На правах рукописи

ФАЗЛИАХМЕТОВ Тимур Ильгизович

АЛГОРИТМЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ РЕЗУЛЬТАТОВ ИЗМЕРЕНИЙ В БАЗАХ ДАННЫХ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

(НА ПРИМЕРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОНТРОЛЯ ТРАНСПОРТА НЕФТИ)

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
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, профессор **Фрид Аркадий Исаакович**

Официальные оппоненты: д-р техн. наук, профессор **Климов Игорь Зенонович** ФГБОУ ВПО «Ижевский государственный технический университет имени М.Т.Калашникова», профессор кафедры «Радиотехника»

канд. техн. наук, доцент **Антонов Вячеслав Викторович** МВД по РБ, начальник информационного центра

Ведущее предприятие: ФГБОУ ВПО «Башкирский государственный университет»

Защита диссертации состоится «28» июня 2013 г. в 10:00 часов на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете в актовом зале 1-го корпуса по адресу: 450000, г. Уфа, ул. К. Маркса, 12

С диссертацией можно ознакомиться в библиотеке Уфимского государственного авиационного технического университета.

Автореферат разослан «28» мая 2013 года

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. До недавнего времени основным интересом киберпреступности были финансовые информационные системы (ИС); ИС, автоматизирующие бизнес-процессы; ИС, содержащие частные данные клиентов организации или сведения, являющиеся государственной тайной. Однако сейчас, предметом киберпреступности становятся и промышленные ИС.

В вопросах информационной безопасности в промышленных ИС (ПИС) важной задачей является обеспечение целостности. Основной информацией, обрабатываемой в ПИС, являются результаты измерений (РИ) параметров промышленных объектов. Именно на их основе принимаются решения по управлению производственными процессами, а также формируется финансовая и налоговая отчетность. Поэтому РИ являются наиболее ценной информацией в ПИС, требующей обеспечения целостности.

Степень разработанности темы. Неотъемлемой частью современных ПИС являются базы данных (БД), в которых хранится информация, обрабатываемая в ИС. РИ параметров промышленных объектов также хранятся в БД. Именно БД являются наиболее привлекательным объектом для совершения несанкционированной модификации (НСМ) РИ. В современных системах управления БД, таких как Oracle, MS SQL и т.д., имеются свои средства обеспечения целостности. Однако они обладают рядом недостатков по отношению к информации, являющейся РИ параметров промышленных объектов. Средства обеспечения *целостности сущностей и ссылочной целостности* подразумевают целостность структур хранения данных, а не непосредственно самих данных. Средства *доменной целостности* хоть и позволяют наложить некоторые ограничения на значения РИ, хранящиеся в столбцах таблиц БД, однако эти ограничения являются либо слишком общими, либо обладают слишком большим диапазоном значений. Средства *пользовательской целостности*, также как и доменной, позволяют наложить некоторые ограничения на значения РИ и учесть их физический смысл. Однако СУБД предоставляют лишь инструменты для реализации обеспечения такой целостности, но не предоставляют методы или алгоритмы, по которым должны проверяться значения РИ.

Из недостатков средств обеспечения целостности, входящих в состав СУБД, следует, что они не могут в полной мере обеспечить целостность РИ. Поэтому необходимо решать эту задачу с помощью средств контроля целостности, реализованных в составе готовых средств защиты информации (СрЗ), например, таких как *«Dallas Lock»*, *«Secret Net»*, электронный замок *«Соболь»* и т.д. Данные СрЗ обладают высокими показателями защиты, обойти которые является трудновыполнимой задачей. Однако все эти СрЗ осуществляют контроль на уровне папок и файлов, в то время как рассматриваемые РИ являются частью файлов БД. В этом случае необходимо контролировать целостность файла БД целиком. Однако такое решение не

представляется целесообразным в силу того, что файлы БД являются непрерывно меняющимися, динамическими объектами. Это связано с малым периодом поступления данных РИ в БД. Следовательно, контрольная сумма, рассчитанная СрЗ для файла в некоторый момент времени, уже через небольшой промежуток времени не будет соответствовать текущему состоянию файла.

Таким образом, применение рассмотренных выше СрЗ для контроля целостности РИ в БД является нецелесообразным. Данную проблему можно решить на уровне прикладного программного обеспечения (ПО) с помощью общих методов контроля целостности, основным из которых является хеширование. Проблеме хеширования посвящены исследования *Р. Риверса*, *Ф. Окслина*, *Ван Сяоюнь*, *Юй Хунбо*, *В. Клима*, *Ф. Менделя* и др. В настоящее время существует ряд хеш-функций, обладающих высокой криптостойкостью, и которые считаются «невзламываемыми». При условии, что их реализация на уровне прикладного ПО будет выполнена качественно с точки зрения ИБ, средства контроля целостности, реализованные на уровне прикладного ПО, можно также считать «невзламываемыми». Однако важно отметить, что условия, в которых используются эти средства, могут оказаться неидеальными. В этом случае для совершения НСМ РИ в БД злоумышленник может воспользоваться не уязвимостями в алгоритмах хеширования и в средствах контроля целостности, а уязвимостями в других компонентах ИС. Кроме того, злоумышленник может воспользоваться уязвимостями не только технического, но и организационного характера. Например, злоумышленник может пересчитать хеш-суммы для модифицированных РИ и модифицировать и сами РИ, и их хеш-суммы. Для этого ему необходим лишь доступ с правами записи в БД РИ и к самим хеш-суммам. Задача совершения несанкционированного доступа (НСД) к БД может оказаться относительно несложной с силу того, что проектирование эффективной системы защиты информации в ИС представляет собой сложный процесс, и учесть все детали ИС на практике представляет собой трудновыполнимую задачу. Трудность выполнения такой задачи обусловлена тем, что ПИС представляют собой большой, сложный и непрерывно меняющийся, динамический объект. Следовательно, в них всегда будут уязвимости, которыми может воспользоваться злоумышленник для совершения НСД.

Таким образом, задача контроля целостности информации, являющейся РИ параметров промышленных объектов и хранящейся в БД ПИС, является актуальной.

Объект исследования – информационная безопасность данных, являющихся результатами измерений параметров промышленных объектов, от внутренней угрозы несанкционированной модификации информации.

