На правах рукописи

Шувалов Илья Александрович

РАЗРАБОТКА И РЕАЛИЗАЦИЯ ИМИТАЦИОННЫХ И АНАЛИТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ИССЛЕДОВАНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Специальность

05.13.18 – Математическое моделирование, численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Махачкала – 2017

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Дагестанский государственный технический университет».

Научный руководитель: доктор физико-математических наук, профессор **Семенчин Евгений Андреевич**

Научный консультант: доктор технических наук, профессор **Мелехин Владимир Борисович**

Официальные оппоненты:

- **Целых Александр Николаевич –** доктор технических наук, профессор, федеральное государственное автономное образовательное учреждение «Южный федеральный университет», Инженерно-технологическая академия, Институт компьютерных технологий и информационной безопасности, кафедра информационно-аналитических систем безопасности, заведующий кафедрой.

Курбанмагомедов Курбанмагомед Динмагомедович – кандидат технических наук, доцент, Учреждение высшего образования «Институт системных технологий», кафедра «Информационные технологии», заведующий кафедрой.

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», г. Краснодар

Защита диссертации состоится «29» сентября 2017 г. в 15.00 часов на заседании диссертационного совета Д.212.052.02 при ФГБОУ ВО «Дагестанский государственный технический университет», 367015, г. Махачкала, пр. Имама Шамиля 70, диссертационный зал административного корпуса, кабинет 201.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБОУ ВО «Дагестанский государственный технический университет» www.dstu.ru. Сведения о защите и автореферат диссертации размещены на официальном сайте ВАК Министерства образования и науки РФ http://www.vak.ed.gov.ru.

Автореферат разослан «28» августа 2017 года

Ученый секретарь диссертационного совета **Меркухин Евгений Николаевич**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В связи со вступлением в силу с 1 июля 2011 года требований Федерального закона от 23 декабря 2010 года № 359-ФЗ «О внесении изменения в статью 25 федерального закона «О персональных данных» проблема приведения информационных систем обработки персональных данных в соответствие с требованиями этого закона является актуальной для всех организаций, как с государственной, так и с частной формой собственности. Одной из основных задач, которую в первую очередь необходимо решить для выполнения требований данного Федерального закона, является выявление актуальных угроз безопасности действующих и проектируемых информационных систем (угроз, от которых исследуемые систем являются слабо защищенными), предназначенных для хранения и переработки персональных данных, с целью своевременного их устранения.

Для выявления актуальных угроз безопасности, т.е. угроз, вероятность реализации которых является высокой, и они представляют опасность для персональных данных в исследуемой системе, необходимо не только для формального исполнения требований законодательства, но и для определения требуемого уровня их защиты. Это является особенно актуальным для информационных систем, используемых в подразделениях различных министерств и ведомств. Для решения данной проблемы без нанесения ущерба информации, хранящейся в действующих информационных системах, целесообразно использовать математическое моделирование процессов их функционирования для выявления различных по характеру воздействия угроз безопасности с высокой вероятностью их возникновения и реализации. Отмеченные выше обстоятельства и определяют актуальность темы настоящего диссертационного исследования.

Степень разработанности исследуемой проблемы. Проблема устранения актуальных угроз в процессе обработки персональных данных в последнее время активно обсуждается различными специалистами в области безопасности информационных систем. В частности при проведении исследования автор опирался на работы в данной области следующих отечественных и зарубежных ученых С. Бармана, Е. Белова, Б. Блинова, В. Герасименко, В. Грибушена, В. Загорского, В. Забирова, О. Казарина, В. Левина, В. Мельникова, А. Манахова, А Росенко, Ю. Сычева, В. Шангина и мн. других.

В области математического моделирования сложных систем автор учитывал работы следующих российских и зарубежных ученых Т. Алиева, А. Атаева, О. Альсова, В. Афонина, В. Бахвалова, В. Боева, Ю. Бродского, В. Емельянова, Ю.Карпова, В. Кельтона, В. Колдаева, Б. Советова, В. Финаева, В. Чернецкого, О Шелухина, Р. Шеннона и мн. других.

Однако в научных публикациях, посвященных безопасности информационных систем, основными темами для обсуждения являются

методы их защиты от реализации различного вида угроз и классификация самих угроз по характеру их влияния, например, на информационную систему хранения и обработки персональных данных (ИСПД). Вопросы же, связанные с математическим моделированием и определением на этой основе актуальных угроз безопасности для конкретных ИСПД, функционирующих в определенных условиях, остаются за бортом проводимых исследований и практически в настоящее время являются открытыми. Кроме того, методов выявления угроз, предложенных в методических рекомендациях ФСТЭК России, явно недостаточно для эффективной оценки актуальности угроз безопасности различных развивающихся информационных систем хранения и обработки данных. Таким образом, возникает объективная необходимость в разработке эффективных математических моделей и методов, позволяющих выявлять актуальные угрозы безопасности как для действующих, так и для проектируемых информационных систем различного назначения.

Отмеченные выше обстоятельства и определи цель, задачи и направление проводимого исследования.

Цель диссертационного исследования заключается в разработке математических моделей и методов, позволяющих определять актуальные угрозы безопасности различных информационных систем, в частности систем обработки персональных данных и обеспечить возможность проведения эффективного анализа причин возникновения и возможностей устранения выявленных угроз на основе данных, полученных путем имитационного моделирования процессов их функционирования в реальных условиях эксплуатации.

Для достижения указанной цели были поставлены и решены следующие **основные задачи:**

- разработана методика оценки вероятности реализации каждой поступающей в информационную систему угрозы;
- синтезированы имитационные модели функционирования информационной системы, на примере системы обработки персональных данных в реальных условиях эксплуатации при воздействии на неё различного вида угроз;
- выявлены угрозы, вероятность возникновения которых является наиболее высокой для исследуемой информационной системы, и на этой основе установлены для нее актуальные угрозы;
- рассмотрена возможность использования полученных результатов моделирования для введения в информационную систему дополнительных средств защиты хранящихся и перерабатываемых в ней данных;
- разработаны аналитические модели реализации и методика выявления актуальных угроз безопасности в исследуемой информационной системе;
- синтезировано программное обеспечение, позволяющее автоматизировать проведение экспериментов с предложенными моделями, и обработать полученные результаты.

Предметом исследования является разработка имитационных и аналитических математических моделей и методов, а также реализующего их комплекса программ, для выявления и последующего устранения актуальных угроз безопасности действующих и проектируемых информационных систем хранения и обработки данных.

Объект исследования являются сложные информационные системы. В качестве примера в работе исследована информационная система «Информационные ресурсы Управления ГИБДД ГУ МВД России по Краснодарскому краю» и даны рекомендации по усилению ее защиты.

Научная новизна проведенного исследования заключается в разработке оригинальных имитационных и аналитических математических моделей и методов, позволяющих провести исследования и на этой основе оценить влияния различного типа угроз безопасности на информационную систему и определить эффективные средства защиты от выявленных актуальных для нее угроз безопасного функционирования.

