На правах рукописи

ФАЙЗУЛЛИН Рустам Рафитович

ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМАХ

(НА ПРИМЕРЕ РЕГИОНАЛЬНОЙ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ РЕСПУБЛИКИ БАШКОРТОСТАН)

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук

Уфа – 2013

Работа выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВПО «Уфимский государственный авиационный технический университет»

Научный руководитель: д-р техн. наук, проф.
Васильев Владимир Иванович

Официальные оппоненты: д-р техн. наук, проф.
Аралбаев Ташбулат Захарович
заведующий кафедрой вычислительной техники и защиты информации ФГБОУ ВПО «Оренбургский государственный университет»;
канд. техн. наук, доцент
Антонов Вячеслав Викторович
начальник Информационного центра МВД по Республике Башкортостан

Ведущая организация: **ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет» (г. Пермь)**

Защита диссертации состоится «24» декабря 2013 г. в 10 ч. 00 мин. на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете по адресу: 450000, г. Уфа, ул. Карла Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «__» ноября 2013 г.

Ученый секретарь
диссертационного совета И. Л. Виноградова
д-р техн. наук, доцент

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Увеличение роли информации, знаний и информационных технологий способствовало инициации государственной программы «Информационное общество 2011-2020». Информатизация государства и общества, как результат данной программы, предполагает не только обеспечение всей страны средствами информационно-коммуникационных технологий, но и разработку и внедрение Электронного правительства. Целью последнего является организация деятельности органов государственной власти, обеспечивающая за счёт комплексного применения информационно-коммуникационных технологий и объединённых информационных ресурсов высокий уровень эффективности, оперативности и удобства исполнения функций, получения организациями и гражданами государственных и муниципальных услуг и информации о результатах деятельности государственных органов. Для реализации подобного рода задач требуется использование интегрированных территориально-распределённых информационных систем (ИС). В рамках развития Электронного правительства такой системой является Система межведомственного электронного взаимодействия (СМЭВ), предназначенная для технологического обеспечения обмена информацией между её участниками (гражданами, органами, организациями). СМЭВ состоит из трёх уровней: федерального, регионального и муниципального. Каждая региональная СМЭВ (РСМЭВ) состоит из ИС государственных органов исполнительной власти субъекта Российской Федерации (региональных органов исполнительной власти, РОИВ), объединённых с помощью сетей передачи данных.

Основанием для обмена данными между РОИВ в рамках оказания (исполнения) государственных услуг (функций) являются ведомственные административные регламенты, устанавливающие объём и состав передаваемой и запрашиваемой информации. Каждый РОИВ в целях автоматизации процедур передачи данных, находящихся в его ведении, формирует свои электронные сервисы, правила разработки которых закреплены соответствующими методическими рекомендациями, и публикует их в Реестре электронных сервисов (Технологическом портале СМЭВ). Другие РОИВ, произведя должные настройки по подключению к электронным сервисам, используют их в целях получения данных. Таким образом в СМЭВ реализуется сервис-ориентированная архитектура.

В отношении РСМЭВ, безусловно, остро стоит вопрос защиты информации (ЗИ). Вследствие значительной сложности информационно-коммуникационных инфраструктур РСМЭВ, основой решения проблемы безопасности является использование интегрированной многоуровневой системы механизмов защиты и доверия. При этом интеллектуализация сервисов ЗИ позволяет реализовать интеллектуальную надстройку над традиционными механизмами защиты.

Развитие инфраструктуры РСМЭВ сопровождается существенным ростом числа разнородных сетевых устройств. В результате увеличивается количество событий, связанных с возможным нарушением информационной безопасности (событий ИБ). Так, например, один межсетевой экран может генерировать за день более 1 Гигабайта данных в *log*-файле, один сенсор системы обнаружения / предотвращения вторжений за день может выдавать до 50 тысяч сообщений. В то же время, сопоставить сигналы, поступающие от разных систем безопасности, чрезвычайно сложно. Становится практически невозможно своевременно отслеживать и локализовывать инциденты информационной безопасности (ИБ), т.е. любые непредвиденные или нежелательные события, которые могут нарушить деятельность или ИБ организации. Возрастающая сложность ИС требует наличия программных (программно-аппаратных) средств сбора и обработки статистических данных для обеспечения адекватной и своевременной ЗИ.

РСМЭВ Республики Башкортостан имеет следующие особенности:

– ИС РОИВ объединены мультисервисной сетью передачи данных, имеющей кольцевую топологию;

– в каждой ИС имеются штатные средства ЗИ, локальная политика безопасности и персонал, уполномоченный за обеспечение ИБ ИС;

– ИС имеют единый выход в сеть Интернет;

– мониторинг функционирования сетевого оборудования осуществляется из единого центра.

Специфика РСМЭВ Республики Башкортостан (РСМЭВ РБ) как объекта защиты заключается в том, что она состоит из ряда гетерогенных ИС РОИВ, различающихся применяемыми организационно-техническими мероприятиями и средствами ЗИ, квалификацией специалистов по ИБ. Учитывая данное обстоятельство, а также постоянное взаимодействие ИС между собой для реализации общих бизнес-процессов, потенциальные риски нарушения ИБ в данном объекте защиты являются весьма высокими.

С точки зрения обеспечения ИБ, основными проблемами в РСМЭВ РБ являются:

– отсутствие в настоящее время централизованного мониторинга безопасности с учётом результатов функционирования механизмов и средств ЗИ каждой ИС, а также возможности наблюдать за текущими показателями защищённости в режиме реального времени;

– необходимость выявлять наиболее важные сигналы тревоги об угрозах и рисках ИБ в РСМЭВ и обеспечивать принятие на их основе своевременных и адекватных мер, направленных на предотвращение угроз и снижение рисков ИБ;

– необходимость обеспечить снижение информационных рисков в РСМЭВ до приемлемого уровня с учётом влияния основных факторов, определяющих значения риска.

