ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

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

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель:

д. ф.-м. н., профессор Е.А. Семенчин

Научный консультант:

д. т. н., профессор В.Б. Мелехин

Махачкала – 2017г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 определения 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 для различных регулярно развивающихся информационных систем хранения и обработки данных подвергающихся различным видам атак. Таким образом, возникает объективная необходимость в разработке эффективных математических моделей и методов, позволяющих выявлять актуальные угроз 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.

В первой главе «Основные проблемы и особенности моделирования сложных информационных систем для выявления актуальных угроз безопасности» исследуются теоретические проблемы построения и реализации имитационных моделей сложных систем; решаются проблемы, связанные с выявлением актуальных угроз безопасности ИСПД; разработан метод, позволяющий на основе экспертных данных получить первоначальные оценки вероятностей наступления и реализации угроз безопасности персональных данных, необходимые для построения имитационной модели процесса функционирования исследуемой информационной системы.

Во второй главе «Имитационные модели сегментов информационной системы обработки персональных данных» предложены имитационные модели различных сегментов информационной системы «Информационные ресурсы УГИБДД», описаны этапы построения данных моделей, проведены машинные эксперименты с разработанными моделями и обработаны результаты проведенного исследования.

В третей главе «Определение актуальных угроз безопасности и необходимости дополнительной защиты» проводятся численные расчеты степени воздействия каждого типа угроз безопасности на отдельные подсистемы исследуемой ИСПД; выделены угрозы, являющиеся актуальными для исследуемой ИСПД «Информационные ресурсы УГИБДД»; проведены расчеты изменения вероятностей реализации угроз в результате использовании в исследуемой информационной системе дополнительных средств защиты информации.

В четвертой главе «Математическое моделирование информационной системы» предложена аналитическая математическая модель определения актуальных угроз безопасности для исследуемой информационной системы, т.е. угроз безопасности, имеющих высокую вероятность реализации при заданных средствах защиты.

В заключении приводятся обобщенные выводы по результатами исследования и описано направление дальнейшего продолжения исследования.

ГЛАВА 1. ОСНОВНЫЕ ПРОБЛЕМЫ И ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ВЫЯВЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ

1.1 Методологические основы построения имитационных моделей процесса функционирования сложных информационных систем при наличии актуальных угроз безопасности.

Моделирование является основополагающим методом изучения поведения сложных систем. В [72] указано: «Моделирование - это один из основных методов познания, это форма отражения действительности, которая заключается в выяснении или воспроизведении тех или иных свойств реальных объектов, предметов и явлений с применением других объектов, процессов, явлений, либо с помощью абстрактного описания в виде изображения, плана, карты, совокупности уравнений, алгоритмов и программ».

Под “моделью” понимается «такая мысленно представляемая или материально реализованная система, которая в процессе познания, анализа замещает реальный объект (или систему), при этом сохраняя часть наиболее важных для исследования его характеристик, причем ее изучение дает нам новую информацию об объекте» [73].

Выделяют несколько основных видов моделей, используемых на практике для описания различных процессов и систем[22]:

– концептуальная модель – модель, описывающая систему с применением специальных символов, знаков, операций над ними или с помощью естественных или искусственных языков;

– физическая модель – моделируемая система воспроизводится исходя из соотношения подобия, вытекающего из схожести физических явлений;

– структурно – функциональная – в качестве модели используют схемы (блок-схемы), диаграммы, графики, таблицы, рисунки со специальными правилами их объединения и преобразования;

– математическая модель – это математическое представление реальности, описание явлений, системы с помощью математических понятий, символики;

– имитационная модель – экономико-математическая модель, применяемая в процессе экспериментального изучения систем или явлений с помощью электронных вычислительных машин (ЭВМ).

При изучении систем указанные виды моделирования могут применяться как самостоятельно, так и несколько одновременно, причем, при использовании имитационного моделирования в той или иной степени задействованы все перечисленные виды моделирования или их отдельно взятые приемы. Помимо этого имитационная модель позволяет наглядно в динамике предоставить конечный или промежуточный результат, что является немаловажным аспектом для успешного понимания полученных результатов лицами, не участвовавшим в её разработке.

В современной литературе не существует единого научного определения имитационного моделирования. Так в [110] имитационное моделирование описывается как «процесс конструирования на вычислительной машине модели сложной реальной системы, функционирующей во времени, и постановки экспериментов над этой моделью с целью либо понять поведение системы, либо оценить различные стратегии, обеспечивающие функционирование данной системы», в [95] – как «один из самых мощных инструментов анализа при разработке сложных систем и анализ процессов их функционирования, имитационное моделирование как метод научного исследования предполагает использование компьютерных технологий для имитации различных процессов или операций – моделирования», в [97] имитационное моделирование рассматривается как метод сбора необходимой информации о поведении системы путем создания её компьютеризированной модели, в [78] – как «метод получения частных численных решений сформулированной задачи на основе аналитических решений или с помощью численных методов».

В сети Интернет также распространены следующие определения понятия имитационное моделирование [53, 54, 55, 66, 76, 77]:

- метод, с помощью которого можно строить модели, описывающие процессы так, как они протекали бы в действительности. Такую модель можно «проиграть» во времени как для одного эксперимента, так и заданного их множества. При этом результаты будут определяться случайным характером процессов;

- метод исследования, когда изучаемая система заменяется моделью, с достаточной точностью описывающей реальную систему, с которой проводятся эксперименты с целью получения информации об этой системе;

- частный случай математического моделирования. Существует класс объектов, для которых по различным причинам не разработаны аналитические модели, либо не разработаны методы решения полученной модели. В этом случае аналитическая модель заменяется имитатором или имитационной моделью;

- логико-математическое описание объекта, которое может быть использовано для экспериментирования на компьютере в целях проектирования, анализа и оценки функционирования объекта.

Обобщая имеющиеся определения, можно сказать, что имитационное моделирование служит для изучения поведения системы с помощью математического аппарата, используя средства вычислительной техники.

Применение средств вычислительной техники позволяет автоматизировать расчет необходимых результатов, имея лишь первоначальные данные, полученные, например, статистически. Это особенно актуально, когда рассматривается сложная система, состоящая из множества узлов, потому что, как правило, для расчетов необходимых результатов требуется применять громоздкие формулы.

Имитационное моделирование применятся для изучения поведения разнообразных систем, в том числе и информационных. В основном при моделировании информационных систем ставится цель получить сведения о

времени обработки заявки, уровня нагрузки какого-либо ресурса и т.п. Однако применение имитационного моделирования для изучения поведения информационной системы обработки персональных данных до настоящего времени широко не рассматривалось.

1.2 Выбор метода определения актуальных угроз безопасности информационной системы

Для определения актуальных угроз безопасности информационной системы обработки персональных данных практически все специалисты прибегают к методике, предложенной ФСТЭК России [82]. В соответствии с данным документом угрозой является «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным (ПДн), результатом которого может стать удаление, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий». Актуальной является угроза, которая может быть реализована в информационной системе обработки персональных данных (ИСПДн) и представляет опасность для ПДн.

Актуальность угрозы, в соответствии с [82], определяется двумя показателями: уровень исходной защищенности информационной системы и вероятность реализации угрозы. Уровень исходной защищенности определяется на основании утвержденных в [82] факторов и может быть рассчитан техническим специалистом без привлечения дополнительных экспертов.

Для определения вероятности реализации угроз используется модель угроз, также предложенная и утвержденная ФСТЭК России [20]. В модели угроз рассматривается воздействие на информационную систему каждой угрозы в отдельности и указаны угрозы, которые являются актуальными. В связи тем, что данный процесс требует высокого уровня подготовки от

специалистов, составляющих модель, и глубокого знания о поведении рассматриваемой системы, разработкой модели угроз, как правило, занимаются специализированные организации.

В связи с тем, что рассматриваемая в качестве примера информационная система «Информационные ресурсы УГИБДД» разработана специалистами УГИБДД и используется ими на протяжении длительного промежутка времени, на оперативном совещании было принято решение о разработке модели угроз специалистами Управления без привлечения сторонних организаций.

В целях более детального изучения влияния каждой угрозы, а также определения качества имеющихся средств защиты, было принято решение помимо формального составления модели угроз расширить количество используемых в ней показателей:

1. Изначально рассматривается вероятность наступления угрозы. Данный показатель добавлен для изучения количества угроз, воздействующих на информационную систему, и их примерной периодичности;

2. Вероятность реализации угрозы при наличии исходного уровня защищенности, рассчитываемого в соответствии с [82].

3. Вероятность реализации угроз при наличии средств дополнительной защиты. Данная вероятность рассматривается в случае, если исходного уровня защищенности было недостаточно, чтобы парировать наступившую угрозу. Вероятность реализации при наличии дополнительных средств защиты в итоге использовалась в качестве вероятности реализации при заполнении модели угроз.

В итоге для того, чтобы угроза была реализована, она должна с определенной вероятностью наступить, после чего с определенной вероятностью обойти исходный уровень защищенности и после этого, также с определенной вероятностью, систему дополнительной защиты.

Для определения актуальных угроз безопасности было предложено и одобрено на оперативном совещании использование имитационного моделирования. В качестве среды моделирования выбрано программное

обеспечение «Anylogic», разработанное российской компанией «Экс Джей Текнолоджис».

Выбор именно этого программного продукта обусловлен следующими факторами [2, 3, 1, 4, 83]:

– облегченный процесс создания моделей с помощью графической среды разработки;

– возможность использования ранее созданных библиотек и модулей для создания новых моделей;

– объектно-ориентированный подход к построению модели;

– наличие большого количества встроенных библиотек для создания имитационных моделей;

– построение модели с использованием языка программирования Java, что позволяет запускать их на любой программной и аппаратной платформе;

– возможность запуска имитационной модели без использования средств разработки.

Для построения математических и, в частности, имитационных моделей различных информационных систем необходимо наличие первоначальных данных, которые в дальнейшем будут использованы при проведении экспериментов с моделью. В качестве исходных данных для рассматриваемой информационной системы принято решение использовать вероятности наступления и реализации угроз. Для определения указанных вероятностей был применен метод экспертных оценок.

1.3 Получение первоначальных данных

Для построения информационного обеспечения имитационной модели, позволяющей определить и проанализировать источники возникновения актуальных угроз безопасности ИСПДн, предлагается использовать двухуровневую систему опроса экспертов.

На первом уровне с целью выявления возникающих в информационной системе угроз создается головная группа экспертов, по полученным от которой данным формируется исходно заданное множество актуальных 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.

Таким образом, одной из основных задач головной группы экспертов является подготовка перечня угроз, которые могут возникнуть в процессе функционирования исследуемой информационной системы. Полученный перечень угроз разбивается на классы в соответствии с причинами их возникновения и характером воздействия на систему. Каждый полученный таким образом класс угроз поступает к соответствующей ему специализированной группе 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 и наличии в системе дополнительных средств защиты.

После определения и утверждения различными группами экспертов оценок вероятностей наступления и реализации угроз, полученные результаты передаются для дальнейшей обработки головной группе экспертов.

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 информационной системы обработки персональных данных.

Другими словами, на данном этапе результаты, представленные специализированными группами экспертов, по каждому виду угроз в отдельности подвергаются статистической обработке. Для каждого отдельного вида угроз 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 имитационной модели функционирования информационной системы.

При изучении ИСПДн «Информационные ресурсы УГИБДД» оценка значений вероятностей наступления и реализации угроз безопасности персональных данных, обрабатываемых в информационной системе, в соответствии с предложенной методикой проводилась в четыре этапа:

1. Сформированы семнадцать групп экспертов: одна в Управлении ГИБДД, в которую включены наиболее подготовленные сотрудники, принимающие непосредственное участие в разработке, внедрении в практическую деятельность и постоянном сопровождении рассматриваемой информационной системы, и по одной группе в каждом из шестнадцати строевых подразделений.

2. Группой экспертов Управления ГИБДД рассмотрен перечень угроз, предложенный ФСТЭК России [82]. Перечень угроз пересматривался для подтверждения наличия в нем всех угроз, которые могут быть реализованы в рассматриваемой информационной системе.

3. Каждой экспертной группе, т.е. в каждое строевое подразделение, передан список угроз безопасности (таблица 1) для проведения оценки вероятности наступления каждой угрозы, вероятности реализации угрозы в случае наступления и вероятности реализации при наличии дополнительных средств защиты. Все значения вероятностей получены с использованием консультационной поддержки группы экспертов Управления ГИБДД методом

мозгового штурма (совещания) с использованием статистических данных, накопленных за время пользования информационной системой. После определения и утверждения группой экспертов вероятностей наступления и реализации угроз, результаты представлены на рассмотрение экспертной группе Управления ГИБДД.

4. Группой экспертов Управления ГИБДД рассмотрены представленные результаты и на их основании выделены значения вероятностей, которые будут использоваться в дальнейших исследованиях информационной системы.

На четвертом этапе изначально рассмотрены все результаты, представленные группами экспертов, по каждому типу угроз в отдельности. Рассмотрены крайние отклонения значений от среднего значения. В случае значительного отклонения значения заслушивался председатель экспертной группы о причинах такого отклонения. Это необходимо было для выяснения, не является ли данное отклонение единственно верным решением. Однако, как показали опросы, вероятности, значительно отличающие от средних значений, указывались вследствие недавней реализации угроз в подразделении, либо вследствие низкого уровня знаний членами комиссии природы возникновения той или иной угрозы. Значения, предоставленные экспертами, представлены в таблицах 1, 2, 3, где значения столбцов – значения, предоставленные каждой из 16 групп экспертов.

Таблица 1 – Значения вероятностей наступления угроз, предоставленные группами экспертов

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Угрозы перехвата акустической информации	0.25	0.1	0.1	0.1	0.01	0.1	0.1	0.01	0.2	0.1	0.05	0.1	0.2	0.1	0.01	0.1
Угрозы перехвата видовой информации	0.25	0.1	0.1	0.1	0.1	0.01	0.01	0.1	0.2	0.1	0.1	0.1	0.01	0.1	0.1	0.2
Угрозы перехвата информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	0.1	0.01	0.01	0.1	0.1	0.1	0.01	0.1	0.01	0.01	0.25	0.1	0.5	0.1	0.1	0.1
Хищение электронной вычислительной машины (ЭВМ)	0.5	0.01	0.01	0.1	0.25	0.1	0.25	0.01	0.01	0.1	0.1	0.01	0.1	0.25	0.1	0.15
Хищение носителей информации	0.01	0.1	0.2	0.1	0.1	0.2	0.1	0.01	0.1	0.1	0.2	0.01	0.1	0.1	0.1	0.1

Продолжение таблицы 1

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Хищение ключей и атрибутов доступа	0.01	0.1	0.1	0.1	0.2	0.1	0.1	0.01	0.1	0.1	0.2	0.01	0.1	0.1	0.1	0.1
Хищение, удаление, модификация информации	0.01	0.1	0.1	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.2	0.01	0.1	0.2	0.1	0.1
Вывод из строя частей ЭВМ, каналов передачи информации	0.5	0.01	0.1	0.1	0.1	0.1	0.2	0.2	0.1	0.1	0.1	0.1	0.01	0.01	0.1	0.01
Нейтрализация средств защиты	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.01
Действия вредоносного ПО (вирусов)	0.5	0.01	0.1	0.25	0.25	0.5	0.25	0.2	0.3	0.25	0.25	0.25	0.25	0.3	0.25	0.2
Скрытый функционал системного программного обеспечения (ПО) и ПО для обработки персональных данных	0.01	0.1	0.1	0.1	0.01	0.1	0.1	0.25	0.25	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Установка ПО, не связанного со служебной деятельностью	0.5	0.1	0.1	0.1	0.01	0.01	0.1	0.1	0.1	0.01	0.1	0.01	0.1	0.1	0.1	0.2
Потеря ключей и атрибутов доступа	0.5	0.01	0.1	0.25	0.25	0.5	0.25	0.25	0.1	0.25	0.25	0.25	0.25	0.3	0.25	0.25
Случайное изменение (удаление) персональных данных сотрудниками, допущенными к их обработке	0.01	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.1	0.01	0.1	0.2	0.1	0.1	0.1	0.1
Случайный вывод из строя средств защиты	0.01	0.1	0.01	0.1	0.25	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Сбой аппаратных и программных средств обработки информации	0.5	0.1	0.1	0.1	0.01	0.1	0.1	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.01	0.1
Нарушение подачи электропитания	0.5	0.01	0.1	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.01	0.1	0.1
Катаклизмы / катастрофы	0.01	0.01	0.1	0.25	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.01	0.1	0.1
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Разглашение персональных данных, модификация, удаление сотрудниками, допущенными к ее обработке	0.5	0.1	0.2	0.25	0.25	0.25	0.5	0.25	0.25	0.25	0.1	0.25	0.25	0.25	0.25	0.15
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны (КЗ))	0.01	0.25	0.25	0.2	0.25	0.25	0.5	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, сторонними нарушителями в пределах КЗ)	0.01	0.1	0.1	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Угроза «Анализ потока информации в сети» (перехват сотрудниками в пределах КЗ информации, передаваемой из ИСПДн и принимаемой из внешних сетей)	0.01	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, незаблокированных портов и др.	0.25	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.01	0.1	0.1	0.1	0.01	0.1

Продолжение таблицы 1

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Угрозы выявления по сети учетных данных	0.75	0.25	0.25	0.1	0.25	0.3	0.01	0.25	0.25	0.25	0.25	0.25	0.25	0.2	0.25	0.2
Угрозы навязывания неверной маршрутизации в сети	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Угрозы замены доверенного объекта в сети	0.01	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.01	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Угрозы типа «Отклонение запроса»	0.25	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.01	0.1
Угрозы несанкционированного удаленного запуска ПО	0.5	0.25	0.25	0.25	0.1	0.25	0.25	0.25	0.15	0.25	0.25	0.25	0.25	0.25	0.15	0.25
Угрозы распространения по сети вредоносного ПО	0.5	0.25	0.25	0.25	0.1	0.25	0.1	0.1	0.5	0.5	0.25	0.25	0.25	0.25	0.01	0.25

Таблица 2– Значения вероятностей реализации угроз при отсутствии дополнительной защиты, предоставленные группами экспертов

