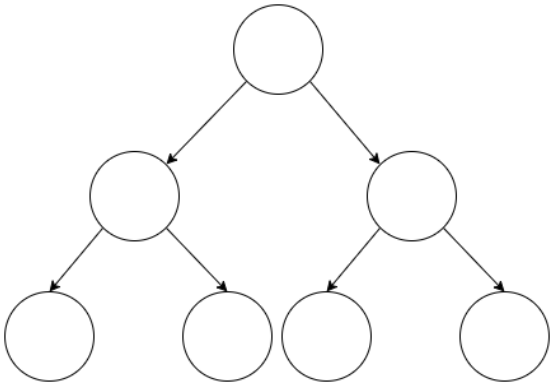


Рисунок 38. Общий вид дерева, составленного из комбинаций возможных маршрутов автомобилей

При использовании данного подхода решения возникающих конфликтных ситуаций, возможен альтернативный путь поиска бесконфликтного проезда перекрестка всеми машинами. Предположим, в некоторый момент времени t_i на перекрестке появляется новый автомобиль, ранее не участвовавший в определении маршрутов движения. На текущий момент времени, на перекрестке находится n автомобилей, создавших безопасный план проезда перекрёстка. Появление нового автомобиля в общем случае требует построения такого же дерева маршрутов, как представлено на рисунке 38. Однако при построении маршрута с учётом возникающих конфликтов только для нового участника коллаборации можно сократить количество перестроений маршрутов до указанных на рисунке 39.

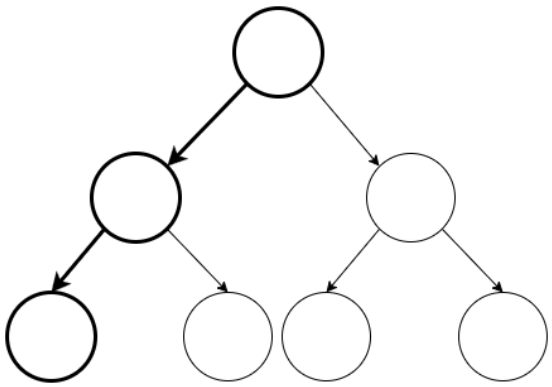


Рисунок 39. Сокращение возможных комбинаций вариантов проезда при адаптации маршрута последнего присоединившегося автомобиля

Таким образом, такой подход позволяет значительно сократить требуемые вычислительные мощности, но не позволяет работать со всеми вариантами проезда перекрестка, что может привести к значительным потерям в области эффективности проезда перекрестка.

Исследуя возможные критерии выбора оптимального маршрута, было определено, что основные критерии можно разделить на три большие группы, исходя из основных параметров, заложенных в данных критериях. В общем виде данные группы можно представить следующим образом:

- Критерии, базирующиеся на скоростных характеристиках автомобилей коллаборации;
- Критерии, базирующиеся на временных характеристиках движения автомобилей;
- Критерии, базирующиеся на характеристиках потерь в пройденном расстоянии от снижения скорости при движении автомобилей.

Для рассмотрения каждой из группы критериев следует уточнить некоторые понятия, используемые в дальнейшем. Все характеристики движения автомобиля, участвующего в процессе уточнения маршрутов, можно разделить на желаемые и фактические. Желаемые характеристики - характеристики, присущие движению транспортного средства при условии отсутствия других автомобилей на перекрестке. Фактические характеристики – характеристики, присущие движением автомобилей после согласования

маршрута с другими участниками дорожного движения. Скорость, время присутствия на перекрестке и некоторые пространственные характеристики могут быть как фактическими, так и желаемыми. При отсутствии необходимости перестраивать маршрут в соответствии с бесконфликтным вариантом перестроения подразумевает совпадение фактических и желаемых характеристик.

Первая группа критериев основывается на скорости движения автомобилей в коллаборации. Базовой характеристикой является скорость движения транспортного средства. Основными рассматриваемыми в данной статье критериями из данной группы будут являться следующие два критерия:

1. Средняя фактическая скорость движения автомобилей;
2. Средняя разница между желаемой и фактической скоростью.

Первый критерий направлен на максимизацию скорость средней скорости движения, второй критерий направлен на снижение количества замедлений автомобилей в коллаборации. Суть второго критерия сводится к минимизации изменений в скорости движения транспортных средств.

Вторая группа критериев направлена на оптимизацию в области временных характеристик движения автомобилей. Основными выделяемыми критериями здесь являются:

3. Среднее фактическое время нахождения автомобилей на перекрестке;
4. Среднее время движения автомобиля не с желаемой скоростью.

Фактическое время нахождения на перекрестке позволяет оценить, насколько долго машины задерживаются на перекрестке в абсолютных числах, а второй критерий позволяет работать с относительными значениями, касающимися различий между желаемым и реальным временем проезда.

Третья группа критериев направлена на выбор плана проезда, исходя из потерь в расстоянии, которое автомобили не прошли из-за вынужденного снижения скорости:

5. Средние потери в пройденном расстоянии в пересчете на одну единицу времени;

6. Средние потери в пройденном расстоянии из-за снижения скоростей.

Критерии данной группы направлены на возможное сокращение издержек от снижения скорости движения. Первый критерий позволяет рассчитать себестоимость каждой задержки, выраженной в величине не пройденного пути (разница между расстоянием, которое могло быть преодолено при условии движения с максимальной скоростью, и расстоянием, которое было пройдено в реальности), в то время как второй критерий направлен на минимизацию общей суммы потерь каждого автомобиля.

Для сравнения работы модели при каждом из критериев определены показатели эффективности, которые позволят оценить результаты применения различных критериев.

Базовыми являются следующие показатели работы системы:

1. Средняя скорость автомобилей;

2. Среднее время нахождения автомобиля на перекрестке;

3. Количество выехавших в зону А автомобилей;

4. Количество автомобилей, находящихся в очереди для выезда в зону А;

5. Количество автомобилей, завершивших проезд перекрестка.

Использование данных показателей позволит не только оценить, как быстро автомобили пересекают перекресток, но и определить длину очереди из автомобилей, еще не вступивших в зону коллаборации. Результаты применения различных критериев при организации дорожного движения на основе КФС представлены в таблице 3.

В ходе ИВ, элементы обмениваются информацией относительно своего состояния и состояния окружающей среды. Рассматривая упрощенный подход для моделирования, сведения об окружающей среде не входят в

список передаваемой информации, т.к. данное ограничение не снижает корректность проверки работоспособности предложенных методов защиты ИВ.

Таблица 3. Результаты применения различных критериев

Критерий	Средняя скорость	Среднее время	На перекрестке	В очереди	Завершило проезд	Затраты
1	0,96	34,14	36,97	47,14	1045,6	134,198
2	0,95	33,60	36,97	44,58	1058,4	134,573
3	0,89	31,41	36,82	5,85	1145,6	135,697
4	0,77	36,13	41,54	13,85	1120,8	142,175
5	0,84	38,69	41,19	53,70	1025,4	143,613
6	0,83	34,29	39,56	11,81	1125,3	139,900

Модель защищенного ИВ группы БТС, предложенная ранее, требует определения блоков информации, по которым будет происходить определение уровня доверия элементов системы. Информацию в данном случае можно представить в виде следующего набора блоков:

1. Идентификатор БТС
2. Текущие координаты
3. Желаемые конечные координаты
4. Желаемая скорость движения
5. Время выезда в зону коллаборации
6. Опционально – маршрут следования

Подобный набор данных в момент обмена позволяет обеспечить автономность разработки плана движения каждого автомобиля и обеспечивает возможность контроля над движением других участников коллаборации. Маршрут следования автомобиля не является обязательной частью передаваемых данных, т.к. автомобили строят свои маршруты по заранее известным принципам. При этом перестроенный в определенный момент времени маршрут и принятый всеми участниками коллаборации, должен быть передан другим участникам. В таком случае, показатель истинности будет проверяться на 6 основных блоках информации.

В контексте предложенной в разделе 2.5 модели защищенного ИВ группы БТС требуется определить функцию принадлежности для определения ЦВЭ для метода временной централизации. Вначале требуется разделить систему на подсистемы. Предлагается использовать понятия принадлежности дороги и направления этой дороги. Таким образом, БТС, находящиеся на одной дороге, но двигающиеся в разных направлениях, относятся к различным подсистемам. Кроме того, автомобили, еще не выехавшие на перекресток и уже проехавшие перекресток, также относятся к разным подсистемам.

ЦВЭ проверяет информацию на наличие нарушений семантической целостности. Если нарушений не обнаружено, он передает полученную информацию элементам своей подсистемы. При обнаружении нарушений целостности, ЦВЭ предпринимает меры по избеганию столкновений – задерживает движение до момента проезда нарушителя. Такой подход не является самым эффективным, однако, является самым безопасным с точки зрения возникновения дорожно-транспортных происшествий.

Как только ЦВЭ проезжает перекресток (выезжает на него), оставшиеся элементы системы определяют новый ЦВЭ на основе предложенной функции. Кроме того, проводится анализ поведения предполагаемого ЦВЭ согласно методу доверия. Если элемент проходит проверку, он становится ЦВЭ и начинает взаимодействие с другими ЦВЭ. В случае, если проверка не была пройдена, выбирается следующий ЦВЭ, который сообщает другим ЦВЭ о наличии нарушителя. Таким образом, предложенная модель защищенного ИВ группы БТС была применена в рамках решения задачи пересечения перекрестка.

Вывод по главе 4

В главе 4 решены следующие задачи:

1. Проведена проверка работоспособности метода обнаружения нарушений семантической информации в группе БТС. Была проведена

оценка вероятности ошибок первого и второго рода при реализации атак bad mouth, ballot stuffing и on-off attack;

2. Проведен анализ использования метода временной централизации. Анализ основывается на проведении имитационного моделирования при использовании метода доверия и репутации;
3. Разработан программный комплекс, подтверждающий возможность использования предложенных методов и моделей в рамках физических групп БТС.

Заключение

В диссертационной работе «Модели и методы обнаружения нарушений целостности информации в группах беспилотных транспортных средств» формализована модель функционирования группы беспилотных транспортных средств, рассмотрена последовательность действий БТС, при выполнении поставленных перед группой задач. В рамках предложенной модели функционирования группы беспилотных транспортных средств разработаны модели нарушителей и модель угроз, согласно которым предлагается модель обеспечения информационной безопасности группы беспилотных транспортных средств.

Одной из составляющих обеспечения информационной безопасности группы беспилотных транспортных средств является модель защищенного информационного взаимодействия беспилотных транспортных средств, позволяющая оценивать целостность информации в процессе функционирования системы. Модель защищенного информационного взаимодействия базируется на двух основных методах – метод обеспечения информационной безопасности на основе социальных механизмов и метод временной централизации.

Метод обеспечения информационной безопасности на основе социальных механизмов позволяет оценивать семантическую целостность на основе анализа поведения беспилотных транспортных средств и/или проверки данных при помощи имеющихся сенсорных устройств.

Метод временной централизации позволяет использовать централизованный подход к организации информационного взаимодействия беспилотных транспортных средств для решения задач в момент времени, при этом, взаимодействие беспилотных транспортных средств остается децентрализованным в другие моменты времени, что позволяет сократить

риск реализации угроз, присущих централизованному подходу к организации информационного взаимодействия.

Предложенная модель и методы были апробированы в рамках имитационных и физических моделей. Проведение экспериментов в условиях имитационного моделирования позволило оценить вероятность корректного обнаружения нарушений семантической целостности информационных сообщений, а также вероятность верной оценки обычных элементов. Кроме того, было проведено сравнение вероятности обнаружения нарушений семантической целостности для существующего метода обеспечения информационной безопасности на основе социальных механизмов и предложенного.

Таким образом, в диссертационной работе решена научная задача разработки моделей, методов и прототипа программного комплекса обнаружения нарушений целостности информации в группах БТС за счет реализации возможности обнаружения СДИВ, обеспечивающих их безопасное информационное взаимодействие. Применение предложенных моделей и методов позволяет повысить уровень безопасности информации в процессе информационного взаимодействия БТС.

В ходе выполнения научно-исследовательской работы были получены следующие научные результаты, составляющие **итоги** исследования:

1. Разработана модель функционирования группы БТС на основе мультиагентного подхода, в которой отсутствует центральный вычислительный элемент;
2. Разработана модель защищенного ИВ группы БТС, основанная на предложенной модели функционирования, позволяющая использовать как традиционные методы обеспечения ИБ, так и перспективные;
3. Разработан метод организации ИВ группы БТС на основе временной централизации, учитывающий условия функционирования группы БТС при выборе центрального вычислительного элемента;

4. Разработан метод обеспечения ИБ на основе репутационных механизмов, позволяющий осуществлять автоматическое обнаружение нарушений целостности информации в группах БТС элементами группы;
5. Разработан прототип программного комплекса обеспечения ИБ на основе разрабатываемых методов для физической модели группы БТС.

Предложенные модели и методы позволяют обнаруживать СДИВ в процессе информационного взаимодействия БТС, что было показано в ходе имитационного моделирования. Практическая применимость разработанных методов и модели подтверждается применением в рамках прототипа программного комплекса для обеспечения ИБ для физических моделей БТС.

Сформулированы **рекомендации** по применению результатов работы в научных исследованиях и в индустрии. Результаты, представленные в диссертации, позволяют обнаруживать нарушения семантической целостности информации в группах БТС. Модель защищенного информационного взаимодействия групп БТС может быть модифицирована для использования в КФС, что позволит обнаруживать нарушения целостности информации в рамках более обширного класса систем. Использование метода временной централизации позволит использовать преимущества централизованного подхода к организации ИВ в группах БТС. Одной из областей применения является использование данного метода для роев БПЛА. В таком случае, представляется возможным использовать традиционные методы обеспечения ИБ для роевой робототехники. Исходя из сформулированных рекомендаций, можно говорить о возможности применения полученных результатов в рамках концепции Индустрии 4.0 для обнаружения нарушений целостности информации.

В качестве **перспектив дальнейшей разработки тематики** можно выделить исследования, сопряженные с развитием модели защищенного ИВ в контексте решения задач обеспечения доступности информации для

изолированных групп БТС. Кроме того, представляется значимым решение задачи защищенного ИВ групп БТС с окружающей средой (объектами инфраструктуры). Также возможно использование модели функционирования, модели защищенного ИВ и предложенных методов для разработки системы критериев оценки защищенности системы, а также величины ущерба, наносимого группе при реализации угроз. Важным развитием темы является разработка методов противодействия и уменьшения ущерба при обнаружении нарушений целостности информации.

