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

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2018

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Научный руководитель: к.ф.-м.н., доцент Комаров Игорь Иванович
ФГБОУ ВО «СПбНИУ ИТМО», доцент

Официальные оппоненты: д.в.н., профессор, Привалов Андрей Андреевич
ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», профессор кафедры Электрическая связь

к.т.н., доцент, Красов Андрей Владимирович
ФГБОУ ВО СПбГУТ, заведующий кафедрой Защищенных систем связи

Ведущая организация: ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Защита диссертации состоится "08" ноября 2018 г. в 16:00 часов на заседании совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Д 002.199.01, созданного на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) по адресу:
199178, Санкт-Петербург, 14-а линия В.О., 39, комн. 401.
Факс: (812)-328-44-50 тел: (812)-328-34-11.

С диссертацией и авторефератом можно ознакомиться на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.
http://www.spiiras.nw.ru/dissovet/

Автореферат разослан « ____ » _____ 2018 года.

Ученый секретарь совета
диссертационного совета Д 002.199.01,
кандидат технических наук  А.А. Зайцева

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 временной 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 AAA-A-16-115043610017-8 – 2015 «Информационная безопасность технологий управления»; проекта AAA-A-16-116072710022-9 – 2016 «Противодействие угрозам информационной безопасности технологий управления»; проекта AAAA-A17-117042410163-4 «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: 4 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

Во введении обосновывается выбор темы, ее актуальность, конкретизированы цель и частные задачи, определены объект и предмет исследования, выбраны методологические подходы, обосновывается новизна и практическая ценность выносимых на защиту результатов, дается краткая характеристика содержания работы, сформулированы положения, выносимые на защиту, приведены сведения об апробации результатов.

В первой главе рассмотрена организация движения на основе БТС и основные проблемы ИБ БТС, меры противодействия угрозам ИБ, поставлена задача 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 защищенного 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.

Во второй главе предлагается модель функционирования группы БТС на основе децентрализованного мультиагентного подхода, класс мягких атак на БТС, модель защищенного ИВ группы БТС.

Пусть $T = \{t_0, \dots, t_{end}\}$ – время функционирования группы БТС. В момент времени t_0 каждое БТС вырабатывает план действий на достижение цели, стоящей перед ним. После разработки планов (момент времени $t_{pln\_cmpl\_f}$) происходит ИВ БТС, в ходе которого все БТС получают информацию о планах действий других БТС.

Процесс верификации семантической целостности информации БТС-объекта оценки основывается на сенсорных устройствах БТС-субъекта оценки. Возможна ситуация, при которой БТС может оценить информацию не для всех остальных БТС группы. В такой ситуации предлагается разделять группу на подгруппы. Кроме того, предлагается ввести элемент централизованной стратегии управления, подразумевающий наличие центрального вычислительного элемента (ЦВЭ). Это позволит повысить качество оценки информации. Однако наличие постоянного ЦВЭ сопряжено с дополнительными угрозами ИБ, поэтому ни одна из БТС не должна выполнять функции ЦВЭ постоянно.

При организации процесса ИВ, ЦВЭ используется для оценки целостности информации, получаемой от других элементов подсистемы. Таким образом, после выработки планов действий в момент времени $t_{pln\_cmpl\_f+1}$ БТС передают информацию ЦВЭ. После получения выработанных планов от других БТС, ЦВЭ начинает проводить оценку целостности информации на наличие нарушений семантической 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 после доработки БТС опять должны будут передать информацию ЦВЭ, который, в свою очередь, должен будет оценить семантическую целостность информации для этих сообщений и переслать планы действий другим ЦВЭ. Момент окончания доработки планов и получения новых планов действий ЦВЭ, а также проведения проверки показателя доверия - t_{pln_cmpl}. Схематичное представление модели показано на рис. 1.