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Перехват акуст.. инф.	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват вид. инф.	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват по каналам побочных наводок	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Хищение ЭВМ	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.005	0.01	0.01	0.01	0.1	0.01	0.01
Хищение носителей информации	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.005	0.01	0.01	0.01	0.1	0.01	0.01
Хищение ключей и атрибутов доступа	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Хищен., мод. инф.	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Вывод из строя частей ЭВМ, каналов передачи инф.	0.25	0.01	0.1	0.01	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.01	0.1	0.025
Несанкц. откл. средств защиты	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Действия вред. прог.	0.5	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.01	0.1	0.1	0.1	0.1
Скрытый функционал ПО	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Установка ПО, не связан. со службой	0.5	0.1	0.1	0.1	0.01	0.01	0.1	0.1	0.1	0.01	0.1	0.01	0.1	0.1	0.1	0.1
Потеря ключей и атрибутов доступа	0.5	0.1	0.1	0.1	0.1	0.25	0.1	0.25	0.25	0.25	0.25	0.25	0.25	0.5	0.25	0.5
Случайное изменение ПДн	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01
Случайный вывод из строя защиты	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Выход из строя АП средств	0.5	0.1	0.1	0.1	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Наруш.электропитан.	0.5	0.1	0.25	0.1	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.5	0.25	0.1	0.25
Катаклизмы/катастр.	0.1	0.25	0.25	0.3	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
Доступ, изм. ПДн. лицами, не допущ.	0.01	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
Разглаш.,модиф. сотрудниками, допущ.	0.1	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01
Перехват вне КЗ	0.01	0.5	0.5	0.75	0.5	0.75	0.5	0.25	0.5	0.25	0.5	0.25	0.5	0.25	0.5	0.5

Продолжение таблицы 2

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Перехват в пределах КЗ внеш.	0.01	0.5	0.25	0.25	0.25	0.25	0.5	0.25	0.2	0.2	0.25	0.25	0.25	0.25	0.2	0.25
Перехват в пределах КЗ сотрудниками	0.01	0.5	0.25	0.25	0.25	0.25	0.25	0.25	0.2	0.2	0.25	0.25	0.25	0.25	0.2	0.25
Угрозы анализа сети	0.25	0.2	0.25	0.25	0.25	0.25	0.5	0.25	0.25	0.25	0.1	0.2	0.25	0.25	0.1	0.25
Угрозы выявления по сети учетных данных	0.1	0.4	0.5	0.25	0.5	0.5	0.25	0.3	0.25	0.5	0.4	0.5	0.5	0.5	0.5	0.5
Навязывание неверн. маршрутизации	0.01	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Замена доверенного объекта	0.01	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Внедрение неверного объекта	0.01	0.1	0.1	0.1	0.1	0.25	0.1	0.1	0.1	0.1	0.01	0.1	0.1	0.1	0.1	0.1
Отклонение запроса	0.1	0.1	0.1	0.25	0.1	0.25	0.25	0.25	0.1	0.25	0.5	0.1	0.25	0.25	0.5	0.5
Несанкц. удал. запуск ПО	0.5	0.5	0.75	0.5	0.25	0.5	0.5	0.5	0.25	0.5	0.5	0.25	0.5	0.5	0.25	0.5
Распространение по сети вред. прог.	0.5	0.4	0.5	0.3	0.4	0.5	0.5	0.5	0.5	0.5	0.4	0.5	0.5	0.3	0.25	0.5

Таблица 3– Значения вероятностей реализации угроз при наличии дополнительной защиты, предоставленные группами экспертов

Наименование угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Перехват акуст. инф.	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Перехват вид. инф.	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват по каналам побочных наводок	0.001	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Хищение ЭВМ	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01
Хищение носителей информации	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01
Хищение ключей и атрибутов доступа	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Хищен, мод. инф.	0.1	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Вывод из строя частей ЭВМ, каналов передачи инф-ции	0.1	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Несанкц. отключение средств защиты	0.25	0.01	0.1	0.01	0.1	0.01	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Действия вредоносного ПО	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Скрытый функционал ПО	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Установка ПО, не связан. со службой	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Потеря ключей и атрибутов доступа	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1
Случайное изменение ПДн	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Случайный вывод из строя защиты	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Выход из строя АП средств	0.9	0.25	0.25	0.5	0.25	0.5	0.5	0.5	0.5	0.5	0.5	0.7	0.5	0.5	0.5	0.5

Продолжение таблицы 3

Тип угрозы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Нарушение подачи электропитания	0.5	0.01	0.1	0.01	0.5	0.5	0.01	0.1	0.1	0.01	0.25	0.1	0.1	0.1	0.01	0.1
Катаклизмы/катастр.	0.9	0.25	0.5	0.3	0.5	0.5	0.5	0.25	0.5	0.5	0.25	0.5	0.5	0.5	0.5	0.5
Доступ, изм., удал. ПДн лицами, не допущ.	0.005	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01
Разглаш.,модиф. ПДн сотрудниками	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват за переделами с КЗ	0.001	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват в пределах КЗ внеш.	0.001	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Перехват в пределах КЗ сотрудниками	0.001	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Угрозы анализа сети	0.25	0.1	0.1	0.1	0.1	0.01	0.1	0.1	0.01	0.1	0.1	0.01	0.1	0.1	0.01	0.1
Выявление по сети учетных данных	0.1	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01
Навязывание неверн. маршрутизации	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Замена доверенного объекта	0.005	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Внедрение неверного объекта	0.005	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Отклонение запроса	0.005	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01
Несанкц. удал. запуск ПО	0.25	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Распространение по сети вред. прог.	0.01	0.01	0.1	0.01	0.01	0.1	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01

Рассмотрев все угрозы в отдельности, проведены расчеты средних арифметических величин предложенных вероятностей для каждой угрозы, а также медианы и моды[34].

Для расчета среднего арифметического сумма всех предложенных экспертами вероятностей для каждого типа угрозы разделена на количество экспертов, например, вероятность наступления угрозы перехвата акустической информации рассчитана следующим образом:

$$\frac{0.25 + 0.1 + 0.1 + 0.1 + 0.01 + 0.1 + 0.1 + 0.01 + 0.2 + 0.1 + 0.05 + 0.1 + 0.2 + 0.1 + 0.01 + 0.1}{16} = 0.10188$$

Для получения медианы и моды предложенные вероятности упорядочены в порядке неубывания. Так, например, вероятности наступления угрозы перехвата акустической информации, предложенные группами экспертов, после упорядочивания приняли следующий вид:

0.01	0.01	0.01	0.05	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.2	0.25

Расположив значения в указанном порядке несложно определить и медиану и моду. Причем в данном случае эти значения оказались равными: и медиана (восьмое и девятое значение) равна 0.1, и мода (значение 0.1 предложено девятью группами экспертов из шестнадцати).

Дальнейшим шагом стал расчет значения дисперсии (Таблица 4) [34]. Проведенные расчеты показали, что значение дисперсии является низкой, что говорит о небольшом разбросе значений. На основании этого можно сделать вывод о том, что мнения экспертов являются согласованными и, соответственно, полученные данные можно считать значимыми и применять для дальнейшего исследования информационной системы.

Таблица 4 – Расчет значений

Типы угроз	Наступления				Реализац. без защиты				Реализац. с защитой			
	Дисперсия	Медиана	Мода	Среднее арифметич.	Дисперсия	Медиана	Мода	Среднее арифметич.	Дисперсия	Медиана	Мода	Среднее арифметич.
Перехват акустич. инф.	0.00462	0.1	0,1	0.10188	0.00051	0.01	0,01	0.0156	0.00051	0.1	0,1	0.09438
Перехват видовой инф.	0.00443	0.1	0,1	0.1050	0.00051	0.01	0,01	0.0156	0.00051	0.01	0,01	0.01563
Перехват по каналам ПЭМИН	0.01482	0.1	0,1	0.1063	0.00051	0.01	0,01	0.0156	0.00001	0.01	0,01	0.00913
Хищение ЭВМ	0.01719	0.1	0,1	0.12813	0.00095	0.01	0,01	0.0209	0.00051	0.01	0,01	0.01563
Хищение носителей инф-ции	0.00362	0.1	0,1	0.10188	0.00051	0.01	0,01	0.0153	0.00051	0.01	0,01	0.01563
Хищение ключей и атрибутов доступа	0.00293	0.1	0,1	0.09563	0.00051	0.01	0,01	0.0156	0.00000	0.01	0,01	0.01000
Хищен, мод. инф.	0.00302	0.1	0,1	0.10750	0.00051	0.01	0,01	0.0156	0.00094	0.01	0,01	0.02125
Вывод из строя частей ЭВМ, каналов передачи инф-ции	0.01392	0.1	0,1	0.11500	0.00499	0.1	0,1	0.0972	0.00094	0.01	0,01	0.02125
Несанкц. откл. ср-тв защиты	0.00070	0.1	0,1	0.09750	0.00051	0.01	0,01	0.0156	0.00306	0.1	0,1	0.09250
Действия вред. прог.	0.01429	0.25	0,25	0.25688	0.01268	0.1	0,1	0.1231	0.00051	0.01	0,01	0.01563
Скрытый функционал ПО	0.00402	0.1	0,1	0.10750	0.00051	0.01	0,01	0.0153	0.00000	0.01	0,01	0.00969
Установка не служб. ПО	0.01341	0.1	0,1	0.10875	0.01282	0.1	0,1	0.1025	0.00051	0.01	0,01	0.01563
Потеря ключей и атрибутов доступа	0.01534	0.25	0,25	0.25063	0.02000	0.25	0,25	0.2500	0.00094	0.01	0,01	0.02125
Случайное изменение ПДн	0.00323	0.1	0,1	0.10438	0.00051	0.01	0,01	0.0153	0.00000	0.01	0,01	0.00969
Случ. вывод из строя защиты	0.00258	0.1	0,1	0.09813	0.00051	0.01	0,01	0.0156	0.00051	0.01	0,01	0.01563
Выход из строя АП средств	0.01222	0.1	0,1	0.10813	0.01081	0.1	0,1	0.1194	0.02574	0.5	0,5	0.49063
Наруш. электропитания	0.01222	0.1	0,1	0.10813	0.01282	0.25	0,25	0.2531	0.03283	0.1	0,1	0.15625
Катаклизмы / катастрофы	0.00306	0.1	0,1	0.0925	0.00163	0.25	0,25	0.2438	0.02457	0.5	0,5	0.46563
Доступ, изменеие, удаление ПДн лицами, не допущ.	0.00051	0.1	0,1	0.09438	0.00360	0.25	0,25	0.2350	0.00051	0.01	0,01	0.01531
Разглаш., модиф. Сотрудниками, допущ.	0.01217	0.25	0,25	0.25313	0.00132	0.01	0,01	0.0269	0.00051	0.01	0,01	0.01563
Перехват за переделами с КЗ	0.00817	0.25	0,25	0.24750	0.03692	0.5	0,5	0.4381	0.00052	0.01	0,01	0.01506

Продолжение таблицы 4

Типы угроз	Наступления				Реализац. Без защиты				Реализац. С защитой			
	Дисперсия	Медиана	Мода	Среднее арифметич.	Дисперсия	Медиана	Мода	Среднее арифметич.	Дисперсия	Медиана	Мода	Среднее арифметич.
Перехват в пределах КЗ внеш.	0.00121	0.1	0,1	0.10063	0.01262	0.25	0,25	0.2569	0.00052	0.01	0,01	0.01506
Перехват в пределах КЗ сотр.	0.00260	0.1	0,1	0.1100	0.00842	0.25	0,25	0.2413	0.00052	0.01	0,01	0.01506
Угрозы анализа сети	0.00402	0.1	0,1	0.1075	0.00741	0.25	0,25	0.2406	0.00348	0.1	0,1	0.08688
Угрозы выявл. по сети уч. Дан.	0.02250	0.25	0,25	0.25375	0.01716	0.5	0,5	0.4031	0.00132	0.01	0,01	0.02688
Навязывание неверной маршрутизации	0.00070	0.1	0,1	0.0975	0.00260	0.1	0,1	0.1100	0.00094	0.01	0,01	0.02125
Замена доверенного объекта	0.00070	0.1	0,1	0.0975	0.00203	0.1	0,1	0.1038	0.00051	0.01	0,01	0.01531
Внедрение неверного объекта	0.00070	0.1	0,1	0.0975	0.00258	0.1	0,1	0.0981	0.00051	0.01	0,01	0.01531
Отклонение запроса	0.00336	0.1	0,1	0.11313	0.02141	0.25	0,25	0.2406	0.00095	0.01	0,01	0.02094
Несанкц. Удал. Запуск ПО	0.00696	0.25	0,25	0.24375	0.01849	0.5	0,5	0.4531	0.00393	0.01	0,01	0.03063
Распростр. По сети вред. Прог.	0.02083	0.25	0,25	0.25375	0.00774	0.5	0,5	0.4406	0.00094	0.01	0,01	0.02125

Результаты медианы и моды для всех типов угроз оказались одинаковые, среднее арифметическое значение при округлении также отличается не более чем на 0.01. Основываясь на вышесказанном, а также на то, что значение дисперсии по каждому показателю мало, было принято решение использовать в качестве исходных данных для дальнейшего исследования информационной системы значения медианы/моды (Таблица 5).

Как показали исследования, наличие большого количества экспертов, имеющих значительный опыт работы с изучаемой информационной системой, позволяют получить первоначальные данные с высоким уровнем достоверности. Однако применение большого количества экспертов, имеющих опыт работы с изучаемой информационной системой, могут позволить себе только организации с многочисленным количеством персонала и широкой географией распределения филиалов.

Для организации хранения результатов экспертных оценок вероятностей наступления и реализации угроз безопасности ИСПДн, полученных для построения имитационной модели системы, разработана и зарегистрирована в государственном реестре программ для ЭВМ программное обеспечение, позволяющее хранить и в автоматическом режиме проводить необходимые математические расчеты с введенными данными.

Таблица 5 –Значения вероятностей, утвержденные экспертами

Наименование угрозы	Вер-ть наступления	Вер-ть реализ. без защиты	Вер-ть реализ. с защитой
Перехват акустич. информации	0,1	0,01	0,1
Перехват видовой информации	0,1	0,01	0,01
Перехват по каналам побочных наводок	0,1	0,01	0,01
Хищение ЭВМ	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, удаление, модификация информации	0,1	0,01	0,01
Вывод из строя частей ЭВМ, каналов передачи инф.	0,1	0,1	0,01
Несанкц. отключение средств защиты	0,1	0,01	0,1
Действия вредоносного ПО	0,25	0,1	0,01
Скрытый функционал ПО	0,1	0,01	0,01
Установка ПО, не связанного со служеб. деятельностью	0,1	0,1	0,01
Потеря ключей и атрибутов доступа	0,25	0,25	0,01
Случайное изменение (удаление) ПДн сотрудниками	0,1	0,01	0,01
Случайный вывод из строя средств защиты	0,1	0,01	0,01
Выход из строя АП средств	0,1	0,1	0,5
Нарушение подачи электропитания	0,1	0,25	0,1
Катаклизмы / катастрофы	0,1	0,25	0,5
Доступ, изм, удаление ПДн лицами, не допущ.	0,1	0,25	0,01
Разглаш.,модификация сотрудниками, допущенными	0,25	0,01	0,01
Перехват за переделами КЗ	0,25	0,5	0,01
Перехват в пределах КЗ внеш.	0,1	0,25	0,01
Перехват в пределах КЗ сотрудниками	0,1	0,25	0,01
Угрозы анализа сети	0,1	0,25	0,1
Угрозы выявления по сети учетных данных	0,25	0,5	0,01
Навязывание неверной маршрутизации в сети	0,1	0,1	0,01
Замена доверенного объекта	0,1	0,1	0,01
Внедрение неверного объекта	0,1	0,1	0,01
Отклонение запроса	0,1	0,25	0,01
Несанкционированный удаленный запуск ПО	0,25	0,5	0,01
Распространение по сети вредоносного ПО	0,25	0,5	0,01

База данных, используемая программным обеспечением для хранения данных, состоит из восьми таблиц (Рисунок 1)

Таблицы «Перечень угроз» и «Перечень экспертов», как следует из названия, содержат сведения о рассматриваемых угрозах и группах экспертов соответственно. Данные из указанных таблиц используются для заполнения полей в других таблицах.

Рисунок 1 - Блок-схема организации хранения и обработки информации

Таблица «Предложенные вероятности наступления угроз» содержит данные о вероятностях наступления угроз безопасности ПДн, представленные группами экспертов.

Таблицы «Предложенные вероятности реализации угроз», «Предложенные вероятности реализации угроз с имеющимися СЗИ» и «Предложенные вероятности реализации угроз при внедрении дополнительных СЗИ» содержат данные по аналогии с предыдущей таблицей.

Таблица «Значения вероятностей, рассчитанных после статистической обработки первоначальных данных» заполняется в автоматическом режиме и содержит результаты статистической обработки значений, введенных в предыдущие таблицы. Полученные значения используются головной группой экспертов при определении значений, которые будут использованы для построения имитационных моделей.

Таблица «Значения вероятностей, принятых для построения моделей» содержит значения вероятностей, утвержденные головной группой экспертов для их дальнейшего использования при построении имитационных моделей информационной системы.

1.4 Исходные данные, используемые экспертами при проведении экспертных оценок

При оценке вероятностей реализации угроз при наличии дополнительных средств защиты информации экспертной комиссией учитывались следующие организационные и технические СЗПДн:

1. Угрозы от перехвата информации по техническим каналам.

