На правах рукописи

ЯНДЫБАЕВА Эмма Эмануиловна

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМЕ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа – 2016

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

Научный руководитель: доктор технических наук, доцент
МАШКИНА Ирина Владимировна,

Официальные оппоненты: доктор технических наук, профессор
СОЛОВЬЕВ Николай Алексеевич,
Оренбургский государственный университет,
заведующий кафедрой программного обеспечения вычислительной техники и автоматизированных систем

кандидат технических наук
ФАЙЗУЛЛИН Рустам Рафитович,
Государственное унитарное предприятие Центр информационно-коммуникационных технологий Республики Башкортостан,
главный специалист отдела сетевого обеспечения

Ведущая организация: Федеральное государственное автономное образовательное учреждения высшего образования «Южный федеральный университет», г. Ростов-на-Дону

Защита диссертации состоится 22 апреля 2016 г. в 12^{00} часов на заседании диссертационного совета Д-212.288.07 на базе ФГБОУ ВПО «Уфимский государственный авиационный технический университет» по адресу: 450000, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «25» февраля 2016 года.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

На сегодняшний день в предпринимательской деятельности все большую популярность завоевывают технологии дистанционной торговли, ключевой особенностью которых является приобретение товара или услуги на основе информации, полученной через Интернет. При этом формируются разнообразные информационно-коммерческие системы, в том числе электронные торговые площадки (ЭТП). На таких площадках проводятся все виды торгово-закупочных процедур и обеспечивается взаимодействие покупателя с продавцом через Интернет на всех этапах заключения сделки.

В России наблюдается всплеск роста рынка электронной торговли, в том числе за счет эффективной нормативно-правовой базы, устанавливающей обязательность использования ЭТП для продажи имущества должников и для осуществления государственного заказа. При этом следует отметить, что в 2015 г. стоимость реализованного имущества должников составила 523 млрд. руб., а объем государственного заказа достиг 6,6 трлн. руб. или 9,8 % ВВП. В то же время в судебной практике увеличивается число случаев признания результата электронного аукциона недействительным из-за выявления утечки конфиденциальной информации и сговора участников аукциона, а также из-за нестабильной работы информационной системы (ИС) ЭТП.

Учитывая важность системы электронной торговли в масштабах экономики страны и рост числа инцидентов нарушения информационной безопасности (ИБ), разработка методов управления ИБ в ИС ЭТП является актуальной проблемой.

Степень разработанности темы

На сегодняшний день отсутствуют серьезные исследования в области ИБ ИС ЭТП. Рассматривается безопасность отдельных элементов ИС ЭТП и отсутствует комплексный подход к защите информации в ИС ЭТП. Так работы Кононова Д.Д., Исаева С.В., Исаевой О.С. посвящены исследованию проблем безопасности и обеспечения кроссплатформенного функционирования веб-сервисов, а также разработке программного обеспечения (ПО) для веб-сервисов поддержки муниципальных закупок. В работах Куприянова А.О., Лекае В.А., Полежаева А.В. исследуются проблемы организации безопасного электронного документооборота на ЭТП и основное внимание уделено процессу аттестации рабочих мест в ИС ЭТП. В работах Соловьева Н.А., Дворового И.Г., Тишиной Н.А. решается задача администрирования безопасности электронного документооборота, частным случаем которого является ИС ЭТП.

Между тем ИС ЭТП является уникальным объектом защиты. Это обусловлено, в том числе, необходимостью использования электронной подписи в каждом документе, создаваемом в процессе торгов, особенностью алгоритмов проведения электронных аукционов, высокими требованиями к доступности системы и большим количеством удаленных пользователей. Поэтому комплексное исследование ИС ЭТП как самостоятельного объекта защиты является актуальной проблемой ИБ.

Объектом исследования является информационная система электронной торговой площадки.

Предметом исследования являются методы моделирования угроз ИБ в ИС ЭТП и методы управления ИБ в ИС ЭТП.

Целью исследования является повышение уровня информационной безопасности при эксплуатации информационных систем электронных торговых площадок.

Задачи исследования:

1. Разработка модели угроз ИБ в ИС ЭТП, позволяющей количественно оценить угрозы ИБ в ИС ЭТП и сравнить полученные оценки для выявления наиболее актуальных угроз.
2. Разработка метода выбора комплекса средств защиты информации (СрЗИ) для ИС ЭТП, обеспечивающего нейтрализацию актуальных угроз ИБ в ИС ЭТП.
3. Разработка методики формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП, предназначенных для конфигурации СрЗИ, используемых в ИС ЭТП.
4. Разработка системы управления ИБ в ИС ЭТП и программного обеспечения для автоматизации процедуры выбора модульного состава системы защиты информации (СЗИ) и процесса формирования политики разграничения доступа.

Методы исследования

При решении поставленных в диссертационной работе задач использованы методы системного анализа, методы принятия решений, методы теории защиты информации, методология графического моделирования, методология функционального моделирования и положения теории вероятностей.

Положения, выносимые на защиту

1. Разработаны графические функциональные модели преднамеренных угроз ИБ в ИС ЭТП с использованием EPC-нотации, позволяющие наглядно и детально отобразить процессы реализации угроз, получить количественную оценку угроз и выявить наиболее актуальные угрозы.
2. Предложен адаптированный для выбора комплекса СрЗИ в ИС ЭТП метод, основанный на попарном сравнения альтернатив Б. Руа, позволяющий сформировать рациональные наборы средств защиты, реализующие механизмы защиты, направленные на нейтрализацию актуальных угроз ИБ в ИС ЭТП, а сам процесс выбора – автоматизировать.
3. Предложена методика формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП на основе ролевой модели, позволяющая автоматизировать сложный процесс разработки политики разграничения доступа в ИС ЭТП и повысить эффективность и производительность работы сотрудников, отвечающих за обеспечение ИБ в ИС ЭТП.
4. Разработана архитектура системы управления ИБ в ИС ЭТП и программное обеспечение, реализующие функции интеллектуальной поддержки принятия решений по выбору модульного состава системы защиты информации и

формирования политики разграничения доступа в ИС ЭТП, позволяющие принимать оперативные и рациональные решения по обеспечению ИБ.