Предмет исследования – методы и средства контроля целостности данных в базах данных информационных систем нефтедобывающего предприятия.

Целью работы является повышение уровня защищенности результатов

измерений от несанкционированной модификации в базах данных информационных систем нефтедобывающего предприятия.

Задачи исследования:

1. Разработка алгоритма контроля целостности результатов измерений параметров промышленных объектов в базах данных, основанного на их функциональной взаимосвязи.

2. Разработка нейросетевой модели оценки расхода жидкости в трубопроводе в процессе транспортировки нефти для ее использования в алгоритме контроля целостности.

3. Разработка алгоритма оценки эффективности контроля целостности результатов измерений параметров промышленных объектов в базах данных.

4. Оценка условий применимости разработанного алгоритма контроля целостности результатов измерений с помощью разработанного алгоритма оценки его эффективности.

5. Разработка программного компонента, реализующего разработанный алгоритм контроля целостности результатов измерений в базах данных.

Научная новизна работы заключается в следующем**:**

1. Разработан алгоритм контроля целостности результатов измерений параметров промышленных объектов, *основанный* на использовании метода *FDI* (*Fault Detection and Identification*) и концепции *DCS* (*Data Centric Security*), *отличающийся* тем, что решение о несанкционированной модификации принимается на основе сравнения фактических значений параметров промышленного объекта или процесса и значений, рассчитанных с помощью модели промышленного объекта или процесса, что *позволяет* повысить уровень защищенности результатов измерений и уменьшить потенциальный ущерб от их несанкционированной модификации.

2. Разработана модель для оценки расхода жидкости в трубопроводе, *основанная* на нейронной сети, *отличающаяся* тем, что структура и параметры нейронной сети выбираются из условия увеличения времени ее обучения, требуемого на выполнение действий для скрытия факта несанкционированной модификации, что *позволяет* уменьшить потенциальный ущерб от несанкционированной модификации результатов измерений.

3. Разработан алгоритм оценки эффективности контроля целостности, *основанный* на методе оценки ущерба с использованием модели «осведомленность – эффективность», *отличающийся* тем, что в нем учитывается вероятность скрытия факта несанкционированной модификации результатов измерений злоумышленником, которая вычисляется как функция времени, требуемого на выполнение действий для скрытия факта несанкционированной модификации, а расчет ущерба осуществляется с учетом величины погрешности нейросетевой модели расхода жидкости в трубопроводе, что *позволяет* оценить условия применимости разработанного алгоритма контроля целостности.

Теоретическая и практическая ценность полученных результатов состоит в том, что решение о несанкционированной модификации принимается

на основе сравнения фактических значений параметров промышленного объекта или процесса, хранящихся в базе данных, и значений, рассчитанных с помощью модели промышленного объекта или процесса, что позволяет повысить уровень защищенности результатов измерений и уменьшить потенциальный ущерб от их несанкционированной модификации.

Применительно к процессу транспортировки нефти разработанный алгоритм контроля целостности позволяет снизить потенциальный ущерб от несанкционированной модификации результатов измерений расхода жидкости в трубопроводе на 11-43% в зависимости от квалификации злоумышленника.

Разработанный алгоритм оценки эффективности контроля целостности позволяет использовать его как один из компонентов методики оценки экономической эффективности комплексных систем защиты информации.

Программный компонент, реализующий разработанный алгоритм контроля целостности, разработан в виде набора классов и интерфейсов, что позволяет адаптировать его для любых данных, обладающих функциональной взаимосвязью.

Методология и методы исследования. В работе использовались методы оценки эффективности систем защиты информации, методы контроля целостности информации, технологии искусственных нейронных сетей, численные методы, а также методы теории вероятности. Широко использовалось моделирование, в том числе с использованием разработанного автором программного обеспечения. Для разработки программного обеспечения использовались методы объектно-ориентированного программирования.

Положения, выносимые на защиту:

1. Алгоритм контроля целостности результатов измерений параметров промышленных объектов в базах данных, основанный на их функциональной взаимосвязи.
2. Модель для оценки расхода жидкости в трубопроводе в процессе транспортировки нефти, основанная на нейронной сети.
3. Алгоритм оценки эффективности контроля целостности результатов измерений параметров промышленных объектов в базах данных, основанный на методе оценки ущерба с использованием модели «осведомленность – эффективность».
4. Условия применимости разработанного алгоритма контроля целостности результатов измерений, полученные с помощью разработанного алгоритма оценки его эффективности.
5. Программный компонент, реализующий разработанный алгоритм контроля целостности результатов измерений в базах данных.

Достоверность полученных результатов основана на использовании известных теоретических подходов, математических методов и моделей. Достоверность и обоснованность выводов и результатов, полученных в работе, подтверждена результатами моделирования на реальных данных, а также соответствием результатов теоретических и экспериментальных исследований.

Апробация результатов. Основные результаты работы обсуждались на: Научно-теоретических конференциях УГАТУ «Неделя науки», Уфа, 2010, 2011 и 2012; Всероссийских молодежных научных конференциях «Мавлютовские чтения» Уфа, 2010, 2011; VI и VII Всероссийских зимних школах-семинарах аспирантов и молодых ученых, Уфа, 2011, 2012; XIII Международной конференции по компьютерным наукам и информационным технологиям *CSIT* 2011, Гармиш-Партенкирхен, Германия, 2011; Международной конференции «Информационные технологии и системы», санаторий «Юбилейный», Республика Башкортостан, 2012; XIV Международной конференции по компьютерным наукам и информационным технологиям *CSIT* 2012, Уфа-Гамбург-Норвежские фьорды, 2012.

Основные результаты диссертационной работы внедрены в качестве методического и математического обеспечения при проектировании автоматизированных систем учета нефти в ООО «Уфанефтемаш».

Также полученные в диссертационной работе результаты внедрены в учебный процесс Уфимского государственного авиационного технического университета в качестве лекционных курсов «Комплексные системы защиты информации на предприятии» и при проведении курсового и дипломного проектирования по специальности 090104 «Комплексная защита объектов информатизации» и бакалаврскому направлению 090900 «Информационная безопасность».