1.1. Угрозы перехвата акустической информации. В связи с тем, что запросы к базе данных, подготовка и направление ответов в определенные службы, а также между сотрудниками осуществляются в электронном виде или на бумажном носителе, данная угроза может быть реализована только при нарушении правил о неразглашении информации и передачи персональных данных по телефонным или иным каналам связи речевой информацией. Для предотвращения нарушений с личным составом проводятся регулярные занятия;

1.2. Угрозы перехвата видовой информации. В качестве защиты применяются требования к установке оборудования и порядка работы с ИСПДн. В соответствии с требованиями, компьютерный монитор устанавливается так, чтобы через окно невозможно было что-либо с него прочитать, рабочее место организовано с учетом скрытия изображения монитора от посторонних лиц, находящихся в помещении, в том числе возможное отражение изображения в зеркале или от другой поверхности; данные на бумажном носителе передаются на отправку в канцелярию сотрудниками, допущенными к обработке персональных данных, в непрозрачной папке;

1.3. Угрозы перехвата информации по каналам побочных электромагнитных излучений и наводок. Защитой от угрозы перехвата информации путем обнаружения и измерения побочных электромагнитных излучений и наводок выступают следующие условия:

а. относительно высокая кучность расположения ЭВМ;

б. все мониторы исключительно имеют жидкокристаллический дисплей;

в. все комплектующие компьютеров и периферийные устройства в основном одинаковые (так как всегда закупаются партиями), имеют одинаковые аппаратные настройки;

г. расположение ЭВМ на отдалении от границ контролируемой зоны не менее 30 метров;

д. отсутствие больших объемов персональных данных на ЭВМ, что приводит к необоснованно высоким затратам на выявление полезной информации путем анализа побочных электромагнитных излучений и наводок по сравнению с ценностью информации; сервер баз данных, в свою очередь, находится в помещении с несущими стенами и металлической дверью в металлическом коммутационном шкафу, что создает дополнительное экранирование. Также в серверной находятся постоянно работающие сплит-системы, множество иных серверов, мультиплексоры, коммутаторы, конверторы сигнала, радиостанция для записи телефонных переговоров, оборудование по приему данных о местоположении патрульных автомобилей, телефонная станция с цифровыми и аналоговыми платами коммутации, источники бесперебойного питания для каждой единицы оборудования. Большое количество оборудования, как однородного, так и разнородного по характеру обрабатываемого сигнала, создает высокий уровень зашумленности, что практически исключает возможность снятия и выделения полезной информации с ПЭМИН, находясь за пределами серверной. Сама серверная является режимным объектом, допуск в который имеется у ограниченного числа сотрудников.

2. Угрозы несанкционированного доступа к информации.

2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн.

2.1.1. Хищение ЭВМ – для предотвращения выноса какого-либо оборудования за пределы подразделения, на контрольно-пропускном пункте ведется журнал, в котором фиксируется кто и что выносит. Информация по технике (наименование, серийный и инвентарный номера), которую выносят, берется из пропуска на вынос техники, выписываемый материально-ответственным лицом. Без наличия пропуска вынос техники запрещен;

2.1.2. Хищение носителей информации. Полная база данных хранится всего на двух носителях информации: жесткие диски сервера обработки баз данных и внешний жесткий диск с резервной копией БД. Оба носителя находятся на пятом этаже административного здания за железной дверью в помещении, куда доступ имеет строго ограниченный круг лиц;

2.1.3. Вывод из строя частей ЭВМ, каналов передачи информации. Для предотвращения преднамеренного вывода из строя частей ЭВМ используется следующая защита:

а. Каждый пользователь, получая ЭВМ, расписывается в карточке закрепления материальной ценности, подтверждая, что с момента передачи за все противоправные действия, которые будут осуществлены с данной ЭВМ либо с ее помощью с иным оборудованием, он несет личную ответственность. Приказом УГИБДД утверждена инструкция «По обеспечению защиты информации Автоматизированных баз данных ГИБДД ГУВД Краснодарского края», регулирующая принципы работы с ИСПДн.

б. Каждая единица оборудования имеет свой инвентарный номер, который нанесен нестираемым маркером на корпусе. Каждый инвентарный номер закреплен за серийным номером оборудования, что, при необходимости, дает возможность установить неизменность оборудования в целом;

в. Для контроля целостности и неизменности комплектующих ЭВМ, каждый системный блок опломбирован. В случае выявления факта повреждения пломбы незамедлительно докладывается начальнику

Регионального отдела информационного обеспечения ГИБДД ГУ МВД России по Краснодарскому краю для дальнейшего доклада для принятия решения начальнику Управления ГИБДД ГУ МВД России по Краснодарскому краю;

г. В целях предотвращения вывода из строя частей ЭВМ путем программного вмешательства, каждый оператор ЭВМ работает с правами пользователя. Пользователю запрещено устанавливать новое программное обеспечение, вносить изменения в настройки операционной системы и системных приложений. Также для пользователя полностью закрыт доступ к базовой системе ввода-вывода и вместе с этим к возможности загрузки операционной системы с правами администратора с компакт диска или иного носителя информации.

Для предотвращения вывода из строя линий связи используются те же методы защиты, что и от действий нарушителей, а именно, все линии коммуникации в соответствии с нормативными документами проведены в кабель каналах, коммутаторы и т.п. находятся в металлическом запираемом шкафу;

2.1.4. Нейтрализация средств защиты. Все программные средства защиты (например, антивирусное программное обеспечение), защищены паролем администратора, без которого невозможно внести какие-либо изменения в конфигурацию либо полностью отключить защиту. Аппаратные средства защиты находятся в недоступном для пользователей месте (если это отдельное оборудование), либо ответственность за него несет сам оператор ЭВМ (если это средство для идентификации пользователей, например, электронный ключ);

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации путем несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

2.2.1. Действия вредоносного ПО (вирусов). Защитой от данного вида угроз в основном является наличие антивирусного программного обеспечения. Для наиболее эффективной работы антивируса базы вирусных регулярно

обновляются (не реже одного раза в неделю), и на всех ЭВМ раз в неделю автоматически запускается сканирование дисков на наличие угрозы;

2.2.2. Скрытый функционал системного ПО и ПО для обработки персональных данных. Для недопущения реализации данной угрозы всё программное обеспечение, прежде чем быть введено в эксплуатацию, проходит тестирование на опытных ЭВМ, а также на ЭВМ, используемых в повседневной работе, но с подключением к резервной базе данных. Ввод в эксплуатацию происходит только после подтверждения администратором безопасности надёжности и стабильности тестируемого программного обеспечения. После ввода в эксплуатацию также происходит мониторинг работы программного обеспечения с целью своевременного выявления необходимости обновления либо переходе на другое ПО;

2.2.3. Установка ПО, не связанного со служебной деятельностью. В качестве защиты используется запрет для пользователей, которыми являются все операторы ЭВМ, на установку, удаление любого программного обеспечения, что осуществляется как программными средствами, так и утверждено приказом УГИБДД ГУ МВД России по Краснодарскому краю [81];

2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, нарушения подачи электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

2.3.1. Потеря ключей и атрибутов доступа. Реализация данной угрозы практически полностью зависит от человеческого фактора. Чаще всего она проявляется в качестве элементарного «забыл», например, после длительного отпуска или командировки сотрудника. В качестве защиты от наступления данной угрозы можно выделить занятия с личным составом, направлены на донесение до слушателей понимания необходимости запоминать свои имена пользователей и пароли, а не записывать (что так же способствует защите от несанкционированного доступа к ИСПДн лиц, не допущенных к работе с ней);

2.3.2. Случайное изменение (удаление) персональных данных сотрудниками, допущенными к обработке. Для недопущения реализации данной угрозы, для доступа к базе данных введено разграничение прав доступа: большинство операторов имеют права только на чтение, остальные (кроме администраторов) – на изменение только тех параметров, которые им дозволено менять для исполнения своих функциональных обязанностей. Помимо этого, каждый день происходит регулярная сверка данных и выявление допущенных ошибок (таких, как удаление одного из полей данных, неполное введение данных и т.п.);

2.3.3. Случайный вывод из строя средств защиты. В качестве защиты от данного вида угроз используются те же методы, что и от угрозы «Нейтрализация средств защиты»;

2.3.4. Сбой аппаратных и программных средств обработки информации. Защита от реализации данного вида угроз является только регулярное профилактическое обслуживание оборудования и своевременное обновление его комплектующих или всего оборудования в целом. В связи с тем, что;

2.3.5. Нарушение подачи электропитания – каждый сервер, ЭВМ (приобретенная с 2011 года) и основные узлы коммутации имеют свой собственный резервный источник питания (источник бесперебойного питания), который поддерживает работоспособность оборудования в течение 10-30 минут. Если же становится известно, что отключение электроэнергии произошло на более длительный период, то запускают дизельный генератор. Генератор, в соответствии с нормами положенности находится в каждом подразделении. Генератор регулярно проверяется на работоспособность, однако, он может оказаться бесполезным, если авария случится на линии между генератором и административным зданием подразделения;

2.3.6. Катаклизмы / катастрофы. Организовать эффективную защиту от данного типа угроз не представляется возможным. В основном сложность построения защиты заключается в том, что защита должна строиться на этапе проектирования здания, помещения и т.п.

2.4. Угрозы преднамеренных действий внутренних нарушителей.

2.4.1. Доступ, изменение, удаление персональных данных лицами, не допущенных к их обработке. Для защиты применяются следующие меры:

а. Операторам, имеющим доступ к базе данных, запрещено хранить имена и пароли на бумажном носителе, оставлять без присмотра электронные ключи или другие атрибуты доступа;

б. Покидая рабочее место, оператор обязан выключить его или заблокировать систему, что также делается автоматически через 5-10 минут при отсутствии активности со стороны пользователя. Для разблокировки ЭВМ также необходимо ввести пароль пользователя или администратора;

в. Пользователям запрещено передавать свои учетные данные третьим лицам, использовать одно имя пользователя нескольким операторам;

г. Каждый пользователь, получая имя и пароль для доступа к ИСПДн расписывается в журнале выдачи паролей, подтверждая, что ознакомился с ответственностью, которая наступает в случае передачи своих учетных данных третьему лицу, либо разглашении информации;

2.4.2. Разглашение персональных данных, модификация, удаление сотрудниками, допущенными к ее обработке. В целях предотвращения наступления указанного типа угроз с сотрудниками на постоянной основе проводятся дополнительные занятия по правилам обработки и предоставления ПДн.

2.5. Угрозы несанкционированного доступа по каналам связи. В качестве защиты от наступления угроз, связанных с необходимостью физического подключения нарушителей (как источника угрозы) к линиям связи выделены следующие:

а. Все коммутаторы, концентраторы, маршрутизаторы и линии проводной связи (за исключением некоторого оборудования операторов связи) находятся в пределах контролируемой зоны. Наличие охраняемой огороженной территории исключает вероятность доступа к линиям связи внешних нарушителей. Наличие ограждения, колючей проволоки на ограждении,

решеток на окнах, механических и стационарных средств, препятствующих проникновению нарушителей, а также контрольно-пропускного пункта, на котором проверяются документы и регистрируются все лица, проходящие на территорию подразделения, является обязательным в соответствии с нормативными документами;

б. Отсутствие на территории подразделений беспроводных каналов связи, что исключает вероятность подключения к сети подразделения нарушителей, находящихся за пределами контролируемой зоны;

в. Все линии коммуникации проведены в кабель каналах, коммутаторы и т.п. находятся в металлическом запираемом ящике. Выполнение данных условий исключает возможность подключения нарушителей к линиям связи подразделения путем врезания в имеющийся кабель либо использования свободных портов коммутационных устройств;

г. В качестве коммутирующих устройств используются только сетевые коммутаторы. В связи с тем, что коммутатор хранит в памяти таблицу коммутации (хранящуюся в ассоциативной памяти), в которой указывается соответствие MAC-адреса узла порту коммутатора, трафик становится локализованным и не рассылается по всем сегментам сети. Данная таблица хранится постоянно, так как коммутаторы всегда находятся во включенном состоянии (за исключением случаев наступления угроз физического выхода из строя). Выполнение данных условий исключает вероятность перехвата трафика или его анализа при подключении нарушителя к коммутатору;

Адресация в локальной сети является статической, что создает дополнительные трудности для нарушителей, так как для, во-первых, необходимо вычислять используемое IP пространство и, во-вторых, сканировать сеть на наличие свободных IP адресов;

2.5.1. Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны):

2.5.1.1. Перехват вне контролируемой зоны. Для защиты от наступления данного вида угрозы все запросы к базе данных производятся только по ведомственным каналам связи, приказами Министерства внутренних дел Российской Федерации, Главного Управления МВД России по Краснодарскому краю и Управления ГИБДД ГУ МВД России по Краснодарскому краю запрещено использовать Интернет и другие внешние сети на ЭВМ, находящихся в ведомственной локальной сети, все виды установления удаленной связи строятся по технологии VPN с использованием различных методов шифрования и криптографии;

2.5.1.2. Перехват в пределах контролируемой зоны сторонними нарушителями. Для предотвращения неправомерных действий со стороны внешних нарушителей принимаются меры описанные выше;

2.5.1.3. Перехват в пределах контролируемой зоны сотрудниками. Для предотвращения неправомерных действий со стороны внутренних нарушителей помимо описанных выше мер проводятся занятия с личным составом, разъясняется какую ответственность можно понести в случае несоблюдения инструкции работы с ИСПДн;

2.5.2. Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др. Для предотвращения данной угрозы, а также угроз выявления по сети учетных данных, угрозы навязывания неверного маршрута, угрозы замены доверенного объекта в сети и угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях, применяются методы недопущения доступа внешних нарушителей к внутренней сети;

2.5.3. Угрозы типа «Отклонение запроса». Данная угроза чаще всего реализовывается в случае аппаратных или программных сбоев или недостаточности аппаратных ресурсов для обработки большого количества запросов. В качестве защиты от реализации угрозы используется мониторинг загруженности отдельных узлов коммутации и вычислительных центров для

установления момента перегрузки узла и необходимости модернизации оборудования, а также, как и в случае с угрозой сбоя аппаратных и программных средств обработки информации, используется профилактическое обслуживание оборудования и своевременное обновление его комплектующих или всего оборудования в целом.

1.5 Схема функционирования имитационной модели

Построим блок-схему функционирования имитационной модели рассматриваемой информационной системы (Рисунок 2). Исходя из блок-схемы, можно выделить две основные группы угроз: угрозы, реализация которых прерывает движение запроса, и угрозы, реализация которых не влияет на продвижение запроса. Все рассматриваемые угрозы разделены на две указанные группы специалистами, входящими в группу экспертов УГИБДД.

В итоге на выходе имитационной модели мы должны получить следующие данные: количество фактов наступления и не наступления угроз, сколько раз наступившие угрозы была парированы первоначальной системой защиты, количество угроз, которые были парированы имеющимися дополнительными СЗПДн, количество реализованных угроз, количество запросов, поступивших в систему, сколько из них успешно завершили движение и движение скольких было прекращено вследствие реализации угроз. Все перечисленные данные должны быть получены как отдельно по угрозам каждого типа, так и обобщенные по всем типам угроз.

Путем численных расчетов, используя перечисленные данные, можно будет не только выявить угрозы, актуальные для рассматриваемой ИСПДн, но и рассмотреть эффективность СЗПДн от каждого типа угроз в отдельности.

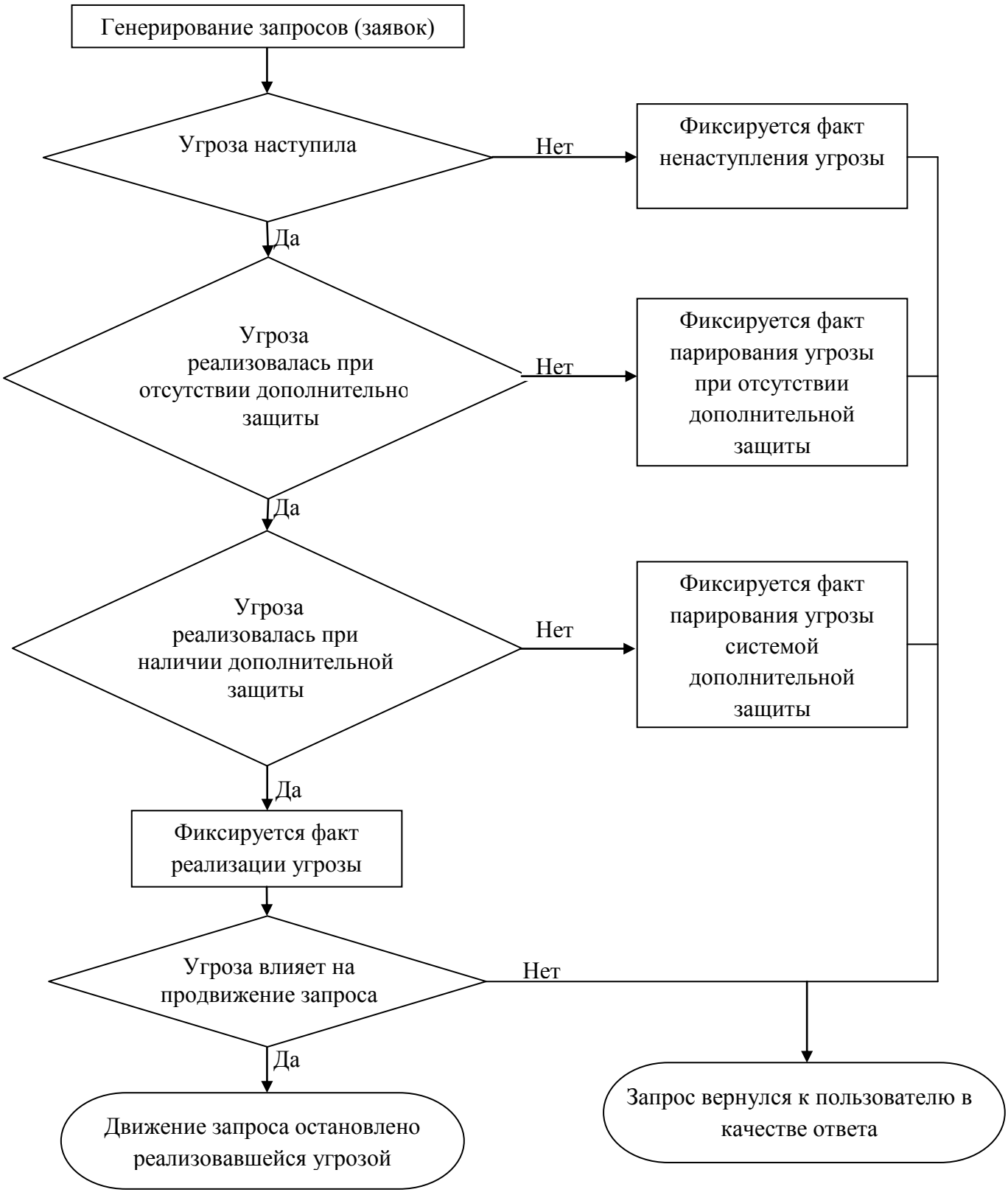

Рисунок 2 – Блок-схема функционирования имитационной модели

Перед построением имитационной модели рассмотрим процесс генерирования запроса и получения ответа. Точкой генерирования запроса и

получения ответа является оператор, который с помощью программного обеспечения обращается к базе данных и производит с ней необходимые действия (просмотр информации, изменение, добавление или удаление данных). Все действия (обращение к серверу баз данных и получение ответа от сервера) можно разделить на пять этапов:

1 этап: оператор с помощью программного обеспечения ЭВМ генерирует запрос к базе данных.