Соответствие паспорту специальности. Положения, выносимые на защиту, соотнесены с пунктами паспорта специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»: «15. Модели и методы управления информационной безопасностью» (результат 1), «13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (результаты 2-3), «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» (результат 3).

Список использованных источников

1. Self-Organizing Factories [Электронный ресурс]. – Электрон. дан. – Режим доступа: www.siemens.com/innovation/apps/pof_microsite/_pof-spring2013/_html_en/industry-40.html. – Загл. с экрана
2. Rowstron A., Druschel P. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems //IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing. – Springer, Berlin, Heidelberg, 2001. – С. 329-350.
3. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications //Peer-to-Peer Computing, 2001. Proceedings. First International Conference on. – IEEE, 2001. – С. 101-102.
4. Каляев И. А., Гайдук А. Р. Стайные принципы управления в группе объектов //Мехатроника, автоматизация, управление. – 2004. – №. 12. – С. 27-38.
5. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. Монография. – 2009.
6. Криницкий Н. А., Китов А. И. Электронные цифровые машины и программирование. – Изд-во физ.-мат. лит., М.-1959, 1959.
7. Юдина М. А. Индустрия 4. 0: перспективы и вызовы для общества //Государственное управление. Электронный вестник. – 2017. – №. 60.
8. Добрынин А. П. и др. Цифровая экономика-различные пути к эффективному применению технологий (BIM, PLM, CAD, IOT, Smart City, BIG DATA и другие) //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 1.
9. Santucci G. The internet of things: Between the revolution of the internet and the metamorphosis of objects //Vision and Challenges for Realising the Internet of Things. – 2010. – С. 11-24.

10. Van Kranenburg R., Bassi A. IoT challenges //Communications in Mobile Computing. – 2012. – Т. 1. – №. 1. – С. 9.
11. Lee E. A. Cyber physical systems: Design challenges //11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC). – IEEE, 2008. – С. 363-369.
12. Люгер Д. Ф. Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание. – Издательский дом Вильямс, 2003.
13. Прангишвили И. В. Энтропийные и другие системные закономерности: Вопросы управления сложными системами. – М.: наука, 2003. – Т. 428.
14. Новиков Д. А. Теория управления организационными системами. – М. : Моск. психол.-соц. ин-т, 2005.
15. Винер Н. Кибернетика, или управление и связь в животном и машине. – Наука, 1983. – С. 344.
16. Тюхтин В. С. Отражение, системы, кибернетика. – М.: Наука, 1972. – Т. 256.
17. Уемов А. И. Системный подход и общая теория систем //М.: мысль. – 1978. – Т. 272. – С. 57.
18. Волкова В. Н., Денисов А. А. Теория систем и системный анализ //М.: Юрайт. – 2010.
19. Wooldridge M. An introduction to multiagent systems. – John Wiley & Sons, 2009.
20. Van der Hoek W., Wooldridge M. Multi-agent systems //Foundations of Artificial Intelligence. – 2008. – Т. 3. – С. 887-928.
21. Ferber J., Gutknecht O., Michel F. From agents to organizations: an organizational view of multi-agent systems //International Workshop on Agent-Oriented Software Engineering. – Springer, Berlin, Heidelberg, 2003. – С. 214-230.
22. McArthur S. D. J. et al. Multi-agent systems for power engineering applications—Part I: Concepts, approaches, and technical challenges //IEEE Transactions on Power systems. – 2007. – Т. 22. – №. 4. – С. 1743-1752.

23. Sabater J., Sierra C. Reputation and social network analysis in multi-agent systems //Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1. – ACM, 2002. – С. 475-482.
24. Baheti R., Gill H. Cyber-physical systems //The impact of control technology. – 2011. – Т. 12. – №. 1. – С. 161-166.
25. Wolf W. H. Cyber-physical systems //IEEE Computer. – 2009. – Т. 42. – №. 3. – С. 88-89.
26. Цветков В. Я. КИБЕР ФИЗИЧЕСКИЕ СИСТЕМЫ //Международный журнал прикладных и фундаментальных исследований. – 2017. – №. 6-1. – С. 64-65.
27. Sha L. et al. Cyber-physical systems: A new frontier //Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on. – IEEE, 2008. – С. 1-9.
28. Rajkumar R. et al. Cyber-physical systems: the next computing revolution //Design Automation Conference (DAC), 2010 47th ACM/IEEE. – IEEE, 2010. – С. 731-736.
29. DoD U. S. DoD Policy Recommendations for the Internet of Things (IoT) //White Paper, DoD Chief Information Officer. – 2016.
30. Андиева Е. Ю., Фильчакова В. Д. Цифровая экономика будущего, индустрия 4.0 //Прикладная математика и фундаментальная информатика. – 2016. – №. 3. – С. 214-218.
31. Позднеев Б. М. и др. Новые горизонты стандартизации в эпоху цифрового обучения и производства //Вестник МГТУ Станкин. – 2015. – №. 4. – С. 101-108.
32. Lee J., Bagheri B., Kao H. A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems //Manufacturing Letters. – 2015. – Т. 3. – С. 18-23.
33. Farhangi H. The path of the smart grid //IEEE power and energy magazine. – 2010. – Т. 8. – №. 1.

34. Amin M. Smart Grid //PUBLIC UTILITIES FORTNIGHTLY. – 2015.
35. Gungor V. C. et al. Smart grid technologies: Communication technologies and standards //IEEE transactions on Industrial informatics. – 2011. – Т. 7. – №. 4. – С. 529-539.
36. Su W. et al. A survey on the electrification of transportation in a smart grid environment //IEEE Transactions on Industrial Informatics. – 2012. – Т. 8. – №. 1. – С. 1-10.
37. Jurgen R. K. Smart cars and highways go global //IEEE spectrum. – 1991. – Т. 28. – №. 5. – С. 26-36.
38. Дудка Н. А. Концепция использования корреляционно-экстремальных систем навигации в беспилотных транспортных средствах //Вестник НЦБЖД. – 2016. – №. 4. – С. 15-21.
39. Ахметзянов И. З., Ионов М. А., Карабцев В. С. Модификация алгоритма RRT для определения оптимальной траектории движения автомобиля при объезде препятствий //Вестник Сибирской государственной автомобильно-дорожной академии. – 2017. – №. 6 (58).
40. Carlino D., Boyles S. D., Stone P. Auction-based autonomous intersection management //Intelligent Transportation Systems-(ITSC), 2013 16th International IEEE Conference on. – IEEE, 2013. – С. 529-534.
41. Wuthishuwong C., Traechtler A. Vehicle to infrastructure based safe trajectory planning for Autonomous Intersection Management //ITS Telecommunications (ITST), 2013 13th International Conference on. – IEEE, 2013. – С. 175-180.
42. Vahidi A., Eskandarian A. Research advances in intelligent collision avoidance and adaptive cruise control //Intelligent Transportation Systems, IEEE Transactions on. – 2003. – Т. 4. – №. 3. – С. 143-153.
43. Ho C., Reed N., Spence C. Multisensory in-car warning signals for collision avoidance //Human Factors: The Journal of the Human Factors and Ergonomics Society. – 2007. – Т. 49. – №. 6. – С. 1107-1114.

44. Au T., Zhang S., Stone P. Autonomous Intersection Management for Semi-Autonomous Vehicles // Handbook of Transportation. - 2015. С. 88–104.
45. Dresner K., Stone P. A multiagent approach to autonomous intersection management //Journal of artificial intelligence research. – 2008. – С. 591-656.
46. Wu J., Abbas-Turki A., El Moudni A. Cooperative driving: an ant colony system for autonomous intersection management //Applied Intelligence. – 2012. – Т. 37. – №. 2. – С. 207-222.
47. Zohdy I. H., Kamalanathsharma R. K., Rakha H. Intersection management for autonomous vehicles using icacc //Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on. – IEEE, 2012. – С. 1109-1114.
48. Gerla M. et al. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds //Internet of Things (WF-IoT), 2014 IEEE World Forum on. – IEEE, 2014. – С. 241-246.
49. Амелин К. С. и др. Адаптивное управление автономной группой беспилотных летательных аппаратов //Стохастическая оптимизация в информатике. – 2009. – Т. 5. – №. 1-1. – С. 157-166.
50. Al-Shihabi T., Mourant R. R. A framework for modeling human-like driving behaviors for autonomous vehicles in driving simulators //Proceedings of the fifth international conference on Autonomous agents. – ACM, 2001. – С. 286-291.
51. Glancy D. J. Autonomous and automated and connected cars-oh my: first generation autonomous cars in the legal ecosystem //Minn. JL Sci. & Tech. – 2015. – Т. 16. – С. 619.
52. Hartenstein H. et al. A tutorial survey on vehicular ad hoc networks //IEEE Communications magazine. – 2008. – Т. 46. – №. 6. – С. 164.
53. Zeadally S. et al. Vehicular ad hoc networks (VANETS): status, results, and challenges //Telecommunication Systems. – 2012. – Т. 50. – №. 4. – С. 217-241.

54. Yousefi S., Mousavi M. S., Fathy M. Vehicular ad hoc networks (VANETs): challenges and perspectives //ITS Telecommunications Proceedings, 2006 6th International Conference on. – IEEE, 2006. – С. 761-766.
55. Toor Y., Muhlethaler P., Laouiti A. Vehicle ad hoc networks: Applications and related technical issues //IEEE communications surveys & tutorials. – 2008. – Т. 10. – №. 3.
56. Narla S. R. K. The evolution of connected vehicle technology: From smart drivers to smart cars to… self-driving cars //Ite Journal. – 2013. – Т. 83. – №. 7. – С. 22-26.
57. Guerrero-Ibanez J. A., Zeadally S., Contreras-Castillo J. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies //IEEE Wireless Communications. – 2015. – Т. 22. – №. 6. – С. 122-128.
58. Dimitrakopoulos G. Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges //ITS Telecommunications (ITST), 2011 11th International Conference on. – IEEE, 2011. – С. 145-151.
59. Zhang T., Antunes H., Aggarwal S. Defending Connected Vehicles Against Malware: Challenges and a Solution Framework //IEEE Internet of Things journal. – 2014. – Т. 1. – №. 1. – С. 10-21.
60. Lu N. et al. Connected vehicles: Solutions and challenges //IEEE internet of things journal. – 2014. – Т. 1. – №. 4. – С. 289-299.
61. Guler S. I., Menendez M., Meier L. Using connected vehicle technology to improve the efficiency of intersections //Transportation Research Part C: Emerging Technologies. – 2014. – Т. 46. – С. 121-131.
62. Gora P., Rüb I. Traffic models for self-driving connected cars //Transportation Research Procedia. – 2016. – Т. 14. – С. 2207-2216.
63. Зикратов И. А., Козлова Е. В., Зикратова Т. В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом //Научно-

технический вестник информационных технологий, механики и оптики. – 2013. – №. 5 (87).

64. Алгулиев Р. М., Имамвердиев Я. Н., Сухостат Л. В. Киберфизические системы: основные понятия и вопросы обеспечения безопасности //Информационные технологии. – 2017. – Т. 23. – №. 7. – С. 517-528.
65. Гуляев Ю. В. и др. Аутентификация в беспроводных локальных сетях на основе.. //Информация и безопасность. – 2007. – Т. 10. – №. 3. – С. 395-402.
66. Gavrilova M. L., Yampolskiy R. V. State-of-the-Art in Robot Authentication [From the Guest Editors] //IEEE Robotics & Automation Magazine. – 2010. – Т. 17. – №. 4. – С. 23-24.
67. Перьков А. А. ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ //Редакционная коллегия: АС Сигов (председатель), ЕГ Андрианова, ДИ Дубровский, ВГ Редько. – 2015. – С. 212.
68. Ястреб Н. А. Индустрия 4.0: киберфизические системы и интернет вещей //Человек в технической среде: сборник научных статей/Под ред. доц. НА Ястреб. Вологда: ВоГУ. – 2015. – №. 2.
69. Kozlowski K. R. Modelling and identification in robotics. – Springer Science & Business Media, 2012.
70. Lee G. S., Thuraisingham B. Cyberphysical systems security applied to telesurgical robotics //Computer Standards & Interfaces. – 2012. – Т. 34. – №. 1. – С. 225-229.
71. Kagal L. et al. Authorization and privacy for semantic web services //IEEE Intelligent Systems. – 2004. – Т. 19. – №. 4. – С. 50-56.
72. Wang E. K. et al. Security issues and challenges for cyber physical system //Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom). – IEEE, 2010. – С. 733-738.

73. Комаров И. И., Дранник А. Л., Юрьева Р. А. Моделирование проблем информационной безопасности мультиагентных систем //В мире научных открытий. – 2014. – №. 4. – С. 61-70.
74. Юрьева Р.А., Комаров И.И., Дородников Н.А. Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением // Программные системы и вычислительные методы - 2016. - № 1(14). - С. 42-48
75. Neeran K. M., Tripathi A. R. Security in the Ajanta MobileAgent system //Technical Report. Department of Computer Science, University of Minnesota. – 1999.
76. Sander T., Tschudin C. F. Towards mobile cryptography //Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on. – IEEE, 1998. – С. 215-224.
77. Зикратов И. А. и др. Модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением //Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17. – №. 3.
78. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios. Proceeding of the 2nd ACM Intl. Workshop on Australian Information Security & Data Mining, v.54, 2004.
79. Тутубалин П. И. Основные задачи прикладной теории информационной безопасности АСУ //Научно-технический вестник информационных технологий, механики и оптики. – 2007. – №. 39.
80. Еременко В. Т. и др. Направления и проблемы интеграции автоматизированных систем управления для предприятий с непрерывным технологическим циклом //Информационные системы и технологии. – 2014. – Т. 83. – №. 3. – С. 51.