Тогда $t_{pln\_cmpl\ +\ 1}$ – момент начала выполнения планов действий каждым БТС. В ходе выполнения планов могут возникнуть внештатные ситуации, что может привести не только к невыполнению одного плана действий (одним БТС), но и всеми остальными, т.к. другие планы вырабатываются с учетом успешного выполнения плана каждым БТС. В таком случае требуется отправить отчет о возникших нарушениях.

Момент окончания действий по плану – t_{tsk_cmpl}. В момент времени $t_{tsk\_cmpl\ +1}$ начинается передача информация о выполнении полученных планов соответствующим ЦВЭ. После чего происходит оценка полученной информации на наличие нарушений семантической целостности. После этого, ЦВЭ осуществляет ИВ с ЦВЭ других подгрупп и передает собранную информацию.

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.

Метод доверия/репутации

Метод доверия и репутации заключается в проведении оценки целостности данных, передаваемых от БТС-источника БТС-приемнику, на основе не только собственных наблюдений БТС, но также на основе данных, полученных о целостности информации БТС-источника от третьих БТС и на основе истории взаимодействий, т.е. ретроспективной оценки качества данных БТС-источника.

В таком случае, метод доверия и репутации сводится к построению векторов, состоящих из оценок основных показателей для всех БТС системы:

$Truth_t = f_{tr_t}(information)$, 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*.

$$Trust_t = f_{trust_t}(R_{t-1}, Truth_t) = f_{trust_t}\left(f_{r_{t-1}}\left(f_{tr_{t-1}}(information)\right), f_{tr_t}(information)\right)$$