2 этап: сформированный запрос отправляется на сервер, проходя на своем пути по каналам связи, состоящим из коммутаторов, маршрутизаторов и линий связи между ними. В зависимости от канала связи, используемым оператором, данный этап можно разделить на под этапы: а) Запрос проходит маршрутизаторы и коммутаторы подразделения и попадает на маршрутизатор, отправляющий его за пределы подразделения; б) Запрос проходит расстояние между подразделением и Управлением и попадает на маршрутизатор Управления; в) Запрос от маршрутизатора Управления через коммутаторы доходит до сервера.

3 этап: сервер обрабатывает запрос, выполняет необходимые действия и отправляет ответ оператору.

4 этап: ответ на запрос проходит от сервера до ЭВМ оператора. Т.к. линии связи и среда передачи данных остается неизменной, данный этап также как и второй разделяется на 3 подэтапа, которые выполняются в обратном порядке.

5 этап: ответ на запрос с помощью программного обеспечения передается оператору и цикл завершается.

В связи с тем, что рассматриваемая информационная система является территориально-распределенной, её модель должна содержать множество узлов и ответвлений. Для детального изучения ИСПДн и упрощения окончательного вида имитационной модели группой экспертов принято решение разработать и рассмотреть имитационные модели отдельных сегментов. Всего выделено пять общих сегментов, из которых в дальнейшем можно построить имитационную модель системы в целом:

1. Сегмент, на котором запрос поступает от оператора к ЭВМ;
2. Сегмент, на котором запрос проходит от ЭВМ до коммутатора, объединяющего несколько ЭВМ и маршрутизатор, либо управляемый коммутатор;
3. Сегмент, на котором запрос поступает от коммутатора к маршрутизатору, позволяющего передавать данные между подразделениями, либо управляемому коммутатору, объединяющему несколько управляемых коммутаторов в случае продвижения запроса в пределах одного подразделения;
4. Сегмент, на котором запрос перемещается между двумя маршрутизаторами по арендуемым или ведомственным каналам связи либо между двумя управляемыми коммутаторами;
5. Сегмент, на котором запрос поступает от коммутатора, объединяющего несколько серверов, к серверу обработки персональных данных.

По каждому сегменту запрос или ответ может двигаться в обоих направлениях, при этом вероятности реализации угроз будут оставаться неизменными.

1.6 Выводы

Проведенный анализ имеющейся научной литературы показал, что вопросы определения угроз безопасности информации, актуальных для какой-либо информационной системы, в настоящее время изучаются в недостаточной степени. Причем следует отметить, то проблемы защиты информации от различных угроз активно обсуждаются и постоянно предлагаются новые методы защиты как производителями средств защиты информации, так и в научных публикациях и обсуждаются на научных конференциях. Однако методы определения типов угроз, защиту от которых необходимо внедрять в

информационную систему, а также методы определения целесообразности внедрения рассматриваются крайне редко.

Основной проблемой, препятствующей проведению мероприятий по определению актуальных угроз безопасности ПДн, является отсутствие первоначальных данных, которые необходимы для изучения системы. Получить необходимые данные, как правило, возможно только с использованием метода экспертных оценок. Однако для получения достоверных данных необходимо большое количество экспертов, подробно изучивших поведение системы в различных ситуациях на протяжение длительного промежутка времени. В случае с рассматриваемой информационной системой «Информационные ресурсы УГИБДД» методом экспертных оценок воспользовались без привлечения внешних экспертов, тем самым сэкономив значительный объём финансовых средств и, в то же время, получив результаты, основанные на опыте использования системы на продолжительном промежутке времени (более пяти лет). Как показали проведенные исследования, наличие большого количества экспертов, имеющих значительный опыт работы с изучаемой информационной системой, полученные результаты имеют высокую степень достоверности. Это подтверждается низким значением дисперсии для всех исследуемых параметров и высоким уровнем схожести таких параметров, как среднее арифметическое представленных результатов, их моды и медианы.

Однако применение большого количества экспертов, имеющих опыт работы с изучаемой информационной системой, могут позволить себе только организации с многочисленным количеством персонала и широкой географией распределения филиалов. В случае отсутствия возможности привлечения для изучения сложной информационной системы экспертов из числа имеющегося персонала, расходы на проведение расчётов первоначальных данных могут оказаться несоизмеримо высокими по сравнению с эффектом, полученным в результате выявления актуальных угроз безопасности ПДн и оценки имеющихся средств защиты.

В ходе исследования рассмотрены варианты исследования систем при помощи их моделирования. Из множества существующих видов моделирования для изучения поведения информационной системы «Информационные ресурсы Управления ГИБДД» выбрано имитационное моделирование. Данный выбор в первую очередь обусловлен тем, что построение модель не требует от исследователя глубоких познаний математического аппарата, используемого при построении, и позволяет наглядно в понятной для неподготовленного человека продемонстрировать результат

Помимо этого проведенные исследования показали, что для описания функционирования имитационной модели сложной информационной системы, состоящей из множества однотипных основных узлов прохождения запроса, можно воспользоваться универсальной блок-схемой функционирования такого узла. Данный подход позволяет существенно сократить описание.

ГЛАВА 2. ИМИТАЦИОННЫЕ МОДЕЛИ СЕГМЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Построение имитационной модели сегмента «Коммутатор – сервер»

Построим имитационную модель для каждого сегмента в отдельности. Изначально рассмотрим сегмент, на котором запрос поступает к серверу баз данных от коммутатора, объединяющего серверы и коммуникационный узел. Угрозы, у которых присутствует вероятность реализации на данном сегменте выделены группой экспертов, созданной из специалистов, отвечающих за информационные подсистемы системы «Информационные ресурсы УГИБДД» (Таблица 6).

Опишем общую схему функционирования предложенной имитационной модели сегмента информационной системы. Запрос генерируется и продвигается от коммутатора до сервера по каналу связи, представленному в виде соединительной линии, на которой расположены точки наступления угроз. Когда запрос проходит точку наступления угрозы, то дальнейшее его продвижение зависит от вероятности наступления угрозы. Если угроза не наступила, то запрос продолжает продвижение, а в счетчике, привязанному к данной угрозе, фиксируется факт того, что угроза не наступила, если же угроза наступила, то запрос попадает на альтернативный путь продвижения и в счетчике фиксируется факт того, что угроза наступила. Выделено два основных типов угроз: влияющих на продвижение запроса, например, угроза типа «Отклонение запроса», когда запрос прекращает движение, и угрозы, не влияющие на дальнейшее продвижение, например, угроза выявления по сети учетных данных, после наступления которых запрос продолжает движение.

Для описания процесса продвижения запроса построим Q-схему наступления модели. Q-схема наступления модели построена из двух основных элементов: наступление угрозы, препятствующей дальнейшему продвижению

модели (Рисунок 3), и наступление угрозы, не влияющей на продвижение запроса (Рисунок 4).

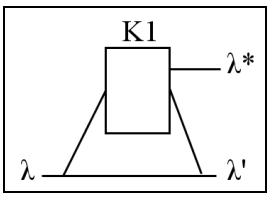

Рисунок 3 -Q-схема наступления угрозы, препятствующей продвижению запроса

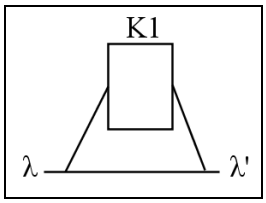

Рисунок 4 -Q-схема наступления угрозы, не влияющей на продвижение запроса

где λ – входной поток, λ′ - выходной поток, λ* - поток заявок, прервавших движение, K1 –блок наступления угрозы (угроза наступила).

В ходе построения модели в качестве первоначальных данных были использованы результаты проведенных экспертных оценок (Таблица 6):

Таблица 6 – Значение вероятностей наступления угроз на сегменте «Коммутатор – сервер»

Наименование угрозы	Вероятность наступления угрозы
Хищение ЭВМ	0.1
Хищение носителей информации	0.1
Хищение ключей и атрибутов доступа	0.1
Хищения, модификации, удаление информации	0.1
Вывод из строя частей ЭВМ, каналов передачи информации	0.1
Действия вредоносного ПО (вирусов)	0.25
Скрытый функционал системного ПО и ПО для обработки ПДн	0.1
Сбой аппаратных и программных средств обработки информации	0.1
Нарушение подачи электропитания	0.1
Катаклизмы / катастрофы	0.1
Доступ, изменение, удаление персональных данных лицами, не допущенными к обработке	0.1
Разглашение персональных данных, модификация, удаление сотрудниками	0.25
Нейтрализация средств защиты	0.1
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, сторонними нарушителями в пределах КЗ)	0.1
Угроза «Анализ потока информации в сети» (перехват информации сотрудниками)	0.1
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов и др.	0.1
Угрозы выявления по сети учетных данных	0.25

Продолжение таблицы 6

Наименование угрозы	Вероятность наступления угрозы
Угрозы навязывания неверной маршрутизации в сети	0.1
Угрозы замены доверенного объекта в сети	0.1
Угрозы внедрения неверного объекта как в пределах системы, так и во внешних сетях	0.1
Угрозы типа «Отклонение запроса»	0.1
Угрозы несанкционированного удаленного запуска ПО	0.25
Угрозы распространения по сети вредоносного ПО	0.25

Общая схема наступления угроз приведена на Рисунок 7.

Для получения результатов, достоверность которых будет достаточной для изучения поведения системы, в ходе проведения экспериментов группой экспертов было принято решение использовать 1 000 000 единиц модельного времени (условных единиц времени, используемых в среде моделирования). За данный промежуток модельного времени, то есть за время проведения одного эксперимента, генерируется в среднем 5 000 000 запросов.

Изучив результаты проведенных экспериментов с предложенной моделью вычислено, что лишь 43,02% запросов завершают движение, то есть большая часть сгенерированных запросов прекращает движение вследствие наступления угроз. Но так как информационных систем с отсутствием хоть какой-нибудь защиты данных в принципе не может существовать, предложенная модель доработана путем добавления на альтернативные линии связи (линии, на которые попадает запрос, если угроза наступила) точек реализации угрозы.

Когда угроза наступила, то есть запрос перешел на альтернативный путь движения, запрос проходит точку реализации угрозы, после чего он либо вернется на первоначальный путь движения (в случае, если угроза нейтрализована), либо попадает на путь реализации угрозы, где уже в зависимости от типа угрозы либо прекращает движение, либо продолжает. Вероятности реализации угрозы также представлены группой экспертов (Таблица 7).

После добавления в предложенную имитационную модель вероятностей реализации, модель приняла вид, представленный на Рисунок 8.

Таблица 7 – Значения вероятностей реализации угроз на сегменте «Коммутатор – сервер»

Наименование угрозы	Вер-ть реализации угрозы
Хищение ЭВМ	0.01
Хищение носителей информации	0.01
Хищение ключей и атрибутов доступа	0.01
Хищения, модификации, удаления информации	0.01
Вывод из строя частей ЭВМ, каналов передачи информации	0.1
Действия вредоносного ПО (вирусов)	0.1
Скрытый функционал ПО	0.01
Сбой аппаратных и программных средств обработки информации	0.1
Нарушение подачи электропитания	0.25
Катаклизмы / катастрофы	0.25
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.25
Разглашение персональных данных, модификация, удаление сотрудниками	0.01
Нейтрализация средств защиты	0.01
Анализ потока информации в сети (перехват сторонними нарушителями в пределах КЗ)	0.25
Анализ потока информации в сети (перехват сотрудниками в пределах контролируемой зоны)	0.25
Угрозы анализа сети, нацеленные на выявление типа системного ПО, адресов и т.д.	0.25
Угрозы выявления по сети учетных данных	0.5
Угрозы навязывания неверного маршрута сети	0.1
Угрозы замены доверенного объекта в сети	0.1
Угрозы внедрения неверного объекта как в пределах инф. системы, так и во внешних сетях	0.1
Угрозы типа «Отклонение запроса»	0.25
Угрозы несанкционированного удаленного запуска ПО	0.5
Угрозы распространения по сети вредоносного ПО	0.5

Q-схема реализации угроз, препятствующей дальнейшему продвижению заявки приняла следующий вид (Рисунок 5):

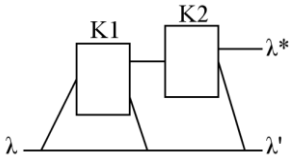

Рисунок 5 - Q-схема реализации угрозы, препятствующей дальнейшему продвижению запроса

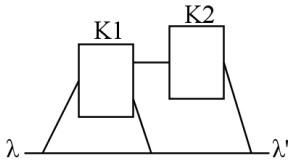

Рисунок 6 -Q-схема реализации угрозы, не влияющей на дальнейшее продвижение запроса

где λ – входной поток, λ´ - выходной поток, λ* - поток заявок, прервавших движение, К1 – блок наступления угрозы, К2 – блок реализации угрозы.

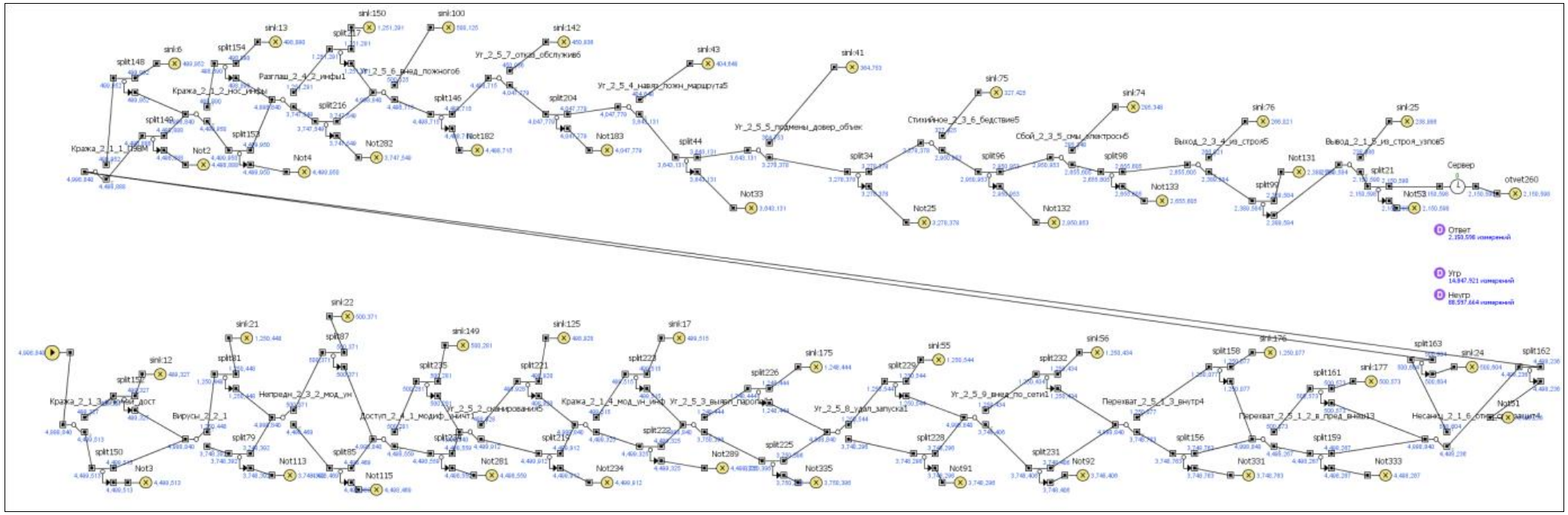

Рисунок 7 – Схема наступления угроз на сегменте «Коммутатор – сервер». Изображение получено с монитора.

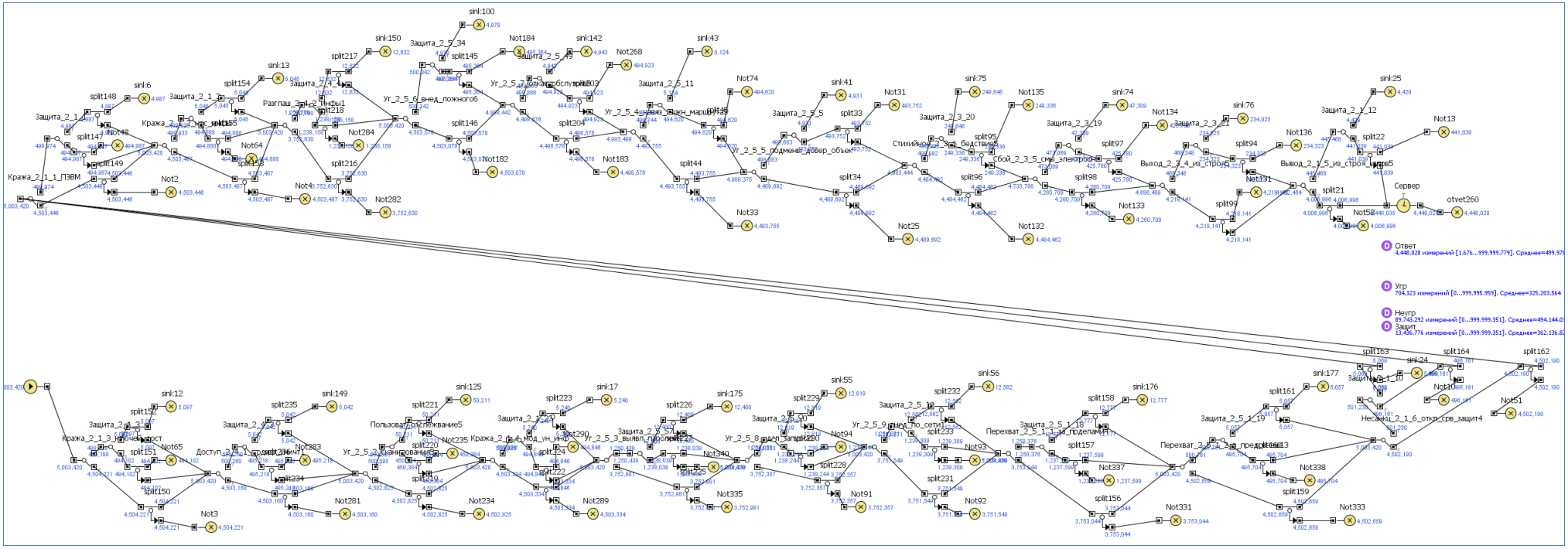

Рисунок 8 –Схема реализации угроз на сегменте «Коммутатор – сервер» (скриншот компьютерной реализации модели)

На следующем этапе имитационная модель, в которой учтены и вероятности наступления угроз, и вероятности реализации, вновь расширена: в ней учтены дополнительные меры защиты от реализации угроз, применяемые в информационной системе. Указанные меры защиты добавлены в модель также в качестве точки на пути движения запроса (альтернативный путь, на который попадает запрос в случае, если угроза реализована). При прохождении добавленной точки запрос с вероятностью, также предложенной группой экспертов (Таблица 8), либо попадает на альтернативный путь движения (угроза реализована при наличии дополнительных средствах защиты), либо возвращается на первоначальный путь продвижения.