81. Цветков В. Я. Семантика сообщений в телекоммуникационных системах //Всерос. конкурс, отбор обзорно-аналит. ст. по приоритет, направлению" Информационно-телекоммуникационные системы. – 2008.
82. Komali R. S., MacKenzie A. B., Gilles R. P. Effect of selfish node behavior on efficient topology design //IEEE Transactions on mobile computing. – 2008. – Т. 7. – №. 9. – С. 1057-1070.
83. Zissis D., Lekkas D. Addressing cloud computing security issues //Future Generation computer systems. – 2012. – Т. 28. – №. 3. – С. 583-592.
84. Кловский Д.Д. Передача дискретных сообщений по радиокана¬ лам. М.: Радио и связь, 1982.;
85. Frater M. R., Ryan M. J., Dunbar R. M. Electromagnetic communications within swarms of autonomous underwater vehicles //Proceedings of the 1st ACM international workshop on Underwater networks. – ACM, 2006. – С. 64-70.;
86. Sichitiu M. L., Kihl M. Inter-vehicle communication systems: a survey //IEEE Communications Surveys & Tutorials. – 2008. – Т. 10. – №. 2.
87. Кручинин С. В. Семиуровневая модель OSI/ISO и стек протоколов TCP/IP: исследование взаимоотношения и интерпретации //Научно-исследовательские публикации. – 2015. – №. 5 (25).
88. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
89. Bucciol P., Masala E., De Martin J. C. Dynamic packet size selection for 802.11 inter-vehicular video communications //Proceedings of Vehicle to Vehicle Communications Workshop (V2VCOM), San Diego, CA. – 2005.
90. Wu H. et al. An empirical study of short range communications for vehicles //Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks. – ACM, 2005. – С. 83-84.

91. Hui F., Mohapatra P. Experimental characterization of multi-hop communications in vehicular ad hoc network //Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks. – ACM, 2005. – С. 85-86.
92. Gunter Y., Grobmann H. P. Usage of wireless LAN for inter-vehicle communication //Intelligent Transportation Systems, 2005. Proceedings. 2005 IEEE. – IEEE, 2005. – С. 408-413.
93. Singh J. P. et al. Empirical observations on wireless LAN performance in vehicular traffic scenarios and link connectivity based enhancements for multihop routing //Wireless Communications and Networking Conference, 2005 IEEE. – IEEE, 2005. – Т. 3. – С. 1676-1682.
94. Chuang B. W. et al. System development and performance investigation of mobile ad-hoc networks in vehicular environments //Intelligent Vehicles Symposium, 2005. Proceedings. IEEE. – IEEE, 2005. – С. 302-307.
95. Horikoshi S. et al. A study on multipath propagation modeling in millimeter wave IVC //Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on. – IEEE, 2002. – Т. 1. – С. 286-290.
96. Sibecas S. et al. On the suitability of 802.11 a/RA for high-mobility DSRC //Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th. – IEEE, 2002. – Т. 1. – С. 229-234.
97. Mizutani K., Kohno R. Inter-vehicle spread spectrum communication and ranging system with concatenated EOE sequence //IEEE Transactions on intelligent transportation systems. – 2001. – Т. 2. – №. 4. – С. 180-191.
98. Taliwal V. et al. Empirical determination of channel characteristics for DSRC vehicle-to-vehicle communication //Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. – ACM, 2004. – С. 88-88.
99. Maurer J. et al. A new inter-vehicle communications (IVC) channel model //Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. – IEEE, 2004. – Т. 1. – С. 9-13.

100. Blum J., Eskandarian A. CARAVAN: A Communications Architecture for Reliable Adaptive Vehicular Adhoc Networks. – SAE Technical Paper, 2006. – №. 2006-01-1427.

101. Blum J. J., Eskandarian A. Fast, robust message forwarding for inter-vehicle communication netw //Intelligent Transportation Systems Conference, 2006. ITSC'06. IEEE. – IEEE, 2006. – С. 1418-1423.

102. Wolf M., Weimerskirch A., Paar C. Secure in-vehicle communication //Embedded Security in Cars. – Springer, Berlin, Heidelberg, 2006. – С. 95-109.

103. Hubaux J. P., Capkun S., Luo J. The security and privacy of smart vehicles //IEEE Security & Privacy. – 2004. – Т. 2. – №. 3. – С. 49-55.

104. Jones W. D. Building safer cars //IEEE Spectrum. – 2002. – Т. 39. – №. 1. – С. 82-85.

105. Zhou L., Haas Z. J. Securing ad hoc networks //IEEE network. – 1999. – Т. 13. – №. 6. – С. 24-30.

106. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code //Journal of Computer and System Sciences. – 2000. – Т. 61. – №. 3. – С. 362-399.

107. Chen C. M. et al. RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks //IEEE Transactions on parallel and distributed systems. – 2012. – Т. 23. – №. 4. – С. 727-734.

108. Самойленко Д. В., Финько О. А. Обеспечение целостности информации в автономной группе беспилотных летательных аппаратов методами модулярной арифметики //Наука. Инновации. Технологии. – 2016. – №. 4.

109. Иванов А. П. Исследование алгоритма обеспечения целостности сигналов в многолучевых каналах //Вестник Пензенского государственного университета. – 2015. – №. 4 (12).

110. Самойленко Д. В., Финько О. А. Имитоустойчивая передача данных в защищенных системах однонаправленной связи на основе

полиномиальных классов вычетов //Нелинейный мир. – 2013. – Т. 11. – №. 9. – С. 642-658.

111. Zhao W., Ammar M., Zegura E. Controlling the mobility of multiple data transport ferries in a delay-tolerant network //INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies. Proceedings IEEE. – IEEE, 2005. – Т. 2. – С. 1407-1418.

112. Burgess J. et al. Maxprop: Routing for vehicle-based disruption-tolerant networks //INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings. – IEEE, 2006. – С. 1-11.

113. Fall K. A delay-tolerant network architecture for challenged internets //Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. – ACM, 2003. – С. 27-34.

114. Farrell S. Endpoint Discovery and Contact Graph Routing in Space and Terrestrial DTNs //Advanced satellite multimedia systems conference (asma) and the 11th signal processing for space communications workshop (spsc), 2010 5th. – IEEE, 2010. – С. 89-93.

115. Pereira P. R. et al. From delay-tolerant networks to vehicular delay-tolerant networks //IEEE Communications Surveys & Tutorials. – 2012. – Т. 14. – №. 4. – С. 1166-1182.

116. Krauß S. Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics : дис. – 1998.

117. Perrone L. F., Nelson S. C. A study of on-off attack models for wireless ad hoc networks //Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on. – IEEE, 2006. – С. 1-10.

118. Bhattacharjee R., Goel A. Avoiding ballot stuffing in ebay-like reputation systems //Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems. – ACM, 2005. – С. 133-137.

119. Ozdemir S., Xiao Y. Secure data aggregation in wireless sensor networks: A comprehensive overview //Computer Networks. – 2009. – T. 53. – №. 12. – C. 2022-2037.

120. Xiang G.Trust Models in VANETs //Journal of Electronics and Information Science. – 2017. – №. 2. – C. 107-111.

121. Guo J., Chen R. A classification of trust computation models for service-oriented internet of things systems //Services Computing (SCC), 2015 IEEE International Conference on. – IEEE, 2015. – C. 324-331.

122. Dellarocas C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior //Proceedings of the 2nd ACM conference on Electronic commerce. – ACM, 2000. – C. 150-157.

123. Ganeriwal S., Balzano L. K., Srivastava M. B. Reputation-based framework for high integrity sensor networks //ACM Transactions on Sensor Networks (TOSN). – 2008. – T. 4. – №. 3. – C. 15.

124. Blaze M., Feigenbaum J., Lacy J. Decentralized trust management //Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. – IEEE, 1996. – C. 164-173.

125. Theodorakopoulos G., Baras J. S. Trust evaluation in ad-hoc networks //Proceedings of the 3rd ACM workshop on Wireless security. – ACM, 2004. – C. 1-10.

126. Sun Y. L. et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks //IEEE Journal on Selected Areas in Communications. – 2006. – T. 24. – №. 2. – C. 305-317.

127. Gambetta D. et al. Can we trust trust //Trust: Making and breaking cooperative relations. – 2000. – T. 13. – C. 213-237.

128. Abdul-Rahman A., Hailes S. A distributed trust model //Proceedings of the 1997 workshop on New security paradigms. – ACM, 1998. – C. 48-60.

129. Lou J. K., Chen K. T., Lei C. L. A collusion-resistant automation scheme for social moderation systems //Consumer Communications and

Networking Conference, 2009. CCNC 2009. 6th IEEE. – IEEE, 2009. – С. 1-5.

130. Teacy W. T. L. et al. Travos: Trust and reputation in the context of inaccurate information sources //Autonomous Agents and Multi-Agent Systems. – 2006. – Т. 12. – №. 2. – С. 183-198.

131. Whitby A., Jøsang A., Indulska J. Filtering out unfair ratings in bayesian reputation systems //Proc. 7th Int. Workshop on Trust in Agent Societies. – 2004. – Т. 6. – С. 106-117.

132. Bankovic Z. et al. Detecting false testimonies in reputation systems using self-organizing maps //Logic Journal of the IGPL. – 2013. – Т. 21. – №. 4. – С. 549-559.

133. Li W., Song H., Zeng F. Policy-based secure and trustworthy sensing for internet of things in smart cities //IEEE Internet of Things Journal. – 2018. – Т. 5. – №. 2. – С. 716-723.

134. Chen R., Guo J., Bao F. Trust management for SOA-based IoT and its application to service composition //IEEE Transactions on Services Computing. – 2016. – Т. 9. – №. 3. – С. 482-495.

135. Głowacka J., Krygier J., Amanowicz M. A trust-based situation awareness system for military applications of the internet of things //Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on. – IEEE, 2015. – С. 490-495.

136. Mendoza C. V. L., Kleinschmidt J. H. Mitigating On-Off attacks in the Internet of Things using a distributed trust management scheme //International Journal of Distributed Sensor Networks. – 2015. – Т. 11. – №. 11. – С. 859731.

137. Chen R., Bao F., Guo J. Trust-based service management for social internet of things systems //IEEE transactions on dependable and secure computing. – 2016. – Т. 13. – №. 6. – С. 684-696.

138. Rawat D. B. et al. Trust On the Security of Wireless Vehicular Ad-hoc Networking //Ad Hoc & Sensor Wireless Networks. – 2015. – Т. 24. – №. 3-4. – С. 283-305.

139. Alriyami Q., Adnane A., Smith A. K. Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs) //Connected Vehicles and Expo (ICCVE), 2014 International Conference on. – IEEE, 2014. – С. 118-123.

140. ElBatt T. et al. Cooperative collision warning using dedicated short range wireless communications //Proceedings of the 3rd international workshop on Vehicular ad hoc networks. – ACM, 2006. – С. 1-9.

141. Chen W., Cai S. Ad hoc peer-to-peer network architecture for vehicle safety communications //IEEE Communications magazine. – 2005. – Т. 43. – №. 4. – С. 100-107.

142. Pérez J., Milanés V., Onieva E. Cascade architecture for lateral control in autonomous vehicles //IEEE Transactions on Intelligent Transportation Systems. – 2011. – Т. 12. – №. 1. – С. 73-82.

143. Dolgov D. et al. Path planning for autonomous vehicles in unknown semi-structured environments //The International Journal of Robotics Research. – 2010. – Т. 29. – №. 5. – С. 485-501.

144. Осипов В. Ю., Воробьев В. И., Левоневский Д. К. Проблемы защиты от ложной информации в компьютерных сетях //Труды СПИИРАН. – 2017. – Т. 4. – №. 53. – С. 97-117.

145. Buchegger S., Le Boudec J. Y. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks //Parallel, Distributed and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on. – IEEE, 2002. – С. 403-410.

146. Zapata M. G. Secure ad hoc on-demand distance vector routing //ACM SIGMOBILE Mobile Computing and Communications Review. – 2002. – Т. 6. – №. 3. – С. 106-107.

147. Perkins C., Belding-Royer E., Das S. Ad hoc on-demand distance vector (AODV) routing. – 2003. – №. RFC 3561.

148. Adnane A., Bidan C., de Sousa Júnior R. T. Trust-based security for the OLSR routing protocol //Computer Communications. – 2013. – Т. 36. – №. 10-11. – С. 1159-1171.

149. Santoso G. Z., Kang M. Performance analysis of AODV, DSDV and OLSR in a VANETs safety application scenario //Advanced communication technology (ICACT), 2012 14th international conference on. – IEEE, 2012. – С. 57-60.

150. Spaho E. et al. Performance evaluation of OLSR and AODV protocols in a VANET crossroad scenario //Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on. – IEEE, 2013. – С. 577-582.

151. Zhang J. A survey on trust management for vanets //Advanced information networking and applications (AINA), 2011 IEEE international conference on. – IEEE, 2011. – С. 105-112.

152. Tangade S. S., Manvi S. S. A survey on attacks, security and trust management solutions in VANETs //Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. – IEEE, 2013. – С. 1-6.

153. Gerlach M. Trust for vehicular applications //null. – IEEE, 2007. – С. 295-304.

154. Minhas U. F. et al. Towards expanded trust management for agents in vehicular ad-hoc networks //International Journal of Computational Intelligence: Theory and Practice (IJCITP). – 2010. – Т. 5. – №. 1. – С. 03-15.

155. Raya M. et al. On data-centric trust establishment in ephemeral ad hoc networks //INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. – IEEE, 2008. – С. 1238-1246.

156. Golle P., Greene D., Staddon J. Detecting and correcting malicious data in VANETs //Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. – ACM, 2004. – С. 29-37.

157. Dotzer F., Fischer L., Magiera P. Vars: A vehicle ad-hoc network reputation system //World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a. – IEEE, 2005. – С. 454-456.

158. Patwardhan A. et al. A data intensive reputation management scheme for vehicular ad hoc networks //Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on. – IEEE, 2006. – С. 1-8.

159. Sahoo R. R. et al. A trust based clustering with Ant Colony Routing in VANET //Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on. – IEEE, 2012. – С. 1-8.

160. Fonseca E., Festag A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETS //NEC network laboratories. – 2006. – Т. 28. – С. 1-28.

161. Botelho S. C., Alami R. M+: a scheme for multi-robot cooperation through negotiated task allocation and achievement //Robotics and Automation, 1999. Proceedings. 1999 IEEE International Conference on. – IEEE, 1999. – Т. 2. – С. 1234-1239.

162. Давыдов О. И., Платонов А. К. Робот и Искусственный Интеллект. Технократический подход //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2017. – №. 0. – С. 112-24.