Теоретическая значимость проведенного исследования заключается в расширении теоретических знаний в следующих областях:

- имитационного моделирования сложных информационных систем обработки персональных данных в реальных условиях их эксплуатации при воздействии различного характера внешних и внутренних угроз безопасности;
- определения актуальных угроз безопасности информационных систем, предназначенных для хранения и обработки персональных данных;
- способов обеспечения защиты персональных данных в информационных системах различного назначения, подверженных влиянию различных по характеру угроз безопасности.

Практическая значимость полученных результатов заключается в эффективности их использования в качестве методической базы и программного обеспечения для определения актуальных угроз безопасности информационных систем обработки персональных данных, с целью обеспечения эффективной их защиты от влияния различных возмущающих факторов окружающей среды и несанкционированных проникновений.

Опираясь на результаты проведенного исследования, разработана реально действующая модель угроз персональных данных при их обработке в ИСПД «Информационные ресурсы Управления ГИБДД», а на основе анализа полученных результатов моделирования даны рекомендации по ее дальнейшей эффективной защите в процессе функционирования в изменяющихся условиях окружающей среды.

Методологической и теоретической основой диссертационного исследования послужили труды российских и зарубежных ученых в области математического и имитационного моделирования, разработки методов экспертной оценки, системного анализа и разработки специального программного обеспечения сложных систем.

В ходе проведения исследований применялись математический аппарат теории массового обслуживания и Марковских процессов, численные

методы решения дифференциальных уравнений, а также математический аппарат теории вероятностей и математической статистики.

К основным **научным положениям, выносимым на защиту**, следует отнести:

1. Предложен метод выявления актуальных угроз безопасности информационной системы обработки персональных данных, отличающийся от известных, способом экспертной оценки вероятностей возникновения различного вида угроз. Это позволяет получить исходные данные для имитационного моделирования процесса функционирования системы в реальных условиях эксплуатации и обеспечить на этой основе условия ее безопасного функционирования.

2. Разработаны имитационные модели, позволяющие исследовать процесс поведения информационной системы при воздействии на нее различных угроз безопасности, отличающиеся от известных моделей учетом имеющегося у системы уровня защиты и его влияния на вероятность реализации различного вида угроз при различном характере их воздействия на исследуемую систему. Это позволяет определить актуальные для конкретной информационной системы, действующие на нее, угрозы безопасности и на этой основе снизить вероятность их реализации.

3. Предложена Марковская модель перехода информационной системы из состояния к состоянию под воздействием актуальных угроз безопасности, отличающаяся от известных способом определения интенсивности входного потока угроз и вероятностей перехода системы из состояния к состоянию за один шаг поведения. Применение предложенной математической модели позволяет повысить адекватность проводимой оценки влияния различных угроз безопасности на информационную систему, функционирующую в нестабильных условиях окружающей среды.

4. Разработан комплекс программ, обеспечивающий автоматизацию проведения экспериментов с разработанными имитационными и аналитическими моделями и систематизировать обработку как исходных, так и полученных в ходе экспериментов с моделями данных. Оригинальность программных модулей подтверждается их государственной регистрацией в реестре программ для ЭВМ.

Степень достоверности и апробация результатов исследования. Достоверность полученных результатов проведенного исследования подтверждается корректным использованием методов системного анализа, метода Коши для решения дифференциальных уравнений, способа определения финальных вероятностей в установившемся режиме для системы с дискретными состояниями и непрерывным временем, а также совпадением результатов имитационного и аналитического математического моделирования исследуемой информационной системы.

Основные положения и результаты диссертационной работы докладывались и получили одобрение на VII и VIII Всероссийских конференциях по актуальным проблемам внедрения и развития сектора IT-

технологий «Современные информационные технологии в проектировании, управлении и экономике» (2012 - 2013 гг.).

Результаты исследования внедрены в служебную деятельность регионального отдела информационного обеспечения Управления ГИБДД ГУ МВД России по Краснодарскому краю, что подтверждается соответствующими актами их внедрения и использования.

Публикации. По теме диссертационной работы опубликовано 12 научных трудов, из них рецензируемых – 8, в том числе 4 статьи в рецензируемых научных изданиях, включенных в Перечень ВАК РФ и 4 авторских свидетельства на программы для ЭВМ.

Объем и структура работы. Диссертация состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений. Основной текст представлен на 136 страницах машинописного текста, включая 47 таблиц, 36 рисунков, 1 стр. принятых сокращений и списка литературы из 120 наименований.

2. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе **«Основные проблемы и особенности моделирования сложных информационных систем для выявления актуальных угроз безопасности»** проведен анализ методологических основ имитационного моделирования сложных информационных систем при атаке на нее различных угроз безопасности; разработан метод определения актуальных угроз безопасности информационных систем; предложена методика получения исходных данных, необходимых для имитационного моделирования исследуемой информационной системы и схема ее реализации.

Для построения информационного обеспечения имитационной модели, позволяющей определить и проанализировать источники возникновения актуальных угроз безопасности исследуемой информационной системы, предлагается использовать двухуровневую схему опроса экспертов.

На первом уровне с целью построения перечня всех атакующих информационную систему угроз создается головная группа экспертов. По полученным от неё данным формируется исходное множество угроз ее безопасности.

На втором уровне, для каждого вида возможных угроз (с учетом различного характера и причин их возникновения) формируется отдельная экспертная группа, по результатам опроса которой определяются вероятности возникновения потенциальных угроз. (Например, при исследовании информационной системы обработки персональных данных ГИБДД Краснодарского края было сформировано семнадцать специализированных групп экспертов).

Основная задача каждой специализированной группы экспертов сводится к анализу класса переданных ей угроз безопасности и определению на этой основе вероятностных оценок возможностей их возникновения и

реализации в информационной системе при различной конфигурации имеющихся в ней средств защиты. Другими словами, данные группы экспертов обеспечивают получение первичных оценок возможности возникновения потенциальных угроз, в случае наступления вызывающих их событий, и первичных оценок возможности их реализации при отсутствии или наличии в системе дополнительных средств защиты.

После определения и утверждения различными группами экспертов оценок вероятностей наступления и реализации угроз, полученные данные передаются для дальнейшей обработки головной группе экспертов (в рассматриваемом примере экспертной группе Управления ГИБДД).

Головной группой экспертов проводится анализ данных, полученных специализированными группами экспертов, и на его основе уточняются и корректируются значения вероятностей возникновения и реализации угроз, которые используются для проведения дальнейшего исследования. Другими словами, на данном этапе результаты, представленные специализированными группами экспертов, по каждому типу угроз в отдельности подвергаются статистической обработке, на основе которой определяются средние арифметические величины полученных экспертным путем вероятностей, их медиана, мода и дисперсия. Затем по полученным оценкам принимается решение о возможности использования имеющихся данных в качестве информационного обеспечения имитационного моделирования процесса поведения информационной системы при атаке на нее соответствующих угроз безопасности .