Другой важной проблемой обеспечения ИБ таких систем является необходимость действовать в условиях наличия факторов

неопределенности, связанных с неточностью и недостоверностью исходных данных, неполнотой знаний об объекте ЗИ, неоднозначностью принимаемых решений. Интеллектуализация систем ЗИ, т.е. наделение их функциями высококвалифицированного эксперта посредством применения методов и технологий искусственного интеллекта, является выходом в данной ситуации, что вызывает всё больший интерес у специалистов в области ЗИ.

Степень разработанности темы. Проблеме построения интегрированных систем мониторинга и управления событиями ИБ посвящены работы Р. Биду, К. Бласка, С. Вандайка, Д. О. Ковалева, И. В. Котенко, Д. Р. Миллера, О. В. Полубевой, И. Б. Саенко, Д. Свифта, В. А. Сердюка, А. А. Харпера, С. Харриса и др. Вопросы интеллектуальной поддержки принятия решений по ЗИ в распределённых информационно-управляющих системах на основе оценки анализа и управления информационными рисками отражены в трудах В. И. Васильева, М. Б. Гузаирова, П. Д. Зегжды, И. В. Котенко, О. Б. Макаревича, И. В. Машкиной, А. Г. Остапенко, С. А. Петренко, С. В. Савкова, С. В. Симонова, В. М. Шишкина, Р. М. Юсупова и др.

Следует отметить, что разработка и применение интеллектуальных систем мониторинга и управления событиями ИБ (*Security Information and Event Management, SIEM*) в настоящее время считается одним из наиболее перспективных направлений в области обеспечения ИБ в компьютерных системах и сетях. *SIEM*-системы позволяют на основе сбора и оперативного анализа данных о событиях ИБ, возникающих в различных местах информационной инфраструктуры и фиксируемых в журналах аудита соответствующих средств и устройств, проводимых в реальном или близком к реальному масштабе времени, обнаруживать и предупреждать атаки, оценивать и прогнозировать уровень защищённости инфраструктуры. В силу этих возможностей технология *SIEM* рассматривается сегодня как ключевая для критически важных инфраструктур. Поэтому решение задач, связанных с осуществлением мониторинга инцидентов ИБ и формированием оперативных решений по ЗИ в интегрированных территориально-распределённых ИС с использованием интеллектуальных технологий поддержки принятия решений, является актуальным.

Целью диссертационной работы является повышение защищённости РСМЭВ на основе разработки и применения интеллектуальной системы поддержки принятия решений (СППР) по защите информации с использованием моделей, методов и алгоритмов мониторинга и управления событиями ИБ.

Для достижения поставленной цели в работе были поставлены и решены следующие **задачи**:

1. Разработка онтологии предметной области и функциональной модели *SIEM*-системы на основе *SADT*-методологии и *IDEF*-технологий.

2. Разработка метода и алгоритма оценки защищённости ИС и РСМЭВ на основе правил нечёткой логики.

3. Разработка методики и алгоритма оценки информационных рисков в РСМЭВ с помощью нечётких когнитивных карт (НКК).

4. Разработка исследовательского прототипа СППР по управлению защитой информации в РСМЭВ.

5. Анализ эффективности функционирования разработанной СППР методом имитационного моделирования.

Объектом исследования является система мониторинга и управления событиями ИБ в РСМЭВ.

Предметом исследования являются модели, методы и алгоритмы обеспечения интеллектуальной поддержки принятия решений по защите информации в РСМЭВ.

Научная новизна:

1. Разработана онтология предметной области, связанной с построением *SIEM*-системы в РСМЭВ *на основе SADT*-методологии и технологии *IDEF5, отличающаяся* учётом основных факторов, определяющих ИБ РСМЭВ, *которая позволяет* выявить основные сущности и их взаимосвязи в данной предметной области и более обоснованно построить функциональную модель исследуемой системы. Предложена функциональная модель *SIEM*-системы *на основе* использования технологии *IDEF0, отличающаяся* учётом специфики реализации процессов мониторинга и реагирования на инциденты ИБ в РСМЭВ, что *позволяет* сформировать требования к этим процессам исходя из поставленных целей обеспечения ИБ РСМЭВ.

2. Разработаны метод и алгоритм оценки защищённости ИС и РСМЭВ в целом на основе правил нечёткой логики, *отличающиеся* учётом корреляции событий ИБ в ИС, *что позволяет* более достоверно осуществлять приоритезацию инцидентов ИБ в РСМЭВ по их степени важности. Использование предложенной методики оценки уровня защищённости ИС и РСМЭВ *позволяет* оценивать в реальном времени защищённость как каждой ИС, входящей в РСМЭВ, так и РСМЭВ в целом, что обеспечивает базу для принятия оперативных решений по ЗИ в РСМЭВ.

3. Разработаны методика и алгоритм оценки информационных рисков в РСМЭВ, *основанные* на использовании аппарата нечётких когнитивных карт, *отличающиеся* учётом специфики процессов ЗИ в РСМЭВ, *что позволяет* решать задачу анализа и управления рисками в РСМЭВ путём принятия решений по выбору соответствующих контрмер, противодействующих влиянию основных угроз в РСМЭВ.

Теоретическая и практическая ценность. Разработан исследовательский прототип СППР, позволяющий:

– обеспечивать централизованный мониторинг РСМЭВ с учётом результатов функционирования традиционных механизмов и средств ЗИ, а

также наблюдать за текущими показателями защищённости в режиме реального времени;

– выявлять наиболее важные сигналы тревоги об угрозах и рисках ИБ в РСМЭВ и обеспечивать принятие на их основе своевременных и адекватных мер, направленных на предотвращение угроз и снижение рисков ИБ;

– обеспечить снижение информационных рисков в РСМЭВ до приемлемого уровня с учётом влияния основных факторов, определяющих значения риска.

Результаты диссертационной работы использованы в ГУП «Центр информационно-коммуникационных технологий Республики Башкортостан» при реализации системы ЗИ Государственной мультисервисной сети передачи данных Республики Башкортостан. Данная сеть объединяет локальные вычислительные сети РОИВ и выступает в качестве телекоммуникационной инфраструктуры реализации единого пространства электронного взаимодействия государственных органов Республики Башкортостан.