Публикации. Результаты работы опубликованы в 13 печатных трудах, в том числе в 5 статьях в рецензируемых журналах, рекомендованных ВАК, и в 8 трудах конференций. Получены 2 свидетельства об официальной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертационная работа состоит из списка сокращений, введения, четырех глав, заключения, библиографического списка и приложений. Содержит 172 страницы машинописного текста, из которых основной текст составляет 163 страницы, включая 47 рисунка и 14 таблиц, приложения составляют 9 страниц. Библиографический список содержит 131 наименования.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обсуждается актуальность решаемой научной задачи, сформулированы цель и задачи работы, изложены основные положения, выносимые на защиту, научная новизна и практическая ценность полученных результатов.

В первой главе проведен анализ методов и средств обеспечения целостности данных в ПИС. Рассмотрена проблема обеспечения целостности информации, являющейся РИ параметров промышленных объектов, в БД ПИС. Приводятся типы БД, используемых в ПИС. Указывается, что в работе рассматриваются реляционные БД, как наиболее популярные при реализации ПИС. Описывается общая модель нарушителя целостности результатов измерений. В работе рассматривается только преднамеренное нарушение

целостности, поэтому вместо нарушителя используется понятие «злоумышленник». В качестве злоумышленника рассматривается инсайдер, цель которого – НСМ РИ в БД. Показаны варианты реализации контроля целостности (КЦ): средствами СУБД, средствами контроля целостности (СКЦ), реализованными в составе готовых СрЗ, или с помощью общих методов КЦ, реализованных в прикладном ПО.

Проводится анализ СКЦ на уровне СУБД (Oracle, MSSQL) и анализ СКЦ, входящих в состав готовых СрЗ таких как «Dallas Lock», «Secret Net», электронный замок «Соболь» и т.д. Дается анализ методов КЦ, основным из которых является хеширование, приводятся различные алгоритмы хеширования. Анализируется опыт использования нейронных сетей (НС) в задачах защиты информации. Приводится анализ подходов к оценке эффективности средств и методов КЦ.

Вторая глава посвящена и разработке алгоритма КЦ РИ на основе НС.

Общая схема потока данных, являющихся РИ параметров промышленных объектов, и применение СКЦ, реализованного на уровне прикладного ПО и основанного на хешировании, показана на рисунке 1.

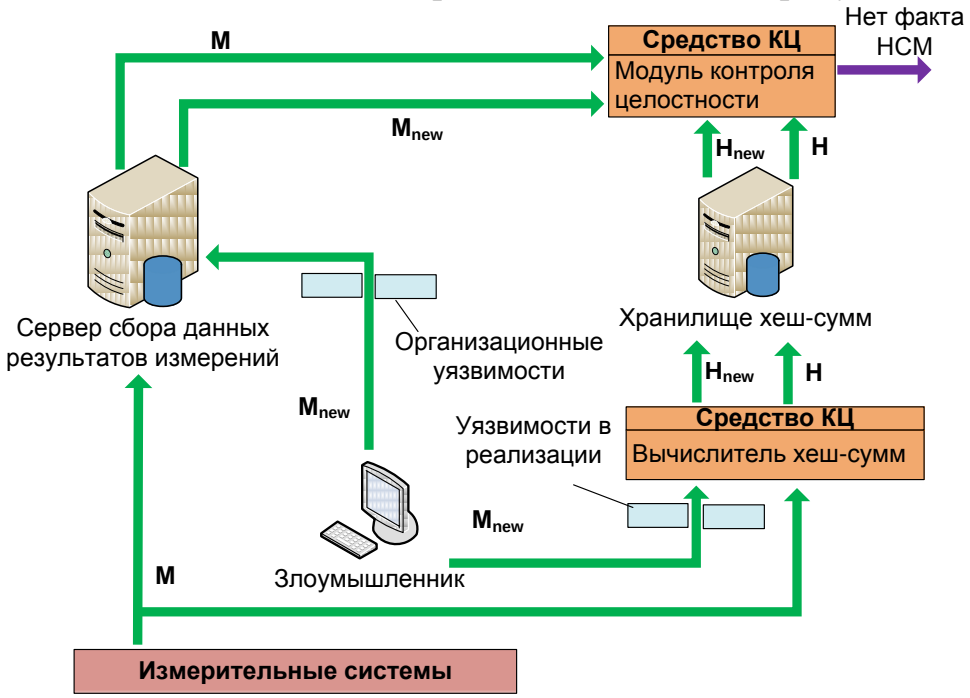

Рисунок 1 – Схема потока РИ и применение средства контроля целостности

Массив данных РИ *M*, из измерительных систем поступает на сервер сбора данных РИ, который представляет собой БД РИ. Кроме того, массив *M* поступает на вход вычислителя хеш-сумм, который является компонентом СКЦ. Вычислитель рассчитывает хеш-сумму *H* для *M* по какому-либо известному алгоритму хеширования. Хеш-сумма поступает и хранится в хранилище хеш-сумм. Это может быть та же БД, в которой хранятся РИ, либо любое другое хранилище.

Вычислитель хеш-сумм представляет собой программу, которая

выполняется не изолированно от других компонентов ИС, а взаимодействует с ними. Следовательно, для данной программы появляется следующая уязвимость: к ней можно обратиться (локально или удаленно) и использовать ее для расчета хеш-суммы для любых данных заданного формата. Назовем это уязвимостью в реализации вычислителя хеш-сумм.

При проверке на целостность модуль КЦ получает массив данных РИ M из БД РИ и соответствующую ему хеш-сумму H из хранилища хеш-сумм. По M рассчитывается хеш-сумма, и если она не совпадает с H, принимается решение о НСМ РИ.

При выполнении НСМ РИ злоумышленник должен скрыть факт НСМ. В противном случае НСМ РИ будет обнаружена с помощью приведенного выше средства КЦ. Для скрытия факта НСМ злоумышленник должен:

1. Выполнить расчет хеш-суммы H_{new} для новых модифицированных данных M_{new}, то есть выполнить пересчет хеш-суммы.

2. Изменить значение H на H_{new} в хранилище хеш-сумм.

Так как вычислитель хеш-суммы представляет собой программу, то злоумышленник может выполнить пересчет хэш-суммы с помощью этой программы.