163. Давыдов О. И., Платонов А. К. База данных для семантической модели операционной среды мобильного сервисного робота //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2017. – №. 0. – С. 7-24.

164. Маслобоев А. В., Путилов В. А. Разработка и реализация механизмов управления информационной безопасностью мобильных

агентов в распределенных мультиагентных информационных системах //Вестник Мурманского государственного технического университета. – 2010. – Т. 13. – №. 4-2.

165. Зикратов И. А., Зикратова Т. В., Лебедев И. С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением //Научно-технический вестник информационных технологий, механики и оптики. – 2014. – №. 2 (90).

166. Тихов М. С., Агеев В. В., Бородина Т. С. Оценивание параметров распределения Вейбулла по случайно цензурированным выборкам //Вестник Нижегородского университета им. НИ Лобачевского. – 2010. – №. 4.

167. Guan X., Yang Y., You J. POM-a mobile agent security model against malicious hosts //hpc. – IEEE, 2000. – С. 1165.

168. Гайдамакин Н. А. Зональная модель разграничения доступа в распределенных компьютерных системах //Научно-техническая информация. Серия. – 2002. – Т. 2. – С. 15-22.

169. Норсеев С. А., Багаев Д. В. Обзор алгоритмов группового управления робототехническими комплексами //Электротехнические системы и комплексы. – 2013. – №. 21.

170. Зикратов И. А., Викснин И. И., Зикратова Т. В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами //Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – №. 5.

171. Alexeevich Z. I., Viksnin Ilya I., Viktorovna Z. T. MULTIAGENT PLANNING OF INTERSECTION PASSAGE BY AUTONOMOUS VEHICLES //Journal Scientific and Technical Of Information Technologies, Mechanics and Optics. – 2018. – Т. 115. – №. 3. – С. 839.

172. Викснин И.И. и др. Подход к обнаружению новых кибератак на киберфизические системы на основании метода обнаружения аномалий // Автоматизация в промышленности -2018. - Т. 2. - С. 48-52

173. Viksnin I. I. et al. Approaches to communication organization within cyber-physical systems //Open Innovations Association (FRUCT), 2017 20th Conference of. – IEEE, 2017. – С. 484-490.

174. Викснин И.И., Патрикеев Р.О., Щепин Н.Д., Комаров И.И. Разработка инструментальных средств моделирования подходов организации связи в мобильных робототехнических системах //Сборник тезисов докладов конгресса молодых ученых. Электронное издание [Электронный ресурс]. Режим доступа: http://kmu.ifmo.ru/collections_article/5020/razrabotka_instrumentalnyh_sredstv_modelirovaniya_podhodov_organizacii_svyazi_v_mobilnyh_robototehnicheskih_sistemah.htm

175. Викснин И.И., Гатауллин Р.И., Шлыков А.А. Разработка имитационной модели мультиагентных робототехнических систем //Сборник тезисов докладов конгресса молодых ученых. Электронное издание [Электронный ресурс]. - Режим доступа: http://kmu.ifmo.ru/collections_article/3965/razrabotka_imitacionnoy_modeli_multiagentnyh_robototehnicheskih_sistem.htm

176. Викснин И.И., Шлыков А.А., Назыров М.В., Комаров И.И. Проектирование архитектуры инструментального средства моделирования поведения сети типа P2P // Альманах научных работ молодых ученых Университета ИТМО -2016. - Т. 5. - С. 274-276

177. Viksnin I. I. et al. Planning of Autonomous Multi-agent Intersection //ITM Web of Conferences. – EDP Sciences, 2016. – Т. 8. – С. 01007.

Список сокращений и условных обозначений

АСУ ТП	Автоматизированная система управления технологическим процессом
АТС	Автономное транспортное средство
БПЛА	Беспилотный летательный аппарат
БТС	Беспилотное транспортное средство
ВУ	Вычислительное устройство
ДИВ	Деструктивное информационное воздействие
ИБ	Информационная безопасность
ИВ	Информационное воздействие
ИТС	Интеллектуальное транспортное средство
КФС	Киберфизическая система
МАС	Мультиагентная система
МРТС	Мобильная робототехническая система
СДИВ	Скрытое деструктивное информационное воздействие
ТС	Транспортное средство
ФУ	Физическое устройство
ЦВЭ	Центральный вычислительный элемент
ЦС	Центр сертификации
DGPS	Differential global positioning system (дифференциальная система глобального позиционирования)
DoS	Denial of service (отказ в обслуживании)

GPS	Global positioning system (система глобального позиционирования)
IoT	Internet of things (интернет вещей)
IVI	In-vehicle infotainment (информационно-развлекательная система в автомобиле)
PO	Police office (полицейский участок)
POM	Police office model (модель полицейских участков)
P2P	Peer-to-peer (пиринговая сеть)
RoQ	Reduction of quality (снижение качества)
UML	Unified modelling language (унифицированный язык моделирования)
VANET	Vehicular ad hoc networks (специальные автомобильные сети)
V2R	Vehicle-to-roadside (сеть между транспортными средствами и объектами дорожной инфраструктуры)
V2V	Vehicle-to-vehicle (сеть между транспортными средствами)

Приложение А

Программный код инструментального средства для проверки продуктивности метода доверия и репутации

Robot

```
package Robots;

import java.util.ArrayList;
import Point.*;
import Targets.*;
import Data.Input;

public class Robot {
    public Boolean isGood;
    public int id;
    public Point coor;
    public ArrayList<Double> DtTs = new ArrayList<Double>();
    public boolean isFree;
    public Input.Saboteur saboteurType;
    private double trustInMe=0;

    public Robot(Point coordinates, boolean goodness, int id, Input.Saboteur
sabType){
        this.coor = coordinates;
        this.isGood = goodness;
        this.id=id;
        this.saboteurType = sabType;
    }

    @Override
    public String toString() {return "Robots " +id+" :"+coor+" "+isGood+"
"+isFree;}

    public boolean checkDistance(Target target){
        if (coor.distanceTo(target.coor)==DtTs.get(target.id)){
            return true;
        } else {
            return false;
        }
    }

    public void setTrustInMe(double trustInMe) {
        this.trustInMe = trustInMe;
    }

    public void distanceToTarget(ArrayList<Target> targets) {
        for (Target target : targets) {
            if (isGood) {
                DtTs.add(coor.distanceTo(target.coor));
            } else {
                if ((Input.saboteurType!=Input.Saboteur.smartTrust) &&
(Input.saboteurType!=Input.Saboteur.smartsmart)) {
                    DtTs.add(coor.distanceTo(target.coor) / 2);
                } else {
                    if (trustInMe >= 0.8) {
                        DtTs.add(0.1);
                    } else {
                        DtTs.add(coor.distanceTo(target.coor));
```

```
                    }
                }
            }
        }
    }
}
```

Swarm

```
package Robots;

import Data.Input;
import Targets.Target;
import Point.*;
import Statistic.Error1Kind;
import Statistic.Error2Kind;

import java.util.ArrayList;


public class Swarm {
    public ArrayList<Robot> auction(ArrayList<Robot> swarm, ArrayList<Target>
targets, double[][] trust){
        boolean[] opinion = setOpinion(swarm, trust);
        Point centre = new Point(0,0);
        if (swarm.size()>0) {
            centre = getCenterOfSwarm(swarm);
        }
        double p=0;
        int idTarget, idRobot;
        for (Robot robot: swarm) {
            robot.isFree = true;
        }
        nullSwarm: while (sizeSwarm(swarm)) {
            idTarget = getNearestTarget(p, centre, targets);
            if (idTarget == -1){
                break;
            }
            p = centre.distanceTo(targets.get(idTarget).coor);
            for (int i = 0; i < targets.get(idTarget).need; i++) {
                idRobot = getNearestRobot(swarm, targets.get(idTarget),
opinion);
                if (idRobot == -1){
                    break nullSwarm;
                }
                moveRobot(swarm.get(idRobot), targets.get(idTarget));
                if (swarm.get(idRobot).isGood) {
                    targets.get(idTarget).currentNeed--;
                }

            }
        }
        return swarm;
    }

    private Point getCenterOfSwarm(ArrayList<Robot> swarm){
        int meanX = 0,
                meanY = 0;
        for (Robot robot: swarm) {
            meanX += robot.coor.x();
            meanY += robot.coor.y();
        }
        if (swarm.size()==0){
            System.out.println(swarm);
```

```
        }
        meanX /= swarm.size();
        meanY /= swarm.size();
        return new Point(meanX,meanY);
    }

    private int getNearestTarget(double distance, Point center,
ArrayList<Target> targets){
        int idMin = -1;
        double min = 1000000000;
        for (Target target: targets) {
            if ((center.distanceTo(target.coor) < min) &&
(center.distanceTo(target.coor)>distance)) {
                min = center.distanceTo(target.coor);
                idMin = targets.indexOf(target);
            }
        }
        return idMin;
    }

    private boolean sizeSwarm(ArrayList<Robot> swarm){
        int size=0;
        for (Robot robot: swarm) {
            if (robot.isFree){
                size++;
            }
        }
        if (size > 0){
            return true;
        } else {
            return false;
        }
    }

    private int getNearestRobot(ArrayList<Robot> swarm,Target target,
boolean[] opinion){
        int idRobot = -1;
        double min = 1000000000;
        for (Robot robot: swarm) {
            if ((robot.coor.distanceTo(target.coor) < min) &&
(opinion[swarm.indexOf(robot)]) && (robot.isFree)){
                min = robot.coor.distanceTo(target.coor);
                idRobot = swarm.indexOf(robot);
            }
        }
        if (idRobot != -1) {
            swarm.get(idRobot).isFree = false;
        }
        return idRobot;
    }

    private void moveRobot(Robot robot, Target target){
        robot.coor = target.coor;
    }

    private boolean[] setOpinion(ArrayList<Robot> swarm, double[][] trust){
        boolean[] opinion = new boolean[swarm.size()];
       for (Robot robot: swarm) {
            opinion[swarm.indexOf(robot)] = checkTrust(robot, trust,
swarm.size());
        }
        return opinion;
    }
```

```
    private boolean checkTrust(Robot robot, double[][] trust,  int
swarmSize){
        if (trust[robot.id][0] >= Input.getEdge()) {
            if (swarmSize>1) {
                if (robot.isGood) {
                    Error1Kind.update(true);
                } else {
                    Error2Kind.update(true);
                }
            }
            return true;
        } else {
            if (swarmSize>1) {
                if (robot.isGood) {
                    Error1Kind.update(false);
                } else {
                    Error2Kind.update(false);
                }
            }
            return false;
        }
    }
}
```

Swarms

```
package Robots;

import java.util.ArrayList;
import java.util.Random;

import Data.Constants;
import Data.Input;
import Point.Point;
import Targets.Target;

public class Swarms {
    public ArrayList<ArrayList<Robot>> swarms = new
ArrayList<ArrayList<Robot>>();
    final static Random random = new Random();
    public static int mapSize;
    public int countSwarms,
               countRobots;

    public void generateMap() {
        int index = 0;
        Point nextRobot;
        countSwarms = Data.Input.getCountSwarms();
        countRobots = Data.Input.getCountRobots();
        mapSize = mapSize(countRobots);

        ArrayList<Integer> countRobotsInSwarms =
countRobotsInSwarms(countSwarms, countRobots),
                           countBadRobotsInSwarms =
countBadRobotsInSwarms(countSwarms, countRobotsInSwarms);

        for (int i = 0; i < countSwarms; i++) {
            ArrayList<Robot> swarm = new ArrayList<Robot>();
            if (Data.Input.getPercentBadRobots() == 100){
                swarm.add(new Robot(CoorFirstRobotinSwarm(i, mapSize), false,
index++, Input.getSaboteurType()));
            } else {
```

```
                swarm.add(new Robot(CoorFirstRobotinSwarm(i, mapSize), true,
index++, Input.Saboteur.none));
            }
            for (int j = 1; j < countRobotsInSwarms.get(i); j++) {
                nextRobot = coorNextRobot(swarm.get(swarm.size() - 1).coor,
i, mapSize);
                if (Data.Input.getPercentBadRobots()!=0 && j %
(100/Data.Input.getPercentBadRobots()) != 0) {
                    swarm.add(new Robot(nextRobot, true, index++,
Input.Saboteur.none));
                } else {
                    swarm.add(new Robot(nextRobot, false, index++,
Input.getSaboteurType()));
                }
            }
            swarms.add(swarm);
        }

    }

    private void clearDistanceToTargets(){
        for (ArrayList<Robot> swarm: swarms ) {
            for (Robot robot: swarm) {
                robot.DtTs.clear();
            }
        }
    }

    public void filingDistanceToTargets(ArrayList<Target> targets){
        clearDistanceToTargets();
        for (ArrayList<Robot> swarm: swarms ) {
            for (Robot robot: swarm) {
                robot.distanceToTarget(targets);
            }
        }
    }

    private int mapSize(int countRobots){
        return  2*((int)Math.sqrt(countRobots)-
1)*Constants.radiusInteraction;
    }

    private ArrayList<Integer> countRobotsInSwarms(int countSwarms, int
countRobots){
        ArrayList<Integer> countRobotsInSwarms = new ArrayList<Integer>();
        for (int i = 0; i < countSwarms-1; i++) {
            countRobotsInSwarms.add(countRobots/countSwarms);
        }
        countRobotsInSwarms.add(countRobots -
(countRobots/countSwarms)*(countSwarms-1));
        return countRobotsInSwarms;
    }

    private ArrayList<Integer> countBadRobotsInSwarms(int countSwarms,
ArrayList<Integer> countRobotsInSwarms){
        ArrayList<Integer> countBadRobotsInSwarms = new ArrayList<Integer>();
        for (int i = 0; i < countSwarms; i++) {

countBadRobotsInSwarms.add(Data.Input.getPercentBadRobots()*countRobotsInSwar
ms.get(i)/100);
        }
        return countBadRobotsInSwarms;
    }
```

```
    private Point CoorFirstRobotinSwarm(int numberOfSwarm, int mapSize) {
        int x = random.nextInt(mapSize);
        int y = random.nextInt(mapSize);
        while (!checkPoint(new Point(x,y))) {
            x = random.nextInt(mapSize);
            y = random.nextInt(mapSize);
        }
            return new Point(x, y);
    }

    private Point coorNextRobot(Point X, int numberOfSwarm, int mapSize){
        int y = X.y(),
            x = X.x();

        int x1 = x+random.nextInt(2* Constants.radiusInteraction)-
Constants.radiusInteraction;
        int y1 = y+random.nextInt(2* Constants.radiusInteraction)-
Constants.radiusInteraction;
//        Проверка точки
        while (!checkPoint(new Point(x1,y1))){
            x1 = x+random.nextInt(2* Constants.radiusInteraction)-
Constants.radiusInteraction;
            y1 = y+random.nextInt(2* Constants.radiusInteraction)-
Constants.radiusInteraction;
        }
        return new Point(x1,y1);
    }

    private boolean checkPoint(Point p){
        for (ArrayList<Robot> swarm: swarms){
            for (Robot robot: swarm) {
                if (p.distanceTo(robot.coor)<=Constants.radiusInteraction*3){
                    return false;
                }
            }
        }
        if ((p.x()<5) || (p.x()>mapSize-5) || (p.y()<5) || (p.y()>mapSize-
5)){
            return false;
        }
        return true;
    }

    public ArrayList<ArrayList<Robot>>
RedistributionOfRobotsInSwarms(ArrayList<Target> targets){
        int amountSwarms = swarms.size(),
            amountRobots;
        Robot robotStorage;
        for (int i = 0; i < targets.size(); i++) {
            swarms.add(new ArrayList<Robot>());
        }
        for (int i = 0; i < amountSwarms; i++) {
            amountRobots = swarms.get(i).size();
            for (int j = 0; j < amountRobots; j++) {
                if (!swarms.get(i).get(j).isFree){
                    robotStorage = swarms.get(i).get(j);
                    swarms.get(i).remove(swarms.get(i).get(j));

swarms.get(amountSwarms+findTarget(robotStorage,targets)).add(robotStorage);
                    j--;
                    amountRobots--;
                    if (swarms.get(i).size()==0){
```

```
                        break;
                    }
                }
            }
        }
        deleteNullSwarm(amountSwarms);
        changeStatus();
        return swarms;
    }

    private int findTarget(Robot robot, ArrayList<Target> targets){
        for (Target target: targets) {
            if(target.coor == robot.coor){
                return target.id;
            }
        }
        return -1;
    }

    private void deleteNullSwarm(int amountSwarms){
        for (int i = 0; i < amountSwarms; i++) {
            if (swarms.get(i).size() == 0){
                swarms.remove(swarms.get(i));
                amountSwarms--;
                i--;
            }
        }
    }

    private void changeStatus(){
        for (ArrayList<Robot> swarm: swarms) {
            for (Robot robot: swarm) {
                robot.isFree = true;
            }
        }
    }
}
```