Методология и методы исследования. При решении поставленных в работе задач использовались методы системного анализа, теории когнитивного моделирования, нечёткой логики, имитационного моделирования, автоматизированного моделирования ИС, методы программирования, методы экспертного оценивания, а также современные подходы к организации мониторинга ИБ компьютерных систем.

Положения, выносимые на защиту:

1. Онтология предметной области, связанной с построением *SIEM*-системы, на основе *SADT*-методологии и технологии *IDEF5*; функциональная модель *SIEM*-системы на основе технологии *IDEF0* с учётом характерных особенностей процессов ЗИ в РСМЭВ.

2. Метод и алгоритм оценки защищённости отдельных ИС и РСМЭВ в целом на основе правил нечёткой логики, отличающиеся учётом корреляции событий ИБ в ИС и приоритезацией инцидентов ИБ в РСМЭВ по их степени важности.

3. Методика и алгоритм оценки информационных рисков в РСМЭВ на основе использования аппарата нечётких когнитивных карт.

4. Исследовательский прототип СППР по управлению защитой информации в РСМЭВ на основе предложенных методов и алгоритмов оценки уровня защищённости и информационных рисков в РСМЭВ.

Достоверность полученных результатов. Полученные в диссертационной работе результаты исследования подтверждаются использованием проверенных на практике методов, результатами расчетов и имитационного моделирования, их соответствия основным теоретическим положениям работы.

Апробация результатов. Основные положения диссертационной работы докладывались и обсуждались на следующих научных конференциях:

– VI и VIII Всероссийских зимних школах-семинарах аспирантов и молодых учёных «Актуальные проблемы науки и техники», Уфа, 2011, 2013;

– XIII, XIV и XV Международных научных конференциях «Компьютерные науки и информационные технологии», Гармиш-Партенкирхен, Германия, 2011; Уфа – Гамбург – Норвежские Фьорды, 2012; Вена – Будапешт – Братислава, 2013;

– VI и VII Всероссийских молодёжных научных конференциях «Мавлютовские чтения», Уфа, 2012, 2013;

– Международной конференции «Информационные технологии интеллектуальной поддержки принятия решений», Уфа, 2013.

Публикации. По теме диссертации опубликовано 12 печатных работ, в том числе 2 статьи в рецензируемых журналах из списка ВАК.

Структура и объём работы. Диссертационная работа состоит из введения, четырёх глав, заключения, списка литературы. Диссертация изложена на 177 страницах машинописного текста, содержит 37 рисунков и 21 таблицу. Библиографический список включает 149 наименований литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, сформулированы цель исследования и содержание решаемых задач, объект и предмет исследования, определены методы исследования, научная новизна и практическая ценность выносимых на защиту результатов.

Первая глава посвящена анализу современного состояния в области построения защищённых территориально-распределённых ИС на уровне субъекта Российской Федерации.

Рассмотрены бизнес-процессы, протекающие в региональной системе межведомственного электронного взаимодействия (РСМЭВ). Сформулированы требования к ИБ РСМЭВ с учётом нормативно-законодательной базы, национальных и международных стандартов. Проведён анализ способов построения моделей ИС; рассмотрены такие виды моделирования, как *IDEF*-технологии, нечёткая логика, нечёткие когнитивные карты (НКК), имитационное моделирование.

Проанализировано современное состояние в области управления рисками и оценки уровня защищённости территориально-распределённых ИС. Обоснована необходимость создания интегрированных систем мониторинга и управления событиями ИБ в классе интеллектуальных *SIEM*-систем. Проведён обзор коммерческих программных продуктов в области построения систем мониторинга территориально-распределённых ИС. Сделан вывод о целесообразности разработки и внедрения СППР по ЗИ в РСМЭВ с целью повышения её ИБ.

На основании сделанных заключений сформулированы цель и задачи исследования, поставленные в диссертационной работе.

Вторая глава посвящена разработке моделей *SIEM*-системы, метода и алгоритма оценки защищённости РСМЭВ, а также методики и алгоритма оценки информационных рисков в РСМЭВ.

Решена задача построения онтологической модели *SIEM*-системы, предназначенной для мониторинга уровня защищённости РСМЭВ, с использованием технологии *IDEF5*, составлен словарь терминов предметной области.

На основе разработанной онтологии предметной области проведено функциональное моделирование бизнес-процессов в *SIEM*-системе с помощью технологии *IDEF0*.

Общая архитектура *SIEM*-системы представлена на рисунке 1.