Таблица 8 – Значения вероятностей реализации угроз при наличии дополнительных СЗПДн на сегменте «Коммутатор – сервер»

Наименование угрозы	Вер-ть реализац с доп. защитой
Хищение ЭВМ	0.01
Хищение носителей информации	0.01
Хищение ключей и атрибутов доступа	0.01
Хищение, модификация, удаления информации	0.01
Вывод из строя частей ЭВМ, каналов передачи информации	0.01
Действия вредоносного ПО (вирусов)	0.01
Скрытый функционал ПО	0.01
Сбой аппаратных и программных средств обработки информации	0.5
Нарушение подачи электропитания	0.1
Катаклизмы / катастрофы	0.5
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.01
Разглашение персональных данных, модификация, удаление сотрудниками, допущенными к их обработке	0.01
Нейтрализация средств защиты	0.1
Анализ потока информации в сети (перехват сторонними нарушителями в пределах КЗ)	0.01
Анализ потока информации в сети (перехват сотрудниками в пределах контролируемой зоны)	0.01
Угрозы анализа сети, нацеленные на выявление типа системного ПО, адресов и т.д.	0.1
Угрозы выявления по сети учетных данных	0.01
Угрозы навязывания неверного маршрута сети	0.01
Угрозы замены доверенного объекта в сети	0.01
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.01
Угрозы типа «Отклонение запроса»	0.01
Угрозы несанкционированного удаленного запуска ПО	0.01
Угрозы распространения по сети вредоносного ПО	0.01

Таким образом, для того чтоб угроза реализовалась, она сначала с определенной долей вероятности должна наступить (запрос при прохождении точки наступления попадает на альтернативный путь), затем реализоваться (запрос при прохождении точки реализации вновь попадает на альтернативный путь), после чего реализоваться при наличии дополнительных мер защиты. Если же на одном из этапов угроза не реализована, то запрос возвращается на основной путь продвижения, а в счетчик фиксируется факт нейтрализации угрозы.

Численные расчеты результатов экспериментов показали, что количество запросов, завершивших движение увеличилось до 88,89% от количества сгенерированных.

Построим Q-схему функционирования имитационной модели (Рисунок 9).

В результате схема модели реализации угроз приняла вид, представленный на Рисунок 10.

Проанализировав полученные результаты экспериментов с моделью рассчитана доля запросов, завершивших движение до сервера, от количества запросов, поступивших в рассматриваемый сегмент информационной системы (97,89%), установлено примерное количество реализовавшихся угроз на один запрос (0,029 или, что равносильно, одна угроза на 35 поступивших запросов), а также вычислен процент угроз, реализованных в процессе функционирования системы, от количества реализованных, нереализованных и не наступивших угроз (0,13%).

В целях выявления угроз, которые наиболее значимо влияют на конечный результат, результаты реализации угроз рассмотрены отдельно от остальных результатов измерений (Таблица 9).

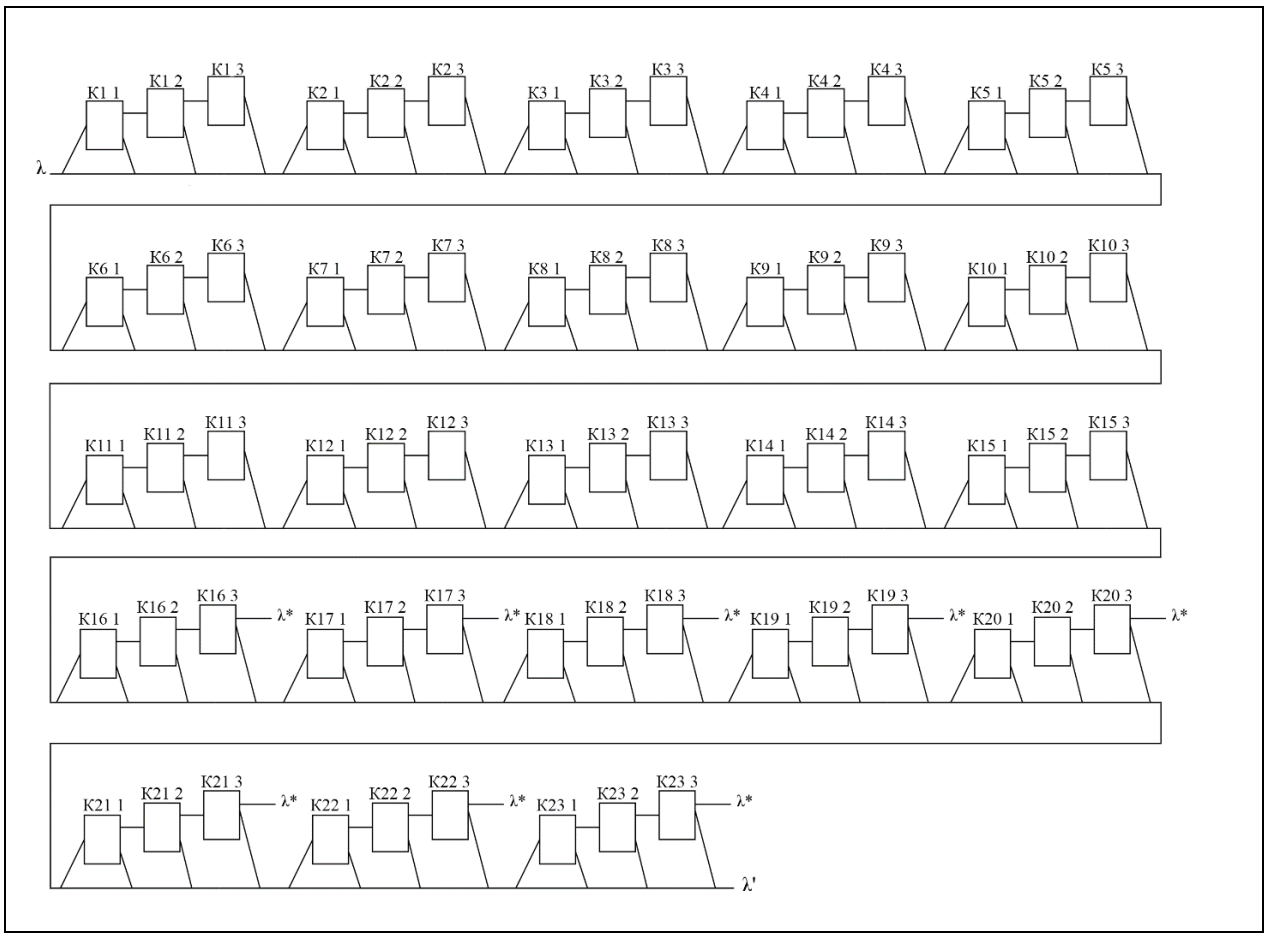

Рисунок 9 - Q-схема реализации угроз при наличии дополнительных СЗПДн на сегменте «Коммутатор – сервер»

где λ – входной поток, λ´ - выходной поток, λ* - заявки, прервавшие движение, Kn 1 – блок наступления n-ой угрозы, Kn2 – блок реализации n-ой угрозы, Kn 3 – блок реализации n-ой угрозы при наличии дополнительных средств защиты, при n=1, 2 … 23 – угрозы, которые могут наступить на рассматриваемом сегменте по мнению группы экспертов.

Проведенные эксперименты с имитационной моделью показали, что к наиболее вероятным угрозам относятся следующие:

Катаклизмы / катастрофы – 42,38% от общего количества реализовавшихся угроз;

Сбой аппаратных и программных средств– 16,53%;

Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, незаблокированных портов и служб, активных соединений и др. – 8,44%;

Нарушение подачи электропитания – 8,32%.

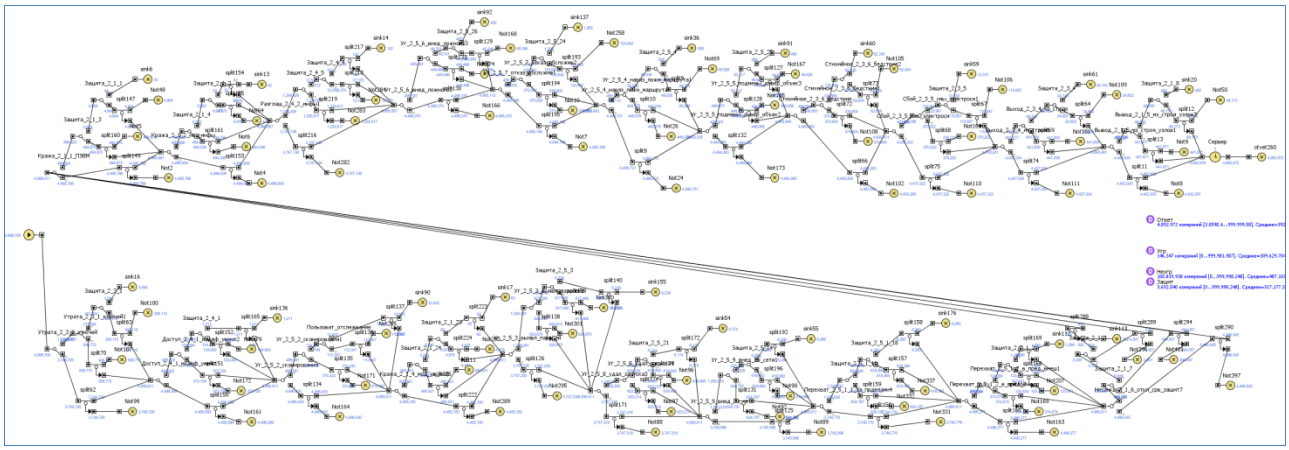

Рисунок 10 –Схема реализации угроз при наличии дополнительных СЗПДн на сегменте «Коммутатор – сервер» (скриншот компьютерной реализации модели)

Таблица 9 –Процент количества реализованных угроз на сегменте «Коммутатор – сервер»

Наименование угрозы	Коли-чество угроз реализ при нал. защиты	% от кол-ва угроз с защ. от общ. кол-ва
Действия вредоносного ПО (вирусов)	1249	0.847
Скрытый функционал ПО	54	0.037
Хищение ключей и атрибутов доступа	3138	2.127
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	1302	0.883
Угрозы анализа сети, нацеленные на выявление незаблокированных портов и др.	12454	8.443
Хищение, модификация, удаление информации	53	0.036
Угрозы выявления по сети учетных данных	6117	4.147
Угрозы несанкционированного удаленного запуска ПО	6303	4.273
Угрозы распространения по сети вредоносного ПО	6135	4.159
Перехват в пределах КЗ внешними нарушителями	6249	4.237
Перехват в пределах КЗ внутренними нарушителями	1220	0.827
Нейтрализация средств защиты	484	0.328
Хищение ЭВМ	55	0.037
Хищение носителей информации	50	0.034
Разглашение персональных данных, модификация, удаление сотрудниками	139	0.094
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	535	0.363
Угрозы типа «Отклонение запроса»	1272	0.862
Угрозы навязывания неверной маршрутизации в сети	481	0.326

Продолжение таблицы 9

Наименование угрозы	Коли-чество угроз реализ при нал. защиты	% от кол-ва угроз с защ. от общ. кол-ва
Угрозы замены доверенного объекта в сети	539	0.365
Катаклизмы / катастрофы	62511	42.381
Нарушение подачи электропитания	12268	8.317
Сбой аппаратных и программных средств обработки информации	24374	16.525
Вывод из строя частей ЭВМ, каналов передачи информации	517	0.351

Для того, чтобы оценить уровень значимости средств защиты от каждого типа угроз в отдельности (рассматриваются только те угрозы, которые выделены группой экспертов для данного сегмента информационной системы), из модели поочередно убиралась защита от каждой угрозы, после чего проводились эксперименты. Результаты, полученные в ходе экспериментов, представлены в Таблица 10.

Таблица 10 – Результаты измерений на сегменте «Коммутатор – сервер»

Наименование угрозы	Количество запросов	Количество завершенных запросов	Количество реализовавшихся угроз	Количество не реализовавшихся угроз	Кол-во не реализовавшихся угроз, вследствие действия защиты	Количество угроз, реализовавшихся при отсутствии защиты
Действия вредоносного ПО (вирусов)	4993880	4887904	272146	110570668	3693680	125354
Скрытый функционал ПО	5004085	4897503	153710	110795699	3822027	5017
Хищение ключей и атрибутов доступа	4993995	4585763	447670	104025090	3291294	311882
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	4996795	4891651	269834	110644307	3693011	124048
Угрозы анализа сети	4996170	4890610	259825	110624849	3706289	124874
Хищение, модификация, удаление информации	4995690	4890601	152116	110617864	3812089	5094
Угрозы выявления по сети уч. данных	5006345	4900374	766846	110854423	3203743	625195
Угрозы несанкционированного удаленного запуска ПО	5010135	4904519	767245	110935740	3209926	625637
Угрозы распространения по сети вредоносного ПО	5010425	4904393	767409	110941787	3210148	625337
Перехват в пределах КЗ внешними нарушителями	5009280	4903336	767176	110915088	3207525	625599
Перехват в пределах КЗ сотрудниками	4997005	4891839	270879	110645451	3695578	124919
Нейтрализация средств защиты	5002770	4896921	152267	110768690	3820155	4976
Хищение ЭВМ	4998260	4887275	152679	110620724	3815023	4932
Хищение носителей информации	5008410	4902003	1538321	110895701	3821578	5031
Разглашение персональных данных	4996240	4890413	160126	110627271	3805936	12559
Угрозы внедрения неверного объекта	4997140	4843243	195975	110305027	3764343	50168
Угрозы типа «Отклонение запроса»	4993445	4767220	268333	109840314	3685929	124753

Продолжение таблицы 10

Угрозы навязывания неверной маршрутизации в сети	5005415	4851313	196030	110585265	3776081	49818
Угрозы замены доверенного объекта в сети	4998825	4835459	195480	110272454	3762298	50099
Катаклизмы / катастрофы	4997210	4830581	208443	110468930	3753644	123972
Нарушение подачи электропитания	4993655	4777905	257955	110351215	3703004	122878
Сбой аппаратных и программных средств обработки информации	5001575	4871065	172243	110719810	3797247	49088
Вывод из строя частей ЭВМ, каналов передачи информации	5000260	4845369	196936	110711931	3774326	49355

На основе результатов, полученных в ходе экспериментов с моделью, рассчитаны следующие значения (Таблица 11): процент количества запросов, завершивших движение, от количества сгенерированных; процент количества реализовавшихся угроз, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от количества нереализованных угроз; процент количества реализованных угроз, защита от которых не учитывалась в ходе проведения эксперимента с моделью, от общего количества реализованных угроз.

В ходе анализа результатов, приведенных в таблице 11, можно выделить угрозы, отсутствие защиты от которых наиболее значимо влияет на конечный результат. Среди таких угроз наибольшее влияние оказывает отсутствие зашиты от угрозы потери ключей и атрибутов доступа (количество запросов, дошедших до окончания модели, сократилось с 97,89% до 91,83%). Также снижение завершенных запросов до 95,47% и 95,68% приводит отсутствие защиты от угрозы типа «Отклонение запроса» и нарушение подачи электропитания соответственно. Отсутствие защиты от остальных угроз влияет на конечный результат в менее значимой мере (не более 1,5%). Также отсутствие защиты виляет на угрозу хищения носителей информации, при отсутствии защиты от которой процент реализованных угроз от количества

реализованных, нереализованных и не наступивших, увеличивается с 0,13 до 1,32.

Таблица 11 –Результаты расчетов значений на сегменте «Коммутатор – сервер»

Наименование угрозы	% пройден-ных запросов	% реализ. угроз от общ кол-ва	% кол-ва угроз, предотвращ. с-мой защиты, от общ. кол-ва угроз	% кол-ва угроз, предотвращ. с-мой защиты, от кол-ва нереализ. угроз	% кол-ва реализ. угроз, без защиты, от общ. кол-ва реализ угроз
Действия вредоносного ПО (вирусов)	97.878	0.238	3.225	3.341	46.061
Скрытый функционал ПО	97.870	0.134	3.330	3.450	3.264
Хищение ключей и атрибутов доступа	91.826	0.415	3.054	3.164	69.668
Доступ, изменение, удаление ПДн лицами, не допущенными к их обработке	97.896	0.235	3.222	3.338	45.972
Угрозы анализа сети	97.887	0.227	3.234	3.350	48.061
Хищение, модификация, удаление информации	97.896	0.133	3.327	3.446	3.349
Угрозы выявления по сети учетных данных	97.883	0.668	2.790	2.890	81.528
Несанкционированный удаленный запуск ПО	97.892	0.668	2.793	2.894	81.543
Угрозы распространения по сети вредоносного ПО	97.884	0.668	2.793	2.894	81.487
Перехват в пределах КЗ внешними нарушителями	97.885	0.668	2.792	2.892	81.546
Перехват в пределах КЗ сотрудниками	97.895	0.236	3.224	3.340	46.116
Нейтрализация средств защиты	97.884	0.133	3.329	3.449	3.268
Хищение ЭВМ	97.780	0.133	3.329	3.449	3.230
Хищение носителей информации	97.875	1.323	3.287	3.446	0.327
Разглашение персонал.данных	97.882	0.140	3.321	3.440	7.843
Угрозы внедрения неверного объекта	96.920	0.172	3.294	3.413	25.599
Угрозы типа «Отклонение запроса»	95.470	0.236	3.239	3.356	46.492
Угрозы навязывания неверной маршрутизации в сети	96.921	0.171	3.296	3.415	25.413
Угрозы замены доверенного объекта в сети	96.732	0.171	3.294	3.412	25.629
Катаклизмы / катастрофы	96.666	0.182	3.280	3.398	59.475
Нарушение подачи электропитания	95.680	0.226	3.239	3.356	47.635
Сбой аппаратных и программных средств	97.391	0.150	3.311	3.430	28.499
Вывод из строя частей ЭВМ, каналов передачи инф-ции	96.902	0.172	3.291	3.409	25.061

Эффективность средств защиты также можно оценить, сравнив процент реализации конкретной угрозы от общего количества реализованных угроз с

процентом количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз (Таблица 12).