Сценарий действий злоумышленника показан на рисунке 1. Злоумышленник, используя уязвимости организационного характера, модифицирует текущие значения M в массиве данных РИ на новые значения M_{new}. Примером организационной уязвимости может быть наличие личных взаимосвязей между администратором БД и злоумышленником, воспользовавшись которыми злоумышленник может узнать идентификационную информацию для доступа к БД РИ. С помощью вычислителя хеш-сумм по M_{new} он рассчитывает значение H_{new}, которое записывает в хранилище вместо H. При проверке на целостность модуль контроля целостности получает массив данных РИ M_{new} из БД РИ и соответствующую ему хеш-сумму H_{new} из хранилища. По M_{new} рассчитывает хеш-сумму. В этом случае она будет совпадать с H_{new} и будет принято неправильное решение, что факта НСМ не было. Таким образом, будет выполнена НСМ РИ, и она не будет обнаружена.

В работе показано, что для совершения НСМ РИ в БД и скрытия этого факта при наличии средств КЦ данных, злоумышленнику требуется лишь доступ с правами записи к тем или иным программно-аппаратным ресурсам ИС. Поэтому задача КЦ РИ параметров промышленных объектов в БД ПИС, является актуальной.

Для решения этой задачи можно использовать особенность РИ, которая заключается в том, что некоторые из них обладают функциональной взаимосвязью. Так, по параметрам потока жидкости в трубопроводе, таким как, давление на концах трубы, вязкости жидкости, температуры и т.д., можно рассчитать значение расхода и сравнить его с реальным значением, хранимым в БД. Если рассчитанное и реальное значения расходов равны, то принимается решение, что НСМ РИ не было. Если эти расходы не равны, то принимается

решение, что имел место факт НСМ РИ.

Для решения задачи вычисления одних параметров по другим в разработанном алгоритме КЦ предлагается использовать НС. Структурная схема предлагаемого решения для КЦ РИ расхода жидкости в трубопроводе показана на рисунке 2.

Первичный источник представляет собой источник поступления РИ в БД ИС. Это могут быть непосредственно датчики, системы телемеханики или другие ИС. НС представляет собой модель потока жидкости в трубопроводе, позволяющая рассчитать значение расхода жидкости по другим параметрам потока. Однако использование только параметров потока для вычисления расхода имеет следующий недостаток: злоумышленник может изменить не только значение расхода, но и значения других параметров, так что модифицированное значение расхода совпадет с вычисленным, и факт НСМ обнаружен не будет.

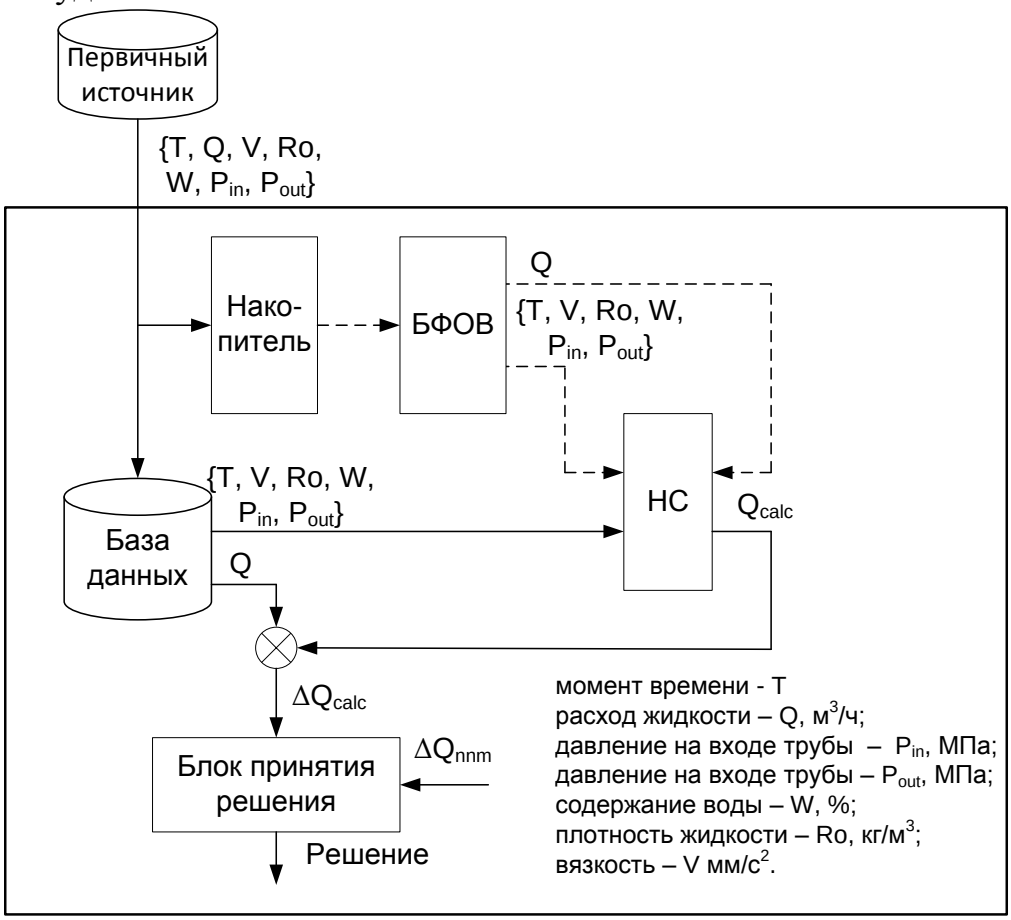

Рисунок 2 – Структурная схема предлагаемого решения для КЦ РИ расхода жидкости в трубопроводе (БФОВ – блок формирования обучающей выборки)

Для решения этой проблемы в модели также используется значение момента времени *T*, которому соответствуют значения других параметров. Параметр момента времени *T*, в отличие от других параметров, нельзя изменять произвольно, так как он является уникальным для каждого измерения.

Перед обучением НС РИ из первичных источников поступают в накопитель, где они накапливаются в течение суток. Далее РИ поступают на БФОВ, в котором происходит подготовка исходных РИ для обучения. После этого происходит обучение НС по подготовленным РИ.