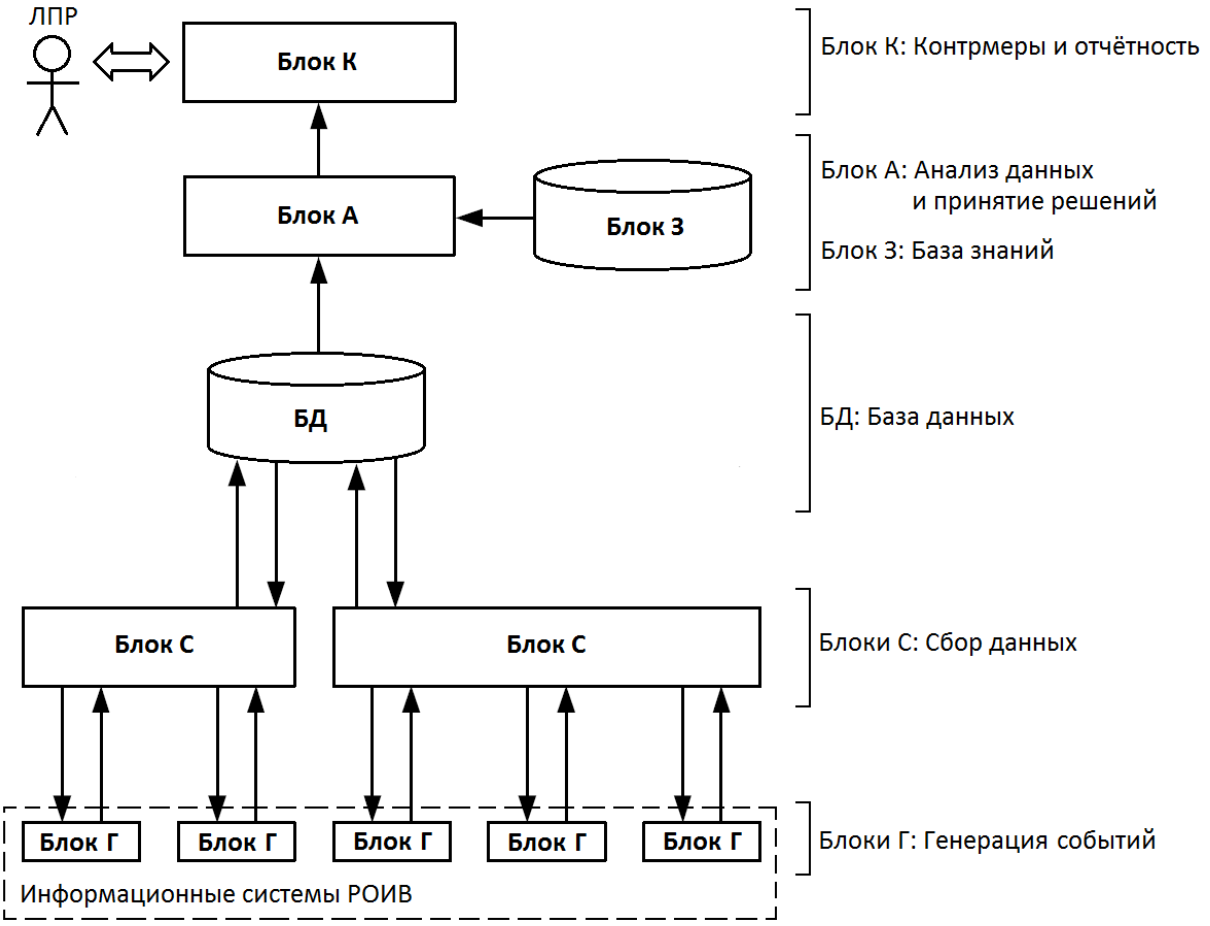

Рисунок 1 – Архитектура *SIEM*-системы

При решении проблемы оценки защищённости отдельных ИС и РСМЭВ на этапе корреляции и приоритезации событий ИБ (Блок А архитектуры) предложено использовать дополнительный параметр ИБ ИС «Уровень защитных мер в ИС», позволяющий более достоверно осуществлять приоритезацию инцидентов ИБ по степени их важности. Таким образом, параметрами ИБ ИС являются {*At*, *As*, *T*, *P*}, где *At* – уровень нарушения ИБ в ИС; *As* – критичность активов ИС; *T* – уровень доверия сообщающему устройству; *P* – уровень защитных мер в ИС.

В каждый период времени лингвистической переменной, определяющей значения параметра ИБ ИС, может быть присвоено целое числовое значение в диапазоне от 1 до 5, в соответствии с таблицей 1.

Таблица 1 – Соответствие лингвистических переменных числовым значениям параметров ИБ ИС

Лингвистическая переменная	Параметры ИБ ИС			
	At	***As***	***T***	***P***
Очень низкий	1	5	5	1
Низкий	2	4	4	2
Средний	3	3	3	3
Высокий	4	2	2	4
Очень высокий	5	1	1	5

Важность инцидента ИБ в отдельной (*i*-й) ИС ($I_{ИСi}$) определяется как:

$$I_{ИСi} = k(m) \times At_i \times As_i \times T_i \times P_i, \quad (1)$$

где *k(m)* – нормирующий коэффициент, позволяющий представить полученный результат в диапазоне [0; 1].

Уровень защищённости *i*-й ИС определяется с помощью формулы:

$$S_{ИСi} = 1 - I_{ИСi}, \quad (2)$$

где $I_{ИСi}$ – важность инцидента ИБ в *i*-ой ИС;

Оценка защищённости РСМЭВ вычисляется по следующей формуле:

$$S_{РСМЭВ} = \prod_{i=1}^{n} (1 - I_{ИСi}), \quad (3)$$

где *n* – количество ИС в РСМЭВ; $I_{ИСi}$ – важность инцидента ИБ в *i*-й ИС.

Подставив значение $I_{ИСi}$ из формулы (1), получаем итоговую формулу, позволяющую получить количественную оценку защищённости РСМЭВ:

$$S_{РСМЭВ} = \prod_{i=1}^{n} (1 - k(m) \times At_i \times As_i \times T_i \times P_i), \quad (4)$$

где *n* – количество ИС в РСМЭВ; At_i – уровень нарушения ИБ в *i*-й ИС; As_i – критичность активов в *i*-й ИС; T_i – уровень доверия сообщающему устройству *i*-й ИС; P_i – уровень защитных мер в *i*-й ИС.

При пересечении пороговых значений, заданных для $S_{ИСi}$ и $S_{РСМЭВ}$, производятся соответствующие автоматизированные ответные действия, связанные с принятием решений по управлению защитой информации в ИС и РСМЭВ соответственно.

Разработана методика оценки информационных рисков в РСМЭВ с помощью НКК, представляющая собой следующую последовательность действий:

1. Определение (*для последующих итераций* – выбор из списка и/или определение новых) угроз ИБ, свойств объекта защиты и видов ущерба (дестабилизирующих (ДФ), промежуточных (ПФ) и целевых факторов (ЦФ) соответственно).

2. Определение (нечётких) переменных «силы связи».

3. Составление матрицы достижимости.

4. Вычисление информационного риска.

4.1. Вычисление непрямых эффектов ДФ-концептов на ЦФ-концепты:

$$T_n(K^i_{ДФ} \to K^j_{ЦФ}) = \min_{k,l} \{B_{kl}\}, \quad (5)$$

где $\{B_{kl}\}$ – множество весов связей на пути между $K^i_{ДФ}$ и $K^j_{ЦФ}$.

4.2. Полный эффект от воздействия $K^i_{ДФ}$ на $K^j_{ЦФ}$:

$$T(K^i_{ДФ} \to K^j_{ЦФ}) = \max \{T_1, T_2, \ldots, T_N\}, \quad (6)$$

где T_k – непрямой k-й эффект между $K^i_{ДФ}$ и $K^j_{ЦФ}$, (k = 1, 2,…, N); N – число непрямых эффектов.