Например, при проведении исследования информационной системы ГИБДД Краснодарского края, полученные в результате обработки первичных данных оценки медиан, мод и вероятностей для всех типов угроз оказались одинаковыми, а среднее арифметическое их значение при округлении отличалось от исходных на величину, равную 0.01. Таким образом, учитывая, что значение дисперсий по каждому отдельному показателю оказалось малым, можно принять решение о допустимости использования в качестве исходных данных для дальнейшего исследования информационной системы, следующие значения медианы/моды (таблица 1).

Для обработки полученных вероятностей наступления и реализации угроз безопасности и их использования при реализации имитационной модели исследуемой информационной системы, разработано программное обеспечение, позволяющее проводить все необходимые математические расчеты. Опираясь на полученные таким образом данные и используя метод Монте-Карло для формирования случайного потока угроз безопасности различного типа и обработки входного потока заявок, в работе предложена имитационная модель процесса функционирования информационной системы в соответствующих условиях ее эксплуатации. Блок схема алгоритма реализации данной модели приводится на рисунке 1.

Приведенная на рисунке 1 имитационная модель функционирования информационной системы отражает не только процесс ее взаимодействия с источниками угроз в заданных условиях эксплуатации, но в ней учитываются

различные характеристики и возможности системы, связанные с обработкой потока заявок (запросов на обслуживание), которые необходимо исследовать и скорректировать по результатам проведенных экспериментов.

Таблица 1 - Вероятности реализации угроз, принятые для разработки имитационной модели функционирования информационной системы

Наименование угрозы	Вер-ть наступления	Вер-ть реализ. без защиты	Вер-ть реализ. с доп.защитой
Утечка акустической информации	0,1	0,01	0,1
Утечка видовой информации	0,1	0,01	0,01
Утечка по каналам побочных электромагнитных излучений	0,1	0,01	0,01
Хищение персональной электронной вычислительной машины	0,1	0,01	0,01
Хищение носителей информации	0,1	0,01	0,01
Хищение ключей и атрибутов доступа	0,1	0,01	0,01
Хищение, модификация информации	0,1	0,01	0,01
Вывод из строя узлов ПЭВМ, каналов связи	0,1	0,1	0,01
Несанкционированное отключение средств защиты	0,1	0,01	0,1
Действия вредоносных программ	0,25	0,1	0,01
Скрытый функционал ПО	0,1	0,01	0,01
Установка стороннего ПО	0,1	0,1	0,01
Потеря ключей и атрибутов доступа	0,25	0,25	0,01
Непреднамеренная модификация информации	0,1	0,01	0,01
Непреднамеренное отключение средств защиты	0,1	0,01	0,01
Выход из строя аппаратно-программных средств	0,1	0,1	0,5
Сбой системы электроснабжения	0,1	0,25	0,1
Катаклизмы / катастрофы	0,1	0,25	0,5
Доступ к информации, модификация лицами, не допущенными к её обработке.	0,1	0,25	0,01
Разглашение, модификация лицами, допущенными	0,25	0,01	0,01
Перехват за переделами контролируемой зоны	0,25	0,5	0,01
Перехват в пределах КЗ внешними нарушителями.	0,1	0,25	0,01
Перехват в пределах КЗ внутренними нарушителями.	0,1	0,25	0,01
Угрозы сканирования сети	0,1	0,25	0,1
Угрозы выявления паролей по сети	0,25	0,5	0,01
Навязывание неверной маршрутизации в сети	0,1	0,1	0,01
Подмена доверенного объекта	0,1	0,1	0,01
Внедрение ложного объекта	0,1	0,1	0,01
Отказ в обслуживании	0,1	0,25	0,01
Удаленный запуск приложений	0,25	0,5	0,01
Внедрения по сети вредоносных программ	0,25	0,5	0,01

Во второй главе **«Имитационные модели сегментов информационной системы обработки персональных данных»** приводятся принципы построения и структура имитационных моделей функционирования различных сегментов (подсистем) сложной информационной системы, используемой для хранения и обработки персональных данных.

После построения имитационной модели и анализа результатов моделирования процесса генерирования запросов информационной системе и получения от нее ответов, было установлено, что для исследования влияния различных угроз безопасности на ее функционирование необходимо разбить ее на сегменты и синтезировать их имитационные модели. Необходимость такого разбиения на подсистемы обусловлена тем, что

информационная система является сложным, территориально распределенным объектом, имеющим достаточно большое количество узлов и ответвлений. Разбиение информационной системы на сегменты целесообразно также осуществлять на основе результатов опроса головной группы экспертов. Исследуемая в качестве примера система была разбита на шесть основных сегментов: коммутатор – сервер, ЭВМ, маршрутизатор – маршрутизатор, ЭВМ – коммутатор, ЭВМ – оператор и коммутатор – маршрутизатор.

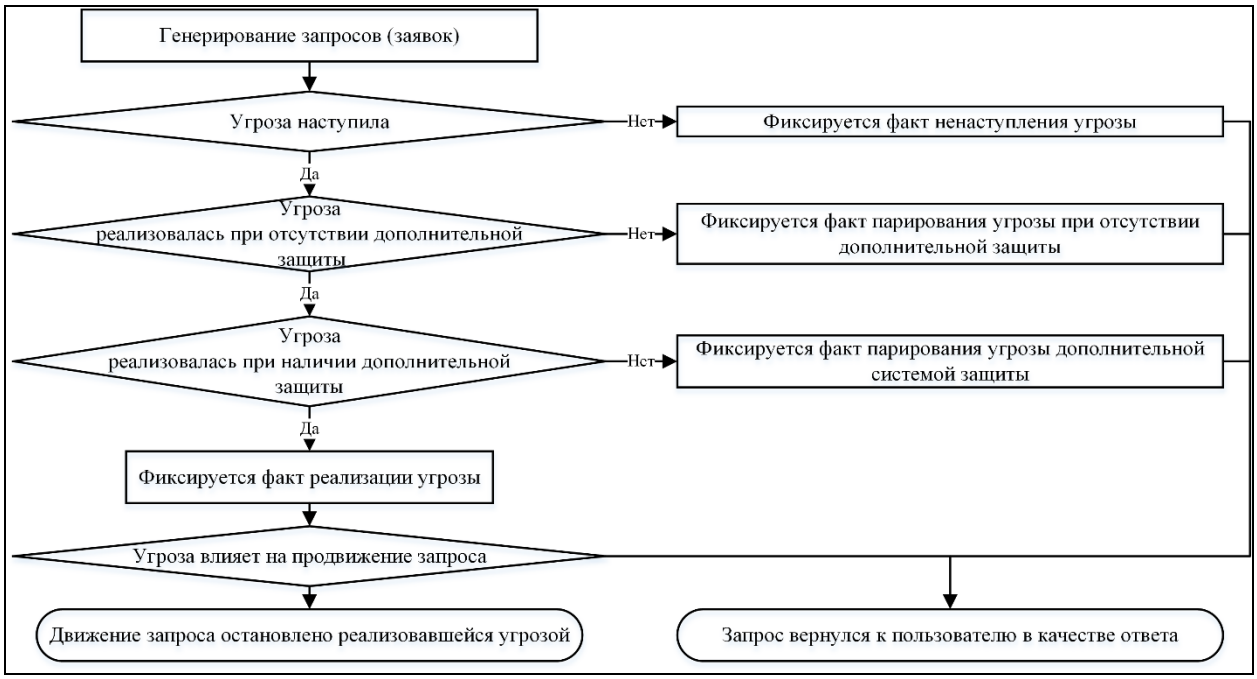

Рисунок 1 - Блок схема алгоритма реализации имитационной модели функционирования информационной системы