Target

```
 package Targets;

import Point.Point;

public class Target {
    public Point coor;
    public int id,
               need,
               currentNeed;


    public Target(Point coordinates,  int id, int need){
        this.coor = coordinates;
        this.id=id;
        this.need = need;
        this.currentNeed = need;
    }

    @Override
    public String toString() {return "Target "+id+" :"+coor+" "+need;}

}
```

Targets

```
package Targets;

import Data.Constants;
import Robots.*;

import java.util.ArrayList;
import java.util.Random;
import Point.*;

public class Targets {
    public ArrayList<Target> targets = new ArrayList<Target>();
    final static Random random = new Random();

    public void levelUp(int countRobots){
        int countTargets = random.nextInt(5)+5;
        targets.clear();
        //Общая потребность целей 100%
        int needCurrentTarget;
        for (int i = 0; i < countTargets-1; i++) {
            Data.Constants.updateTargetNeedPercent();
            needCurrentTarget = (countRobots/countTargets)*
Constants.targetNeedPercent/100;
            targets.add(new Target(new Point(random.nextInt(Swarms.mapSize),
random.nextInt(Swarms.mapSize)), i, needCurrentTarget));
        }
        Data.Constants.updateTargetNeedPercent();
        needCurrentTarget = (countRobots -
(countRobots/countTargets)*(countTargets-1))*Constants.targetNeedPercent/100;
        targets.add(new Target(new Point(random.nextInt(Swarms.mapSize),
random.nextInt(Swarms.mapSize)), countTargets-1, needCurrentTarget));
    }
}
```

Reputation

```
package Trust;

import Robots.*;

import java.util.ArrayList;

/**
 * Created by Vasovski on 19.07.2017.
 */
public class Reputation {

    private double[][] notNormReputation;
    public static double[][] reputation;
    public Reputation(int countRobots) {
        notNormReputation = new double[countRobots][countRobots];
        reputation = new double[countRobots][countRobots];
    }

    public void reReputation(int iteration, ArrayList<ArrayList<Robot>>
swarms) {
        for (ArrayList<Robot> swarm : swarms) {
            for (Robot obj : swarm) {
                for (Robot sub : swarm) {
                    if (obj.id != sub.id) {
                        if (iteration > 0) {
                            if (Verity.normVerity[obj.id][sub.id] >= 0.5) {
```

```
                                notNormReputation[obj.id][sub.id] +=
Verity.normVerity[obj.id][sub.id];
                            } else {
                                notNormReputation[obj.id][sub.id] =
notNormReputation[obj.id][sub.id] - ((notNormReputation[obj.id][sub.id] /
(iteration) - Math.pow(2.7, -1 * (iteration + 1) * (1 -
Verity.normVerity[obj.id][sub.id]))));
                            }
                        } else {
                            notNormReputation[obj.id][sub.id] +=
Verity.normVerity[obj.id][sub.id];
                        }
                    }
                }
            }
        }
        for (ArrayList<Robot> swarm : swarms) {
            for (Robot obj : swarm) {
                for (Robot sub : swarm) {
                    if (obj.id != sub.id) {
                        if (iteration > 0) {
                            reputation[obj.id][sub.id] =
notNormReputation[obj.id][sub.id] / (Verity.meetengs[obj.id][sub.id]);
                        } else {
                            reputation[obj.id][sub.id] =
notNormReputation[obj.id][sub.id];
                        }
                    }
                }
            }
        }
    }
}
```

Trust

```
package Trust;

import Data.Input;
import Robots.*;

import java.util.ArrayList;
import java.util.Map;


public class Trust {
    public double[][] reTrust(ArrayList<ArrayList<Robot>> swarms,double[][][]
verity, int countRobots, int countTargets){
        double A = Input.getAlpha();
        double B = 1-A;
        double[][][] confidence = new
double[countRobots][countRobots][countTargets];
        double[][] normConfidence = new double[countRobots][countTargets];
        for (ArrayList<Robot> swarm: swarms) {
            for (Robot obj : swarm) {
                for (Robot sub : swarm) {
                    for (int i=0; i<countTargets; i++ ) {
                        if (obj.id!=sub.id) {
                            double v = verity[obj.id][sub.id][i], r =
Reputation.reputation[obj.id][sub.id];
                            confidence[obj.id][sub.id][i] =
```

```
Math.sqrt(v*v+r*r)-Math.sqrt((1-v)*(1-v)+(1-r)*(1-r));
                            //вес
                            //confidence[obj.id][sub.id][i] = (A *
verity[obj.id][sub.id][i] + B * Reputation.reputation[obj.id][sub.id]);
                        }
                    }
                }
            }
        }
        for (ArrayList<Robot> swarm: swarms) {
            for (Robot obj: swarm) {
                for (int j = 0; j < countTargets; j++) {
                    double sum=0;
                    int count = 0;
                    for (Robot sub: swarm) {
                        if ((obj.id != sub.id)) {
                            sum += confidence[sub.id][obj.id][j];
                            count++;
                        }
                    }
                    if (count != 0) {
                        normConfidence[obj.id][j] = sum / count;
                    }
                    obj.setTrustInMe(normConfidence[obj.id][j]);
                }
            }

        }
        return normConfidence;
    }
}
```

Verity

```
package Trust;

import Data.Constants;
import Data.Input;
import Robots.*;
import Targets.*;


import java.util.ArrayList;
import java.util.Random;


public class Verity {
    public static double[][] normVerity;
    public static double[][] meetengs;
    int countRobots;
    final static Random random = new Random();
    public Verity(int countRobots) {
        this.countRobots = countRobots;
        normVerity = new double[countRobots][countRobots];
        meetengs = new double[countRobots][countRobots];
    }

    public double[][][] reVerity(ArrayList<ArrayList<Robot>> swarms,
ArrayList<Target> targets, int iteration){
        double[][][] verity = new
double[countRobots][countRobots][targets.size()];
```

```
        // Выставения всем значения отсутсвия данных.
        for (int i = 0; i < countRobots; i++) {
            for (int j = 0; j < countRobots; j++) {
                for (int k = 0; k < targets.size(); k++) {
                    verity[i][j][k] = 0.5;
                }
            }
        }
        // Заполнение массива встреч
        for (ArrayList<Robot> swarm: swarms) {
            for (Robot obj : swarm) {
                for (Robot sub : swarm) {
                    if (obj.id != sub.id) {
                        meetengs[obj.id][sub.id]=meetengs[obj.id][sub.id]+1;
                    }
                }
            }
        }

//        System.out.println("Выставление");
        //Выставление истинности соседей в зоне видимости
        for (ArrayList<Robot> swarm: swarms) {
            for (Robot obj : swarm) {
                for (Robot sub : swarm) {
                    if (obj.id != sub.id) {
                        if (obj.coor.distanceTo(sub.coor) <=
Constants.radiusVision) {
                            for (Target target : targets) {
//                                ВЫЗОВ МЕТОДА ВЫСТАВЛЕНИЯ ИСТИННОСТИ
                                verity[obj.id][sub.id][target.id] =
getVerity(obj, sub, target, iteration);
//                                if (!obj.isGood){
//                                    System.out.println(obj.id+" ->
"+sub.id+" = "+verity[obj.id][sub.id][target.id]);
//                                }
                            }
                        }
                    }
                }
            }
        }

//        System.out.println("Опрос");
//        Выставление истинности через опрос соседей
        for (Target target: targets) {
            for (ArrayList<Robot> swarm : swarms) {
                for (Robot obj : swarm) {
                    for (Robot sub : swarm) {
                        int count = 0;
                        if (obj.id != sub.id) {
                            if ((obj.coor.distanceTo(sub.coor) >
Constants.radiusVision) && (obj.coor.distanceTo(sub.coor) <
Constants.radiusVision+Constants.radiusInteraction)) {
                                for (Robot neighbor : swarm) {
                                    if ((obj.coor.distanceTo(neighbor.coor) <
Constants.radiusInteraction) && (sub.coor.distanceTo(neighbor.coor) <
Constants.radiusVision) && (verity[neighbor.id][sub.id][target.id] != 0.5)) {
                                        if ((obj.id != neighbor.id) &&
(sub.id != neighbor.id)) {
                                            verity[obj.id][sub.id][target.id]
+= verity[neighbor.id][sub.id][target.id];
                                            count++;
                                        }
```

```
                                    }
                                }
                                if (count != 0) {
                                    verity[obj.id][sub.id][target.id] -= 0.5;
                                    verity[obj.id][sub.id][target.id] /=
count;
                                }
                            }
                        }
                    }
                }
            }

//          Нормирование истинности по количеству целей
            for (int i = 0; i < countRobots; i++) {
                for (int j = 0; j < countRobots; j++) {
                    double sum=0;
                    for (int k = 0; k < targets.size(); k++) {
                        sum+= verity[i][j][k];
                    }
                    normVerity[i][j] = sum/targets.size();
                }
            }
            return verity;
        }
        private double getVerity(Robot obj, Robot sub, Target target, int
iteration){

            if (obj.isGood){
                if (sub.checkDistance(target)) {
                    return  1;
                } else {
                    return  0;
                }
            } else {
                switch(obj.saboteurType) {
                    case BALLOT_STUFFING:
                        return 1;
                    case BAD_MOUTH:
                        return 0;
                    case inversion:
                        return inversion(sub, target);
                    case ON_OFF:
                        return random.nextInt(2) == 0 ? legitimate(sub, target) :
inversion(sub, target);
                    case smartTrust:
                        return legitimate(sub, target);
                    case smartDist:
                        return smartDist(obj, sub, target, iteration);
                    case none:
                        return legitimate(sub, target);
                    case smartsmart:
                        return smartDist(obj, sub, target, iteration);
                    default:
                        return 0;
                }
            }
        }

        private int smartDist(Robot obj, Robot sub, Target target, int
iteration){
            if ((iteration == 0)){
```

```
            return legitimate(sub, target);
        } else{
                if (sub.checkDistance(target)) {
                    if(((1-
Input.A.doubleValue())*Reputation.reputation[obj.id][sub.id]+Input.A.doubleVa
lue()<=0.6)&&(1-
Input.A.doubleValue())*Reputation.reputation[obj.id][sub.id]+Input.A.doubleVa
lue()>=0.5){
                        return inversion(sub, target);
                    }else {
                        return legitimate(sub, target);
                    }
                } else{
                    if(((1-
Input.A.doubleValue())*Reputation.reputation[obj.id][sub.id]<=0.5)&&(1-
Input.A.doubleValue())*Reputation.reputation[obj.id][sub.id]>=0.4){
                        return inversion(sub, target);
                    }else {
                        return legitimate(sub, target);
                    }
                }
        }
    }
    private int legitimate(Robot sub, Target target){
        if (sub.checkDistance(target)) {
            return  1;
        } else {
            return  0;
        }
    }
    private int inversion(Robot sub, Target target){
        if (sub.checkDistance(target)) {
            return  0;
        } else {
            return  1;
        }
    }
}
```