Таблица 12 –Сравнение процентов реализации угроз на сегменте «Коммутатор – сервер»

Наименование угрозы	% реализ. угрозы, с защитой, от общ. кол-ва реализ угроз	% реализ. угрозы, без защиты, от общ. кол-ва реализ угроз
Действия вредоносного ПО (вирусов)	0.847	46.061
Скрытый функционал ПО	0.037	3.264
Хищение ключей и атрибутов доступа	2.127	69.668
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.883	45.972
Угрозы анализа сети, нацеленные на выявл. активных соединений и т.д.	8.443	48.061
Хищение, модификация, удаление информации	0.036	3.349
Угрозы выявления по сети учетных данных	4.147	81.528
Угрозы несанкционированного удаленного запуска ПО	4.273	81.543
Угрозы распространения по сети вредоносного ПО	4.159	81.487
Перехват в пределах КЗ внешн. нарушителями	4.237	81.546
Перехват в пределах КЗ сотрудниками	0.827	46.116
Нейтрализация средств защиты	0.328	3.268
Хищение ЭВМ	0.037	3.230
Хищение носителей информации	0.034	0.327
Разглашение перс. данных, модификация, удаление сотрудниками	0.094	7.843
Угрозы внедрения неверного объекта	0.363	25.599
Угрозы типа «Отклонение запроса»	0.862	46.492
Угрозы навязывания неверной маршрутизации в сети	0.326	25.413
Угрозы замены доверенного объекта в сети	0.365	25.629
Катаклизмы / катастрофы	42.381	59.475
Нарушение подачи электропитания	8.317	47.635
Сбой аппаратных и программных средств обработки информации	16.525	28.499
Вывод из строя частей ЭВМ, каналов передачи информации	0.351	25.061

Исходя из результатов, представленных в Таблица 12, можно сделать вывод, что в целом система защиты ИСПДн от реализации угроз является эффективной. Вероятность реализации таких угроз, как угрозы сбоя аппаратных и программных средств обработки информации и наступления катаклизмов или катастрофы, достаточно высокая и, в то же время, наличие защиты кардинальным образом не влияет на общий результат. Внедрить эффективную защиту от указанных угроз не представляется возможным в связи

с тем, что их наступление и реализация лишь в малой доли зависит от регулируемых факторах, и, в основном, носят спонтанный характер.

2.2 Построение имитационной модели сегмента «Электронная вычислительная машина – коммутатор»

Процесс построения имитационной модели сегмента «ЭВМ – коммутатор» аналогичен процессу построения имитационной модели сегмента «Коммутатор – сервер». Общая схема функционирования имитационной модели сегмента аналогично схеме, описанной в параграфе 2.1, представляет собой соединительную линию (канал связи) между ЭВМ и маршрутизатором подразделения, по которой движется запрос. На указанной линии также расположены точки наступления угроз, проходя которые запрос либо продолжает движение и фиксируется факт того, что угроза не наступила, либо с вероятностью наступления угрозы запрос продолжает движение по альтернативному пути и фиксируется факт наступления угрозы. Во втором случае запрос также может либо продолжить движение, если угроза не влияет на его продвижение, например, угроза анализа сети, нацеленная на выявление типа системного ПО, сетевых адресов ЭВМ информационной системы и т.п., либо остановиться, если угроза влияет на его продвижение, например нарушение подачи электропитания.

Для определения вероятности наступления угроз при построении модели использованы данные, полученные с привлечением экспертов (Таблица 13).

Вид компьютерной реализации наступления угроз представлен на Рисунок 11.

По результатам многократных экспериментов с моделью рассчитан процент количества запросов, завершивших движение, от количества сгенерированных запросов (32,28%).

На следующем этапе предложенная модель расширена путем добавления вероятностей реализации угроз, предоставленных группой экспертной (Таблица 14). Данные вероятности по аналогии с предыдущей моделью добавлены в виде точки реализации угрозы, расположенной на альтернативном пути продвижения запроса.

Таблица 13 – Значения вероятностей наступления угроз на сегменте «ЭВМ – коммутатор»

Наименование угрозы	Вероятность наступления угрозы
Угрозы несанкционированного удаленного запуска ПО	0.25
Угрозы распространения по сети вредоносного ПО	0.25
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др.	0.1
Доступ, изменение, удаление ПДн лицами, не допущенными к их обработке	0.1
Угрозы выявления по сети учетных данных	0.25
Перехват в пределах контролируемой зоны внешними нарушителями	0.1
Перехват в пределах контролируемой зоны внутренними нарушителями	0.1
Угрозы навязывания неверной маршрутизации в сети	0.1
Потеря ключей и атрибутов доступа	0.25
Угрозы внедрения неверной объекта как в ИСПДн, так и во внешних сетях	0.1
Угрозы замены доверенного объекта в сети	0.1
Катаклизмы / катастрофы	0.1
Нарушение подачи электропитания	0.1
Сбой аппаратных и программных средств обработки информации	0.1
Угрозы типа «Отклонение запроса»	0.1
Вывод из строя частей ЭВМ, каналов передачи информации	0.1

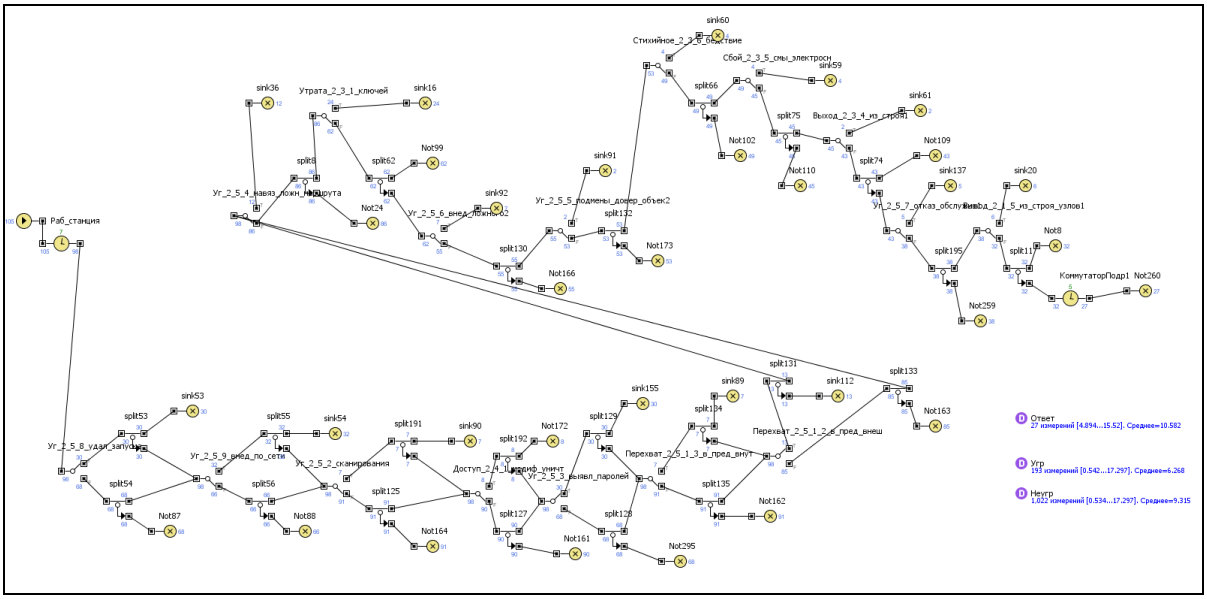

Рисунок 11 –Общая схема наступления угроз на сегменте «ЭВМ – коммутатор» (скриншот компьютерной реализации модели)

Вид компьютерной реализации модели после добавления вероятностей реализации представлен на Рисунок 12. Численные расчеты результатов экспериментов показали, что количество запросов, завершивших движение увеличилось до 82,65% от количества сгенерированных.

Таблица 14 – Значения вероятностей реализации угроз на сегменте «ЭВМ – коммутатор»

Наименование угрозы	Вероятность наступления угрозы	Вероятность реализации наступивших угроз
Угрозы несанкционированного удаленного запуска ПО	0.25	0.5
Угрозы распространения по сети вредоносного ПО	0.25	0.5
Угрозы анализа сети, нацеленные на выявление активных соединений, типа системного ПО и др.	0.1	0.25
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.1	0.25
Угрозы выявления по сети учетных данных	0.25	0.5
Перехват в пределах контролируемой зоны внешними нарушителями	0.1	0.25
Перехват в пределах контролируемой зоны внутренними нарушителями	0.1	0.25
Угрозы навязывания неверной маршрутизации в сети	0.1	0.25
Потеря ключей и атрибутов доступа	0.25	0.5
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.1	0.25
Угрозы замены доверенного объекта в сети	0.1	0.25
Катаклизмы / катастрофы	0.1	0.25
Нарушение подачи электропитания	0.1	0.25
Сбой аппаратных и программных средств обработки информации	0.1	0.25
Угрозы типа «Отклонение запроса»	0.1	0.25
Вывод из строя частей ЭВМ, каналов передачи информации	0.1	0.25

На следующем этапе имитационная модель сегмента, в которой учтены и вероятности наступления угроз, и вероятности реализации, вновь расширена: в ней учтены дополнительные меры защиты от реализации угроз, применяемые в информационной системе. Указанные меры защиты также добавлены в модель в качестве точки на альтернативном пути движения запроса. При прохождении добавленной точки запрос с вероятностью, также предложенной группой

экспертов (Таблица 15), либо попадает на альтернативный путь движения, либо возвращается на первоначальный путь продвижения.

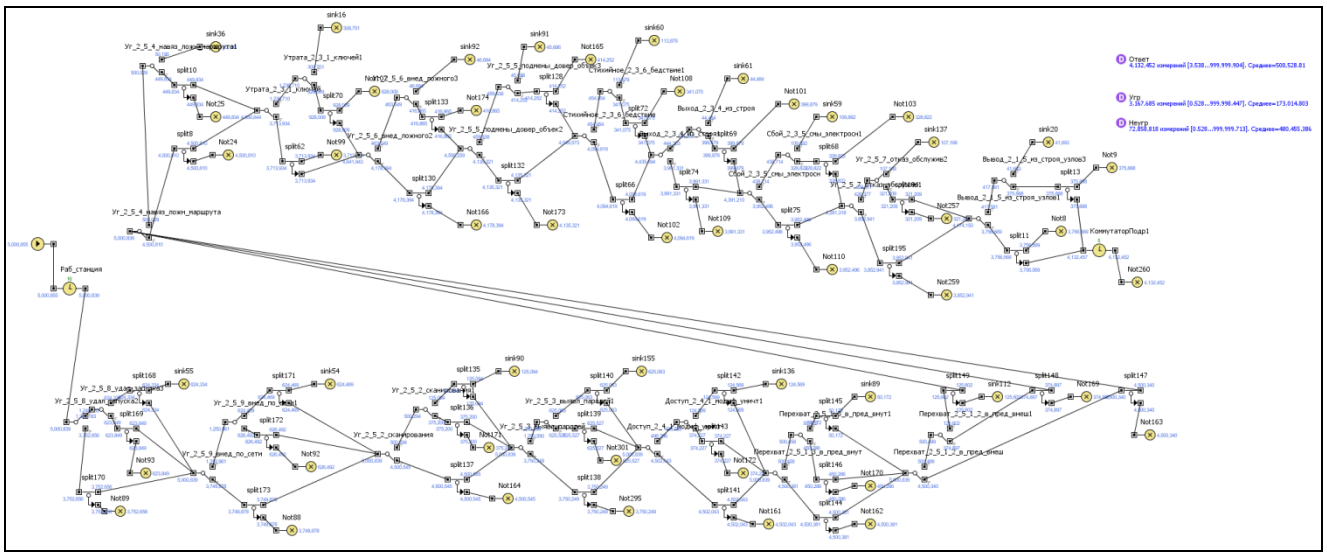

Рисунок 12 –Схема реализации угроз на сегменте «ЭВМ – коммутатор» (скриншот компьютерной реализации модели)

Таблица 15 – Значения вероятностей реализации угроз при наличии дополнительных СЗПДн на сегменте «ЭВМ – коммутатор»

Наименование угрозы	Вероятность реализации при наличии защиты
Угрозы несанкционированного удаленного запуска ПО	0.01
Угрозы распространения по сети вредоносного ПО	0.01
Угрозы анализа сети, нацеленные на выявление активных соединений и др.	0.1
Доступ, изменение, удаление ПДн лицами, не допущенными к их обработке	0.01
Угрозы выявления по сети учетных данных	0.01
Перехват в пределах контролируемой зоны внешними нарушителями	0.01
Перехват в пределах контролируемой зоны внутренними нарушителями	0.01
Угрозы навязывания неверной маршрутизации в сети	0.01
Потеря ключей и атрибутов доступа	0.01
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.01
Угрозы замены доверенного объекта в сети	0.01
Катаклизмы / катастрофы	0.5
Нарушение подачи электропитания	0.1
Сбой аппаратных и программных средств обработки информации	0.5
Угрозы типа «Отклонение запроса»	0.01
Вывод из строя частей ЭВМ, каналов передачи информации	0.01

Q-схема имитационной модели реализации угроз на сегменте при наличии дополнительных средств защиты имеет следующий вид (Рисунок 13):

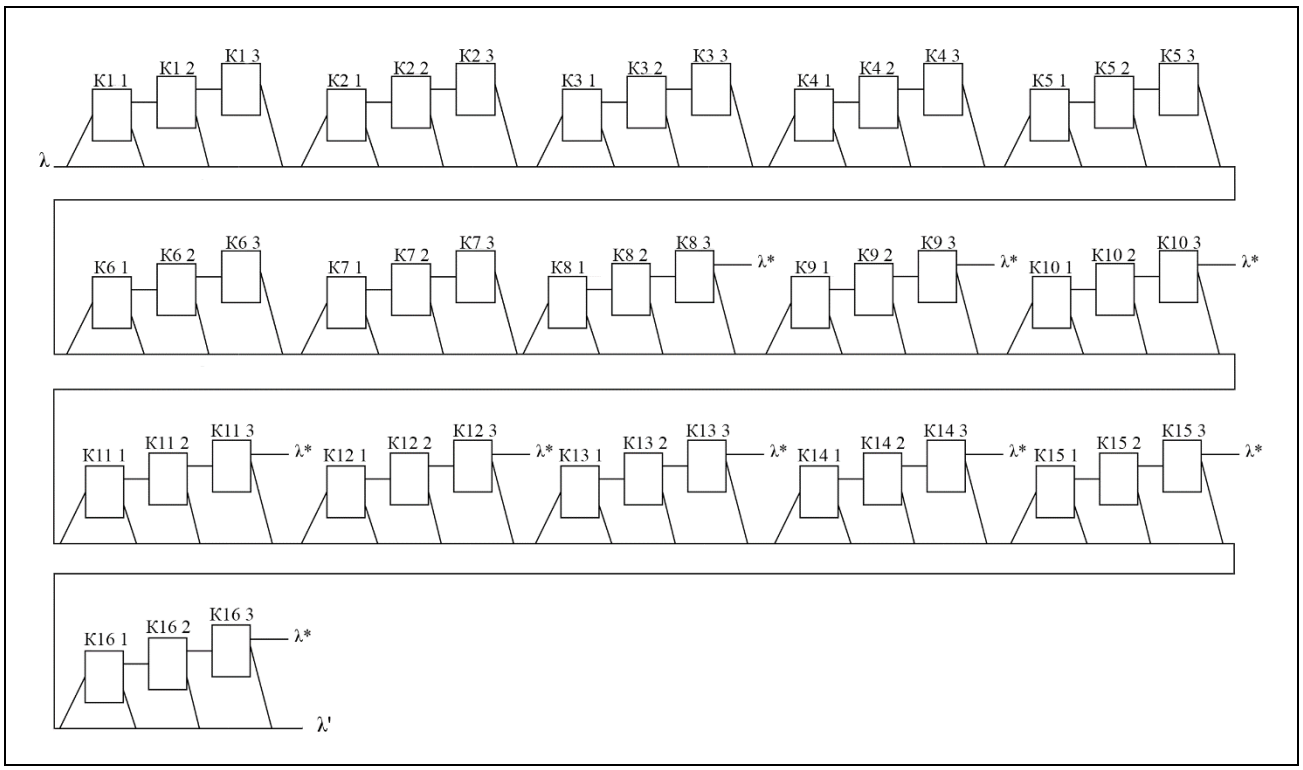

Рисунок 13 - Q-схема реализации угроз при наличии дополнительных средств защиты на сегменте «Электронная вычислительная машина – коммутатор»

где λ – входной поток, λ´ - выходной поток, λ* - поток заявок, прервавших 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.

В итоге компьютерная реализация предложенной модели приняла вид, представленный на Рисунок 14.

Проанализировав полученные результаты экспериментов с моделью по аналогии с предыдущим рассмотренным сегментом рассчитана доля запросов, завершивших движение, от количества запросов, которые были сгенерированы (97,89%), а также установлено примерное количество реализовавшихся угроз на один запрос (0,028).

В целях выявления угроз, которые наиболее значимо влияют на конечный результат, результаты реализации угроз рассмотрены отдельно от остальных результатов измерений (Таблица 16).