Научная новизна

1. Новизна моделей угроз ИБ на основе EPC-нотации в графическом представлении угроз как последовательности событий и функций с учетом всех исполнителей и всех используемых для реализации угроз объектов и уязвимостей компьютерной инфраструктуры, что позволяет получить количественную оценку угроз на основании положений теории вероятностей, сравнить угрозы ИБ между собой, определить, успешная реализация какой из угроз наиболее вероятна относительно других угроз и, как следствие, выявить наиболее актуальные угрозы ИБ в ИС ЭТП.

2. Новизна адаптированного метода выбора комплекса СрЗИ для ИС ЭТП, базирующегося на попарном сравнении альтернатив Б. Руа, заключается в формализации метода применительно к задаче выбора комплекса СрЗИ, принадлежащих разным функциональным подсистемам, в разработке иерархических структур критериев выбора СрЗИ и таблиц расчетов индексов согласия и несогласия для функциональных подсистем, что позволяет сформировать рациональный набор СрЗИ, реализующих механизмы защиты, направленные на нейтрализацию актуальных угроз ИБ в ИС ЭТП, а сам процесс выбора – автоматизировать.

3. Новизна методики формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП на основе математической модели ролевого разграничения доступа, заключается в выявлении множества сущностей в ИС ЭТП, определении множества возможностей для ИС ЭТП и введении иерархической структуры на указанном множестве, разработке правил контроля доступа в ИС ЭТП на основе сведений об объектах доступа, ролях пользователей и их возможностях, в определении правил администрирования, предназначенных для административных ролей ИС ЭТП и позволяющих администрировать множество авторизованных ролей пользователей, множество прав доступа, которыми обладают роли, и иерархию ролей, с учетом специфичных для ИС ЭТП условий и ограничений.

4. Новизна архитектуры системы управления ИБ в ИС ЭТП заключается в реализации функций интеллектуальной поддержки принятия решений по выбору модульного состава системы защиты информации и функций формирования политики разграничения доступа в ИС ЭТП, что позволяет, с одной стороны, осуществлять управление модульным составом СЗИ на основе данных об объективных технических характеристиках СрЗИ, декларируемых производителем, с другой стороны, оперативно и корректно вносить изменения в правила взаимодействия сущностей ИС ЭТП при изменении бизнес-процессов.

Степень достоверности и апробация результатов

Достоверность результатов, полученных в диссертационной работе, основывается на использовании апробированных методов исследования, корректном применении математического аппарата, согласованности новых результатов с известными теоретическими положениями.

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

– V, VI, VII и VIII Всероссийских молодежных научных конференциях «Мавлютовские чтения», Уфа, 2011, 2012, 2013, 2014;

– Международной научно-практической конференции «Современные тенденции в образовании и науке», Тамбов, 2012;

– XII и XIII Международных научно-практических конференциях «ИБ-2012» и «ИБ-2013», Таганрог, 2012, 2013;

– XX, XXI и XXII Всероссийских научно-практических конференциях «Проблемы информационной безопасности в системе высшей школы», Москва, 2013, 2014, 2015.

Результаты диссертационного исследования внедрены в производственной компании ООО «Башкерамика», являющейся клиентом ЭТП, и в учебный процесс кафедры «Вычислительная техника и защита информации» ФГБОУ ВПО «Уфимский государственный авиационный технический университет». На ПО, автоматизирующее процедуру выбора модульного состава системы защиты информации, получено свидетельство о государственной регистрации программы для ЭВМ.

Теоретическая и практическая значимость работы

Теоретическая и практическая значимость полученных результатов заключается в:

- разработанных моделях преднамеренных угроз ИБ в ИС ЭТП, позволяющих количественно оценить угрозы ИБ в ИС ЭТП и сравнить полученные оценки для выявления наиболее актуальных угроз;
- выявленном множестве актуальных угроз ИБ в ИС ЭТП, требующих для их нейтрализации применения дополнительных организационных и технических мер защиты информации;
- разработанном методе выбора комплекса СрЗИ для ИС ЭТП, реализующего механизмы защиты, направленные на нейтрализацию актуальных угроз ИБ в ИС ЭТП;
- разработанной методике формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП, подлежащей реализации с помощью используемых в ИС ЭТП средств защиты информации от несанкционированного доступа и исключающей утечку конфиденциальной информации на множестве ролей пользователей ИС ЭТП;
- разработанной архитектуре системы управления ИБ в ИС ЭТП и программном обеспечении, которые позволяют автоматизировать процедуру рационального выбора набора СрЗИ и процесс формирования политики разграничения доступа, в соответствии с предлагаемым методом выбора комплекса СрЗИ для ИС ЭТП и разработанной методикой формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП.

Результаты работы позволяют повысить уровень ИБ информационного взаимодействия участников электронного аукциона, проводимого в ИС ЭТП.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи исследования, определены объект и методы исследования, указаны научная новизна и практическая ценность выносимых на защиту результатов.

Первая глава посвящена исследованию объекта защиты – ИС ЭТП. В рамках данного исследования проведен анализ нормативно-правовой базы Российской Федерации в части определения требований к функционированию ИС ЭТП, в том числе к обеспечению ИБ в ИС ЭТП. Следует отметить, что одним из наиболее важных требований законодательства является использование технологии электронной подписи для обеспечения юридической значимости документооборота, совершаемого в рамках ИС ЭТП. Кроме того рассмотрены инфраструктура исследуемого объекта защиты и используемые в ИС ЭТП механизмы обеспечения безопасности. Выявлены привлекательные для заинтересованного субъекта информационные объекты, в отношении которых могут быть совершены атаки.