4.3. Суммарный риск целевого фактора от действия всех угроз:

$$R = \sum_{i,j} (З_j \cdot T(K^i_{ДФ} \to K^j_{ЦФ}) \cdot Ц_j), \quad (7)$$

где $Ц_j$ – цена j-го ресурса; $З_j$ – значимость (вес) j-го ресурса, определяемая экспертно.

5. Определение (*для последующих итераций* – выбор из списка и/или определение новых) контрмер (управляющих факторов).

6. Определение нечётких правил.

7. Оценивание информационного риска с учётом внедрения контрмер.

8. Оценка эффективности внедрения контрмер: вычисляется по формуле:

$$Э = \frac{R - R'}{R} \cdot 100\%, \quad (8)$$

где R – первоначальное значение риска; R' – значение риска после введения контрмер.

При решении задачи выбора контрмер для снижения информационных рисков предусматривается минимизация затрат на мероприятия по ЗИ при обеспечении допустимого уровня риска, представляемая как:

$$S_\Sigma \to min \text{ при } R \le R_{ДОП}, \quad (9)$$

где R и S_Σ – соответственно общий риск и суммарные затраты на мероприятия (контрмеры) по ЗИ; $R_{ДОП}$ – допустимое значение риска.

В третьей главе проведено имитационное моделирование блоков подсистемы поддержки принятия решений (ППР), осуществляющих оценивание уровня защищённости и информационных рисков РСМЭВ.

Основными блоками подсистемы ППР являются:

– Блок оценивания защищённости РСМЭВ (Блок 1);

– Блок оценивания информационных рисков в РСМЭВ (Блок 2);

– Консоль управления.

Блоки оценивания функционируют в соответствии с разработанными алгоритмами ПР, блок-схемы которых представлены на рисунках 2 и 3.

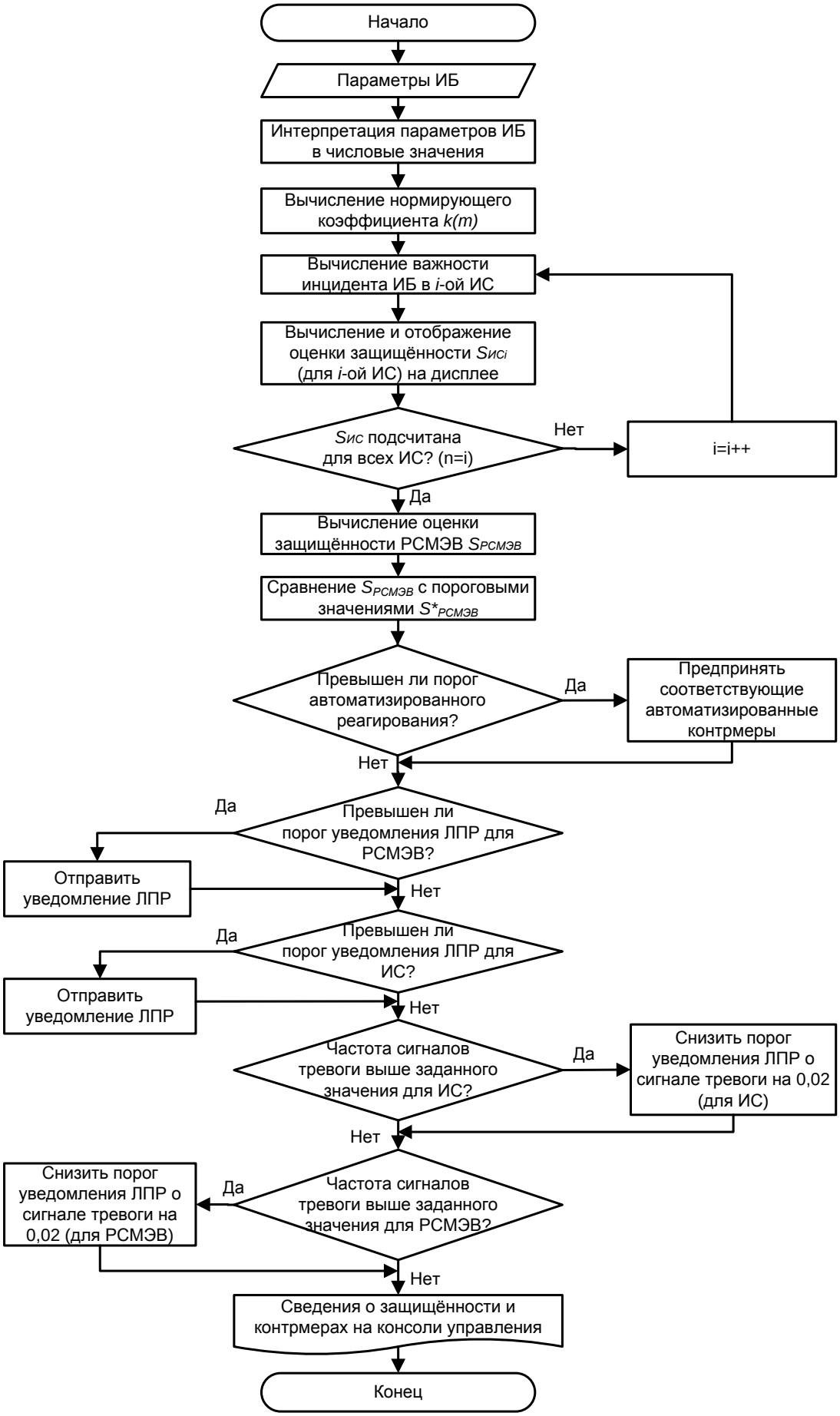

Рисунок 2 – Блок-схема алгоритма ПР по оперативному управлению ИБ в РСМЭВ на основе оценки уровня защищённости (для Блока 1)