Во время проверки РИ, хранящихся в БД, на целостность, на вход нейросетевой модели подаются значения параметров $\{T, V, Ro, W, P_{in}, P_{out}\}$. На выходе модели рассчитывается значение Q_{calc}. Между значениями Q и Q_{calc} по модулю вычисляется разница ΔQ_{calc}. Если ΔQ_{calc} больше вычислительной погрешности модели ΔQ_{model}, это означает, что значение Q не соответствует значениям $\{T, V, Ro, W, P_{in}, P_{out}\}$, поэтому блок принятия решения констатирует факт НСМ значения Q.

Накопитель и БФОВ необходимы потому, что, как показали эксперименты, НС не обучается на исходном количестве наборов $\{T, V, Ro, W, P_{in}, P_{out}\}$. В исходной таблице для конкретного производства было 1440 наборов. Прежде, чем данные поступят на обучение, необходимо уменьшить их количество. Эта задача решена путем их прореживания, реализованного в БФОВ.

Для КЦ РИ по Q алгоритм должен проверить значения Q во все моменты времени T_i. Следовательно, для вычисления $Q_{cacl(i)}$ в момент времени T_i в модель должен подаваться соответствующий набор значений $\{ T_i, V_i, Ro_i, W_i, P_{in(i)}, P_{out(i)}\}$. Блок-схема алгоритма проверки данных по расходу за определенный период времени в этом случае представлена на рисунке 3.

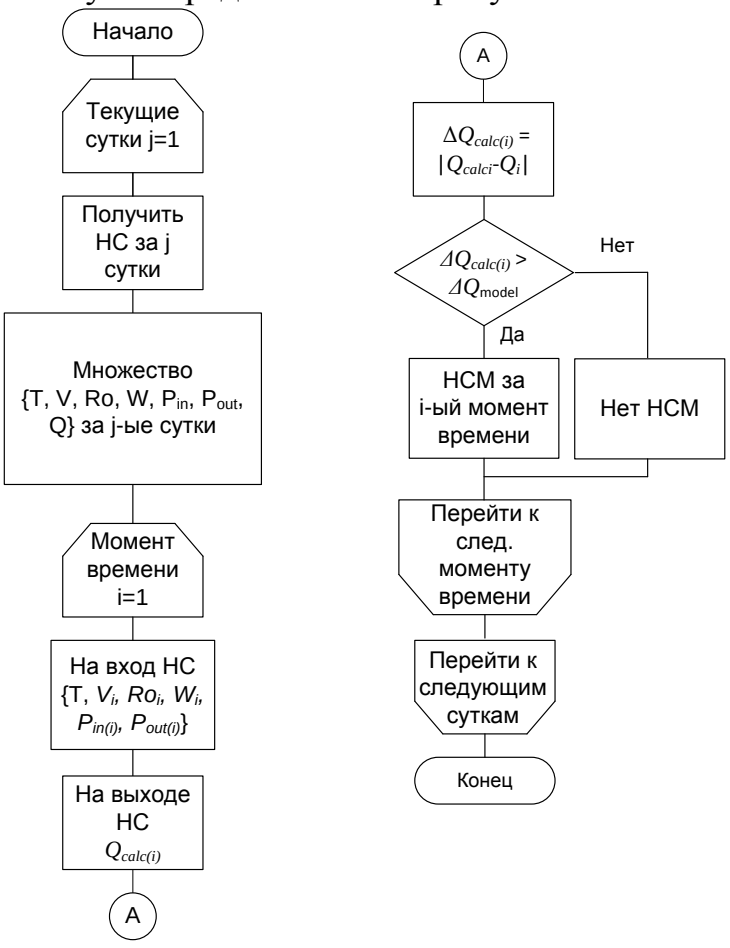

Рисунок 3 – Блок-схема алгоритма КЦ РИ за определенный период

В качестве архитектуры НС была выбрана сеть прямого распространения. В качестве алгоритма обучения был принят алгоритм с обратной ошибкой распространения. Задача выбора структуры НС, параметров ее обучения была поставлена следующим образом:

$$\begin{aligned} &\Delta Q_{nnm} = f(k_2, \Delta E_{nn}, \Delta Dist) \to min, \text{при} \\ &k_2 = [1; +\infty] \\ &\Delta E_{nn} = [1; 0] \\ &\Delta Dist = [0{,}1; +\infty] \end{aligned} \quad , \qquad (1)$$

где ΔQ_{nnm} – погрешности нейросетевой модели;

k_2 – количество нейронов во скрытом слое НС;

ΔE_{nn} – ошибка обучения НС.

$\Delta Dist$ – разница между образами {*T, V, Ro, W,* P_{in}, P_{out}} при формировании обучающей выборки.

В качестве НС выбран многослойный персептрон со структурой {[6], [6], [1]}, выбран алгоритм обучения с обратным распространением ошибки со следующими характеристиками:

1) скорость обучения = 0,9;

2) момент обучения = 0,4;

3) ошибка обучения = 10E-6.

Это позволило получить погрешность вычисления расхода жидкости не превосходящую 2%, при разнице между образами от 2 до 10%.

В третье главе проведено исследование эффективности разработанного алгоритма контроля целостности результатов измерений. Эффективность определяется через ущерб, который может быть нанесен компании вследствие НСМ РИ. Для оценки ущерба применительно к расходу жидкости в трубопроводе предложено использовать следующие формулы:

$$U_1 = 0{,}443 \cdot \frac{M}{m} \cdot \left(\sum_{g=1}^{m} \sum_{j=1}^{k} \sum_{i=1}^{n} (Q_{i,j,g}) - n \cdot k \cdot m \cdot Q_{min} \right) \cdot S \qquad (2)$$

$$U_2 = 0.443 \cdot \frac{M}{m} \cdot \left(n \cdot k \cdot m \cdot Q_{max} - \sum_{g=1}^{m} \sum_{j=1}^{k} \sum_{i=1}^{n} (Q_{i,j,g}) \right) \cdot S, \qquad (3)$$

где U_1 – ущерб при расчете через Q_{min};

U_2 – ущерб при расчете через Q_{max};

Q_{min} , Q_{max} – минимальное и максимальное значения, который может принимать Q. Данное значение может определяться, например, технологическими режимами протекания жидкости в трубопроводе, и задаваться с помощью ограничений в таблице БД;

i – порядковый номер момента времени;

n – общее количество моментов времени за определенный период;

j – порядковый номер промышленного объекта;

k – общее количество промышленных объектов;

g – порядковый номер периода времени;

m – количество периодов, за которые имеется информация;

M – общее количество периодов времени в году;

$Q_{i,j,g}$ – текущее значение расхода жидкости;

S - стоимость единицы измерения расхода жидкости (в данном случае используется стоимость одной тонны нефти).