Проведено исследование научно-теоретических разработок построения системы защиты информации для ИС ЭТП. Результаты показали ограниченную возможность применения в ИС ЭТП существующих подходов для количественной оценки угроз ИБ. Кроме того приведены результаты анализа существующих методов оценки и сравнения многокритериальных альтернатив применительно к выбору СрЗИ, внедрение которых может потребоваться для нейтрализации актуальных угроз ИБ в ИС ЭТП. А также рассмотрены методы разработки политики разграничения доступа, на основе которых могут быть созданы правила разграничения доступа в ИС ЭТП.

На основании сделанных заключений сформулированы основные научно-теоретические задачи, решаемые в диссертационной работе.

Во второй главе проводится моделирование угроз ИБ в ИС ЭТП и разрабатывается метод численной оценки вероятностей реализации угроз ИБ, с помощью которого становится возможным определение их актуальности.

Разработана модель нарушителя ИБ в ИС ЭТП, основанная на существующих в нормативных документах ФСТЭК и ФСБ классификациях. Лица, потенциально опасные с точки зрения обеспечения ИБ в ИС ЭТП, разделены на две категории злоумышленников и семь категорий нарушителей с учетом опыта и знаний таких лиц, доступных им ресурсов, необходимых для реализации угрозы, а также возможной мотивации их действий. (В диссертационной работе под нарушителем понимается лицо, которое действует в пределах контролируемой зоны ИС и совершает заранее обдуманное действие с осознанием его опасных последствий. Под злоумышленником понимается лицо, осуществляющее атаки из-за пределов контролируемой зоны ИС.) Злоумышленники и нарушители рассматриваются в качестве источников угроз при построении модели угроз ИБ в ИС ЭТП.

Проведен анализ возможных угроз ИБ в ИС ЭТП и выявлены следующие преднамеренные угрозы:

- хищение ключа электронной подписи;

- удаленное несанкционированное управление ключом электронной подписи;
- подмена документа при передаче его на подпись;
- хищение логина и пароля от личного кабинета;
- несанкционированный доступ к внутренним ресурсам ЭТП из сети Интернет;
- срыв нормального функционирования сайта ЭТП.

Исследование выявленных угроз позволило разработать структурную вербальную модель угроз ИБ в ИС ЭТП, представленную в виде таблицы и содержащую такие сведения, как атакуемые информационные активы, категории нарушителей и злоумышленников, пострадавшие стороны и возможные негативные последствия от реализации угрозы.

С целью более детального и наглядного представления угрозы ИБ, дающего возможность в дальнейшем оценить ее количественно, предложено графическое моделирование угрозы ИБ с помощью EPC-нотации, основными элементами которой являются События и Функции. На основе предложенного подхода разработано шесть EPC-моделей выявленных преднамеренных угроз ИБ в ИС ЭТП, наглядно отображающих процессы реализации угроз, источники угроз и используемые для реализации угроз объекты. На рисунке 1 представлена разработанная EPC-модель угрозы подмены документа при передаче его на подпись, где события и функции обозначены переменными E1 … E6 и F1 … F4 соответственно.

Для сравнения исследуемых угроз в количественном выражении предлагается оценить вероятность их реализации путем проведения оценки вероятностей событий и активации функций для каждой разработанной EPC-модели угрозы. Вероятность наступления события (активации функции) вычисляется на основе статистических данных. В случае их отсутствия, если наступление события зависит от успешности преодоления барьера, установленного на пути реализации угрозы и представляющего собой СрЗИ, вероятность такого события принимается равной уровню уязвимости данного средства защиты. В свою очередь уровень уязвимости СрЗИ может быть получен нормированием величины уязвимости, приведенной в международной базе данных для соответствующего СрЗИ. При отсутствии данных о частоте наступления события и если наступление события не зависит от уязвимости СрЗИ либо нет сведений о ее величине, тогда при оценке исходного для реализации угрозы события, расположенного в верхней точке ветви EPC-модели, рассматривается наихудший случай, когда вероятность наступления такого события принимается равной 1. Во всех остальных случаях вероятность оцениваемого события вычисляется с использованием принципа недостаточного основания Я. Бернулли, утверждающего, что если нет оснований предпочесть исход одного события другому, несовместные события, составляющие полное множество событий, считаются равновероятными.

В таблице 1 представлены результаты ранжирования угроз ИБ в ИС ЭТП в порядке убывания расчетных значений вероятностей их реализации.