В общем случае процесс построения имитационных моделей, для каждого выделенного сегмента включает три основных этапа (на рисунке 2 приведен пример передачи запроса от рабочей станции к маршрутизатору):

- на первом этапе построена имитационная модель функционирования информационной подсистемы системы в виде соединительной линии (канала связи) между двумя точками, например, коммутатором и сервером, на которой расположены точки наступления угроз безопасности. Запрос, проходя точку наступления угрозы, либо продолжает движение дальше к серверу, и фиксируется тот факт, что угроза либо оказалась нереализованной, либо с вероятностью ее наступления она попадает на альтернативный путь движения, где и фиксируется факт ее реализации. Если наступившая угроза препятствует дальнейшему продвижению запроса, например, угроза типа «Отказ в обслуживании», то цикл заканчивается и в счетчик наступивших угроз добавляется одно значение. Если угроза не препятствует дальнейшему продвижению запроса, например, угроза выявления паролей по сети, то в счетчик наступивших угроз также прибавляется одно значение, но запрос

продолжает движение. В результате многократно проведенных опытов выявлено, что количество обслуженных запросов в анализируемой в качестве примера системе составляет 32,28% от общего количества сгенерированных запросов. Также получены значения вероятностей реализации каждого типа угроз при отсутствии дополнительных средств защиты;

- на втором этапе, в имитационной модели учитываются вероятности реализации угроз, определенные экспертным путем. Данные вероятности реализованы в виде точек возникновения угроз, расположенных на альтернативных путях продвижения запроса;

- на третьем этапе в модели учтены вероятности реализации угроз при наличии дополнительной системы защиты. Система защиты добавлена также в виде точки, расположенной на пути реализации угроз. Вероятности определены экспертным путем по выше описанному принципу.

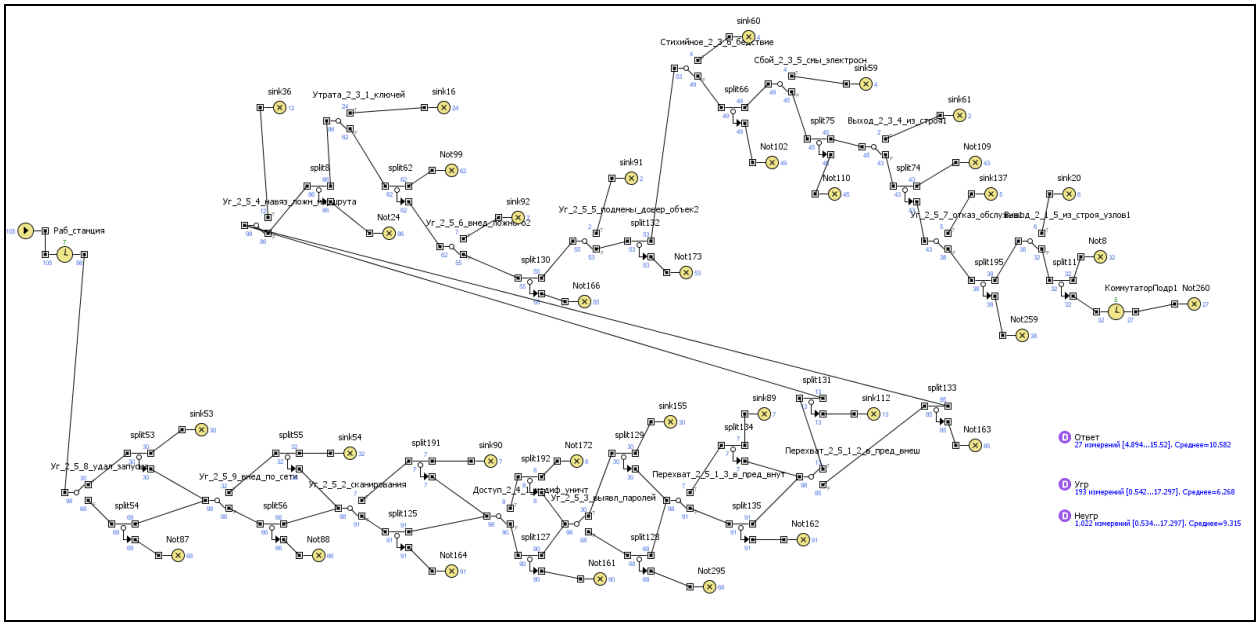

Рисунок 2 – Схема наступления угроз на сегменте «Рабочая станция – маршрутизатор» (изображение компьютерной реализации модели)

Q-схема имитационной модели реализации угроз на сегменте «Рабочая станция – коммутатор» представлена на рисунке 3.

Для автоматизации запуска реализованных имитационных моделей функционирования ИСПД при наличии различного вида угроз ее безопасности, а также обеспечения систематизированного хранения и автоматизированной обработки полученных данных разработано и зарегистрировано в государственном реестре программ для ЭВМ соответствующее программное обеспечение.

В целях выявления угроз, которые наиболее сильно влияют на конечный результат, результаты реализации каждой из угроз рассмотрены отдельно от остальных результатов измерений.

Аналогичным образом построены имитационные модели остальных сегментов информационной системы. Результаты проведенных экспериментов представлены в таблице 2.

Рисунок 3 - Q-схема имитационной модели реализации угроз на сегменте «Рабочая станция – коммутатор» (где λ – входной поток; λ′ - поток обработанных заявок; λ* - заявки, прервавшие движение; Kn 1 – блок наступления n-ой угрозы, Kn 2 – блок реализации n-ой угрозы, Kn 3 – блок реализации n-ой угрозы при наличии дополнительных средств защиты, при n=1, 2 … 16 – угрозы, которые могут наступить на рассматриваемом сегменте по мнению группы экспертов)

Таблица 2 -Результаты экспериментов, проведенных на различных сегментах исследуемой системы

Сегмент информационной системы	% завершенных запросов, от кол-ва поступивших	% реализ. угроз от общего кол-ва реализ. и нереализ. угроз	% реализ. угроз от кол-ва поступивших запросов
От оператора до раб.станции без защиты	78,47	2,56	39,19
От оператора до раб.станции с защитой	97,89	0,13	2,32
От коммутатора до сервера без защиты	88,89	0,73	16,66
От коммутатора до сервера с защитой	97,89	0,13	2,95
От коммутатора до маршрутизатора без защиты	88,91	0,98	12,69
От коммутатора до маршрутизатора с защитой	97,94	0,19	2,59
По каналу связи без защиты	88,92	1,04	12,6
По каналу связи с защитой	97,95	0,20	2,59
От раб.станции до коммутатора без защиты	82,63	4,17	63,34
От раб. станции до коммутатора с зашитой	97,89	0,18	2,80

После проведения экспериментов дана оценка качества и значимости защиты от каждого вида угроз безопасности информационной системы. Для получения такой оценки из модели поочередно убиралась дополнительная защита от каждого вида угроз и проводилась имитация функционирования системы.