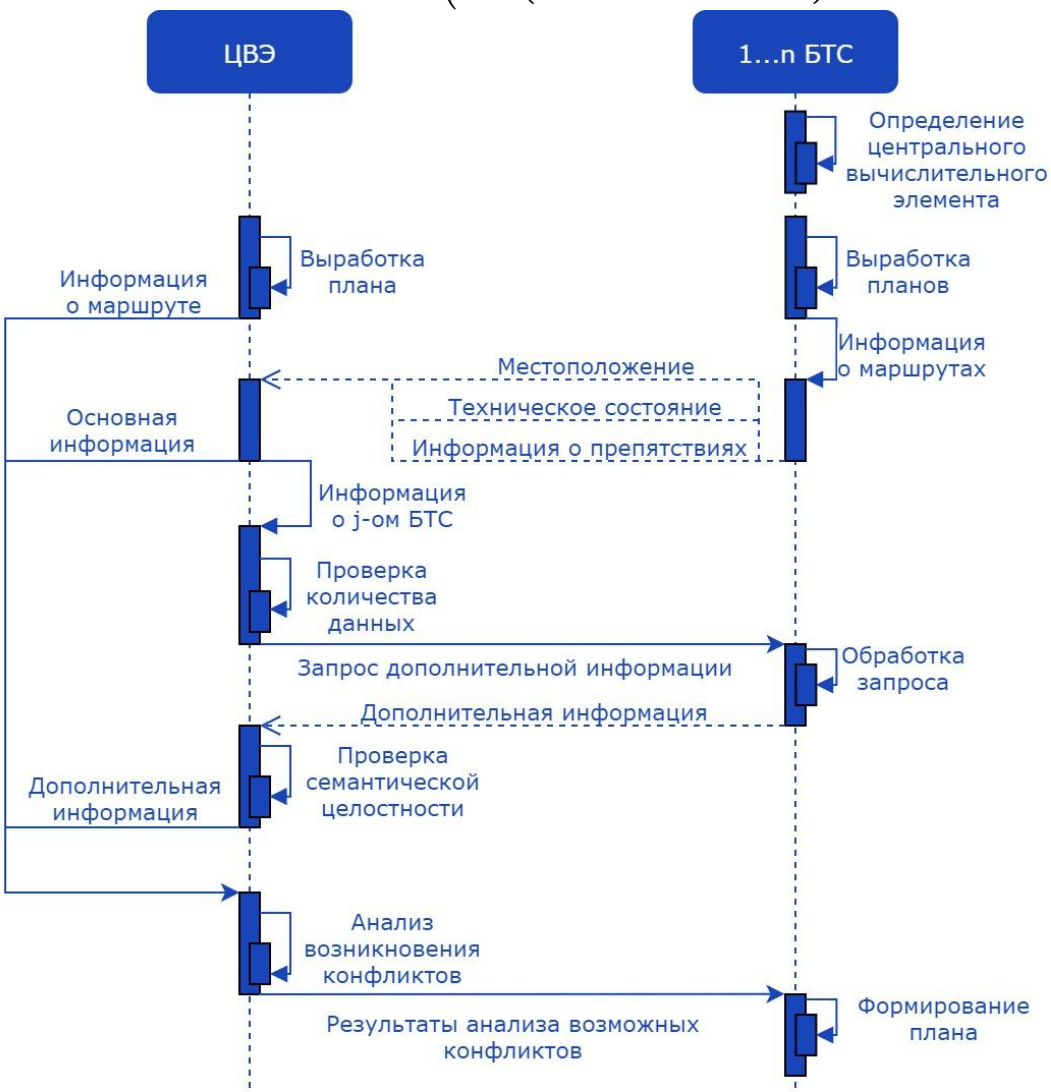

Рисунок 1. Модель контроля семантической целостности информации в группе БТС

где $Trust_t$ –показатель *доверия* в момент времени *t*, f_{trust_t} – функция оценки значения уровня доверия в момент времени *t*.

Результаты экспериментов показали, что параметр *репутации* должен отвечать двум основным требованиям - медленный рост значения при отсутствии нарушений целостности и значительное уменьшение значения при наличии нарушений целостности. Для достижения этой цели предлагается использовать функцию следующего вида:

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

где $Truth_{e\_ei\_t}$ – показатель истинности информации, получаемой от БТС e_i БТСом e в момент времени t, R_j – показатель репутации БТС-объекта в

момент времени j. Нормирование значения $R^{S}_{e_ei_t}$по количеству прошедших итераций позволяет использовать значение репутации в диапазоне [0;1].

Параметр *доверия* вычисляется на основе значений параметров *истинности* и *репутации*. В общем случае для расчёта значения параметра доверия используется метрическая функция:

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

В качестве базовых параметров предлагается использовать следующие значения – $R_{min} = T_{min} = 0$, $R_{max} = T_{max} = 1$. Данные значения показателей репутации и истинности могут быть представлены как эталонные показатели (первая пара значений соответствует значениям показателей БТС, сообщения которого постоянно содержат нарушения семантической целостности, вторая пара – значения показателей БТС, в сообщениях которого не было выявлено нарушений семантической целостности).

Метод вре́менной централизации

Принадлежность БТС некоторой подгруппе может быть описан следующим образом: $E_i = \{(e, \mu_{E_i}(e)) | e \in E\}$.

Предположим, что требуется выделить две подгруппы $\mathrm{E_i}, \mathrm{E_j} \in \mathrm{E}$. Тогда $\mu_{E_i}(e) = 0, \mu_{E_j}(e) = 1 \Leftrightarrow \left(e, \overline{\mu_{E_\iota}(e)}\right), \left(e, \overline{\mu_{E_j}(e)}\right)$ и $\overline{\mu_{E_\iota}(e)} < \overline{\mu_{E_j}(e)}$, где $\overline{\mu_{E_\iota}(e)}$ – функция принадлежности элемента e подмножеству E_i, $\overline{\mu_{E_j}(e)}$ – функция принадлежности элемента e подмножеству E_j, $\mu_{E_i}(e)$ – модифицированная функция принадлежности e подмножеству E_i, $\mu_{E_j}(e)$ – модифицированная функция принадлежности элемента e подмножеству E_j. На рис.2а представлена схема разделения группы БТС на три подгруппы.