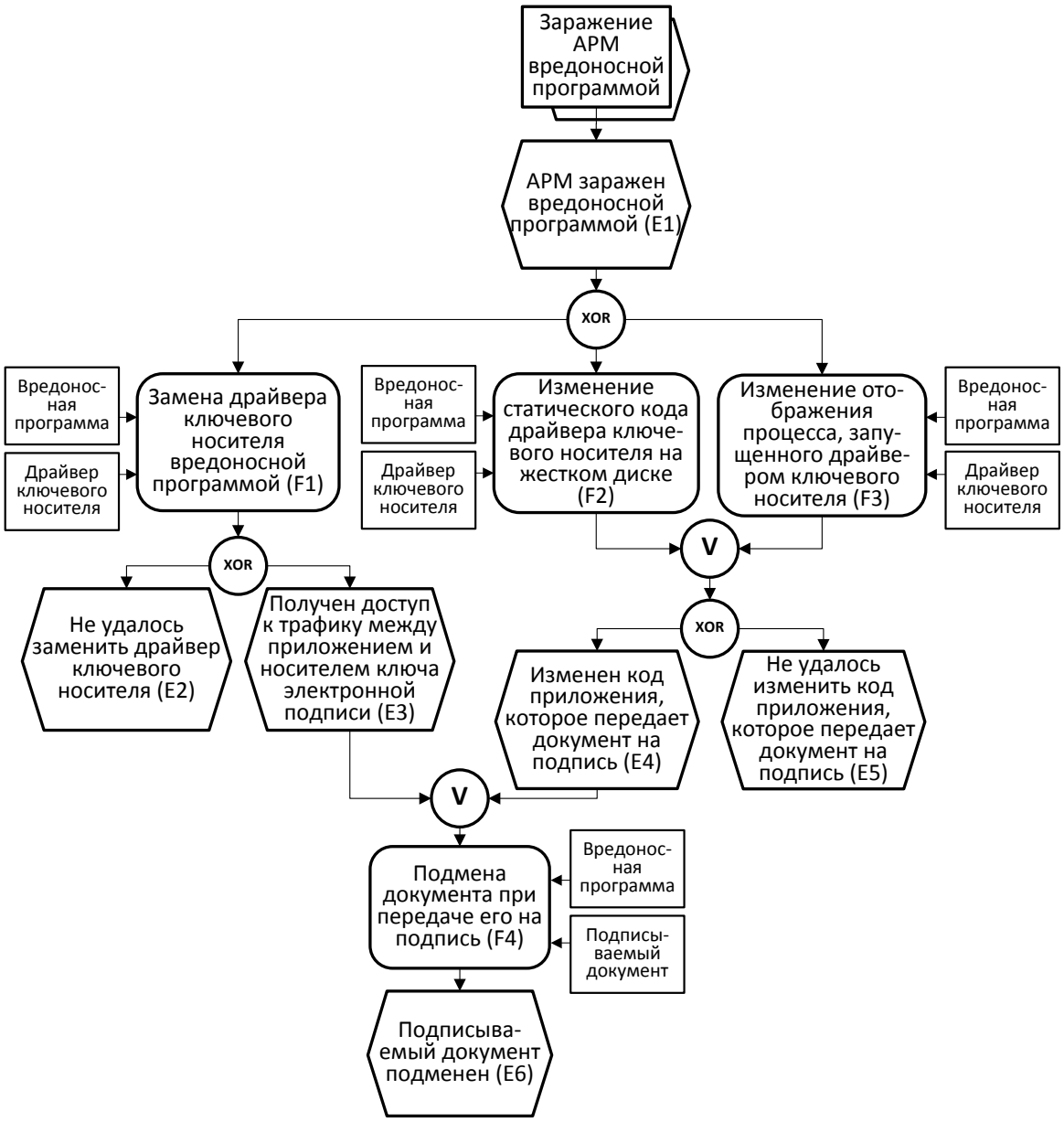

Рисунок 1 – EPC-модель угрозы подмены документа при передаче его на подпись

Таблица 1 – Результаты ранжирования угроз ИБ в ИС ЭТП

Наименование угрозы	**Ранг угрозы**
Хищение ключа электронной подписи	1
Срыв нормального функционирования сайта ЭТП	2
Хищение логина и пароля от личного кабинета	3
Удаленное несанкционированное управление ключом электронной подписи	4
Подмена документа при передаче его на подпись	5
Несанкционированный доступ к внутренним ресурсам ЭТП из сети Интернет	6

Вычисленные значения вероятностей являются показателями актуальности угроз и представлены в виде круговой диаграммы, где данные о каждом секторе

отображены в виде процентов от площади всего круга, а сами сектора пронумерованы в соответствии с номерами угроз в таблице 1 (рисунок 2).

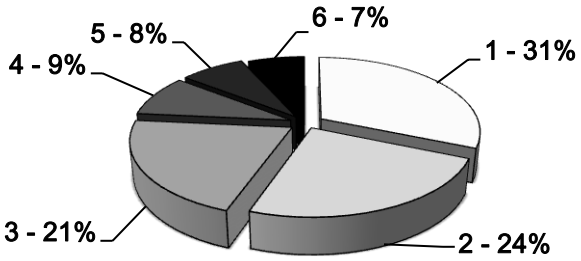

Рисунок 2 – Визуальное представление показателей актуальности угроз

Такое наглядное представление показателей актуальности угроз существенно облегчает работу эксперта. Так из полученной диаграммы стало очевидным значительное преобладание актуальности первых трех угроз и установлено, что актуальными угрозами ИБ в ИС ЭТП являются:

- хищение ключа электронной подписи;
- хищение логина и пароля от личного кабинета;
- срыв нормального функционирования сайта ЭТП.

Третья глава посвящена разработке моделей и методов управления ИБ в ИС ЭТП. Рассмотрены такие аспекты управления ИБ в ИС ЭТП как разработка политики безопасности и планирование модульного состава системы защиты информации и точек установки средств защиты в ИС.

Для реализации первой из перечисленных функций управления разработана методика формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП, основанная на математической модели ролевого разграничения доступа (РРД), отличающаяся определением множеств сущностей и возможностей, специфичных для ИС ЭТП, формированием детальных иерархических структур на указанных множествах и определением правил администрирования с учетом специфичных для ИС ЭТП условий и ограничений. Предложенная методика впоследствии может быть реализована с помощью настроек используемых в ИС ЭТП средств защиты.

Для реализации модели РРД на рассматриваемом объекте защиты выявлено множество сущностей в ИС ЭТП, фрагмент которого представлен в таблице 2.

Таблица 2 – Фрагмент выявленного множества сущностей ИС ЭТП

Наименование	**Тип**
Ключи электронных подписей клиентов ЭТП и администраторов ЭТП	Объект доступа
Сведения о клиентах ЭТП, подавших заявку на участие в торгах, которые не должны быть раскрыты до проведения аукциона	
Документы, подписываемые клиентами ЭТП	
Работник клиента ЭТП с правом объявления аукциона и правом подачи заявки на участие в торгах	Роль пользо-теля
Работник клиента ЭТП с правом подписания контракта	
Работник клиента ЭТП с правами администратора личного кабинета	

На множестве ролей пользователей сформирована иерархическая структура. Иерархия ролей пользователей ИС ЭТП задает на множестве R отношение частичного порядка «≤», при котором выполняется условие: для $u \in U$, если r_i, $r_j \in R$, $r_j \in UA(u)$ и $r_i \leq r_j$, то $r_i \in UA(u)$, где R – множество ролей, U – множество пользователей, $UA: U \rightarrow 2^R$ – функция, определяющая для каждого пользователя множество ролей, на которые он может быть авторизован. Кроме того сформирован перечень возможностей для ИС ЭТП, и разработана детальная иерархическая структура таких возможностей, которая также задает на указанном множестве отношения частичного порядка. На множестве ролей пользователей ИС ЭТП и множестве объектов доступа ИС ЭТП разработана матрица доступа, элементами которой являются перечисленные возможности.