Приведенные формулы используются для расчета ущерба по минимальному и максимальному возможным значениям РИ расхода жидкости. В качестве окончательного ущерба следует выбрать большее значение.

В качестве показателя, влияющего на ущерб, предлагается использовать показатель вероятности выполнения действий для скрытия факта НСМ. Данный показатель говорит о том, какова вероятность P_{ist} скрытия факта НСМ РИ при наличии тех или иных алгоритмов КЦ. При учете вероятности P_{ist} под ущербом будем понимать потенциальный ущерб, который может понести компания вследствие НСМ РИ. Для вычисления P_{ist} предлагается использовать следующую формулу:

$$P_{ist} = e^{-\lambda t_{ist}}, \tag{4}$$

где t_{ist} – время, которое требуется для скрытия факта НСМ;

λ – коэффициент, характеризующий квалификацию злоумышленника.

Описаны сценарии действий злоумышленника, выполняемые для скрытия факта НСМ в случаях, когда КЦ реализован с помощью хеш-функции, резервного хранения данных или использования нейросетевой модели промышленного объекта.

При учете вероятности скрытия факта НСМ потенциальный ущерб L в общем случае будет рассчитываться как:

$$L = U \cdot P_{ist} \cdot F, \tag{5}$$

где U – ущерб, рассчитанный по формулам (2) и (3);

P_{ist} – вероятность скрытия факта НСМ РИ;

F – частота реализации угрозы НСМ РИ.

При сравнительной оценке ущерба от НСМ РИ до и после введения разработанного алгоритма КЦ была получена следующая формула для определения эффективности E_f алгоритма КЦ:

$$E_f = 1 - e^{-\lambda t_{nn}}, \tag{6}$$

где t_{nn} – время, требуемое на переобучение нейронной сети.

Из формулы (6) следует, что для увеличения эффективности разработанного алгоритма КЦ, необходимо увеличить время обучения НС. Задача увеличения времени обучения НС была поставлена следующим образом:

$$\begin{aligned} & t_{nn} = f(k_2, \Delta E_{nn}) \to max, при \\ & k_2 = [6; +\infty] \\ & \Delta E_{nn} = [1; 0] \end{aligned}, \tag{7}$$

При решении задачи (8) было учтено, чтобы ее решение не противоречило решению задачи (1). В результате экспериментов получена НС со структурой {[6], [40], [1]}, ошибка обучения была принята равной 10E-6. Время переобучения НС при этом составило 1,12 часа, эффективность составила 21%.

Показано, что при введении разработанного алгоритма КЦ ущерб следует рассчитывать, учитывая погрешность нейросетевой модели. В этом случае ущерб рассчитывается как:

$$U_{\Delta} = 2 \cdot \frac{M}{m} \cdot \frac{(1 - ln2)\Delta Q_{nnm}}{ln2 - ln2\Delta Q_{nnm}} \cdot \sum_{g=1}^{m} \sum_{j=1}^{k} \sum_{i=1}^{n} (Q_{i,j,g}) \cdot S, \quad (8)$$

где ΔQ_{nnm} – погрешность нейросетевой модели.

Алгоритм оценки ущерба от НСМ РИ показан на рисунке 4. Сначала выполняется расчет ущербов U_1 и U_2, из которых в качестве окончательного значения U выбирается максимальное значение. Далее выполняется расчет двух значений потенциального ущерба: $L(t)$ – в зависимости от времени, требуемого на переобучение НС, и $L(\Delta)$ – в зависимости от погрешности НС:

$$\begin{aligned} L(t) &= U \cdot P_a \cdot F \\ L(\Delta) &= U_{\Delta} \cdot P_b \cdot F \end{aligned}, \quad (9)$$

где P_a – вероятность скрытия НСМ РИ после введения разработанного алгоритма контроля целостности;

P_b – вероятность скрытия НСМ РИ до введения разработанного алгоритма контроля целостности.

В качестве окончательного значения L выбирается максимальное.

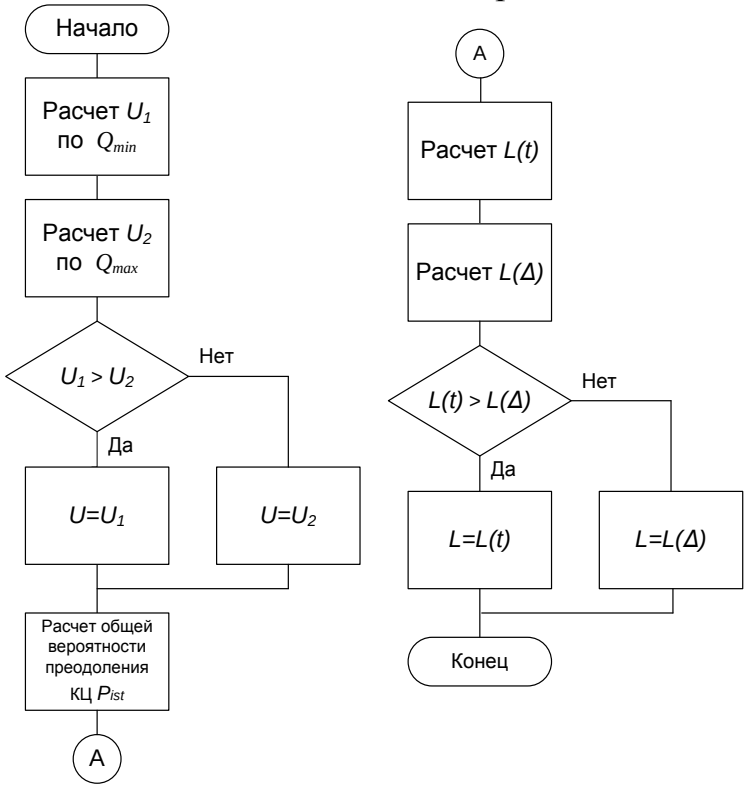

Рисунок 4 – Блок-схема алгоритма оценки ущерба от НСМ РИ

Оценено максимальное значение погрешности НС, при котором применение разработанного алгоритма КЦ уже окажется нецелесообразным. Оно составило 14,7%. Также было исследовано влияние шума в данных на эффективность разработанного алгоритма КЦ. Было выявлено, что его применение является целесообразным при наличии в данных белого шума, мощностью до 10%.