Таким образом, все БТС подгруппы могут осуществлять ИВ с другими БТС подгруппы без посредников. В таком случае, в каждую итерацию определяется новый ЦВЭ подгруппы на основе расчета функции принадлежности, которая зависит от заранее определённых факторов.

$\forall e_o \in E_i: \overline{\mu_{E_\iota}(e_l)} > \overline{\mu_{E_\iota}(e_o)}$, где $e_l \in E_i$. В таком случае, можно говорить о том, что БТС e_l является ЦВЭ подсистемы.

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 напрямую, т.е. каждый элемент осуществляет ИВ с каждым. Рис. 2б демонстрирует каналы связи и БТС после нескольких итераций при использовании описанного подхода.

На рис. 3 показано сравнения количества ложных действий при различных начальных процентах диверсантов при проведении атаки ballot stuffing для постоянной централизации и на основе метода временной централизации. Таким образом, можно говорить об эффективности метода

временной централизации с учетом наличия других методов обеспечения ИБ группы БТС.

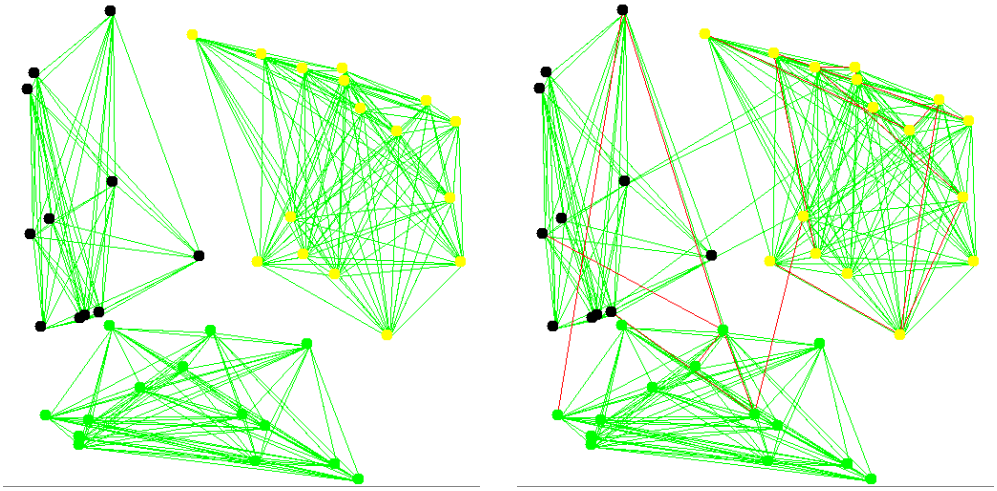

Рисунок 2. Представление элементов и каналов связи в начале функционирования группы БТС (а) и после нескольких итераций (б). (БТС – символы, обозначающие их принадлежность к одной подгруппе, существующие каналы связи – сплошные линии.)