Для определения правил администрирования множества авторизованных ролей пользователей и множеств прав доступа сформировано множество административных ролей в ИС ЭТП и проведены расчеты значений функций can-assign, can-revoke, can-assign$_p$ и can-revoke$_p$. Для определения правил администрирования, позволяющих изменять иерархию ролей, использованы помимо иерархии возможностей еще две разработанные иерархии, элементами которой соответственно являются группы (множества пользователей и других групп) и объединения (множества пользователей, прав доступа, групп, возможностей и других объединений). Следует отметить, что при формировании иерархии объединений считалось, что $up_j \leq up_i$ для $up_i, up_j \in UP$, $p_i, p_j \in P$, $g_i, g_j \in G$, если $p_i, g_i \in up_i$, $p_j, g_j \in up_j$ и $p_j \in p_i$, $g_i \in g_j$, где UP – множество объединений, P – множество прав доступа, G – множество групп. С учетом разработанных иерархий рассчитаны функции can-assign$_a$, can-revoke$_a$, can-assign$_g$ и can-revoke$_g$, значения которых являются элементами выявленного множества объединений.

Таким образом, определены правила контроля доступа в ИС ЭТП и правила администрирования в ИС ЭТП, которые позволяют гибко изменять политику разграничения доступа в процессе функционирования ИС ЭТП.

В целях реализация такой функции управления как планирование модульного состава системы защиты информации и точек установки средств защиты в сети, разработана модель планирования модульного состава системы защиты информации в ИС ЭТП. Планирование предложено выполнить в три этапа: во-первых, составить перечень требований к состоянию защищенности объекта защиты, во-вторых, определить модульный состав системы защиты информации и, в-третьих, осуществить процедуру выбора конкретных СрЗИ.

Для рассматриваемого в диссертации объекта защиты определено требование обеспечения нейтрализации выявленных актуальных угроз ИБ. Задача определения модульного состава системы защиты информации в ИС ЭТП сведена к вопросу определения дополнительных типов СрЗИ, внедрение которых в уже существующую СЗИ обеспечит нейтрализацию актуальных угроз ИБ в ИС ЭТП. С целью решения данной задачи проведен анализ мер, как технических, так и организационных, принятие которых позволит нейтрализовать угрозу хищение ключа электронной подписи, угрозу хищение логина и пароля от личного

кабинета и угрозу срыва нормального функционирования сайта ЭТП. Исходя из предложенных мер по нейтрализации актуальных угроз ИБ в ИС ЭТП сделано заключение о необходимости введения в ИС ЭТП следующих видов СрЗИ:

- системы распределенной фильтрации трафика (для фильтрации трафика, входящего в локально-вычислительную сеть оператора ЭТП);
- системы предотвращения вторжений (для локально-вычислительной сети оператора ЭТП).

Кроме того отмечено, что особое внимание следует уделить выбору антивирусного средства для рекомендации клиентам ЭТП.

Для каждого из перечисленных видов СрЗИ существует конечное множество альтернатив с широким набором критериев выбора. Следовательно, чтобы сделать выбор конкретных СрЗИ, необходимо применить аналитический метод, позволяющий осуществлять многокритериальный выбор. На основании анализа методов принятия решений установлено, что наиболее подходящим для данной задачи является метод Б. Руа. Данный метод адаптирован для выбора дополнительного набора СрЗИ в ИС ЭТП, включающего в себя подсистему распределенной фильтрации трафика, подсистему предотвращения вторжений и антивирусное средство.

Определение критериев выбора СрЗИ является творческой неформализуемой задачей, которая выполняется экспертом в области ИБ на основе его знаний, опыта и характеристик, декларируемых производителями СрЗИ. В диссертационной работе для каждого вида средств защиты, принадлежащих различным функциональным подсистемам, выявлен набор критериев, на основании которого осуществляется выбор лучшей альтернативы, а также разработаны иерархические структуры выявленных критериев. Проведена оценка длин шкал выявленных критериев выбора. Каждому критерию присвоен вес – целое число w_i, характеризующее важность критерия.

Рассматриваемые функциональные подсистемы защиты информации обозначены переменными Ф1, Ф2 и Ф3. Альтернативы СрЗИ для каждой из трех функциональных подсистем обозначены переменными A_{11} … A_{1K}, A_{21} … A_{2L} и A_{31} … A_{3M}, где K, L, M – количество рассматриваемых альтернатив для каждой функциональной подсистемы соответственно.

Согласно методу Б. Руа, если выдвигается гипотеза о превосходстве альтернативы A над альтернативой B, то множество I, состоящее из N критериев, разбивается на три подмножества:

- I^+ – подмножество критериев, по которым A предпочтительнее B;
- $I^=$ – подмножество критериев, по которым A равноценно B;
- I^- – подмножество критериев, по которым B предпочтительнее A.

Формируются индекс согласия c_{AB} и индекс несогласия d_{AB} с гипотезой о превосходстве A над B:

$$c_{AB} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{N} w_i},$$

$$d_{AB} = \max_{i \in I^-} \frac{l_B^i - l_A^i}{L_i},$$

где l_A^i, l_B^i – значения альтернатив A и B по i-му критерию; Li – длина шкалы i-го критерия.

В диссертационной работе метод Б. Руа адаптирован и формализован для решения задачи многокритериального и многоальтернативного выбора набора СрЗИ, входящих в состав нескольких функциональных подсистем. Результаты формализованного подхода представлены в виде таблиц для проведения расчетов индексов согласия (таблица 3) и индексов несогласия.