Iteration

```
package WorkSpace;

import java.util.ArrayList;
import Data.Input;
import Robots.*;
import java.util.concurrent.TimeUnit;
import Robots.Robot;
import Statistic.Error1Kind;
import Statistic.Error2Kind;
import Targets.Targets;
import Trust.*;
import java.awt.*;
import Graphic.ExperimentFrame;

public class Iteration {
    public static double[] iteration(ExperimentFrame f, Graphics g) throws
InterruptedException {
        //Начальный блок генерации карты
        Swarm swarm = new Swarm();
        Swarms swarms = new Swarms();
```

```
        Targets targets = new Targets();
        Error1Kind error1 = new Error1Kind();
        Error2Kind error2 = new Error2Kind();
        //Создание карты, целей
        swarms.generateMap();
        targets.levelUp(swarms.countRobots);

        //Графика
        if (swarms.swarms == null) {
            TimeUnit.SECONDS.sleep(5);
        }
        try {
            f.updateData(swarms.swarms, targets.targets, swarms.countRobots,
error1.get(), error2.get(), true, 0);
            f.paint(g);
            TimeUnit.SECONDS.sleep(4);
        } catch (NullPointerException e) {
            System.out.println("Error");
        }


        //Начальный блок доверия
        Verity verity = new Verity(swarms.countRobots);
        Reputation reputation = new Reputation(swarms.countRobots);
        Trust trust = new Trust();

        for (int i = 0; i < Input.getCountLevels(); i++) {
            System.out.print(".");
            swarms.filingDistanceToTargets(targets.targets);
            ////Определение параметров доверия - каждую итерацию
            double[][][] verityTable = verity.reVerity(swarms.swarms,
targets.targets, i);
            reputation.reReputation(i, swarms.swarms);
            double[][] trustTable = trust.reTrust(swarms.swarms, verityTable,
swarms.countRobots, targets.targets.size());
            for (ArrayList<Robot> currentSwarm : swarms.swarms) {
                currentSwarm = swarm.auction(currentSwarm, targets.targets,
trustTable);
            }

            //Распределение роботов по новым роям
            swarms.swarms =
swarms.RedistributionOfRobotsInSwarms(targets.targets);

            //Создание целей
            targets.levelUp(swarms.countRobots);
        }
        double[] result = new double[4];
        result[0] = error1.get();
        result[1] = error2.get();
        return result;
    }
}
```

Main

```
package WorkSpace;

import Data.Input;
import Graphic.ExperimentFrame;
```

```
import java.awt.*;
import java.io.File;
import java.math.BigDecimal;
import java.util.Vector;

public class Main {
    public static void main(String[] args) throws InterruptedException {
        deleteOldResult();
        //В этих 2-х строках выкидывает ошибку NullPointer (я умнее Кати )
        ExperimentFrame f = new ExperimentFrame();
        Graphics g = f.getGraphics();
        defineSaboteurType( f, g);

    }
    private static void defineSaboteurType( ExperimentFrame f, Graphics g )
throws InterruptedException{
        Input.A = new BigDecimal("0");
        getExperiment(f, g);
    }

    private static void getExperiment( ExperimentFrame f, Graphics g) throws
InterruptedException {
        double[] result = new double[3];
        double[] currentResult = new double[2];
        currentResult[0]=0; currentResult[1]=0;
        result[0] = 0; result[1] = 0; result[2] = 0;
        while (Input.haveNext(currentResult[0], currentResult[1])){
            currentResult = Iteration.iteration(f, g);
        }
    }

    private static void deleteOldResult(){
        File file = new File("result.csv");
        if(file.delete()){
            System.out.println("Старый файл удален");
        }else System.out.println("Файла  не обнаружено");
    }
}
```

Приложение Б

Программный код инструментального средства для проверки продуктивности метода временной централизации

SimulationEngine

```
package com.sit.core;

import com.sit.entity.*;
import com.sit.logic.abstr.Generator;
import com.sit.logic.abstr.InputGenerator;
import com.sit.logic.abstr.Logic;
import com.sit.logic.impl.DefaultGenerator;
import com.sit.logic.impl.TestInputGenerator;
import com.sit.statistic.StatCollector;
import com.sit.ui.SimulatorWindow;
import com.sit.util.EntityLocator;
import com.sit.util.Logger;

public class SimulationEngine {
    public static final String
            EVENT_SIMULATION_END = "SIMULATION_END",
            EVENT_NEXT_ITERATION = "NEXT_ITERATION";
    private SimulationContainer simulationContainer;
    private SimulatorWindow window;
    private static SimulationEngine instance;
    private Logic logic;
    private InputGenerator inputGenerator;
    private boolean end_simulation, next_iteration;
    private Generator generator;
    private StatCollector statCollector;
    private boolean repaint = true;

    private SimulationEngine(){}

    public static SimulationEngine getInstance() {
        if (instance == null)
            instance=new SimulationEngine();
        return instance;
    }

    void startEngine(){
        init();
        while (inputGenerator.hasNext()){
            iterationLoop();
        }
        statCollector.print();
    }

    private void init(){
        inputGenerator = new TestInputGenerator();
        Generator tmpGenerator = new
DefaultGenerator(inputGenerator.getNexInputData());
        window = tmpGenerator.getSimulationWindow();
        logic = tmpGenerator.getLogic();
        statCollector = new StatCollector();
    }

    private void iterationLoop(){
```

```
        InputData inputData = inputGenerator.getNexInputData();
        logic.setClear_chance_percent(inputData.getClear_chance_percent());
        generator = new DefaultGenerator(inputData);
        statCollector.addRecord(inputData);
        simulationContainer = generator.generate();
        logic.setEntityLocator(new EntityLocator(simulationContainer));
        end_simulation = false;
        if (inputData.getDelay() == 0)
            repaint=false;
        while (!end_simulation) {
            if (generator.newTasks()) {
                next_iteration = false;
            } else {
                end_simulation=true;
                continue;
            }
            for (String event: logic.getInitEvents()){
                applyEvent(event);
            }
            for (Message message: logic.getInitMessages()){
                sendMessage(message);
            }
            while (!next_iteration) {
                simulationStep();
                if (repaint) {
                    try {
                        Thread.sleep(inputData.getDelay());
                    } catch (InterruptedException e) {
                        e.printStackTrace();
                    }
                }
            }
        }
        statCollector.confirmRecord(simulationContainer);
    }

    private void simulationStep(){
        for (Agent a: simulationContainer.getAgents()){
            a.step();
        }
        for (Agent a: simulationContainer.getAgents()){
            if (a.haveTransaction()) continue;
            Transaction transaction = findNewTransaction(a);
            if (transaction!=null) {
                applyTransaction(transaction);
            }
        }
        if (window!=null && repaint)
            window.repaint();
    }

    private Transaction findNewTransaction(Agent a){
        for (Message message:a.getUnsended_messages()){
            if (message.getReceiver().haveTransaction()) continue;
            return new Transaction(message);
        }
        return null;
    }

    public void completeTransaction(Transaction transaction){
        Agent sender = transaction.getSender(), receiver =
transaction.getReceiver();
        if (sender.getTransaction()== transaction)
```

```
            sender.setTransaction(null);
        else throw new RuntimeException("Transaction already removed from
sender!");
        if (receiver.getTransaction()== transaction)
            receiver.setTransaction(null);
        else throw new RuntimeException("Transaction already removed from
receiver!");
        logic.venom(transaction);
        for (Message message:logic.getNextMessages(transaction)){
            sendMessage(message);
        }
        for (String event: logic.getNextEvents(transaction)){
            applyEvent(event);
        }
    }

    private void applyTransaction(Transaction transaction){
        Agent sender = transaction.getSender(), receiver =
transaction.getReceiver();
        if (receiver==sender)
            Logger.log("CAUTION! SENDER == RECEIVER");
        if (sender.haveTransaction() || receiver.haveTransaction())
            throw new RuntimeException("Transaction is not empty! Can't apply
new transaction");
        sender.removeMessage(transaction.getMessage());
        sender.setTransaction(transaction);
        receiver.setTransaction(transaction);
    }

    private void sendMessage(Message message){
        message.getSender().addMessage(message);
    }

    public SimulationContainer getSimulationContainer() {
        return simulationContainer;
    }

    private void applyEvent(String event){
        switch (event){
            case EVENT_SIMULATION_END: endSimulation(); break;
            case EVENT_NEXT_ITERATION: nextIteration(); break;
        }
    }

    private void endSimulation(){
        end_simulation=true;
    }

    private void nextIteration(){
        next_iteration=true;
    }
}
```

Agent

```
package com.sit.entity;

import com.sit.util.Logger;
```

```
import java.awt.*;
import java.util.Collection;
import java.util.HashSet;

public class Agent implements Entity {
    //physical properties
    private int x,y;
    private Color color = Color.BLUE;
    private int radius = 10;

    //logic properties
    private boolean
        saboteur,
        manager,//true if agent manager, false if executor
        broken,//can be true only for managers
        leader;
    private Collection<Agent> executors = new HashSet<>();//dependant
executors
    private Transaction transaction;
    private Collection<Message> unsended_messages = new
HashSet<>();//messages waiting to open chanel
    private int wrong_actions = 0;

    public void step(){
        if (transaction != null)
            transaction.step();
    }

    public void receiveMessage(Message message){

    }

    public boolean haveTransaction(){
        return transaction != null;
    }

    public Color getColor() {
        return color;
    }

    public void setColor(Color color) {
        this.color = color;
    }

    public int getRadius() {
        return radius;
    }

    public void setRadius(int radius) {
        this.radius = radius;
    }

    public boolean isSaboteur() {
        return saboteur;
    }

    public void setSaboteur(boolean saboteur) {
        this.saboteur = saboteur;
    }

    public boolean isManager() {
        return manager;
    }
```

```
public void setManager(boolean manager) {
    this.manager = manager;
}

public boolean isBroken() {
    return broken;
}

public void setBroken(boolean broken) {
    this.broken = broken;
}

public boolean isLeader() {
    return leader;
}

public void setLeader(boolean leader) {
    this.leader = leader;
}

public void removeMessage(Message message){
    if (!unsended_messages.remove(message))
        Logger.log("CAUTION: message was not removed");
}

public int getX() {
    return x;
}

public void setX(int x) {
    this.x = x;
}

public int getY() {
    return y;
}

public void setY(int y) {
    this.y = y;
}

public Collection<Agent> getExecutors() {
    return executors;
}

public Transaction getTransaction() {
    return transaction;
}

public Collection<Message> getUnsended_messages() {
    return unsended_messages;
}

public void addExecutor(Agent a){
    executors.add(a);
}

public void addMessage(Message message){
    unsended_messages.add(message);
}

public void setTransaction(Transaction transaction) {
```

```
        this.transaction = transaction;
    }

    public int getWrong_actions() {
        return wrong_actions;
    }

    public void addWrong_action(){
        wrong_actions++;
    }

    @Override
    public void completeCreation() {

    }
}
```

Cluster

```
package com.sit.entity;

import java.awt.*;
import java.util.Collection;
import java.util.HashSet;

public class Cluster implements Entity {
    //physical properties
    private Color color;

    //logic properties
    private Collection<Agent> agents = new HashSet<>(), managers = new
HashSet<>(), executors = new HashSet<>();
    private Agent phys_lead, manager_lead;

    public void addAgent(Agent a){
        agents.add(a);
    }

    public void addAgents(Collection<Agent> agents){
        this.agents.addAll(agents);
    }

    @Override
    public void completeCreation() {
        for (Agent a: agents){
            a.setColor(color);
            if (a.isLeader()){
                if (a.isManager()){
                    manager_lead = a;
                } else {
                    phys_lead = a;
                }
            }
            if (a.isManager()){
                managers.add(a);
            } else {
```

```
                executors.add(a);
            }
        }
    }

    public Collection<Agent> getAgents() {
        return agents;
    }

    public Agent getPhys_lead() {
        return phys_lead;
    }

    public Agent getManager_lead() {
        return manager_lead;
    }

    public Collection<Agent> getManagers() {
        return managers;
    }

    public Collection<Agent> getExecutors() {
        return executors;
    }

    public void setColor(Color color) {
        this.color = color;
    }
}
```

InputData

```
package com.sit.entity;

public class InputData {
    //Logic part
    private int
            agent_num,
            saboteur_percent,
            cluster_num,
            iter_num,
            broken_managers_percent,
            clear_chance_percent = 101,
            error_1st_type_percent;

    //UI part
    private int
        robot_zone_height = 600,
        robot_zone_width = 600,
        border = 60,
        managers_executors_dif = 80,
        delay = 0;

    //other
    private int transaction_time = 1;
```

```
public int getAgent_num() {
    return agent_num;
}

public void setAgent_num(int agent_num) {
    this.agent_num = agent_num;
}

public int getSaboteur_percent() {
    return saboteur_percent;
}

public void setSaboteur_percent(int saboteur_percent) {
    this.saboteur_percent = saboteur_percent;
}

public int getCluster_num() {
    return cluster_num;
}

public void setCluster_num(int cluster_num) {
    this.cluster_num = cluster_num;
}

public int getError_1st_type_percent() {
    return error_1st_type_percent;
}

public void setError_1st_type_percent(int error_1st_type_percent) {
    this.error_1st_type_percent = error_1st_type_percent;
}

public int getIter_num() {
    return iter_num;
}

public void setIter_num(int iter_num) {
    this.iter_num = iter_num;
}

public int getRobot_zone_height() {
    return robot_zone_height;
}

public void setRobot_zone_height(int robot_zone_height) {
    this.robot_zone_height = robot_zone_height;
}

public int getRobot_zone_width() {
    return robot_zone_width;
}

public void setRobot_zone_width(int robot_zone_width) {
    this.robot_zone_width = robot_zone_width;
}

public int getBorder() {
    return border;
}

public void setBorder(int border) {
    this.border = border;
}
```

```
    public int getManagers_executors_dif() {
        return managers_executors_dif;
    }

    public void setManagers_executors_dif(int managers_executors_dif) {
        this.managers_executors_dif = managers_executors_dif;
    }

    public int getBroken_managers_percent() {
        return broken_managers_percent;
    }

    public void setBroken_managers_percent(int broken_managers_percent) {
        this.broken_managers_percent = broken_managers_percent;
    }

    public int getTransaction_time() {
        return transaction_time;
    }

    public void setTransaction_time(int transaction_time) {
        this.transaction_time = transaction_time;
    }

    public int getClear_chance_percent() {
        return clear_chance_percent;
    }

    public void setClear_chance_percent(int clear_chance_percent) {
        this.clear_chance_percent = clear_chance_percent;
    }

    public int getDelay() {
        return delay;
    }

    public void setDelay(int delay) {
        this.delay = delay;
    }
}
```