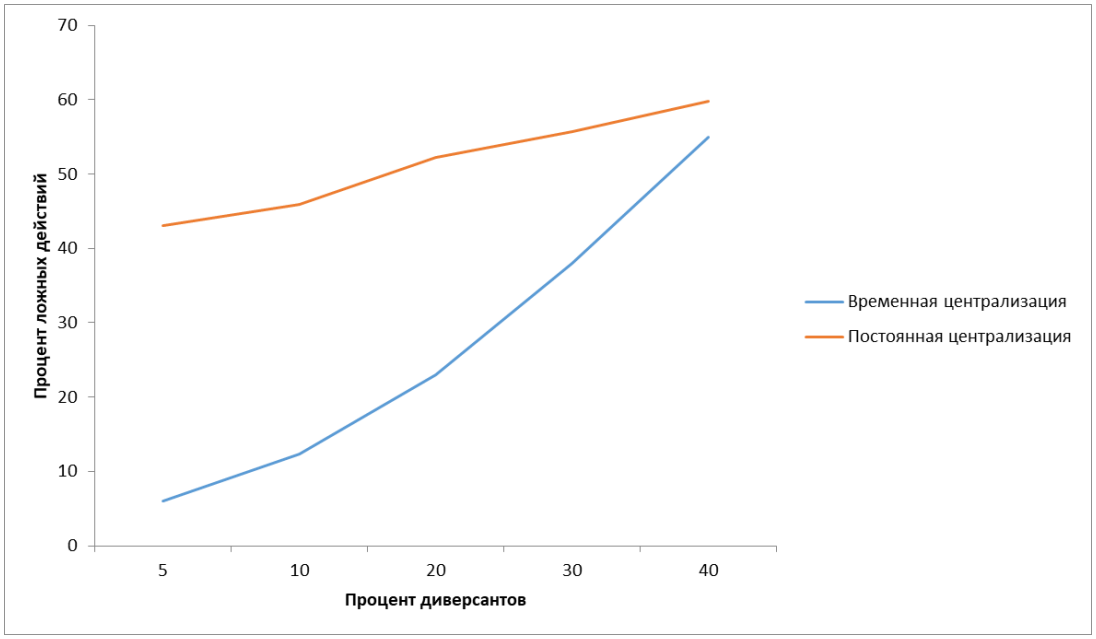

Рисунок 3. Сравнение числа ложных действий для различного начального числа диверсантов для метода временной централизации и для централизованной группы

В четвертой главе представлены результаты экспериментов по использованию предложенных моделей и методов, а также показана их продуктивность на примере группы БТС.

Группа БТС является естественным развитием понятия мобильной робототехнической системы (МРТС). Под МРТС понимается множество роботов, способных перемещаться в пространстве, осуществлять информационное взаимодействие и выполнять функции, исходя из

специфики роботов. Система движения БТС является частным случаем МРТС, когда помимо внутренних правил системы существуют также внешние – действия по различным сигналам светофора, движения согласно знакам приоритета и т.д.

Рассматривая МРТС с задачей достижения участка местности, проверка *истинности* будет заключаться в анализе местоположения других элементов. Кроме того, может быть осуществлена проверка согласно имеющимся у элементов знаниям. В рамках экспериментов рассматривается система, состоящая из гомогенных элементов. Дополнительным ограничением для проведения рассматриваемых экспериментов будет равный запас энергии элементов в момент инициализации эксперимента.

Для проведения эксперимента было разработано специализированное инструментальное средство, позволяющее провести имитационное моделирование функционирования МРТС. Оно предоставляет возможность варьировать количество элементов системы, создавать задачи для МРТС, изменять параметры элементов и некоторые условия окружающей среды, а именно – размер полигона, количество и тип препятствий. Под параметрами элементов МРТС понимаются: затраты на прохождение единицы расстояния; запас энергии элемента; радиус работы модулей связи; дистанция работы сенсорных устройств.

Под нарушителем понимается такой элемент, поведение которого отличается от поведения других элементов системы только семантической целостностью передаваемой информации, т.е. семантическая целостность передаваемой элементом информации будет нарушена. Основная информация, циркулирующая в данной системе – собственная оценка затрат элемента на выполнение задачи (прибытия в определенную область). Таким образом, элемент-нарушитель нарушает целостность информации о предполагаемых затратах на выполнение задач. Исходя из допущения о гомогенности системы, каждый элемент (элемент-субъект) может определить затраты другого элемента (элемента-объекта) на выполнение задачи.