Четвертая глава посвящена разработке программного компонента, реализующего разработанный алгоритм КЦ РИ, оценке ущерба от НСМ с помощью этого компонента, а также демонстрации работы компонента.

Программный компонент имеет три модуля: модуль обучения НС, модуль проверки целостности РИ и модуль расчета ущерба.

Структурная схема модуля проверки целостности показана на рисунке 5, где сплошные стрелки показывают информационные потоки, пунктирные – управляющие потоки.

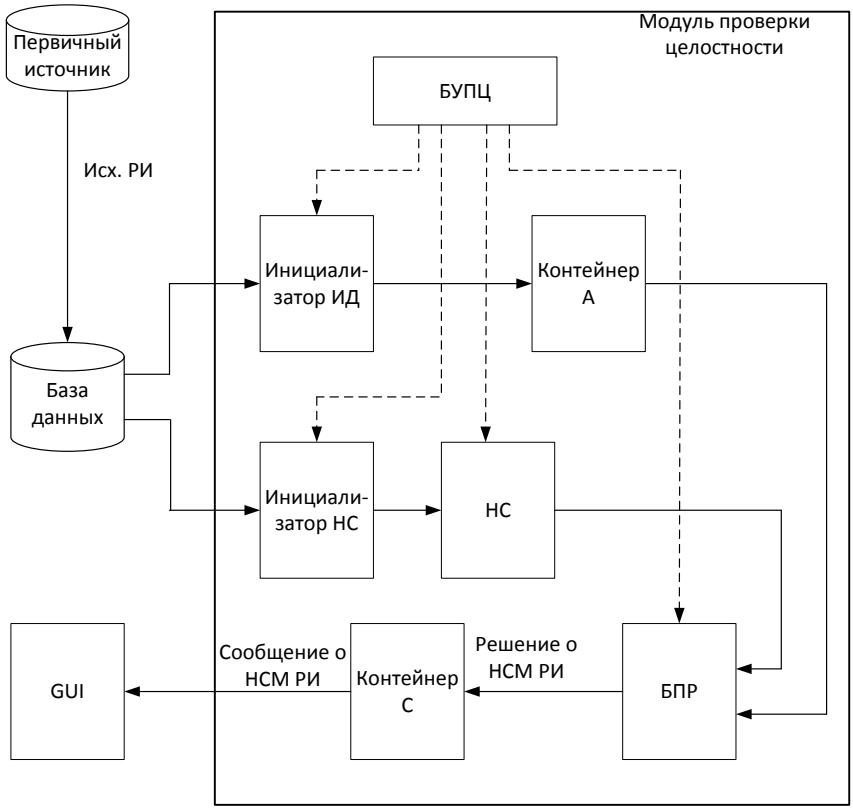

Рисунок 5– Структурная схема модуля проверки целостности

Модуль проверки целостности состоит из следующих компонентов:

1. *Инициализатор ИД*. Получает исходные РИ из накопителя и приводит их к единому формату. На выходе инициализатора получается компонент типа «контейнер А».

2. *Контейнер А*. Хранит исходные РИ в формате, удобном для использования внутри программы.

3. *Инициализатор НС*. Получает описание НС, хранящейся в БД в определенном формате.

4. *НС* – нейросетевая модель потока жидкости в трубопроводе для расчета расход жидкости. Представляет собой программную реализацию НС.

5. *БПР* – блок принятия решения. Выполняет алгоритм проверки целостности РИ, и в случае обнаружения НСМ РИ формирует и выдает об этом сообщение в виде компонента «контейнер С».

6. *Контейнер С*. Хранит сообщение и информацию о НСМ РИ.

7. *БУПЦ* – блок управления проверкой целостности. Управляет взаимодействием программных компонентов модуля.

Программный компонент, реализующий разработанный алгоритм КЦ РИ, разработан в виде набора интерфейсов и классов. Это позволяет относительно легко адаптировать его для любых аналогичных РИ, обладающих функциональной взаимосвязью.

С помощью разработанного компонента была выполнена сравнительная оценка ущерба от НСМ РИ до и после введения разработанного алгоритма КЦ РИ. Расчет показал, что его введение позволило снизить потенциальный ущерб от 11% до 43% в зависимости от квалификации злоумышленника, что в денежном эквиваленте составило от 130 тыс. у.е. до 530 тыс. у.е.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработан алгоритм контроля целостности РИ параметров промышленных объектов, *основанный* на использовании метода *FDI* (*Fault Detection and Identification*) и концепции *DCS* (*Data Centric Security*). Алгоритм *отличается* тем, что в нем дополнительно используется функциональная взаимосвязь РИ, *позволяющая* рассчитать одни значения РИ по другим, вычислить разницу между рассчитанными и реальными значениями, и если она превышает погрешность вычислений, принять решение о НСМ. Введение разработанного алгоритма *позволяет* повысить эффективность защиты РИ за счет уменьшения ущерба от их НСМ.

2. Для оценки расхода жидкости в трубопроводе разработана модель, *основанная* на НС. Данная модель *отличается* тем, что структура НС и параметры алгоритма ее обучения *позволяют* уменьшить ущерб от НСМ РИ за счет увеличения времени ее обучения, требуемого на выполнение действий для скрытия факта НСМ.

3. Для оценки эффективности контроля целостности разработан алгоритм оценки, *основанный* на существующих подходах к оценке экономической эффективности комплексных систем защиты информации. Предложенный алгоритм оценки ущерба *отличается* тем, что в нем учитывается вероятность скрытия факта НСМ РИ злоумышленником, которая вычисляется как функция времени, требуемого на выполнение действий для скрытия факта НСМ, а расчет ущерба осуществляется с учетом величины погрешности нейросетевой модели расхода жидкости в трубопроводе, что *позволяет* оценить условия применимости разработанного алгоритма контроля целостности.

4. Разработанный алгоритм оценки ущерба НСМ РИ *позволяет* использовать его как один из компонентов методики оценки экономической эффективности комплексных систем защиты информации.