Рассмотрим полученные результаты имитационного моделирования на примере сегмента, на котором запрос проходит от рабочей станции до

коммутатора. На основе полученных результатов моделирования были рассчитаны параметры системы (Таблица 3).

Таблица 3 - Результаты численных расчетов частоты реализации различного вида угроз при наличии и отсутствии защиты

Наименование угрозы	% пройден-ных запросов	% реализ. угроз от общ.кол-ва	% угроз, нейтарил. сис-мой защиты	% реализ. угроз при отсутствии защиты от кол-ва реализ. угроз
Угрозы удаленного запуска приложений	97,89	0,98	3,20	82,39
Угрозы внедрения по сети вредоносного ПО	97,89	0,98	3,20	82,39
Угрозы сканирования	97,89	0,10	3,90	49,53
Доступ к инф лицами, не допущенными к ней	97,88	0,34	3,87	47,36
Угрозы выявления паролей по сети	97,89	0,98	3,20	82,40
Перехват в пределах КС внешними нарушителями	97,89	0,34	3,88	47,47
Перехват в пределах КС внутр. нарушителями	97,87	0,25	3,97	26,37
Угрозы навязывания неверной маршрутизации в сети	96,92	0,25	3,98	26,56
Потеря ключей и атрибутов доступа	91,83	0,59	3,69	70,56
Угрозы внедрения ложного объекта	96,91	0,25	3,98	26,64
Угрозы подмены доверенного объекта в сети	96,92	0,25	3,98	26,48
Катаклизмы / катастрофы	96,66	0,26	3,96	62,00
Сбой системы электроснабжения	95,67	0,33	3,90	49,53
Выход из строя аппаратно-программных средств	97,37	0,22	4,01	29,99
Угрозы типа «Отказ в обслуживании»	95,46	0,34	3,88	18,13
Вывод из строя узлов ПЭВМ, каналов связи	96,92	0,25	3,97	25,95

Проанализировав результаты, представленные в таблице 3, можно выделить угрозы, отсутствие защиты от которых наиболее существенно влияет на безопасность функционирования исследуемой информационной системы.

Помимо этого, эффективность средств защиты можно оценить, сравнив процент реализации конкретного вида угроз от общего количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента (Таблица 4).

Таблица 4 - Сравнение процентов реализации наступивших угроз

Наименование угрозы	% с защитой от реализованных	% без защиты от реализ. угр
Угрозы удаленного запуска приложений	4.58	82.39
Угрозы внедрения по сети вредоносных программ	4.42	82.39
Угрозы сканирования, направленные на выявление открытых портов и др.	8.80	49.53
Доступ к информации, уничтожение лицами не допущенными к ней	0.93	47.36
Угрозы выявления паролей по сети	4.57	82.40
Перехват в пределах контролируемой зоны внешними нарушителями	0.90	47.47
Перехват в пределах контролируемой зоны внутренними нарушителями	0.35	26.37
Угрозы навязывания неверной маршрутизации в сети	0.37	26.56
Потеря ключей и атрибутов доступа	2.19	70.56
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0.36	26.64
Угрозы подмены доверенного объекта в сети	0.33	26.48
Катаклизмы / катастрофы	44.35	62.00
Сбой системы электроснабжения	8.85	49.53
Выход из строя аппаратно-программных средств	17.75	29.99
Угрозы типа «Отказ в обслуживании»	0.85	18.13
Вывод из строя узлов ПЭВМ, каналов связи	0.35	25.95

По данным, приведенным в таблице 4, видно, что на исследуемом сегменте наиболее эффективной является защита от угрозы потери ключей и атрибутов доступа (при отсутствии защиты от данного вида угрозы процент количества реализованных угроз указанного типа от общего количества всех реализованных угроз возрастает с 2,19 до 70,56).

В целях организации систематизированной обработки и хранения полученных результатов имитационного моделирования разработана программа для ЭВМ «Результаты моделирования». В качестве примера, данная программа апробирована с использованием численных данных, при проведении машинного эксперимента на основе имитационной модели информационной системы «Информационные ресурсы УГИБДД».

В целях обеспечения универсальности применения разработанных имитационных моделей, эффективного доступа к базам данных и повышения наглядности представления полученной информации, разработана программа для ЭВМ «Обработка данных имитационной модели (ОДИМ)». Данная программа объединяет в себе возможности обработки данных от момента получения их исходных значений до вывода окончательных результатов. Кроме того, разработанная программа позволяет использовать внешние базы данных и обеспечивает возможность обработки сведений, определяющих результаты имитационного моделирования разных информационных систем.

В третьей главе **«Определение актуальных угроз безопасности и необходимости дополнительной защиты»** разработана модель воздействия различных угроз безопасности на исследуемую информационную систему в целом, предложены методики определение актуальности угроз безопасности и расчета необходимости дополнительных мер защиты исследуемой информационной системы.

Для дальнейшего анализа безопасности функционирования исследуемой системы необходимо определить актуальные для нее угрозы. Для моделирования процесса воздействия различных угроз на рассматриваемую в качестве примера информационную систему, целесообразно выделить четыре вида коммутации операторов с сервером, отличающихся набором сегментов, которые проходит запрос: по спутниковым линиям связи, с использованием оптоволоконных линий связи и с использованием технологии xDSL; по коммутируемым линиям связи или по сотовым каналам связи (GPRS/3G); по сотовым линиям связи по технологии GPRS/3G с использованием промежуточного сервера; при прохождении запроса от рабочей станции, находящейся непосредственно в Управлении ГИБДД.

Например, для моделирования ситуации, когда передача запроса в базу данных пользователями осуществляется в пределах локальной вычислительной сети, выделены следующие сегменты: поступление запроса от пользователя к рабочей станции; передача запроса от рабочей станции к коммутатору, установленному и объединяющему рабочие станции для каждого пользователя с межэтажным коммутатором; от межэтажного

коммутатора, до управляемого коммутатора (маршрутизатора), объединяющего все коммутаторы, расположенные у разных пользователей на одном этаже и коммутатор, объединяющий серверы управления; от управляемого коммутатора (маршрутизатора) до коммутатора, объединяющего все межэтажные коммутаторы и серверы управления; от коммутатора до сервера. При этом обработанный запрос поступает обратно к пользователю в качестве ответа через те же сегменты.