Таблица 3 – Таблица индексов согласия

		A_{11}	A_{12}	…	A_{1K}
Ф1	A_{11}	*	$c_{A_{11}A_{12}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$	…	$c_{A_{11}A_{1K}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$
	A_{12}	$c_{A_{12}A_{11}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$	*	…	$c_{A_{12}A_{1K}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$
	…	…	…	*	…
	A_{1K}	$c_{A_{1K}A_{11}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$	$c_{A_{1K}A_{12}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{10} w_i}$	…	*
		A_{21}	A_{22}	…	A_{2L}
Ф2	A_{21}	*	$c_{A_{21}A_{22}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$	…	$c_{A_{21}A_{2L}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$
	A_{22}	$c_{A_{22}A_{21}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$	*	…	$c_{A_{22}A_{2L}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$
	…	…	…	*	…
	A_{2L}	$c_{A_{2L}A_{21}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$	$c_{A_{2L}A_{22}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{13} w_i}$	…	*
		A_{31}	A_{32}	…	A_{3M}
Ф3	A_{31}	*	$c_{A_{31}A_{32}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$	…	$c_{A_{31}A_{3M}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$
	A_{32}	$c_{A_{32}A_{31}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$	*	…	$c_{A_{32}A_{3M}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$
	…	…	…	*	…
	A_{3M}	$c_{A_{3M}A_{31}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$	$c_{A_{3M}A_{32}} = \frac{\sum_{i \in I^+,\ I^=} w_i}{\sum_{i=I}^{31} w_i}$	…	*

Формализовано правило отбора лучшей альтернативы:

$$f = (c_{AB} \geq c_i)\ \&\ (d_{AB} \leq d_i),$$

где A и B – сравниваемые альтернативы, c_i и d_i – заданные уровни согласия и несогласия.

Если f = 1, то альтернатива A объявляется лучшей по сравнению с альтернативой B. Если f = 0, то при заданных уровнях согласия и несогласия сравнить альтернативы не удалось. Процесс выбора СрЗИ из произвольного количества альтернатив для заданных выше трех функциональных подсистем защиты информации ИС ЭТП может быть описан в виде программного кода, включающего в себя множество циклов логических операций.

Таким образом, описанные выше расчеты позволяют сделать рациональный выбор средств защиты из множества существующих на рынке систем распределенной фильтрации трафика, систем предотвращения вторжений и средств антивирусной защиты для рассматриваемого в диссертационной работе объекта защиты – ИС ЭТП. При этом расчеты являются очень трудоемкими и в свою очередь требуют автоматизации данного процесса.

Четвертая глава посвящена разработке архитектуры системы управления ИБ в ИС ЭТП и ПО для автоматизации процедур управления. Предлагаемая система управления ИБ состоит из двух функциональных подсистем: подсистемы поддержки принятия решений по выбору модульного состава СЗИ и подсистемы формирования политики разграничения доступа (рисунок 3).

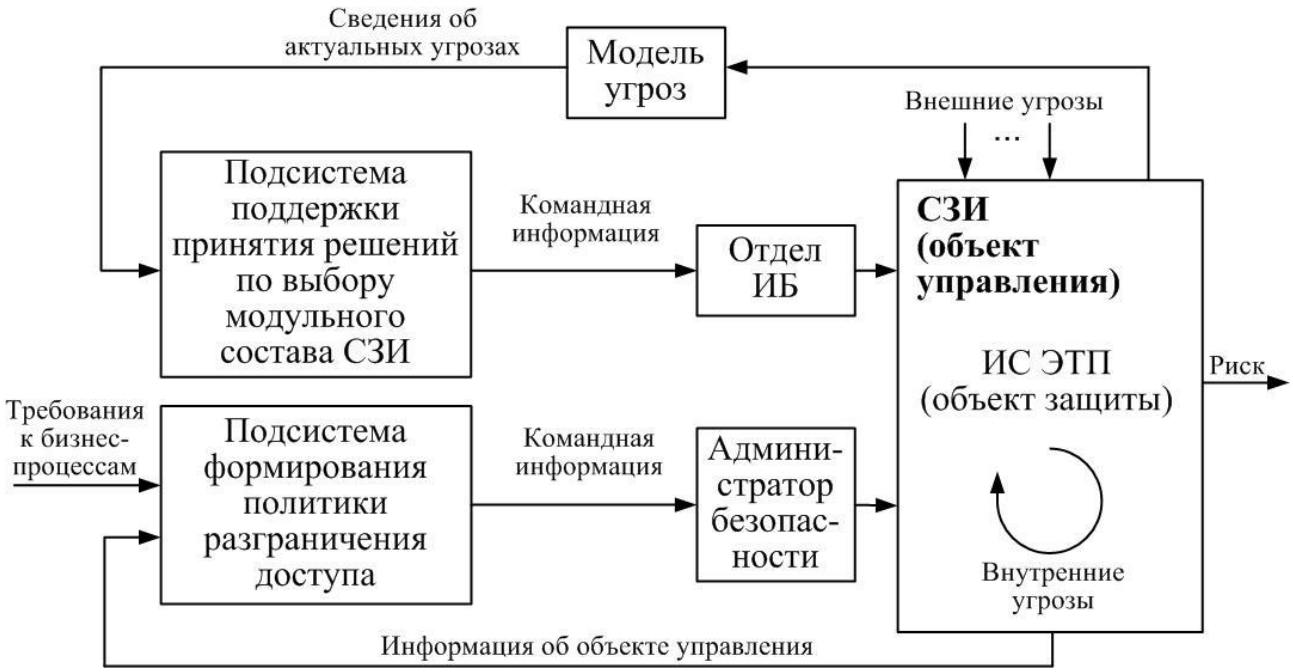

Рисунок 3 – Архитектура системы управления ИБ

В рамках подсистемы поддержки принятия решений по выбору модульного состава СЗИ разработано ПО для автоматизации процесса выбора набора СрЗИ, реализующее предложенный в диссертационной работе адаптированный метод выбора комплекса СрЗИ в ИС ЭТП. Для обеспечения работы второй из рассматриваемых подсистем управления ИБ разработано ПО, автоматизирующее процесс формирования политики разграничения доступа и основанное на предложенной в диссертационной работе методике формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП

Для понимания функций разрабатываемых программ произведено их функциональное моделирование с использованием графической нотации IDEF0, а также составлены алгоритмы работы ПО в виде функциональных схем согласно ГОСТ 19.701-90. На рисунке 4 представлена функциональная схема проекта ПО, автоматизирующего процесс формирования политики разграничения доступа. Также в диссертационной работе представлены экранные формы, демонстрирующие поэтапный процесс работы с разработанным ПО.