5. Программный компонент, реализующий разработанный алгоритм

контроля целостности, спроектирован и реализован в виде набора классов и интерфейсов, что *позволяет* легко адаптировать их для любых аналогичных задач контроля целостности, РИ, обладающих функциональной взаимосвязью.

6. Результаты оценки ущерба от НСМ РИ свидетельствуют о том, что внедрение разработанного алгоритма контроля целостности РИ расхода жидкости в трубопроводе позволяет снизить потенциальный ущерб от их НСМ на 11-43% в зависимости от квалификации злоумышленника.

Перспективы дальнейшей разработки темы. Перспективными направлениями для дальнейших исследований являются разработка методов и алгоритмов обнаружения и предотвращения попыток НСМ РИ с помощью моделей промышленных объектов или процессов, а также разработка методов и алгоритмов обеспечения целостности данных, не являющихся РИ, но обладающих функциональной взаимосвязью.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Алгоритм обеспечения целостности метрологических данных в оперативных информационных системах нефтегазового комплекса / Т.И. Фазлиахметов // Автоматизация, телемеханизация и связь в нефтяной промышленности: науч. – техн. журн. М.: ОАО «ВНИИОЭНГ». 2011. № 4. С. 21-23.

2. Модель для оценки эффективности обеспечения целостности метрологических данных в производственных системах нефтегазового комплекса / Т.И. Фазлиахметов, А.И. Фрид // Вопросы защиты информации: науч. – практ. журн. М: ФГУП «ВИМИ». 2011. №2. С. 31-36.

3. Влияние погрешности одного метода обеспечения целостности метрологических данных на риск их несанкционированной модификации / Т.И. Фазлиахметов, А.И. Фрид // Вопросы защиты информации: науч. – практ. журн. М: ФГУП «ВИМИ». 2012. №1. С. 24-30.

4. Модель анализа рисков несанкционированной модификации метрологических данных в производственных системах / Т.И. Фазлиахметов, А.И. Фрид // Вестник УГАТУ: науч. журн. Уфимск. гос. авиац. техн. ун-та. УГАТУ. 2012. Т. 16. №3 (48). С. 187-193.

5. Нейросетевой метод обеспечения целостности метрологических данных в АСУП нефтегазового комплекса / Т.И. Фазлиахметов // Автоматизация, телемеханизация и связь в нефтяной промышленности: науч. – техн. журн. М.: ОАО «ВНИИОЭНГ». 2012. № 4. С.25-27.

В других изданиях

6. Проблема защиты метрологических данных в информационных системах нефтегазового комплекса / Т.И. Фазлиахметов // Мавлютовские чтения: материалы Всероссийской молодежной научной конференции. Уфа: УГАТУ, 2010. Т. 3. С. 48-50.

7. Анализ эффективности алгоритма обеспечения целостности

метрологических данных в производственных системах нефтегазового комплекса / Т.И. Фазлиахметов // Актуальные проблемы науки и техники: материалы VI Всероссийской зимней школы-семинара аспирантов и молодых ученых. Уфа: УГАТУ, 2011. Т. 1, С. 131-136.

8. Алгоритм обеспечения целостности метрологической информации в промышленных автоматизированных системах / Т.И. Фазлиахметов, А.И. Фрид // CSIT 2011: материалы XIII Международной конференции по компьютерным наукам и информационным технологиям. Гармиш-Партенкирхен, 2011. Т.1. С.91-94. (статья на англ. яз).

9. Оценка эффективности метода защиты метрологической информации от НСМ, основанного на математической взаимосвязи данных / Т.И. Фазлиахметов // Мавлютовские чтения: материалы Всероссийской молодежной научной конференции. Уфа: УГАТУ, 2011. Т. 3. С. 56-58.

10. Модель анализа рисков несанкционированной модификации метрологических данных в производственных системах / Т.И. Фазлиахметов // Всероссийский конкурс научно-исследовательских работ студентов и аспирантов в области информатики и информационных технологий в рамках всероссийского фестиваля науки: Сб. науч. работ. Белгород: НИУ БелГУ. 2011. Т.1. С. 380-388.

11. Свидетельство о государственной регистрации программы для ЭВМ №2011616347. Моделирование многофазных жидкостных потоков / Т. И. Фазлиамхетов. Роспатент. М.: Зарег. в Реестре программ для ЭВМ 12.08.2011.

12. Уязвимость одного метода защиты метрологических данных от несанкционированной модификации, основанного на математической взаимосвязи данных / Т.И. Фазлиахметов // Актуальные проблемы науки и техники: материалы VII Всероссийской зимней школы-семинара аспирантов и молодых ученых. Уфа: УГАТУ, 2012. Т. 1. С. 257-260.

13. Зависимость эффективности одного метода обеспечения целостности метрологических данных от погрешности вычислений / Т.И. Фазлиахметов // Информационные технологии и системы: материалы Первой Междунар. конф., оз. Банное, сан. Юбилейный, Россия. Челябинск: Изд-во Челяб. гос. ун-та, 2012. С. 60-62.

14. Влияние средств обеспечения целостности на вероятность несанкционированной модификации метрологической информации / Т.И. Фазлиахметов, А.И. Фрид // CSIT 2012: материалы XIV Международной конференции по компьютерным наукам и информационным технологиям. Уфа-Гамбург-Норвежские фьорды, 2012. Т.1. С.189-194. (статья на англ. яз).

15. Свидетельство о государственной регистрации программы для ЭВМ №2012614405. Система обнаружения несанкционированной модификации метрологических данных технологического объекта или процесса / Т. И. Фазлиамхетов. Роспатент. М.: Зарег. в Реестре программ для ЭВМ 17.05.2012.

Диссертант  Т.И. Фазлиахметов

ФАЗЛИАХМЕТОВ Тимур Ильгизович

АЛГОРИТМЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ РЕЗУЛЬТАТОВ ИЗМЕРЕНИЙ В БАЗАХ ДАННЫХ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

(НА ПРИМЕРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОНТРОЛЯ ТРАНСПОРТА НЕФТИ)

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати 27.05.2013. Формат 60x84 1/16.
Бумага оберточная. Печать плоская. Гарнитура Таймс.
Усл.печ.л. 1,0. Уч.-изд.л. 0,9.
Тираж 100 экз. Заказ № 336.

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