Результаты проведенных экспериментов на основе, разработанной в работе, имитационной модели процесса функционирования информационной системы представлены в таблице 5.

Таблица 5 - Результаты проведенных экспериментов при исследовании различных типов связи информационной системы с защитой

Тип связи с защитой	% полученных ответов от кол-ва поступивших запросов	% угроз от общего кол-ва угр. и неугр.	% угроз от кол-ва запросов
Спутниковая, оптоволоконная	97,91	0,16	2,64
Dial-Up, GPRS/3G	97,92	0,16	2,61
GPRS/3G с промежуточным сервером	97,91	0,15	2,70
В одной подсети	97,91	0,16	2,65

Как видно из проведенных расчетов конечные результаты для различных моделей при наличии защиты практически не отличаются. Наблюдаемая разница в показателях настолько мала, что ее возникновении можно считать как результат погрешности измерений.

С помощью общей имитационной модели всей системы в целом проведены такие же эксперименты, что и отдельно с каждым из ее сегментов. В итоге были выделены угрозы, вероятность реализации которых является наиболее высокой (Таблица 6).

Таблица 6 - Сводная таблица результатов проведенных экспериментов

№ п/п	Продв. запроса по 3G каналам	По спутн. каналам	По локал. сети	По 3G каналам с доп. сервером	Сегмент от оператора до раб. станции	Сегмент от раб. станции до коммут.	Сегмент продв. от комм. до маршр.	Сегмент продв. по каналу связи	Сегмент продв. от комм. до сервера
1.	Катаклизмы 47,65%	Катаклизм 47,2%	Катаклизм 47,06%	Катаклизмы 46,15%	Катаклизм 53,31%	Катаклизмы 44,52%	Катаклизм 48,3%	Катаклизм 47,93%	Катаклизм 42,38%
2.	Выход из строя 18,95%	Выход из строя 18,72%	Выход из строя 18,6%	Выход из строя 18,27%	Выход из строя 21,57%	Выход из строя 17,6%	Выход из строя 18,99%	Выход из строя 19,31%	Выход из строя 16,53%
3.	Сбой электр. 9,48%	Электр. 9,41%	Электр. 9,38%	Электр. 9,16%	Электр. 10,71%	Угр.скан 8,99%	Электр. 9,68%	Электр. 9,52%	Угр.скан 8,44%
4.	Угр.скан 7,04%	Угр.скан 7,78%	Угр.скан. 7,47%	Угр.скан 7,64%	Удал. зап. 5,27%	Электр.. 8,86%	Угр.скан 9,45%	Угр.скан 9,38%	Электр. 8,32%
5.	Перехват вне КЗ 3,54%	Выявл. паролей 3,84%	Выявл. паролей 3,68%	Выявл. паролей 3,77%	Потеря ключей 2,68%	Угр. внедр. вред. прог. 4,48%	Перехват вне КЗ 4,68%	Перехват вне КЗ 4,79%	Удал. зап.прил 4,27%
6.	Выявл. паролей 3,68%	Удал. зап. прил. 2,35%	Удал. зап. прил. 2,81%	Удал. зап. прил. 3,07%	Хищение ключей 2,66%	Выявл. паролей 4,43%	Выявл. паролей 4,65%	Выявл. паролей 4,69%	Перехват вне КЗ 4,24%
7.	Удал. зап.прил 2,38%	Перехват вне КЗ 2,34%	Потеря ключей 2,33%	Перехват вне КЗ 3,06%	Действия вирусов 1,07%	Удал. зап.прил 4,41%	Перехв в КЗ внеш. 0,94%	Перехв в КЗ внеш. 0,96%	Внедр. по сети 4,16%

В целях повышения качества защиты исследуемой системы можно дополнительно использовать сертифицированное ФСТЭК программное обеспечение. Однако использование данного стандартного программного обеспечения не позволяет защитить систему в целом от всех видов актуальных угроз, в частности от угроз стихийного характера или сбоев оборудования, но практически полностью исключает реализацию угроз, связанных с действием нарушителей на программном уровне.

Для изучения поведения информационной системы после введения в неё дополнительного средства защиты, в имитационных моделях выполнена следующая доработка - учтена вероятность реализации угроз при наличии дополнительной системы защиты.

Полученные вероятности реализации различных угроз безопасности при наличии дополнительной защиты приводятся в таблице 7.

Таблица 7 - Результаты экспериментов при исследовании сегментов прохождения запроса

Сегмент прохождения запроса	% заверш. запросов	% угроз от кол-ва реали и нереализ угроз	% угроз от кол-ва запросов
От оператора до раб.станции	97,90	0,12	2,14
От рабочей станции до коммутатора	97,92	0,13	2,08
От коммутатора к маршрутизатору	97,99	0,15	2,03
По каналу связи	97,97	0,16	2,03
От коммутатора до сервера	97,91	0,10	2,23
Обобщенные данные, Dial-Up, GPRS/3G	97,94	0,13	2,11
Спутниковые, оптоволоконные линии связи	97,95	0,13	2,09
Обобщенные данные, GPRS/3G с сервером	97,93	0,12	2,12
Обобщенные данные, в одной подсети	97,94	0,13	2,1

Как видно по данным таблицы 7 с введением дополнительной защиты снижается вероятность реализации актуальных для системы угроз безопасности.

В четвертой главе **«Разработка аналитических моделей процесса влияния угроз безопасности на функционирование информационных систем»** разработаны аналитические модели позволяющие исследовать влияние угроз безопасности на функционирование информационной системы обработки персональных данных.

Основным недостатком имитационного моделирования является привязка полученных результатов к условиям проведения экспериментов. В этой связи, для получения общих результатов моделирования целесообразно разработать и использовать аналитические модели процесса функционирования информационных систем. Для построения аналитических математических моделей исследуемую информационную систему целесообразно рассмотреть как систему массового обслуживания, в которую поступают два вида входных событий: угрозы и заявки на обслуживание. На первом этапе моделирования исследована ситуация с использованием упрощенной аналитической модели, когда на вход системы поступают угрозы одного типа, предполагая, что более одной угрозы данного типа не

может быть реализовано или поступить на вход системы в один и тот же момент времени. При выполнении данного допущения исследуемая система может находиться в одном из трех допустимых состояниях, представленных на рисунке 4:

- угроза не поступала, а значит, не была реализована;
- угроза поступала, но не была реализована;
- угроза поступала и была реализована.