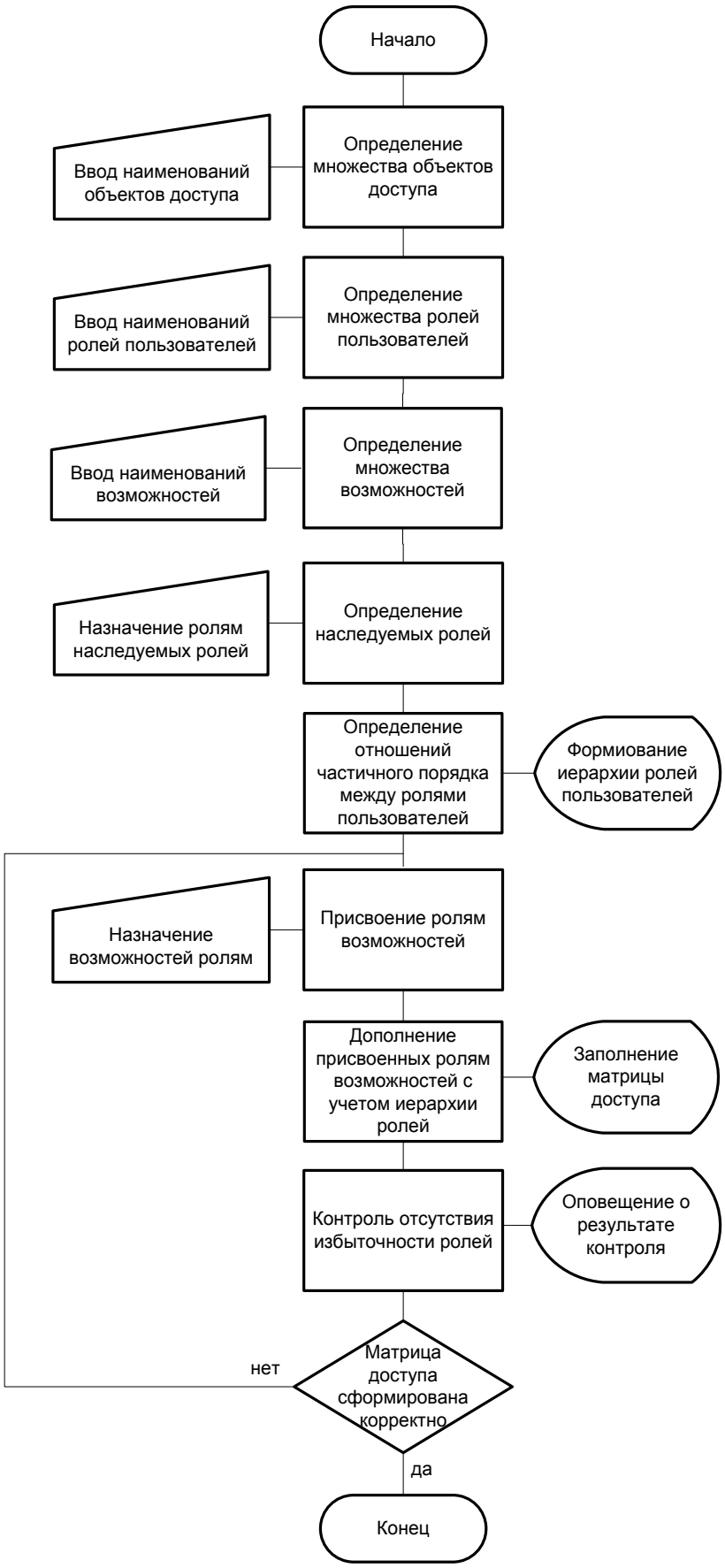

Рисунок 4 – Функциональная схема проекта ПО, автоматизирующего процесс формирования политики разграничения доступа

Произведена апробация предложенной системы управления ИБ. С помощью разработанных средств автоматизации подсистем управления ИБ произведен выбор рационального набора СрЗИ для нейтрализации актуальных угроз ИБ в ИС ЭТП и доказана корректность предложенной политики разграничения доступа в ИС ЭТП.

В заключении приведены основные результаты диссертационного исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Разработаны **графические функциональные модели преднамеренных угроз информационной безопасности в информационной системе электронной торговой площадки** *с использованием* EPC-нотации, *отличающиеся* выявлением источников угроз, наглядным и детальным отображением процесса реализации угроз, определением используемых для реализации угроз объектов и уязвимостей компьютерной инфраструктуры, *что позволяет* получить количественную оценку угроз на основании положений теории вероятностей, сравнить угрозы между собой, определить, успешная реализация какой из угроз наиболее вероятна относительно других угроз и, как следствие, выявить наиболее актуальные угрозы.

2. Предложен **адаптированный для выбора комплекса средств защиты информации в информационной системе электронной торговой площадки метод**, *основанный* на попарном сравнения альтернатив Б. Руа, *отличающийся* формализацией метода применительно к задаче выбора комплекса средств защиты информации, принадлежащих разным функциональным подсистемам, разработкой иерархических структур критериев выбора средств защиты и таблиц расчетов индексов согласия и несогласия для функциональных подсистем, *что позволяет* сделать рациональный выбор наборов средств защиты информации, а сам процесс выбора – автоматизировать.