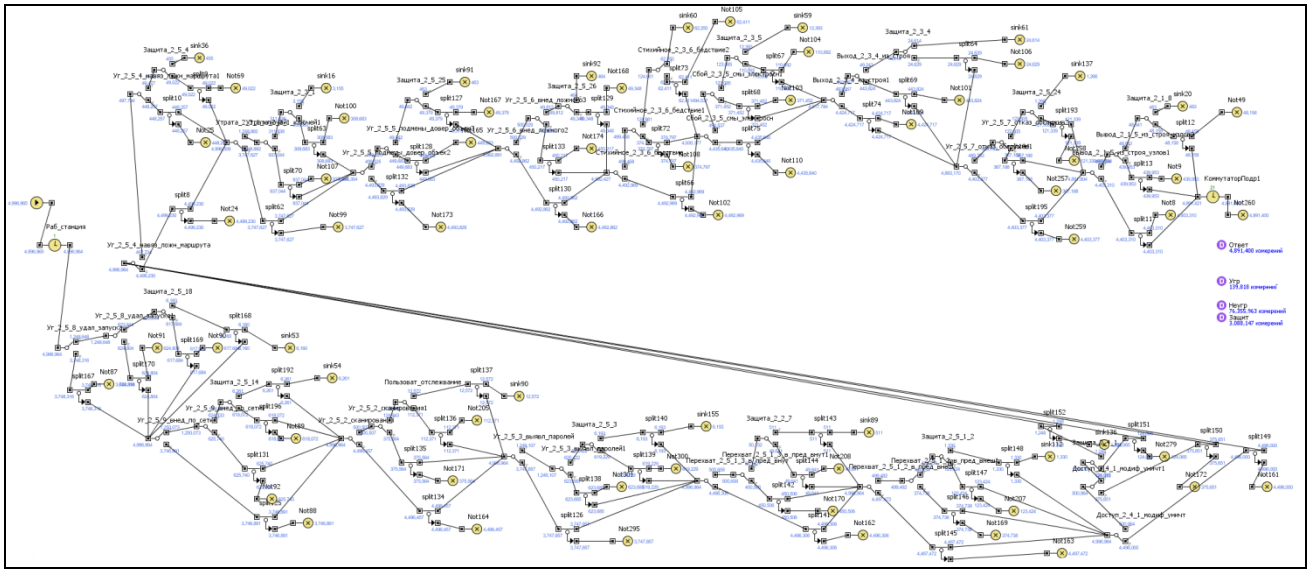

Рисунок 14 –Схема реализации угроз при наличии дополнительных средств защиты на сегменте «ЭВМ – коммутатор» (скриншот компьютерной реализации модели)

Таблица 16 – Процент количества реализованных угроз на сегменте «ЭВМ – коммутатор»

Наименование угрозы	Количество угроз, при наличии защиты	% от общего количества реализовав-шихся угроз
Угрозы несанкционированного удаленного запуска ПО	6383	4.58%
Угрозы распространения по сети вредоносного ПО	6157	4.42%
Угрозы анализа сети, нацеленные на выявление активных соединений и др.	12250	8.80%
Доступ, изменение, удаление ПДн лицами, не допущенными к их обработке	1296	0.93%
Угрозы выявления по сети учетных данных	6360	4.57%
Перехват в пределах контролируемой зоны внешними нарушителями	1258	0.90%
Перехват в пределах контролируемой зоны внутренними нарушителями	493	0.35%
Угрозы навязывания неверной маршрутизации в сети	511	0.37%
Потеря ключей и атрибутов доступа	3055	2.19%
Угрозы внедрения неверного объекта	499	0.36%
Угрозы замены доверенного объекта в сети	453	0.33%
Катаклизмы / катастрофы	61739	44.35%
Нарушение подачи электропитания	12326	8.85%
Сбой аппаратных и программных средств обработки информации	24712	17.75%
Угрозы типа «Отклонение запроса»	1180	0.85%
Вывод из строя частей ЭВМ, каналов передачи информации	494	0.35%

Проведенные эксперименты с имитационной моделью показали, что к наиболее вероятным угрозам относятся следующие:

Катаклизмы / катастрофы – 44,35% от общего количества реализовавшихся угроз;

Сбой аппаратных и программных средств – 17,75%;

Нарушение подачи электропитания – 8,85%;

Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, незаблокированных портов и служб, активных соединений и др. – 8,80%.

Для того, чтобы оценить уровень значимости средств защиты от каждого типа угроз в отдельности (рассматриваются только те угрозы, которые выделены группой экспертов для данного сегмента информационной системы), из модели поочередно убиралась защита от каждой угрозы, после чего проводились эксперименты. Результаты, полученные в ходе экспериментов, представлены в Таблица 17.

Таблица 17 –Результаты измерений на сегменте «Электронная вычислительная машина – коммутатор»

Наименование угрозы	Количество запросов	Количество завершенных запросов	Количество реализовавшихся угроз	Количество не реализовавшихся угроз	Кол-во не реализ. угроз, вследствие защиты	Количество угроз, реализовавшихся при отсутствии защиты
Угрозы несанкционированного удаленного запуска ПО	4997928	4892413	757927	76370748	2470412	624452
Угрозы распространения по сети вредоносного ПО	4996221	4890826	758858	76341888	2470916	625251
Угрозы анализа сети, нацеленные на выявление активных соединений и др.	4999154	4893639	252917	76387755	2978757	125271
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	5001566	4895580	263763	76422761	2968676	124925
Угрозы выявления по сети уч. данных	4997370	4891853	757646	76361606	2471055	624277
Перехват в пределах контролируемой зоны внешними нарушителями	5004848	4899335	263710	76471898	2973694	125176
Перехват в пределах контролируемой зоны внутренними нарушителями	5000014	4893707	190434	76397115	3042227	50208

Продолжение таблицы 17

Угрозы навязывания неверной маршрутизации в сети	5000588	4846344	188074	76024522	3035742	49954
Потеря ключей и атрибутов доступа	5008889	4599630	443366	74423491	2759188	312856
Угрозы внедрения неверного объекта в пределах системы, и во внешних сетях	5001072	4846670	188540	76174950	3040385	50236
Угрозы замены доверенного объекта в сети	5002703	4848533	188594	76153374	3039615	49948
Катаклизмы / катастрофы	5000874	4833776	201158	76169773	3027627	124711
Нарушение подачи электропитания	4992127	4776118	250279	75951349	2972525	123974
Сбой аппаратных и программных средств обработки информации	4992499	4861356	165507	76233008	3061432	49630
Угрозы типа «Отклонение запроса»	4993285	4766711	260498	76177635	2965418	47222
Вывод из строя частей ЭВМ, каналов передачи информации	5000806	4846556	188586	76413218	3042455	48940

На основе результатов, полученных в ходе экспериментов с моделью рассчитаны следующие значения (Таблица 18): процент количества запросов, завершивших движение, от количества сгенерированных; процент количества реализовавшихся угроз, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от количества нереализованных угроз; процент количества реализованных угроз, защита от которых не учитывалась в ходе проведения эксперимента с моделью, от общего количества реализованных угроз.

Если провести анализ результатов, приведенных в таблице 17, можно выделить угрозы, отсутствие защиты от которых наиболее значимо влияет на конечный результат. Среди таких угроз наибольшее влияние оказывает отсутствие зашиты от угрозы потери ключей и атрибутов доступа (количество запросов, дошедших до окончания модели, сократилось с 97,89% до 91,83%). Также снижение завершенных запросов до 95,46% и 95,67% приводит отсутствие защиты от угрозы типа «Отклонение запроса» и нарушение подачи электропитания соответственно. Отсутствие защиты от остальных угроз в меньшей мере сказывается на конечном результате (не более 1,5%).

Таблица 18 –Результаты расчетов на сегменте «ЭВМ – коммутатор»

Наименование угрозы	% пройден-ных запросов	% кол-ва реализовав-шихся угроз	% кол-ва угроз, реализ. которых предотвращена с-мой защиты,от общ. кол-ва угроз	% зкол-ва угроз, реализ. которых предотвращена с-мой защиты, от кол-ва нереализ. угроз	% кол-ва реализ. угроз, при отсутсвии защиты от угрозы, от общ. кол-ва реализ угроз
Несанкционированный удаленный запуск ПО	97.89%	0.98%	3.20%	3.23%	82.39%
Угрозы распространения по сети вредоносного ПО	97.89%	0.98%	3.20%	3.24%	82.39%
Угрозы анализа сети, нацеленные на выявление активных соединений и др.	97.89%	0.10%	3.90%	3.90%	49.53%
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	97.88%	0.34%	3.87%	3.88%	47.36%
Угрозы выявления по сети учетных данных	97.89%	0.98%	3.20%	3.24%	82.40%
Перехват в пределах контролируемой зоны внешними нарушителями	97.89%	0.34%	3.88%	3.89%	47.47%
Перехват в пределах контролируемой зоны внутренними нарушителями	97.87%	0.25%	3.97%	3.98%	26.37%
Угрозы навязывания неверной маршрутизации	96.92%	0.25%	3.98%	3.99%	26.56%
Потеря ключей и атрибутов доступа	91.83%	0.59%	3.69%	3.71%	70.56%
Угрозы внедрения неверного объекта в пределах системы, и во внешних сетях	96.91%	0.25%	3.98%	3.99%	26.64%
Угрозы замены доверенного объекта в сети	96.92%	0.25%	3.98%	3.99%	26.48%
Катаклизмы / катастрофы	96.66%	0.26%	3.96%	3.97%	62.00%
Нарушение подачи электропитания	95.67%	0.33%	3.90%	3.91%	49.53%
Сбой аппаратных и программных средств обработки информации	97.37%	0.22%	4.01%	4.02%	29.99%
Угрозы типа «Отклонение запроса»	95.46%	0.34%	3.88%	3.89%	18.13%
Вывод из строя частей ЭВМ, каналов пер-чи	96.92%	0.25%	3.97%	3.98%	25.95%

Эффективность средств защиты также можно оценить, сравнив процент реализации конкретной угрозы от общего количества реализованных угроз с процентом количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз (Таблица 19).

Исходя из результатов, представленных в Таблица 19 можно сделать вывод, что в целом система защиты ИСПДн от реализации угроз является эффективной. Вероятность реализации таких угроз, как угрозы сбой аппаратных и программных средств обработки информации и наступления катаклизмов или катастроф, достаточно большая и, в то же время, наличие защиты кардинальным образом не влияет на общий результат. Внедрить

эффективную защиту от указанных угроз не представляется возможным в связи с тем, что их наступление и реализация лишь в малой доли зависит от регулируемых факторах, и, в основном, носят спонтанный характер.

Таблица 19 –Сравнение процентов реализации угроз на сегменте «ЭВМ – коммутатор»

Наименование угрозы	% реализации угрозы, при наличии защиты	% реализации угрозы, при отсутствии защиты
Угрозы несанкционированного удаленного запуска ПО	4.58%	82.39%
Угрозы распространения по сети вредоносного ПО	4.42%	82.39%
Угрозы анализа сети, нацеленные на выявление активных соединений и др.	8.80%	49.53%
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.93%	47.36%
Угрозы выявления по сети учетных данных	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 неверного объекта в пределах системы, и во внешних сетях	0.36%	26.64%
Угрозы замены доверенного объекта в сети	0.33%	26.48%
Катаклизмы / катастрофы	44.35%	62.00%
Нарушение подачи электропитания	8.85%	49.53%
Сбой аппаратных и программных средств обработки информации	17.75%	29.99%
Угрозы типа «Отклонение запроса»	0.85%	18.13%
Вывод из строя частей ЭВМ, каналов передачи информации	0.35%	25.95%

2.3 Построение имитационной модели сегмента «Маршрутизатор – маршрутизатор»

Рассмотрим сегмент, на котором запрос поступает к маршрутизатору Управления ГИБДД от маршрутизатора подразделения по арендуемым (при использовании технологий VSAT или xDSL) или ведомственным (волоконно-оптические линии связи) каналам связи. Угрозы, вероятность реализации которых присутствует на данном сегменте, также выделены сформированной группой экспертов (Таблица 20).

Рассмотрим общую схему функционирования имитационной модели данного сегмента. Запрос, аналогично двум предыдущим моделям, движется по

соединительной линии, представляющей собой канал связи между двумя маршрутизаторами. На данной соединительной линии расположены точки наступления угроз, при прохождении которых запрос либо продолжает движение к маршрутизатору и фиксируется факт того, что угроза не наступила, либо с вероятностью наступления угрозы попадает на альтернативный путь движения и фиксируется факт наступления угрозы. Угрозы также могут быть двух типов: угрозы, влияющие на продвижение запроса, и угрозы, не влияющие на продвижение. Для каждой угрозы сформированы два счетчика: один фиксирует факт наступления угрозы, когда запрос не меняет своей траектории движения к конечной точке (в данном случае – к маршрутизатору), и факт наступления угрозы, когда запрос попадает на альтернативный путь продвижения.

Вероятности наступления рассматриваемых угроз безопасности также предоставлены сформированной группой экспертов (Таблица 20):

Таблица 20 – Значения вероятностей наступления угроз на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	Вероятностьь наст. угрозы
Вывод из строя частей ЭВМ, каналов передачи информации	0.1
Сбой аппаратных и программных средств обработки информации	0.1
Нарушение подачи электропитания	0.1
Катаклизмы / катастрофы	0.1
Угроза замены довер. объекта в сети	0.1
Угроза «Анализ потока информации сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, сторонними нарушителями в пределах КЗ)	0.1
Угроза «Анализ потока информации сети» (перехват сотрудниками в пределах контролируемой зоны информации, передаваемой из ИСПДн и принимаемой из внешних сетей)	0.1
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и др.	0.1
Угрозы выявления по сети учетных данных	0.25
Угрозы навязывания неверной маршрутизации в сети	0.1
Угроза «Анализ потока информации сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны)	0.25
Угрозы внедрения неверного объекта в пределах информационной системы, и во внешних сетях	0.1
Угрозы типа «Отклонение запроса»	0.1

Общая схема наступления угроз (вид компьютерной реализации модели) представлена на Рисунок 15.

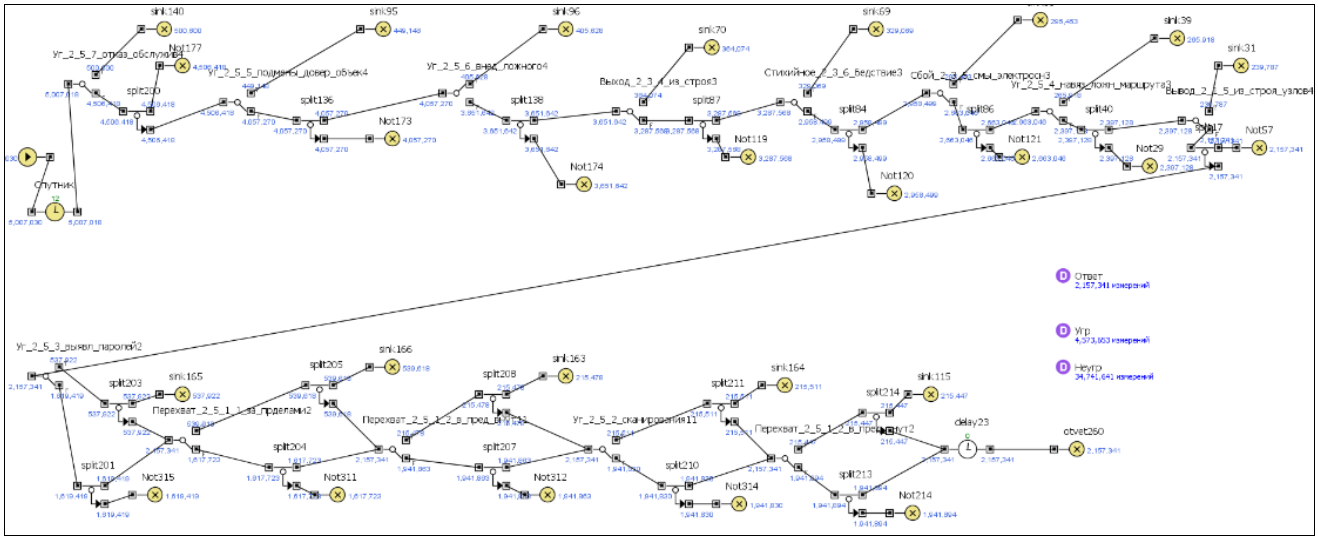

Рисунок 15 – Схема наступления угроз на сегменте «Маршрутизатор – маршрутизатор» (скриншот компьютерной реализации модели)

В ходе многократных экспериментов с моделью установлено, что количество запросов, завершивших движение, составляет 43,09% от количества сгенерированных.

На следующем этапе в построенную модель добавлены вероятности реализации угроз (Таблица 21), также определенные экспертами. Данные вероятности добавлены в виде точки реализации угрозы, расположенной на альтернативном пути продвижения запроса.

Компьютерная реализация имитационной модели после добавления дополнительной точки реализации угроз приняла вид, представленный на Рисунок 16. Численные расчеты результатов экспериментов показали, что количество запросов, завершивших движение увеличилось до 88,92% от количества сгенерированных.

На следующем этапе имитационная модель по аналогии с предыдущими описанными моделями вновь расширена: в ней учтены дополнительные меры защиты от реализации угроз, применяемые в информационной системе,

которые добавлены в модель также в качестве точки на альтернативном пути движения запроса. При прохождении добавленной точки запрос с вероятностью, также предложенной группой экспертов (Таблица 22), либо попадает на альтернативный путь движения, либо возвращается на первоначальный. Q-схема модели представлена на Рисунок 17.