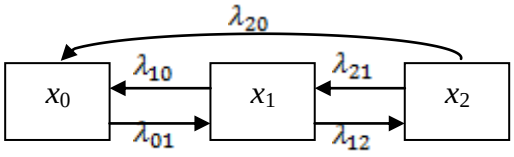

Рисунок 4- Граф состояний системы

Рассматриваемая система является системой с восстановлением, так как состояние x_2 не является поглощающим, а значит, система может вернуться из x_2 в состояние x_0. Переход из состояния в состояние в системе реализуется согласно ориентированному графу, представленному на рисунке 4. Для описания процесса перехода системы из состояния в состояние за промежуток времени Δt на основе интенсивностей поступления действующих на нее событий, построена следующая матрица вероятностей перехода системы из состояния в состояние за один шаг поведения:

$$\|p_{ij}\| = \begin{vmatrix} p_0(t)(1-\lambda_{01})\Delta t & p_0(t)\lambda_{01}\Delta t & 0 \\ p_1(t)\lambda_{10}\Delta t & p_1(t)(1-(\lambda_{10}+\lambda_{12}))\Delta t & p_1(t)\lambda_{12}\Delta t \\ p_2(t)\lambda_{20}\Delta t & p_2(t)\lambda_{21}\Delta t & p_2(t)(1-(\lambda_{20}+\lambda_{21}))\Delta t \end{vmatrix}, \quad (1)$$

Интенсивности поступления заявок и, соответственно, переходов системы из состояния в состояние можно определить также методом экспертных оценок, опираясь на (1) и представить в виде следующей матрицы вероятностей перехода:

$$\|\lambda_{ij}\| = \begin{vmatrix} \lambda_{01} & \lambda_{01} & 0 \\ \lambda_{10} & \lambda_{10}+\lambda_{12} & \lambda_{12} \\ \lambda_{20} & \lambda_{21} & \lambda_{20}+\lambda_{21} \end{vmatrix}. \quad (2)$$

Для определения изменения во времени вероятностей состояния системы $p_0(t)$, $p_1(t)$, $p_2(t)$ используем систему дифференциальных уравнений Колмогорова следующего вида:

$$\begin{cases} \frac{dp_0(t)}{dt} = -p_0(t)\lambda_{01} + p_1(t)\lambda_{10} + p_2(t)\lambda_{20}, \\ \frac{dp_1(t)}{dt} = p_0(t)\lambda_{01} - p_1(t)(\lambda_{10}+\lambda_{12}) + p_2(t)\lambda_{21}, \\ \frac{dp_2(t)}{dt} = p_1(t)\lambda_{12} - p_2(t)(\lambda_{20}+\lambda_{21}) \end{cases} \quad (3)$$

При следующих начальных условиях:

$$p_0(0) = 1,\ p_1(0) = 0,\ p_2(0) = 0. \quad (4)$$

Полученная система уравнений при $t \to \infty$ $\frac{dP_i(t)}{dt} = 0, i = \overline{0,2}$ позволяет найти финальные вероятности нахождения системы в различных состояниях, которые можно интерпретировать как долю времени ее пребывания в течении отчетного периода в этих состояниях.

Вероятности перехода системы из состояния i в состояние j за один шаг p_{ij}, будут определяться следующим образом:

$$p_{ij} \to p_i \Delta t \lambda_{ij} \qquad (5)$$

где p_i – вероятность того, что в текущий момент времени система будет находиться в i-м состоянии.

Отсюда, если за начальное состояние принимается состояние системы x_0, то вероятности перехода системы из i-го состояния в j состояние за n шагов перехода будет определяться следующим образом:

$$P_{ij}(n) = P(t_0)\left\|P_{ij}(1)\right\|^n. \qquad (6)$$

Для построения аналитической математической модели воздействия на информационную систему угроз нескольких видов в силу ординарности потока входных угроз будем полагать, что:

1) угрозы одного типа не могут быть одновременно реализованы или одновременно поступать на вход системы на малом промежутке времени Δt;

2) в один и тот же момент времени не могут поступать и быть реализованы несколько угроз различного типа.

Тогда количество состояний системы x_{ij} будет определяться следующим образом: x_0 – ни одна из угроз не наступила и, соответственно, не реализовалась; x_1– первая угроза из рассматриваемых наступила, но не реализовалась, x_2– первая рассматриваемая угроза реализована; общее количество рассматриваемых угроз – (n-1)/2; общее количество состояний, в которых может находиться система – n+1. Представленный ранее ориентированный граф переходов (Рисунок 4) примет в этом случае следующий вид (Рисунок 5). Система дифференциальных уравнений для определения динамики изменения вероятностей состояний $p_0(t)\ldots p_n(t)$, где n – количество состояний системы, когда на неё воздействует угроза, будет иметь следующий вид:

$$\begin{cases}
\frac{dp_0(t)}{dt} = -p_0(t)(\lambda_{01} + \cdots + \lambda_{0k} + \cdots + \lambda_{0\,n-1}) + p_1(t)\lambda_{10} + p_2(t)\lambda_{20} + \cdots + p_k(t)\lambda_{k0} + p_{k+1}(t)\lambda_{k+1\,0} + \cdots + \\
\qquad + p_{n-1}(t)\lambda_{n-1\,0} + p_n(t)\lambda_{n\,0}, \\
\frac{dp_1(t)}{dt} = p_0(t)\lambda_{01} - p_1(t)(\lambda_{10} + \lambda_{12}) + p_2(t)\lambda_{21}, \\
\frac{dp_2(t)}{dt} = p_1(t)\lambda_{12} - p_2(t)(\lambda_{21} + \lambda_{20}), \\
\cdots \\
\frac{dp_k(t)}{dt} = p_0(t)\lambda_{0\,k} - p_k(t)(\lambda_{k0} + \lambda_{k\,k+1}) + p_{k+1}(t)\lambda_{k+1\,k}, \\
\frac{dp_{k+1}(t)}{dt} = p_k(t)\lambda_{k\,k+1} - p_{k+1}(t)(\lambda_{k+1\,0} + \lambda_{k+1\,k}), \\
\cdots \\
\frac{dp_{n-1}(t)}{dt} = p_0(t)\lambda_{0n} - p_{n-1}(t)(\lambda_{n-1\,0} + \lambda_{n-1\,n}) + p_n(t)\lambda_{n\,n-1}, \\
\frac{dp_n(t)}{dt} = p_{n-1}(t)\lambda_{n-1\,n} - p_n(t)(\lambda_{n0} + \lambda_{n\,n-1}).
\end{cases}$$

При переходе системы из состояния в состояние в установившийся режим функционирования полученная система уравнений позволяет определить финальные вероятности ее пребывания в различных состояниях и

таким образом, определить условия, при выполнении которых, система будет функционировать без сбоя или в нормальном режиме при атаке на нее различных видов угроз.