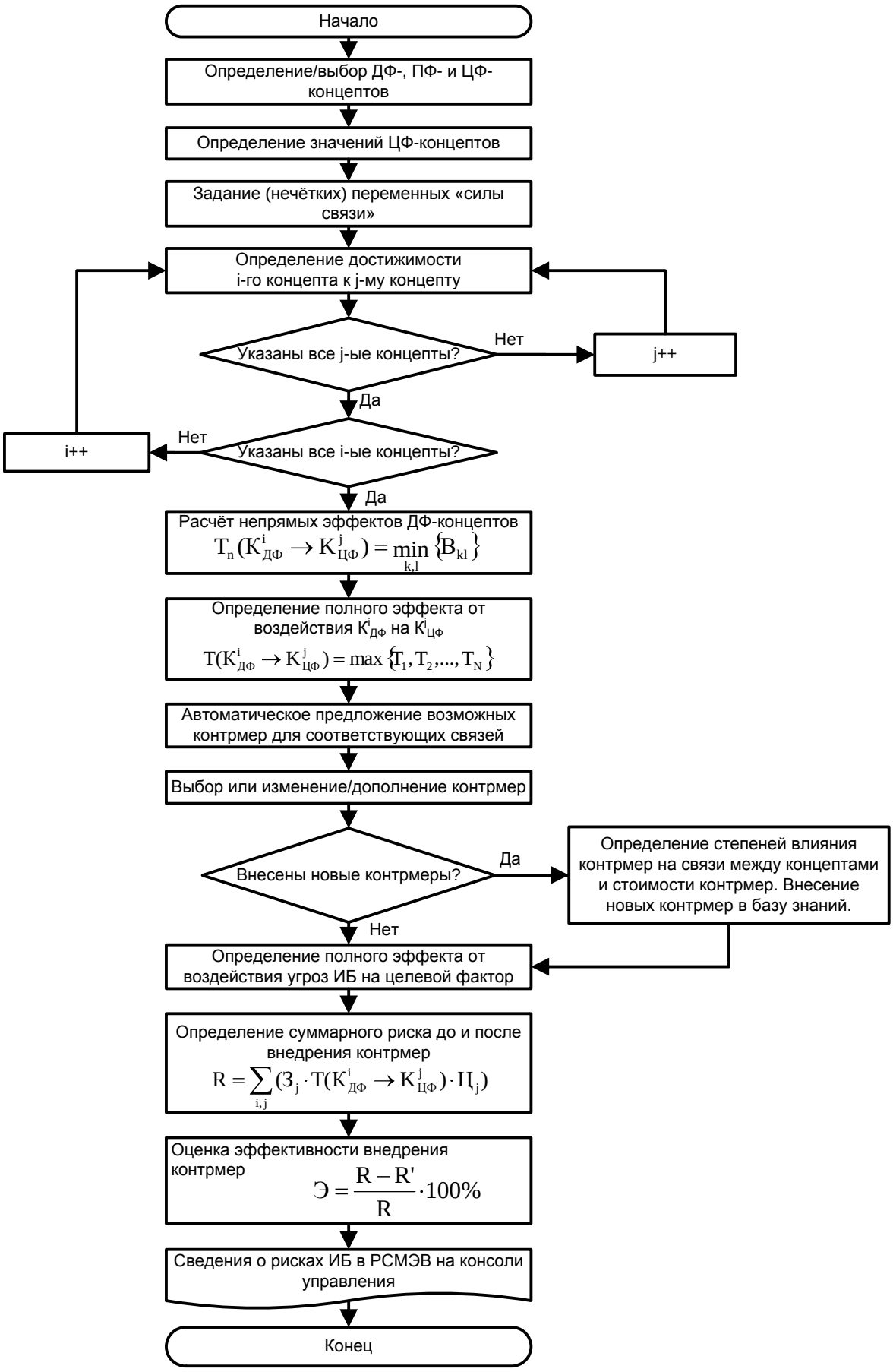

Рисунок 3 – Блок-схема алгоритма ПР по организационно-техническому управлению ИБ в РСМЭВ на основе оценки рисков ИБ (для Блока 2)

Блок 1 реализует метод оценки защищённости ИС и РСМЭВ на уровне оперативного управления ЗИ на основе правил нечёткой логики; Блок 2 – методику оценки информационных рисков на уровне организационно-технического управления ЗИ в РСМЭВ с помощью НКК.

Имитационное моделирование подтвердило адекватность реакции указанных блоков на возмущающие факторы, воздействующие на защищаемый объект, а также корректность функционирования исследовательского прототипа СППР по ЗИ в РСМЭВ.

В четвертой главе представлено описание исследовательского прототипа СППР, выполненного на языке программирования *C#*.

На рисунке 4 показана консоль управления, обеспечивающая ППР посредством отображения показателей защищённости ИС и РСМЭВ в режиме реального времени и указания предпринятых контрмер.