Message

```
package com.sit.entity;


public class Message {
    private Agent receiver, sender;
    private Task task;
    private String message;
    private int time;

    public Agent getReceiver() {
        return receiver;
    }

    public void setReceiver(Agent receiver) {
        this.receiver = receiver;
```

```
    }

    public Agent getSender() {
        return sender;
    }

    public void setSender(Agent sender) {
        this.sender = sender;
    }

    public Task getTask() {
        return task;
    }

    public void setTask(Task task) {
        this.task = task;
    }

    public String getMessage() {
        return message;
    }

    public void setMessage(String message) {
        this.message = message;
    }

    public int getTime() {
        return time;
    }

    public void setTime(int time) {
        this.time = time;
    }

}
```

Task

```
package com.sit.entity;

public class Task implements Entity {
    private Agent executor, manager;
    private TaskState state = TaskState.ENTERING;
    private int transaction_time, counter;
    private boolean plan_infected=false, report_infected=false;

    public Agent getExecutor() {
        return executor;
    }

    public void setExecutor(Agent executor) {
        this.executor = executor;
    }

    public Agent getManager() {
        return manager;
    }

    public void setManager(Agent manager) {
        this.manager = manager;
    }

    public TaskState getState() {
```

```
        return state;
    }

    public void setState(TaskState state) {
        this.state = state;
    }

    public int getTransaction_time() {
        return transaction_time;
    }

    public void setTransaction_time(int transaction_time) {
        this.transaction_time = transaction_time;
    }

    public boolean isPlan_infected() {
        return plan_infected;
    }

    public void setPlan_infected(boolean plan_infected) {
        this.plan_infected = plan_infected;
    }

    public boolean isReport_infected() {
        return report_infected;
    }

    public void setReport_infected(boolean report_infected) {
        this.report_infected = report_infected;
    }

    public int getCounter() {
        return counter;
    }

    public void setCounter(int counter) {
        this.counter = counter;
    }

    public void counterIncr(){
        counter++;
    }

    @Override
    public void completeCreation() {

    }
}
```

TaskState

```
package com.sit.entity;

public enum TaskState {
    ENTERING,
    CONFIRM_PLAN_WITH_MANAGERS,
    PLAN_SENT_TO_INF_LEAD,
    SENT_TO_PHY_LEADER,
    SENT_TO_EXECUTOR,
    REPORT_SENT_TO_PHY_LEADER,
    REPORT_SENT_TO_INF_LEADER,
    SHARE_REPORT,
```

```
    FINISHED
}
```

Transaction

```
package com.sit.entity;

import com.sit.core.SimulationEngine;

public class Transaction {
    private Agent receiver, sender;
    private int remaining_time;
    private Message message;

    public Transaction(Message message) {
        this.receiver = message.getReceiver();
        this.sender = message.getSender();
        this.remaining_time = message.getTime();
        this.message=message;
    }

    public void step(){
        if (remaining_time==0) return;
        remaining_time--;
        if (remaining_time == 0){
            SimulationEngine.getInstance().completeTransaction(this);
        }
    }

    public Agent getReceiver() {
        return receiver;
    }

    public Agent getSender() {
        return sender;
    }

    public int getRemaining_time() {
        return remaining_time;
    }

    public Message getMessage() {
        return message;
    }
}
```

ClusterIterableLogic

```
package com.sit.logic.impl;

import com.sit.core.SimulationEngine;
import com.sit.entity.*;
import com.sit.logic.abstr.Logic;
import com.sit.util.EntityLocator;

import java.util.*;

public class ClusterIterableLogic implements Logic {
    private EntityLocator entityLocator;
    private int clear_chance_percent;
    private int error_1st_type_percent;
```

```
    private final static Collection<TaskState>
            PLAN_STATES = Arrays.asList(
                TaskState.CONFIRM_PLAN_WITH_MANAGERS,
                TaskState.PLAN_SENT_TO_INF_LEAD,
                TaskState.SENT_TO_PHY_LEADER,
                TaskState.SENT_TO_EXECUTOR
            ),
            REPORT_STATES = Arrays.asList(
                    TaskState.REPORT_SENT_TO_PHY_LEADER,
                    TaskState.REPORT_SENT_TO_INF_LEADER,
                    TaskState.SHARE_REPORT
            );

    @Override
    public void setEntityLocator(EntityLocator entityLocator) {
        this.entityLocator = entityLocator;
    }

    @Override
    public void venom(Transaction transaction) {
        Task task = transaction.getMessage().getTask();
        if (PLAN_STATES.contains(task.getState())){
            if (transaction.getSender().isSaboteur())
                task.setPlan_infected(true);
        }
        if (REPORT_STATES.contains(task.getState())){
            if (transaction.getSender().isSaboteur())
                task.setReport_infected(true);
        }
        //infect plan if task manager saboteur
        if (task.getState().equals(TaskState.CONFIRM_PLAN_WITH_MANAGERS) &&
task.getManager() == transaction.getSender()
                && task.getManager().isBroken()){
            task.setPlan_infected(true);
        }
        if (!transaction.getSender().isSaboteur()){
            if (task.isPlan_infected()) {
                if (new Random().nextInt(100) < clear_chance_percent) {
                    task.setPlan_infected(false);
                    task.setReport_infected(false);
                }
            } else {
                if (new Random().nextInt(100)< error_1st_type_percent){
                    task.setPlan_infected(true);
                }
            }
        }
        if (task.isPlan_infected()){
            if (!transaction.getReceiver().isManager()) {
                if (task.getExecutor() == transaction.getReceiver()){
                    transaction.getReceiver().addWrong_action();
                }
            }
        }
    }

    @Override
    public Collection<Message> getNextMessages(Transaction transaction) {
        return nextAction(transaction);
    }

    @Override
    public Collection<String> getNextEvents(Transaction transaction) {
```

```
        Collection<String> events = new HashSet<>();
        if
(transaction.getMessage().getTask().getState().equals(TaskState.FINISHED)){
            boolean f=true;
            for (Task t: entityLocator.getTasks()){
                if (!t.getState().equals(TaskState.FINISHED)){
                    f=false;
                    break;
                }
            }
            if (f){
                events.add(SimulationEngine.EVENT_NEXT_ITERATION);
            }
        }
        return events;
    }

    @Override
    public Collection<Message> getInitMessages() {
        Collection<Message> messages = new HashSet<>();
        for (Task task: entityLocator.getTasks()){
            messages.addAll(sendPlanInfLead(task));
        }
        return messages;
    }

    @Override
    public Collection<String> getInitEvents() {
        return new HashSet<>();
    }

    private Collection<Message> nextAction(Transaction transaction){
        switch (transaction.getMessage().getTask().getState()){
            case CONFIRM_PLAN_WITH_MANAGERS: return confirmPlan(transaction);
            case PLAN_SENT_TO_INF_LEAD: return
sendPlanToPhyLead(transaction);
            case SENT_TO_PHY_LEADER: return sendToExecutor(transaction);
            case SENT_TO_EXECUTOR: return sendReport(transaction);
            case REPORT_SENT_TO_PHY_LEADER: return
sendReportToInfLeader(transaction);
            case REPORT_SENT_TO_INF_LEADER: return shareReport(transaction);
            case SHARE_REPORT: return tryToFinish(transaction);
        }
        return new HashSet<>();
    }

    private Collection<Message> sendPlanInfLead(Task task){
        Collection<Message> messages = new HashSet<>();
        task.setState(TaskState.CONFIRM_PLAN_WITH_MANAGERS);
        task.setCounter(1);
        if (task.getManager().isLeader()){
            Collection<Agent> agents = new HashSet<>();
            agents.addAll(entityLocator.getManagerLeaders());

agents.addAll(entityLocator.getSameClusterManagers(task.getManager()));
            agents.remove(task.getManager());
            for (Agent a: agents){
                Message m=new Message();
                m.setTime(task.getTransaction_time());
                m.setSender(task.getManager());
                m.setTask(task);
                m.setReceiver(a);
                messages.add(m);
```

```
            }
        } else {
            Message m = new Message();
            m.setTime(task.getTransaction_time());
            m.setSender(task.getManager());
            m.setTask(task);
            m.setReceiver(entityLocator.getManagerLeader(task.getManager()));
            messages.add(m);
        }
        return messages;
    }

    private Collection<Message> confirmPlan(Transaction transaction){
        Collection<Message> messages = new HashSet<>();
        Message message = transaction.getMessage();
        Task task = message.getTask();
        task.counterIncr();
        if (task.getCounter() == entityLocator.getManagers().size()){
            //if all managers confirm plan it is time to send plan
            if (task.getManager().isLeader()){
                messages.add(sendPlanToPhyLead(task));
            } else {
                messages.add(sendPlanToInfLead(task));
            }
        } else if (transaction.getReceiver().isLeader()){
            Collection<Agent> agents;
            if
(entityLocator.getSameClusterManagers(transaction.getReceiver()).contains(tra
nsaction.getSender())){
                //if from dependant manager
                agents = entityLocator.getManagerLeaders();

agents.addAll(entityLocator.getSameClusterManagers(transaction.getReceiver())
);
                agents.remove(transaction.getSender());
            } else {
                //if receiver leader send plan to other cluster's managers
                agents =
entityLocator.getSameClusterManagers(transaction.getReceiver());
            }
            agents.remove(transaction.getReceiver());
            messages.addAll(sendMultiple(agents, task,
transaction.getReceiver()));
        }
        return messages;
    }

    private Message sendPlanToInfLead(Task task){
        Message m = new Message();
        m.setTime(task.getTransaction_time());
        m.setSender(task.getManager());
        m.setReceiver(entityLocator.getManagerLeader(task.getManager()));
        m.setTask(task);
        task.setState(TaskState.PLAN_SENT_TO_INF_LEAD);
        return m;
    }

    private Collection<Message> sendPlanToPhyLead(Transaction transaction){
        return
Collections.singleton(sendPlanToPhyLead(transaction.getMessage().getTask()));
    }

    private Message sendPlanToPhyLead(Task task){
```

```
        Message m = new Message();
        m.setTime(task.getTransaction_time());
        m.setSender(entityLocator.getManagerLeader(task.getManager()));
        m.setReceiver(entityLocator.getExecutorLeader(task.getExecutor()));
        m.setTask(task);
        task.setState(TaskState.SENT_TO_PHY_LEADER);
        return m;
    }

    private Collection<Message> sendToExecutor(Transaction transaction){
        Collection<Message> messages = new HashSet<>();
        Message message = transaction.getMessage();
        Task task = message.getTask();
        if (transaction.getReceiver() == task.getExecutor()){
            return sendReport(transaction);
        }
        Message m = new Message();
        m.setTime(task.getTransaction_time());
        m.setTask(task);
        m.setReceiver(task.getExecutor());
        m.setSender(transaction.getReceiver());
        task.setState(TaskState.SENT_TO_EXECUTOR);
        messages.add(m);
        return messages;
    }

    private Collection<Message> sendReport(Transaction transaction){
        Collection<Message> messages = new HashSet<>();
        Message message = transaction.getMessage();
        Task task = message.getTask();
        if (transaction.getReceiver().isLeader()){
             return sendReportToInfLeader(transaction);
        } else {
            Message m = new Message();
            m.setTime(task.getTransaction_time());
            m.setSender(transaction.getReceiver());
            m.setReceiver(transaction.getSender());
            m.setTask(task);
            task.setState(TaskState.REPORT_SENT_TO_PHY_LEADER);
            messages.add(m);
        }
        return messages;
    }

    private Collection<Message> sendReportToInfLeader(Transaction
transaction){
        Collection<Message> messages = new HashSet<>();
        Message message = transaction.getMessage();
        Task task = message.getTask();
        Message m = new Message();
        m.setTime(task.getTransaction_time());

m.setReceiver(entityLocator.getManagerLeader(transaction.getReceiver()));
        m.setSender(transaction.getReceiver());
        m.setTask(task);
        task.setState(TaskState.REPORT_SENT_TO_INF_LEADER);
        messages.add(m);
        return messages;
    }

    private Collection<Message> shareReport(Transaction transaction){
        Message message = transaction.getMessage();
        Task task = message.getTask();
```

```
        task.setState(TaskState.SHARE_REPORT);
        task.setCounter(1);
        Collection<Agent> agents=entityLocator.getManagerLeaders();

agents.addAll(entityLocator.getSameClusterManagers(transaction.getReceiver())
);
        agents.remove(transaction.getReceiver());
        agents.remove(transaction.getReceiver());
        return sendMultiple(agents, task, transaction.getReceiver());
    }

    private Collection<Message> tryToFinish(Transaction transaction){
        Collection<Message> messages = new HashSet<>();
        Message message = transaction.getMessage();
        Task task = message.getTask();
        task.counterIncr();
        if (task.getCounter()==entityLocator.getManagers().size()){
            task.setState(TaskState.FINISHED);
        } else if (transaction.getReceiver().isLeader()) {
            Collection<Agent>
agents=entityLocator.getSameClusterManagers(transaction.getReceiver());
            agents.remove(transaction.getReceiver());
            messages.addAll(sendMultiple(agents, task,
transaction.getReceiver()));

        }
        return messages;
    }

    private Collection<Message> sendMultiple(Collection<Agent> receivers,
Task task, Agent sender){
        Collection<Message> messages = new HashSet<>();
        for (Agent a: receivers){
            Message m = new Message();
            m.setTask(task);
            m.setTime(task.getTransaction_time());
            m.setSender(sender);
            m.setReceiver(a);
            messages.add(m);
        }
        return messages;
    }

    public void setClear_chance_percent(int clear_chance_percent) {
        this.clear_chance_percent = clear_chance_percent;
    }

    public void setError_1st_type_percent(int error_1st_type_percent) {
        this.error_1st_type_percent = error_1st_type_percent;
    }
}
```

Приложение В

Программная документация на разработку стенда для проверки алгоритмов движения беспилотных транспортных средств

В данном приложении приведена программная на программное обеспечение для физических моделей автономных транспортных средств, приведено описание работы моделей, базовые компоненты программы и алгоритмы функционирования.

46 9631

СОГЛАСОВАНО

Проректор по НР Университета ИТМО

_____ В.О. Никифоров

«___»_____ 201____ г.

М.П.

УТВЕРЖДАЮ

Аспирант Университета ИТМО, руководитель темы

_____ И.И. Викснин

«___»_____ 201____ г.

СТЕНД-АТС

ПО ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ МАТС

Описание программы
ЛИСТ УТВЕРЖДЕНИЯ
СНАБ.469631.001.13-ЛУ

Научный консультант,
доцент Университета ИТМО
_____ Комаров И.И.
“____”_____ 2018 г.