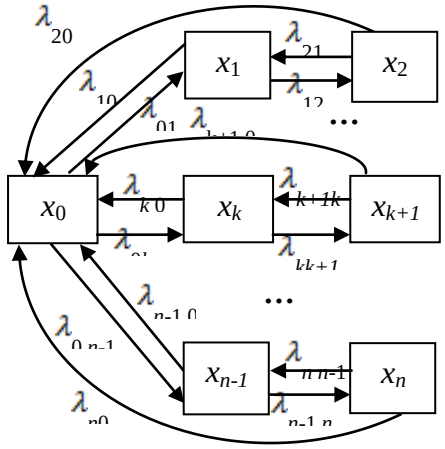

Рисунок 5 - Ориентированный граф переходов системы из одного состояния в другое

Также автором показано, что предложенные математические модели можно использовать и для исследования поведения экономических систем, занимающихся производством различного вида продукции. Например, рассмотрим модель, которая описывает поведение некоторой фирмы на рынке, которая может находиться в произвольный момент времени $t \in [0,T]$ в одном из следующих трёх состояний (Рисунок 4):

1) фирма выпускает инновационную продукцию, которая не имеет аналогов на рынке и пользуется спросом у потребителей (состояние x_0);

2) у продукции фирмы появились аналоги, которые составляют ей конкуренцию (состояние x_1);

3) у продукции фирмы появилось значительное число аналогов, которые дешевле и доступнее, она не может больше конкурировать на рынке и нуждается в замене или модернизации (состояние x_2).

При изучении экономических объектов следует учитывать характерную особенность рынка: интенсивности переходов λ_{10} (из состояния x_1 в состояние x_0), λ_{20} и λ_{21} (из состояния x_2 в состояние x_0 или x_1) равны или близки к 0.

Начальные условия вида (5) не всегда удовлетворяют реальным условиям, складывающимся на рынке товаров. Поэтому в каждом конкретном случае целесообразно их задавать, прибегая к методу экспертных оценок.

3. Заключение

В ходе выполнения исследования в соответствии с поставленными задачами, автором получены следующие научные результаты, использование которых как в отдельности, так и совместно позволяет выявить актуальные

угрозы безопасности для исследуемой системы и обеспечить ее эффективную защиту

1. Для формирования имитационной модели функционирования системы в реальных условиях эксплуатации и определения на этой основе условий обеспечения безопасности хранения и обработки персональных данных, предложен метод определения характеристик угроз безопасности, отличающийся от известных способом оценки вероятности возникновения различного вида угроз, в том числе несанкционированных проникновений в систему.

2. С целью определения влияния различных по характеру воздействия угроз на безопасность хранения и обработки в информационной системе персональных данных и снижения на этой основе вероятности их реализации, разработана имитационная модель воздействия угроз безопасности на информационную систему обработки персональных данных, отличающаяся от известных учетом вероятностей возникновения угроз и характера их воздействия на информационную систему.

3. Для повышения адекватности проводимой оценки характера влияния различных угроз на безопасность информационной системы обработки персональных данных, предложена математическая модель оценки вероятностей возникновения угроз безопасности, отличающаяся от известных способом определения интенсивности их входного потока.

4. С целью обеспечения автоматизации проведения экспериментов с предложенными моделями, а также организации систематизированного хранения и обработки полученных данных, как первоначальных, так и в ходе экспериментов с моделями, разработан комплекс программ для ЭВМ.

5. В настоящее время предложенные модели нашли применение для исследования информационной системы обработки персональных данных, которая эксплуатируется подразделениями МВД России по Краснодарскому краю.

6. В работе показано, что предложенные математические модели можно также использовать и для исследования поведения экономических систем, занимающихся производством различного вида продукции. В качестве примера в работе приведена модель, которая описывает поведение производственного предприятия на рынке.

Основные положения и результаты диссертационного исследования опубликованы в следующих работах:

I.Статьи, опубликованные в ведущих рецензируемых научных журналах и изданиях, определенных Высшей аттестационной комиссией:

1. Шувалов, И.А. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте “Маршрутизатор – маршрутизатор” /И.А. Шувалов, Е.А. Семенчин // Фундаментальные исследования. - 2012. - № 9. - С 425-431. (1,12/0,37 п.л.)

2. Шувалов, И.А. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте «коммутатор – сервер» /И.А. Шувалов, А.П. Росенко // Вестник Дагестанского государственного университета. Технические науки. – 2013. – Вып. 1. – С. 112-123.(1,35/0,67 п.л.)

3. Шувалов, И.А. Математическое моделирование конкурентоспособности микроэкономических систем /И.А. Шувалов, Е.А. Семенчин // Современные проблемы науки и образования. – Электронный журнал. – 2013. – Режим доступа: www.science-education.ru, № ГР 0421200037. (0,37/0,16 п.л.)

4. Шувалов, И.А. Математическая модель воздействия угроз на информационную систему обработки персональных данных / И.А. Шувалов, Е.А. Семенчин // Фундаментальные исследования.– 2013.– № 10.– Ч.3. - С. 529-533. (0,47/0,23 п.л.)

II. Статьи, опубликованные в других научных журналах и изданиях:

5. Шувалов, И.А. Имитационная модель угроз безопасности информационной системы обработки персональных данных / И.А. Шувалов // Современные информационные технологии в проектировании, управлении и экономике: материалы Седьмой Всероссийской конференции по актуальным проблемам внедрения и развития сектора IT-технологий, 26-28 сентября 2012 г. – Махачкала: ДГТУ, 2012. – Т. 2. – С.141-144.(0,17 п.л.)

6. Шувалов, И.А. Имитационная модель реализации внутренних и внешних угроз безопасности сегмента системы «Информационные ресурсы Управления ГИБДД» /И.А. Шувалов, А.П. Росенко, Е.А. Семенчин // Известия Кубанского государственного университета. Естественные науки. – 2012. – №1. – С. 32-41. (1,12/0,37 п.л.)

7. Шувалов, И.А. Моделирование сегментов информационной системы обработки персональных данных /И.А. Шувалов // Современные информационные технологии в проектировании, управлении и экономике: материалы Восьмой Всероссийской конференции по актуальным проблемам внедрения и развития сектора IT-технологий, 24-27 сентября 2013 г. – Махачкала: ДГТУ, 2013. – Т. 2. – С. 157-161. (0,26 п.л.)

8. Шувалов, И.А. Методы определения актуальных угроз безопасности персональных данных / И.А. Шувалов // Наука, образование и культура. – 2017. – №3 (18). – С. 7-10. (0,375 п.л.)

III. Полученные свидетельства о регистрации разработанных программ:

9. Шувалов, И.А. Программа для ЭВМ «Автоматизация запуска имитационных моделей» / Шувалов И.А., Семенчин Е.А. // Свидетельство о государственной регистрации №2013618676. Зарегистрировано в реестре программ для ЭВМ 13.09.2013.

10. Шувалов, И.А. Программа для ЭВМ «Результаты экспертных оценок» / Шувалов И.А., Семенчин Е.А. // Свидетельство о государственной регистрации №№2013618908. Зарегистрировано в реестре программ для ЭВМ 20.09.2013.

11. Шувалов, И.А. Программа для ЭВМ «Результаты моделирования» / Шувалов И.А., Семенчин Е.А. // Свидетельство о государственной регистрации №№2013660093. Зарегистрировано в реестре программ для ЭВМ 23.10.2013.

12. Шувалов, И.А. Программа для ЭВМ «Результаты экспертных оценок» / Шувалов И.А., Семенчин Е.А. // Свидетельство о государственной регистрации №№2014610678. Зарегистрировано в реестре программ для ЭВМ 15.01.2014.