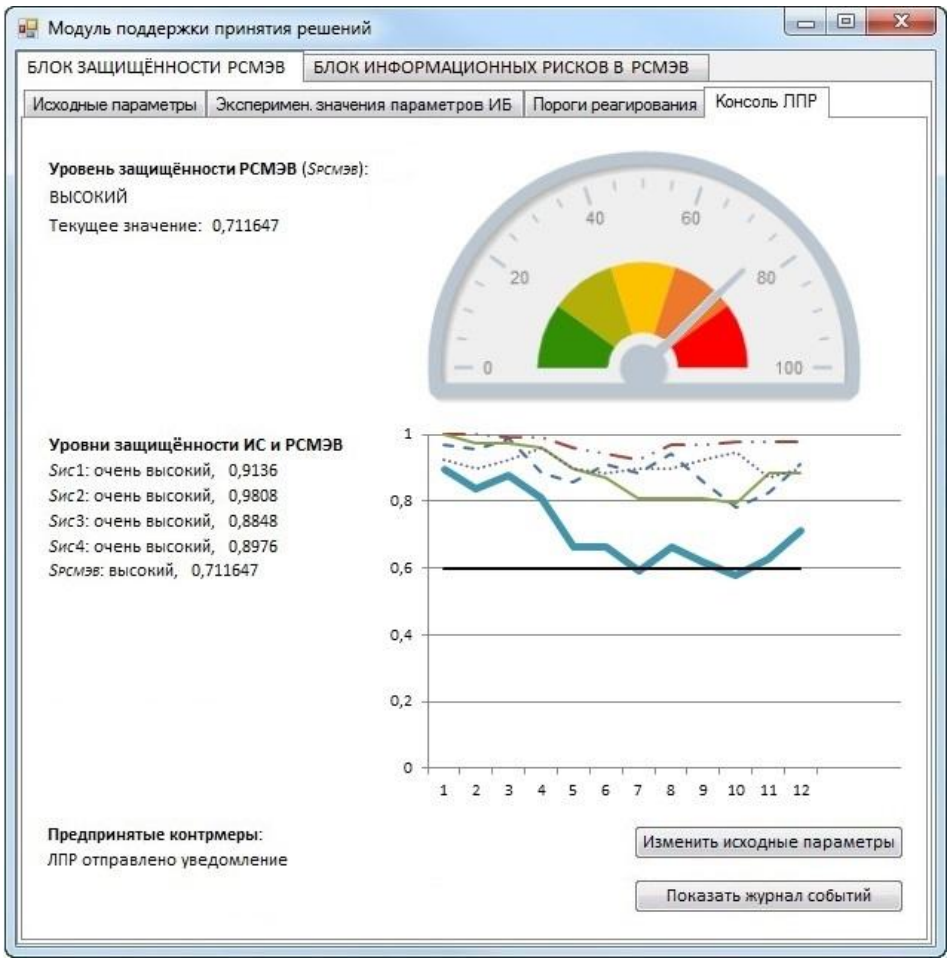

Рисунок 4 – Консоль управления

К функциям программного продукта, реализующего прототип СППР, относятся:

– формирование перечней угроз ИБ, воздействующих на объект защиты, свойств объекта защиты, а также перечня видов ущерба с дальнейшим их сохранением в базе знаний;

– отображение текущих значений качественной и количественной оценки защищённости каждой ИС, подключенной в РСМЭВ, и оценки защищённости самой РСМЭВ;

– отображение динамического графика защищённости ИС и РСМЭВ с указанием порогов реагирования;

– снижение порога формирования сигнала тревоги при превышении количества сигналов тревоги заданной нормы;

– формирование перечня контрмер, направленных на снижение угроз ИБ, с дальнейшим их сохранением в базе знаний;

– отображение информационных рисков до и после внедрения контрмер, оценка эффективности предложенных контрмер.

Уровни защищённости ИС и РСМЭВ представляются в графическим виде, а также в виде числовой (количественной) и лингвистической (качественной) оценок.

Для ИС, входящих в РСМЭВ, предусмотрены 4 вида контрмер, применяемых в различных комбинациях:

1) уведомление ответственного лица, принимающего решение (ЛПР);

2) реконфигурирование маршрутизатора, через который ЛВС информационной системы соединяется с РСМЭВ;

3) выявление фактора(ов) риска, т.е. одного или нескольких параметров ИБ с худшими значениями;

4) блокирование доступа ИС, на которой был зафиксирован инцидент ИБ, к РСМЭВ (так называемое «помещение ИС в карантин»).

Для РСМЭВ предусмотрено 5 видов автоматизированных ответных действий:

1) уведомление ЛПР;

2) реализация строгих настроек безопасности на оборудовании мониторируемой инфраструктуры объекта защиты (разрешается использовать только специально указанные, разрешённые приложения; по умолчанию, разрешено пользоваться любыми приложениями, кроме запрещённых);

3) реализация очень строгих настроек безопасности (используются только приложения и протоколы безопасности);

4) выявление фактора(ов) риска;

5) закрытие доступа в глобальную сеть Интернет со стороны РСМЭВ.

Управление и мониторинг устройств, входящих в состав ИС, осуществляется по протоколу *SNMP*. Передача данных в системные журналы осуществляется по протоколу *syslog*.

В заключении приведены основные результаты и подведены итоги исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

Основным результатом диссертационной работы является построение интеллектуальной системы поддержки принятия решений по обеспечению информационной безопасности, применение которой позволяет повысить защищённость РСМЭВ. Разработанная СППР построена с использованием моделей, методов и алгоритмов мониторинга и управления событиями ИБ. СППР позволяет лицам, принимающим решения, принимать своевременные и адекватные меры по противодействию угрозам и снижению рисков информационной безопасности в РСМЭВ.

Для разработки данной СППР были решены следующие задачи:

1. Разработана онтология предметной области, связанной с построением *SIEM*-системы в РСМЭВ на основе *SADT*-методологии и технологии *IDEF5*, отличающаяся учётом основных факторов, определяющих ИБ РСМЭВ, которая позволила выявить основные сущности и их взаимосвязи в данной предметной области и более обоснованно построить функциональную модель исследуемой системы. Предложена функциональная модель *SIEM*-системы на основе использования технологии *IDEF0*, отличающаяся учётом специфики реализации процессов мониторинга и реагирования на инциденты ИБ в РСМЭВ, что позволило сформировать требования к этим процессам исходя из поставленных целей обеспечения ИБ РСМЭВ.
2. Разработаны метод и алгоритм оценки защищённости ИС и РСМЭВ в целом на основе правил нечёткой логики, отличающиеся учётом корреляции событий ИБ в ИС, что позволило более достоверно осуществлять приоритезацию инцидентов ИБ в РСМЭВ по их степени важности. Использование предложенной методики оценки защищённости ИС и РСМЭВ позволяет оценивать в реальном времени защищённость как каждой ИС, входящей в РСМЭВ, так и системы в целом, что обеспечивает базу для принятия оперативных решений по ЗИ в РСМЭВ.
3. Разработаны методика и алгоритм оценки информационных рисков в РСМЭВ, основанные на использовании аппарата НКК, отличающиеся учётом специфики процессов ЗИ в РСМЭВ, что позволило решать задачу анализа и управления рисками в РСМЭВ путём принятия решений по выбору соответствующих контрмер, противодействующих влиянию основных угроз в РСМЭВ.
4. Разработан исследовательский прототип СППР, позволяющий производить оперативную оценку защищённости и оценку информационных рисков РСМЭВ, а также принятие своевременных решений по ЗИ в РСМЭВ на основе этих оценок.
5. Эффективность и корректность функционирования СППР подтверждена методом имитационного моделирования. Показано, что реализация СППР позволяет обеспечить повышение уровня автоматизации и централизации мониторинга защищённости РСМЭВ. За счёт этого

можно сократить время информирования ответственных лиц об инцидентах ИБ в 7,2–7,5 раз. Информационные риски, присутствующие в РСМЭВ, при этом могут быть снижены в 1,5 раза.