Возможность непосредственной оценки не всегда имеется у элемента. Более того, не всегда имеется возможность провести оценку показателя истинности на основе значения данного показателя у других элементов. В результате, возможна ситуация, при которой корректно действующий элемент считается нарушителем. В таком случае, можно говорить об *ошибке первого рода*, когда гипотеза об отсутствии нарушения целостности информации ошибочно отвергается, т.е. корректный элемент МРТС исключается из процесса выполнения задач. Однако, в общем случае, представляется возможным 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 такой элемент системы, который может ее не выполнить (нарушитель). Однако нарушитель может выполнить задачу, 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 элементом.

На рис. 4 представлены графики ошибок первого и второго рода при использовании метрической функции нахождения значения параметра доверия.

Таким образом, результат применения метода доверия и репутации позволяет обнаружить все сообщения, в которых присутствуют нарушения семантической целостности информации. Стоит отметить, что данные результаты верны только при условии наличия ИВ между всеми элементами группы.

Предлагается рассмотреть серию экспериментов, в рамках которой существовало несколько изолированных друг от друга групп роботов. Перед всеми группами стояли одинаковые цели, алгоритмы выбора целей были также одинаковы. После получения целей каждая группа выбирала цели для достижения (для каждой цели требовалось несколько роботов). В каждой группе имеются нарушители, проводящие атаки с использованием семантической целостности информации. После достижения изначальных целей до всех роботов МРТС доводились новые цели (цели второго уровня). После достижения целей первого уровня МРТС также была разделена на подгруппы, но состав подгрупп после достижения целей первого уровня отличается от состава до достижения целей первого уровня. Результаты экспериментов представлены в таблице 1.

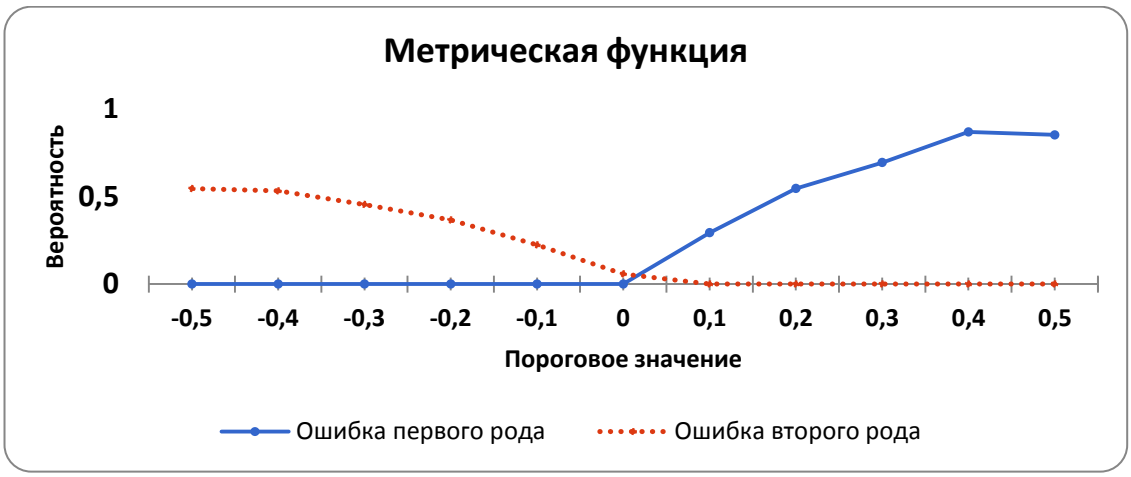

Рисунок 4. Вероятность ошибок первого и второго рода при использовании метрической функции при расчете показателя доверия

Таким образом, было показано, что совместное использование метода плавающего центра и метода доверия и репутации позволяет повысить процент обнаруженных нарушителей в условиях частичной изолированности

некоторых элементов МРТС. Результаты, полученные на примере МРТС, являются также актуальными для групп БТС, что было показано по результатам разработки прототипа программного комплекса обеспечения ИБ для групп БТС.

Таблица 1. Процент достигнутых целей при использовании метода плавающего центра и без него.

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

В заключении приведены выводы, выполненные задачи и перспектива дальнейшей разработки тематики.