Исполнитель
_____ Викснин И.И.
“____”_____ 2018 г.

УНИВЕРСИТЕТ ИТМО

Взам. инв
Подпись и
Инв. №

УТВЕРЖДЕН

СНАБ.469631.001.13-ЛУ

ЭКСПЕРИМЕНТАЛЬНЫЙ СТЕНД ДЛЯ ПРОВЕРКИ АЛГОРИТМОВ ДВИЖЕНИЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

«СТЕНД-АТС»

ПО ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ МАТС

СНАБ.469631.001.13

ОПИСАНИЕ ПРОГРАММЫ

Листов 11

Санкт-Петербург, 2018 год

Инв. № | Подпись и | Взам. инв

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование программы

Наименование программы – «ПО для обеспечения функционирования МАТС».

Обозначение программы – ПО Стенд-АТС.

1.2 Программное обеспечение, необходимое для функционирования программы

В ходе разработки определено необходимое для функционирования программы программное обеспечение (ПО):

RASPBIAN STRETCH LITE (с версией ядра не ниже 4.9);

Java SE Runtime Environment (сборка не ранее 8u161);

компилятор Python (версии 3.6 или позже).

1.3 Языки программирования, на которых написана программа

Модули программы написаны на следующих языках программирования (ЯП):

Таблица 1. Используемые языки программирования

Обозначение	Использование	ЯП
Модуль A	Связующий модуль	C++
Модуль B	Обработка данных с видеокамеры	Python 3.6
Модуль C	Вычисление маршрута	Kotlin 1.1
Модуль D	Коммуникация между АТС	C++
Модуль E	Управление сервоприводами, обработка данных с датчиков	C++

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

Программная часть отвечает за построение маршрута и следование по этому маршруту. ПО обеспечивает возможность безаварийного прохождения маршрутов с приоритетным прохождением перекрестков.

Программа состоит из пяти модулей:

Модуль A – связующий модуль, обеспечивающий взаимодействие между модулями B-E. Обозначение в тексте программы – robotcore;

Модуль B – модуль, считывающий данные с видеокамеры, обрабатывающий их при помощи алгоритмов машинного зрения и обеспечивающий коррекцию маршрута по ходу движения. Обозначение – robotcontroller;

Модуль C – модуль, высчитывающий маршрут АТС. Обозначение – routeplanner;

Модуль D – модуль, регулирующий степень коммуникации между АТС. Обозначение – datatransfermodule;

Модуль E – модуль, отвечающий за управление сервоприводами АТС и обработку данных, поступающих с датчиков. Обозначение – arduinocontrol.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1 Алгоритм программы

На естественном языке алгоритм программы выглядит следующим образом:

Модуль E принимает данные о взаимодействии с другими АТС от Модуля D, полученные сведения передает Модулю C. В свою очередь, Модуль C на основе полученных данных корректирует маршрут текущего АТС, который возвращается в Модуль E.

Модуль E анализирует изменения маршрута по ходу движения: если изменения затрагивают прохождение текущего элементарного участка местности, то Модуль E отправляет новую команду в Модуль A, в противном случае движение продолжается без изменений.

Модуль Б обрабатывает потоковое видео с камеры, вычисляет необходимый угол корректировки и передает эту информацию в Модуль E. Модуль E формирует команду на корректировку маршрута и отправляет ее в Модуль A.

3.2 Используемые методы

Метод нисходящей разработки - основной используемый метод в разработке данного проекта. Это подход к разработке программного обеспечения, при котором оно разбивается на программные модули, образующие многоуровневую структуру. Каждый модуль – это короткая программа, решающая отдельную задачу. В процессе разработки модули нижележащих уровней заменяются заглушками. Таким образом, в любой момент разработки есть действующий вариант программного обеспечения.

3.3 Структура программы с описанием функций составных частей и связи между ними

Модуль A принимает информацию от модулей B-E. Обрабатывает, формирует набор управляющих команд, передает их модулю E.

Виды возможных управляющих команд:

- проехать элементарный участок местности;

- повернуть влево/вправо на 90 градусов;

- скорректировать движение на N градусов;

- прекратить движение.

Модуль B: считывает потоковое видео с камеры, анализирует и передает в Модуль E значение для корректировки.

Модуль C: отвечает за корректировку маршрута. Модуль строит маршрут движения, учитывая сведения о расположении и целях движения других АТС.

Модуль D: занимается формированием и последующей обработкой входящих и исходящих сигналов, регламентирующих связь между АТС.

Формат пакета данных, которым обмениваются участники движения:

- id АТС;

- время отправки сообщения;

- положение АТС;

- цель движения АТС.

Модуль E: исполнение команд от Модуля A, обработка сигналов, получаемых от датчиков (дальномера) и передача их Модулю A. Датчиком расстояния является дальномер HC-SR04. Модель сервоприводов приведена в Пояснительной записке.

Текст программы с делением на модули приведен в документе «Текст программы».

3.4 Связи программы с другими программами

«ПО для обеспечения функционирования МАТС» - единственная программа в структуре работы АТС, поэтому считается, что связи с другими программы отсутствуют.

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

При работе программы используются следующие вычислительные устройства:

- одноплатный компьютер Raspberry Pi 3 Model B;
- микроконтроллер ATmega328.

5. ВЫЗОВ И ЗАГРУЗКА

Единственным способ запуска АТС является запуск скомпилированного модуля движения сервоприводов и обработки данных (модуля E), в котором содержатся параметры для запуска остальных модулей программы.

Объём программы составляет 724 Кб.

При работе программы объём используемой оперативной памяти не превышает возможный объем ОЗУ для Raspberry Pi 3 Model B (1 Гб).

6. ВХОДНЫЕ ДАННЫЕ

Входные данные ниже описаны по модулям.

Для Модуля A:

на вход подаётся конфигурационный файл. Структура файла выглядит следующим образом:

```
{
    id: число, // idATC
    position: { // начальная позиция ATC
        x: число,
        y: число
    },
    map: {      // граф карты
        nodes: [{x, y}] // список координат, описывающих узлы графа
        edges: [{from, to}] // список ребер между вершинами графа
    },
    connection: {
        enable: boolean, // активировать модуль связи
        mode: «wifi» | «xbee» // режим передачи данных
    }
}
```

Для Модуля B:

модуль принимает на вход видеопоток с изображениями, полученными от камеры, с разрешением 640 x 480p и частотой 60 кадров в секунду.

Для Модуля C:

входными данными являются сведения о соседнем агенте:

- id ATC;
- время отправки сообщения;
- положение ATC;
- цель движения ATC.

Для Модуля D:

входными данными являются следующие сведения о соседнем агенте:

- id АТС;

- положение АТС;

- цель движения АТС.

Для Модуля Е:

команды представляют из себя строку на языке С:

- проехать элементарный участок местности («FWD»);

- повернуть влево/вправо на 90 градусов («LFT»/«RGT»);

- скорректировать движение на N градусов («LC<NUM>»/ «RC<NUM>», где <NUM> - это параметр корректировки целое число 16бит);

- прекратить движение («STP»).

7. ВЫХОДНЫЕ ДАННЫЕ

Модуль A, Модуль E:

выходных данных нет.

Модуль B:

выводит целочисленное число (коэффициент корректировки).

Модуль C:

выводит список команд для текущего агента.

Модуль D:

формирует информацию об агенте в виде:

- id АТС (8бита);
- время отправки сообщения (64бита);
- положение АТС (32бита);
- цель движения АТС (32бита).

Приложение Г

Копии актов о внедрении результатов диссертационной работы

УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

_____№_____

УТВЕРЖДАЮ
Проректор по научной работе
д.т.н., профессор
Никифоров И.О.
«__» _____ 2018 г.

АКТ
об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений целостности
информации в группах беспилотных транспортных средств»

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- модели функционирования и защищенного информационного взаимодействия группы беспилотных транспортных средств
- метод обнаружения нарушений целостности информации на основе репутационных механизмов
- метод временной централизации локальных коалиций групп беспилотных транспортных средств

использовались при выполнении проекта AAAA-A17-117042410163-4 «Разработка экспериментального стенда для проверки алгоритмов движения автономных транспортных средств».

Использование методов обеспечения информационной безопасности, предложенных Викснимым И.И., позволило создать децентрализованную защищенную группу беспилотных транспортных средств, передвигающихся в рамках разработанного полигона.

В результате применения методов и моделей для организации дорожного движения в рамках разработанного полигона удалось увеличить устойчивость группы беспилотных транспортных средств к возникающему деструктивному информационному воздействию.

Научный руководитель проекта,
к.ф.-м.н., доцент Комаров И.И.

УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

_____№_____

УТВЕРЖДАЮ
Проректор по научной работе
д.т.н., профессор
Никифоров В.О.
«__» _____ 2018 г.

АКТ

об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений целостности
информации в группах беспилотных транспортных средств»

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- метод временной централизации локальных коалиций групп беспилотных транспортных средств

использовались при выполнении проекта ААА-А-16-116072710022-9 – 2016 «Противодействие угрозам информационной безопасности технологий управления».

Предложенный Викснины И.И. метод временной централизации локальных коалиций позволяет минимизировать риски использования центральных вычислительных устройств, сохранив при этом эффективность применения таких устройств. Данный метод использовался не только в рамках наземных беспилотных транспортных средств, но и беспилотных летательных аппаратов.

Декан факультета БИТ,
К.т.н., доцент Заколдаев Д.А.

УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

_____№_____

УТВЕРЖДАЮ
Проректор по научной работе
д.т.н., профессор
Никифоров В.О.
«__» _____ 2018 г.

АКТ

об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений целостности
информации в группах беспилотных транспортных средств»

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- модели функционирования и защищенного информационного взаимодействия группы беспилотных транспортных средств
- метод обнаружения нарушений целостности информации на основе репутационных механизмов

использовались при выполнении проекта ААА-А-16-115043610017-8 – 2015 «Информационная безопасность технологий управления».

Децентрализованный подход к организации дорожного движения позволяет обеспечить информационную безопасность беспилотных транспортных средств и эффективное противодействие различного рода атакам.

Применение репутационных механизмов для противодействия нарушениям семантической целостности информации позволило повысить эффективность применения мобильных робототехнических систем в условиях агрессивной окружающей среды.

Декан факультета БИТ,
К.т.н., доцент — Заколдаев Д.А.

УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

_____№_____

УТВЕРЖДАЮ
Проректор по научной работе
д.т.н., профессор
Никифоров В.О.
«__» _____ 2018 г.

АКТ

об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений целостности
информации в группах беспилотных транспортных средств»
в учебном процессе университета

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- модели функционирования и защищенного информационного взаимодействия группы беспилотных транспортных средств
- метод обнаружения нарушений целостности информации на основе репутационных механизмов

используются факультетом БИТ (безопасности информационных технологий) Санкт-Петербургского национального исследовательского университета инфомрационных технологий, механики и оптики в учебном процессе при подготовке бакалавров по специальности 10.03.01 «Информационная безопасность» по дисциплинам «Теория систем и системный анализ» и «Информационные технологии», а также при подготовке магистров по специальности 10.04.01 «Информационная безопасность» по дисциплинам «Обучение машин» и «Управление рисками информационной безопасности» при чтении курсов лекций, проведении практических и лабораторных работ.

Декан факультета БИТ,
К.т.н., доцент — Заколдаев Д.А.

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(СПбГУ)
Университетская наб., 7/9, Санкт-Петербург, 199034
тел./факс 328-97-88
http://www.spbu.ru
ОКПО 02068516 ОГРН 1037800006089
ИНН/КПП 7801002274/780101001

27.07.2018 № 01-115-17665

на № _____ от _____

Ученому секретарю
Диссертационного Совета
Д 002.199.01
к.т.н. А.А.Зайцевой

Уважаемая Александра Алексеевна!

Направляю Вам акт об использовании результатов диссертационной работы Викснина Ильи Игоревича «Модели и методы обнаружения нарушений целостности информации в группах беспилотных транспортных средств» в учебном процессе Санкт-Петербургского государственного университета.

Приложение: Акт об использовании результатов диссертационной работы Викснина И.И. – 1 л.

Заместитель начальника Учебного управления
по направлениям международные отношения,
политология, социология и экономика О.Е.Ремизова

АКТ

об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений
целостности информации в группах беспилотных
транспортных средств» в учебном процессе
университета

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- модели функционирования и защищенного информационного взаимодействия группы беспилотных транспортных средств
- метод временной централизации локальных коалиций групп беспилотных транспортных средств

используются экономическим факультетом Санкт-Петербургского государственного университета в учебном процессе при подготовке магистров по направлению 38.04.01 Экономика по дисциплинам «Индустрия 4.0», «Блокчейн» при чтении курсов лекций, проведении практических и лабораторных работ.

Заведующая кафедрой информационных систем в экономике
к.ф.-м..н., доцент Лезина Т.А.

26.07.18

УТВЕРЖДАЮ
Генеральный директор
АО «НИИ Специальных проектов»
_____ М.А. Борботько
«03» 08 2018 г.

АКТ

об использовании результатов диссертационной работы
Викснина Ильи Игоревича
«Модели и методы обнаружения нарушений целостности информации в группах беспилотных транспортных средств»

Настоящий Акт составлен в том, что результаты диссертационной работы Викснина Ильи Игоревича, а именно:

- модели функционирования и защищенного информационного взаимодействия группы беспилотных транспортных средств;
- метод обнаружения нарушений целостности информации на основе репутационных механизмов;
- метод временной централизации локальных коалиций групп беспилотных транспортных средств

использовались при проектировании системы поддержки принятия решений при управлении беспилотными летательными аппаратами, разрабатываемой в 2016 и 2017 годах в рамках составной части опытно-конструкторской работы (шифр – «Глориус») для решения задач контроля состояния одиночного агента на основе независимой оценки поведения летательных аппаратов всеми агентами.

Основной идеей подхода является использование адаптированного автором метода обеспечения информационной безопасности на основе социальных механизмов. Помимо непосредственного контроля поведения объектов управления в зоне выполнения текущих задач, предложенный подход создаёт предпосылки для повышения уровня целостности и доступности данных в процессе информационного взаимодействия элементов группировки при различной конфигурации. А метод временной централизации обеспечивает многовариантность автоматического формирования группировок из аутентичных объектов.

Заместитель генерального директора
кандидат военных наук, доцент Коршунов Н.А.