3. Разработана **методика формализации правил взаимодействия информационных субъектов и объектов в системе электронной торговой площадки** *на основе* математической модели ролевого разграничения доступа, базирующегося на группировании прав доступа субъектов к объектам с учетом специфики их применения. Предложенная методика *отличается* выявлением множеств сущностей и возможностей в информационной системе электронной торговой площадки, формированием иерархических структур на указанных множествах, разработкой правил контроля доступа в информационной системе электронной торговой площадки на основе сведений об объектах доступа, ролях пользователей и возможностях, определением правил администрирования, предназначенных для административных ролей информационной системы электронной торговой площадки и позволяющих администрировать множество авторизованных ролей пользователей, множество прав доступа, которыми обладают роли, а также иерархию ролей, *что позволяет* автоматизировать разработку политики разграничения доступа в информационной системе электронной торговой площадки и повысить эффективность и

производительность работы сотрудников, отвечающих за обеспечение информационной безопасности в информационной системе электронной торговой площадки.

4. Разработана **архитектура и программное обеспечение системы управления информационной безопасностью в информационной системе электронной торговой площадки**, *базирующейся* на анализе основных аспектов управления информационной безопасностью и общих закономерностях построения систем управления, *новизна* которой заключается в реализации функций интеллектуальной поддержки принятия решений по выбору модульного состава системы защиты информации и формирования политики разграничения доступа в информационной системе электронной торговой площадки, *что позволяет,* с одной стороны, осуществлять управление модульным составом системы защиты информации на основе данных об объективных технических характеристиках средств защиты информации, декларируемых производителем, с другой стороны, оперативно и корректно вносить изменения в правила взаимодействия сущностей информационной системы электронной торговой площадки при изменении бизнес-процессов.

Перспективы дальнейшей разработки темы. Дальнейшим развитием диссертационной работы может быть исследование таких аспектов управления информационной безопасностью в системе электронной торговой площадки, как мониторинг и управление составом событий безопасности в реальном времени, а также получение и оценка объективных данных о состоянии защищенности информационной системы.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых журналах из списка ВАК

1. Яндыбаева, Э.Э. Политика безопасности использования электронной подписи на предприятии / Э.Э. Яндыбаева, И.В. Машкина // Безопасность информационных технологий. – 2013. – № 1. – С. 128–130.

2. Яндыбаева, Э.Э. Модель нарушителя информационной безопасности в информационной системе электронной торговой площадки / Э.Э. Яндыбаева, И.В. Машкина // Безопасность информационных технологий. – 2014. – № 1. – С. 80–81.

3. Яндыбаева, Э.Э. Оценка актуальности угроз информационной безопасности в информационной системе электронной торговой площадки / Э.Э. Яндыбаева, И.В. Машкина // Безопасность информационных технологий. – 2014. – № 1. – С. 41–44.

4. Яндыбаева, Э.Э. Разработка модели планирования используемых средств защиты информации для информационной системы электронной торговой площадки / Э.Э. Яндыбаева, И.В. Машкина // Вестник УГАТУ. – 2015. – Том 19, № 1 (67). – С. 264–269.

5. Яндыбаева, Э.Э. Методика формализации правил взаимодействия информационных субъектов и объектов в системе электронной торговой площадки / Э.Э. Яндыбаева, И.В. Машкина // Безопасность информационных технологий. – 2015. – № 1. – С. 119–121.

Объекты интеллектуальной собственности

6. Свидетельство о государственной регистрации программы для ЭВМ № 2016610163. Планирование модульного состава системы защиты информации / Э.Э. Яндыбаева. Зарег. 11.01.2016 г. – М.: Роспатент, 2016.

В других изданиях

7. Яндыбаева, Э.Э. Проблемы внедрения электронной подписи на предприятии / Э.Э. Яндыбаева // Труды V Всероссийской молодежной научной конференции «Мавлютовские чтения». Том 3. – Уфа: Изд-во УГАТУ, 2011. – С. 45–47.

8. Яндыбаева, Э.Э. Анализ угроз информационной безопасности при использовании электронной подписи / Э.Э. Яндыбаева // Материалы XII Международной научно-практической конференции «ИБ-2012» Ч. II. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 76–81.

9. Яндыбаева, Э.Э. Классификация угроз информационной безопасности при использовании электронной подписи / Э.Э. Яндыбаева, И.В. Машкина // Труды VI Всероссийской молодежной научной конференции «Мавлютовские чтения». Том 3. – Уфа: Изд-во УГАТУ, 2011. – С. 45–47.

10. Яндыбаева, Э.Э. Политика безопасности использования электронной подписи на предприятии. / Э.Э. Яндыбаева, И.В. Машкина // Современные тенденции в образовании и науке: Сборник научных трудов по материалам Международной научно-практической конференции. Часть 8. – Тамбов: Издательство ТРОО «Бизнес-Наука-Общество», 2013 – С. 161–162.

11. Яндыбаева, Э.Э. Модель угроз информационной безопасности электронной торговой площадки / Э.Э. Яндыбаева // Материалы XIII Международной научно-практической конференции «ИБ-2013» Ч. II. Материалы III Всероссийской молодежной конференции «Перспектива-2013». – Таганрог: Изд-во ЮФУ, 2013. – С. 215–219.

12. Яндыбаева, Э.Э. Политика контроля доступа в информационной системе электронной торговой площадки / Э.Э. Яндыбаева // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 181–185.

Диссертант  Э. Э. Яндыбаева

ЯНДЫБАЕВА Эмма Эмануиловна

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМЕ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ

Специальность
05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 16.02.2016. Формат 60×84 1/16
Бумага офсетная. Печать плоская. Гарнитура Times New Roman.
Усл. печ. л. 1,0. Уч.-изд. л. 0,9.
Тираж 100 экз. Заказ № 41.

ФГБОУ ВПО «Уфимский государственный авиационный
технический университет»
Центр оперативной полиграфии
450000, Уфа-центр, ул. К. Маркса, 12