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).

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях ВАК:

1. Викснин И.И. Модель обеспечения информационной безопасности кибер-физических систем // Наука и бизнес: пути развития – 2018. – с. 14-19
2. Викснин И.И., Зикратов И.А., Зикратова Т.В., Шлыков А.А., Медведков Д.И. Модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 439–449. doi: 10.17586/2226-1494-2017-17-3-439-449
3. Викснин И.И., Зикратов И.А., Зикратова Т.В. Мультиагентное планирование проезда перекрёстка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики - 2016. - Т. 16. - № 5(105). - С. 839-849
4. Викснин И.И., Комаров И.И., Пантюхин И.С., Юрьева Р.А., Масленников О.С., Мурадов А.Р. Подход к обнаружению новых кибератак на киберфизические системы на основании метода обнаружения аномалий // Автоматизация в промышленности - 2018. - Т. 2. - С. 48-52

Публикации в изданиях Scopus:

5. Viksnin I.I., Iureva R.A., Komarov I.I., Drannik A.L. Assessment of Stability of Algorithms Based on Trust and Reputation Model // Proceeding of the 18th conference of FRUCT association - 2016, pp. 364-369
6. Viksnin I.I., Zikratov I.A., Shlykov A.A., Belykh D.L., Komarov I.I., Botvin G.A. Planning of Autonomous Multi-agent Intersection // ITM Web of Conferences - 2016, Vol. 8, pp. 01007
7. Viksnin I.I., Drannik A.L., Iureva R.A., Komarov I.I. Flocking Factors' Assessment in Case of Destructive Impact on Swarm Robotic Systems // Proceedings of the 18th Conference of Open Innovations Association FRUCT - 2016, pp. 357-363
8. Ilya I. Viksnin, Alexey Chechet, Ruslan Gataullin, Alexandr Muradov, Ivan Danilov, Nikita Tursukov. Modeling People Behavior in Emergency Situations //Proceedings of the 20th conference of FRUCT association – 2017, pp. 478-483
9. Ilya I Viksnin, Nikita D Schcepin, Roman O Patrikeev, Andrei A Shlykov, Igor I Komarov. Approaches to Communication Organization Witin Cyber-Physical Systems // Proceeding of the 20th conference of FRUCT association – 2017, pp.484-490

10. Ilya Viksnin, Alexandr Muradov, Liubov Iurtaeva, Nikita Tursukov. The Model of Information Diffusion in Social Networking Service // proceeding of the 20th conference of FRUCT association – 2017, pp. 731-734

Публикации в иных изданиях:

11. Викснин И.И., Назыров М.В., Гатауллин Р.И. Анализ защищённости алгоритмов, базирующихся на коэффициентах доверия и репутации // Сборник тезисов докладов V Всероссийского конгресса молодых учёных – 2016
12. Шлыков А.А., Гатауллин Р.И., Викснин И.И. Разработка имитационной модели мультиагентных робототехнических систем // Сборник тезисов докладов V Всероссийского конгресса молодых учёных – 2016
13. Ботвин Г.А., Белых Д.Л., Викснин И.И. Модели ИТ-инфраструктур в инновационном бизнесе // Обозрение прикладной и промышленной математики - 2016. - Т. 23. - № 4. - С. 328-329
14. Гатауллин Р.И., Викснин И.И. Постановка задачи определения оптимального коэффициента пропускной способности узла // Сборник тезисов докладов V Всероссийского конгресса молодых учёных – 2016
15. Викснин И.И., Патрикеев Р.О., Щепин Н.Д. Разработка инструментальных средств моделирования подходов организации связи в мобильных робототехнических системах // Сборник тезисов докладов конгресса молодых учёных. Электронное издание – 2017
16. Викснин И.И., Юрьева Р.А., Комаров И.И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал - 2015. - № 5(50). - С. 87-91