Перспективы дальнейшей разработки темы. Дальнейшим развитием данной работы может быть проработка форматов взаимодействия (интерфейсов) между традиционными механизмами безопасности, обрабатывающими первичную информацию, и модулями *SIEM*-системы.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых журналах ВАК

1. Файзуллин, Р. Р. Методика оценки информационных рисков в сетях передачи данных с помощью нечётких когнитивных карт / Р. Р. Файзуллин, В. И. Васильев // Системы управления и информационные технологии. – 2013. – № 1.1(51). – С. 192–195.

2. Файзуллин, Р. Р. Метод оценки защищённости сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечёткой логики / Р. Р. Файзуллин, В. И. Васильев // Вестник УГАТУ. – 2013. – Т. 17, № 2 (55). – С. 150–156.

Другие публикации

3. Файзуллин, Р. Р. Особенности защиты персональных данных в образовательных учреждениях при переводе государственных и муниципальных услуг в электронный вид / Р. Р. Файзуллин // Труды шестой Всероссийской зимней школы-семинара аспирантов и молодых учёных «Актуальные проблемы науки и техники» (15-18 февраля 2011 г., Уфа). Том 1. – Уфа: Изд-во УГАТУ, 2011. – С. 233–236.

4. Файзуллин, Р. Р. Требования к информационной безопасности региональных информационных систем / Р. Р. Файзуллин // Вычислительная техника и новые информационные технологии. Вып.7. – Уфа: Изд-во УГАТУ, 2011. – С. 185–190.

5. Файзуллин, Р. Р. Защита информации как превентивная мера по предотвращению отказа информационной системы // Труды 13-й Междунар. конференции «Компьютерные науки и информационные технологии (*CSIT'2011*)» (27 сентября–2 октября 2011 г., Гармиш-Партенкирхен, Германия). Том 1. – Уфа: Изд-во УГАТУ, 2011. – С. 95–97. (Статья на англ. яз.).

6. Файзуллин, Р. Р. Поддержка принятия решений по защите информации в мультисервисной сети передачи данных // Труды 14-й Междунар. конференции «Компьютерные науки и информационные технологии (*CSIT'2012*)» (20–26 сентября 2012 г., Уфа – Гамбург – Норвежские Фьорды). Том 2. – Уфа: Изд-во УГАТУ, 2012. – С. 118–121. (Статья на англ. яз.).

7. Файзуллин, Р. Р. *SIEM*-система как средство соответствия требованиям и неотъемлемая часть системы защиты информации предприятия // Труды 14-й Междунар. конференции «Компьютерные науки и информационные технологии (*CSIT'2012*)» (20–26 сентября 2012 г., Уфа – Гамбург – Норвежские Фьорды). Том 1. – Уфа: Изд-во УГАТУ, 2012. – С. 194–197. (Статья на англ. яз.).

8. Файзуллин, Р. Р. Моделирование мультисервисной сети передачи данных при построении интеллектуальной системы мониторинга и управления событиями информационной безопасности / Р. Р. Файзуллин // Труды VI Всероссийской молодежной научной конференции «Мавлютовские чтения» (7–9 ноября 2012 г., Уфа). Том 3. – Уфа: Изд-во УГАТУ, 2012. – С. 17–18.

9. Файзуллин, Р. Р. Четырёхфакторная модель оценки защищённости сетей передачи данных на основе нечёткой логики / Р. Р. Файзуллин // Труды VIII Всероссийской зимней школы-семинара аспирантов и молодых учёных «Актуальные проблемы науки и техники» (19–20 февраля 2013 г., Уфа). Том 1. – Уфа: Изд-во УГАТУ, 2013. – С. 345–348.

10. Файзуллин, Р. Р. Система поддержки принятия решений системы мониторинга в сетях передачи данных / Р. Р. Файзуллин, В. И. Васильев // Труды Междунар. конференции «Информационные технологии интеллектуальной поддержки принятия решений (*ITIDS'2013*)» (21–25 мая 2013 г., Уфа, Россия). Том 2. – Уфа: Изд-во УГАТУ, 2013. – С. 87–90. (Статья на англ. яз.).

11. Файзуллин, Р. Р. Метод оценки рисков информационной безопасности в сетях передачи данных на основе нечётких когнитивных карт / Р. Р. Файзуллин, В. И. Васильев // Труды 15-й Междунар. конференции «Компьютерные науки и информационные технологии (*CSIT'2013*)» (15–21 сентября 2013 г., Вена – Будапешт – Братислава). Том 1. – Уфа: Изд-во УГАТУ, 2013. – С. 87–90. (Статья на англ. яз.).

12. Файзуллин, Р. Р. Поддержка принятия решений по защите информации в региональном сегменте Электронного правительства / Р. Р. Файзуллин // Труды VII Всероссийской молодежной научной конференции «Мавлютовские чтения» (22-24 ноября 2013 г., Уфа). Том 3. – Уфа: Изд-во УГАТУ, 2013. – С. 19–20.

Диссертант Р. Р. Файзуллин

ФАЙЗУЛЛИН Рустам Рафитович

ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМАХ

(НА ПРИМЕРЕ РЕГИОНАЛЬНОЙ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ РЕСПУБЛИКИ БАШКОРТОСТАН)

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать __.11.2013г. Формат 60×84 1/16.
Усл. печ. л. 1,0. Усл. кр. – отт. 1,0. Уч. – изд. л. 0,9.
Тираж 100 экз. Заказ № ___

ФГБОУ ВПО «Уфимский государственный авиационный технический университет»
Центр оперативной полиграфии
450000, г. Уфа, ул. Карла Маркса, 12.