Таблица 21 – Значения вероятностей реализации угроз на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	Вероятность реализации угрозы
Вывод из строя частей ЭВМ, каналов передачи информации	0.1
Сбой аппаратных и программных средств обработки информации	0.1
Нарушение подачи электропитания	0.25
Катаклизмы / катастрофы	0.25
Угроза замены довер. объекта в сети	0.1
Угроза «Анализ потока информации сети» (перехват информации сторонними нарушителями в пределах КЗ)	0.25
Угроза «Анализ потока информации сети» (перехват информации сотрудниками в пределах контролируемой зоны)	0.25
Угрозы анализа сети, нацеленные на выявление топологии сети, типа системного ПО, незаблокированных портов и др.	0.25
Угрозы выявления по сети учетных данных	0.5
Угрозы навязывания неверной маршрутизации в сети	0.1
Угроза «Анализ потока информации сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны)	0.5
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.1
Угрозы типа «Отклонение запроса»	0.25

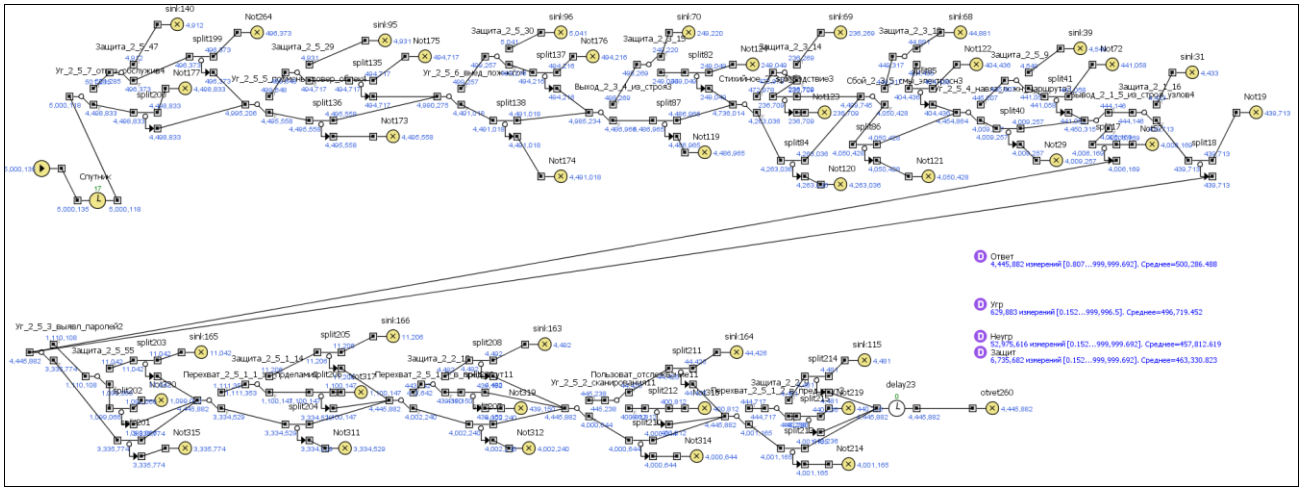

Рисунок 16 –Схема реализации угроз на сегменте «Маршрутизатор – маршрутизатор» (скриншот компьютерной реализации модели)

В итоге компьютерная реализация предложенной модели приняла вид, представленный на Рисунок 18.

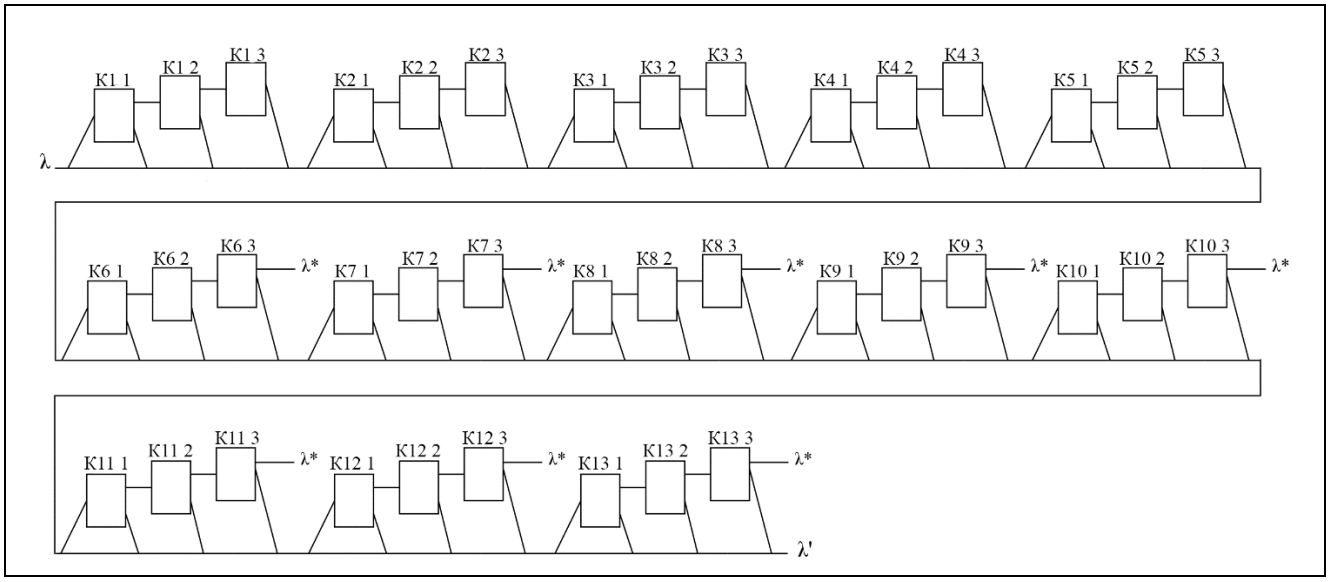

Рисунок 17 - Q-схема реализации угроз при наличии дополнительных средств защиты на сегменте «Маршрутизатор – маршрутизатор»

где λ – входной поток, λ´ - выходной поток, λ* - поток заявок, прервавших 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 … 13 – угрозы, которые могут наступить на рассматриваемом сегменте по мнению группы экспертов.

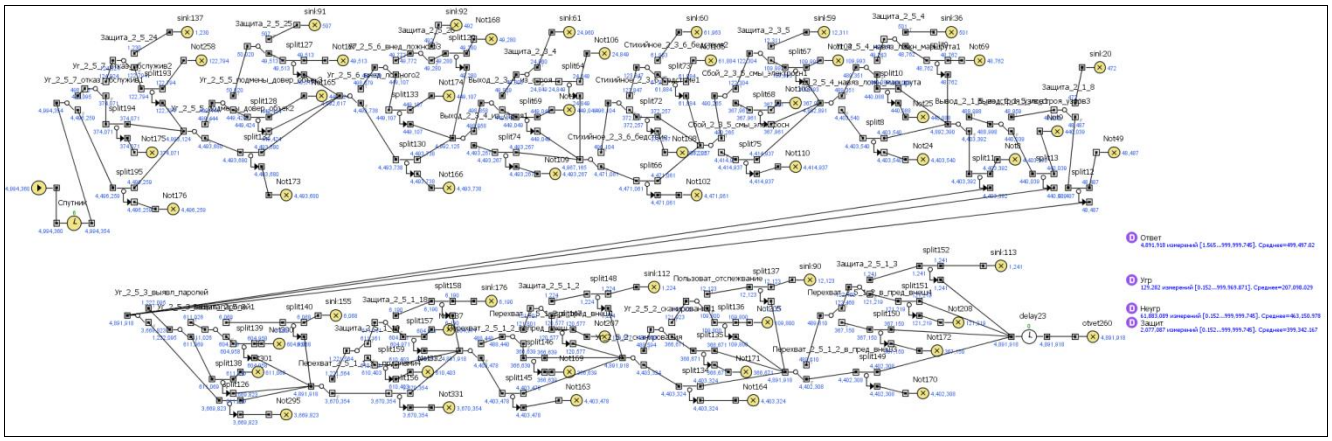

Рисунок 18 – Схема реализации угроз при наличии дополнительных средств защиты на сегменте «Маршрутизатор – маршрутизатор» (скриншот компьютерной реализации модели)

Проанализировав полученные результаты экспериментов с моделью рассчитана доля запросов, поступивших к маршрутизатору, от количества запросов, которые были сгенерированы (97,95%), установлено примерное количество реализовавшихся угроз на один запрос (0,026 или, что равносильно, одна угроза на 39 поступивших запросов), а также вычислен процент угроз, реализованных в процессе функционирования системы, от количества реализованных, нереализованных и не наступивших угроз (0,2%).

Таблица 22 –Вероятности реализации угроз при наличии дополнительных средств защиты информации на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	Вероятность реализации угрозы с защитой
Вывод из строя частей ЭВМ, каналов передачи информации	0.01
Сбой аппаратных и программных средств обработки информации	0.5
Нарушение подачи электропитания	0.1
Катаклизмы / катастрофы	0.5
Угроза замены довер. объекта	0.01
Угроза «Анализ потока информации сети» (перехват информации сторонними нарушителями в пределах КЗ)	0.01
Угроза «Анализ потока информации сети» (перехват информации сотрудниками в пределах КЗ)	0.01
Угрозы анализа сети, нацеленные на выявление топологии сети, незаблокированных портов, типа системного ПО и др.	0.1
Угрозы выявления по сети учетных данных	0.5
Угрозы навязывания неверной маршрутизации в сети	0.01
Угроза «Анализ потока информации сети» (перехват информации вне контролируемой зоны)	0.01
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.01
Угрозы типа «Отклонение запроса»	0.01

В целях выявления угроз, которые наиболее значимо влияют на конечный результат, результаты реализации угроз рассмотрены отдельно от остальных результатов измерений (Таблица 23).

Проведенные эксперименты с имитационной моделью показали, что к наиболее вероятным угрозам относятся:

Катаклизмы / катастрофы – 47,93% от общего количества реализовавшихся угроз;

Сбой аппаратных и программных средств – 19,31%;

Нарушение подачи электропитания – 9,52%;

Угрозы анализа сети, нацеленные на выявление типа системного ПО, незаблокированных портов и служб, активных соединений и др. – 9,38%.

Таблица 23 – Процент количества реализованных угроз на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	Количество угроз с защитой	% от кол-ва угроз с защ. от общ. кол-ва
Вывод из строя частей ЭВМ, каналов передачи информации	472	0.365
Сбой аппаратных и программных средств обработки информации	24960	19.307
Нарушение подачи электропитания	12311	9.523
Катаклизмы / катастрофы	61963	47.929
Угроза замены довер. объекта	507	0.392
Угроза «Анализ потока информации в сети» (перехват информации сторонними нарушителями в пределах КЗ)	1224	0.947
Угроза «Анализ потока информации в сети» (перехват информации сотрудниками в пределах контролируемой зоны)	1241	0.960
Угрозы анализа сети, нацеленные на выявление типа системного ПО и т.д.	12123	9.377
Угрозы выявления по сети учетных данных	6068	4.694
Угрозы навязывания неверной маршрутизации в сети	501	0.388
Угроза «Анализ потока информации в сети» (перехват информации вне контролируемой зоны)	6190	4.788
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	492	0.392
Угрозы типа «Отклонение запроса»	1230	0.951

Для того, чтобы оценить уровень значимости средств защиты от каждого типа угроз в отдельности, по аналогии с предыдущими моделями поочередно убиралась защита от каждой угрозы, после чего проводились эксперименты. Результаты, полученные в ходе экспериментов, представлены в Таблица 24.

На основе полученных результатов были рассчитаны (Таблица 25): процент количества запросов, завершивших движение, от количества сгенерированных; процент количества реализовавшихся угроз, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от общего количества реализованных и нереализованных угроз; процент количества угроз, которые были нейтрализованы системой защиты, от количества нереализованных угроз; процент количества реализованных угроз, защита от которых не учитывалась в

ходе проведения эксперимента с моделью, от общего количества реализованных угроз.

Таблица 24 –Результаты измерений на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	Количество запросов	Количество завершенных запросов	Количество реализовавшихся угроз	Количество не реализовавшихся угроз	Количество не реализовавшихся угроз, вследствие защиты	Количество угроз, реализовавшихся при отсутствии защиты
Вывод из строя частей ЭВМ, каналов передачи информации	4997275	4846486	177394	61690498	2018342	48880
Сбой аппаратных и программных средств обработки информации	5004910	4877560	154190	61799198	2048685	49943
Нарушение подачи электропитания	5003060	4789537	239928	61248833	1935840	123117
Катаклизмы / катастрофы	4999970	4835475	191280	61476302	1997640	124135
Угроза замены довер. объекта	5007475	4856558	177781	61529762	2016343	49854
Угроза «Анализ потока информации в сети» (перехват информации сторонними нарушителями в пределах КЗ)	4997500	4894671	251281	61916330	1959505	122881
Угроза «Анализ потока информации в сети» (перехват информации сотрудниками в пределах контролируемой зоны)	4993975	4890926	251022	61871221	1957135	122124
Угрозы анализа сети	4996915	4894668	237608	61913327	1971119	122717
Угрозы выявл. по сети уч. данных	4995535	4894067	735484	61908465	1473383	612318
Угрозы навязывания неверной маршрутизации в сети	5004440	4852972	178139	61730070	2017331	49250
Угроза «Анализ потока информации в сети» (перехват информации вне КЗ)	4994540	4891885	735148	61879219	1475212	611745
Угрозы внедрения неверного объекта в сетях	5004825	4853402	178383	61540698	2015855	48793
Угрозы типа «Отклонение запроса»	4992680	4768869	249957	60443111	1908623	125026

Проанализировав результаты, представленные в таблице 23, можно выделить угрозы, отсутствие защиты от которых наиболее очевидно влияет на конечный результат. Среди угроз наибольшее влияние оказывает отсутствие зашиты от угрозы типа «Отклонение запроса» (количество запросов, дошедших до окончания модели, сократилось с 97,95% до 95,52%). Также снижение завершенных запросов до 95,73% приводит отсутствие защиты от угрозы нарушения подачи электропитания соответственно. Отсутствие защиты от

остальных угроз в меньшей мере сказывается на конечном результате (не более 1,5%). Помимо указанных угроз можно отметить угрозу выявления по сети учетных данных и угрозу «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны), отсутствие защиты от которых приводит к увеличению процента реализованных угроз от количества всех учтенных угроз до 1,15.

Таблица 25 – Результаты расчетов на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	% пройден-ных запросов	% кол-ва реализ. угроз	% кол-ва угроз, реализ. Которыхпредотвр. с-мой защиты,от общ. кол-ва угроз	% кол-ва реализ. угроз, при отсутсвии защиты от угрозы, от кол-ва реализ угроз
Вывод из строя частей ЭВМ, каналов передачи информации	96.983	0.278	3.159	27.554
Сбой аппаратных и программных средств обработки информации	97.455	0.241	3.201	32.391
Нарушение подачи электропитания	95.732	0.378	3.052	51.314
Катаклизмы / катастрофы	96.710	0.300	3.138	64.897
Угроза замены довер. объекта	96.986	0.279	3.164	28.042
Перехват в пределах КЗ внешними нарушит.	97.942	0.392	3.056	48.902
Перехват в пределах КЗ внутренними нарушит.	97.937	0.392	3.054	48.651
Угрозы анализа сети	97.954	0.371	3.074	51.647
Угрозы выявления по сети учет. данных	97.969	1.147	2.298	83.254
Угрозы навязывания неверной маршрутизации в сети	96.973	0.279	3.156	27.647
Угроза «Анализ потока информации в сети» (перехват информации вне КЗ)	97.945	1.147	2.302	83.214
Угрозы внедрения неверного объекта в пределах системы, и во внешних сетях	96.974	0.280	3.163	27.353
Угрозы типа «Отклонение запроса»	95.517	0.399	3.049	50.019

Эффективность средств защиты также можно оценить, сравнив процент реализации конкретной угрозы от общего количества реализованных угроз с процентом количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз (Таблица 26).

Проанализировав результаты, представленные в Таблица 26, можно сделать вывод, что в целом система защиты ИСПДн от реализации угроз является эффективной. Вероятность реализации таких угроз, как угрозы сбоя

аппаратных и программных средств обработки информации и наступления катаклизмов / катастроф, достаточно высокая и, в то же время, наличие защиты кардинальным образом не влияет на общий результат. Внедрить эффективную защиту от указанных угроз не представляется возможным в связи с тем, что их наступление и реализация лишь в малой степени зависит от регулируемых факторах, и, в основном, носят спонтанный характер.

Таблица 26 –Сравнение процентов реализации угроз на сегменте «Маршрутизатор – маршрутизатор»

Наименование угрозы	% реализации угрозы, при наличии защиты	% реализации угрозы, при отсут. защиты
Вывод из строя частей ЭВМ, каналов передачи информации	0.365	27.554
Сбой аппаратных и программных средств обработки информации	19.307	32.391
Нарушение подачи электропитания	9.523	51.314
Катаклизмы / катастрофы	47.929	64.897
Угроза замены довер. объекта	0.392	28.042
Анализ потока информации в сети (перехват информации сторонними нарушителями в пределах КЗ)	0.947	48.902
Анализ потока информации в сети (перехват информации сотрудниками в пределах контролируемой зоны)	0.960	48.651
Угрозы анализа сети	9.377	51.647
Угрозы выявления по сети учетных данных	4.694	83.254
Угрозы навязывания неверной маршрутизации в сети	0.388	27.647
Анализ потока информации в сети (перехват информации вне КЗ)	4.788	83.214
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.392	27.353
Угрозы типа «Отклонение запроса»	0.951	50.019

2.4 Построение имитационной модели сегмента «Оператор – электронная вычислительная машина»

Рассмотрим сегмент информационной системы, на котором запрос поступает к ЭВМ от оператора. Экспертной комиссией так же, как и с в случае с предыдущими моделями, выделены угрозы, которые могут быть реализованы на рассмотренном сегменте (Таблица 27).

Общая схема данной имитационной модели такая же, как и для имитационных моделей описанных выше, за исключением того, что запрос движется от оператора до ЭВМ (вводится пользователем в программу) или от ЭВМ до оператора (оператор получает ответ в качестве текстового сообщения).

Вероятности наступления угроз, реализации и реализации при наличии дополнительной системы защиты, использованные при построении имитационной модели, представлены в Таблица 27:

Таблица 27 – Значения вероятностей наступления и реализации угроз на сегменте «Оператор – ЭВМ»

Наименование угрозы	Вероятность наступления угрозы	Вероятность реализации угрозы	Реализ с защитой
Угрозы перехвата акустической информации	0.1	0.01	0.1
Угрозы перехвата видовой информации	0.1	0.01	0.01
Угрозы перехвата информации по каналам побочных электромагнитных излучений и наводок	0.1	0.01	0.01
Хищение ЭВМ	0.1	0.01	0.01
Потеря ключей и атрибутов доступа	0.25	0.25	0.01
Хищение ключей и атрибутов доступа	0.1	0.01	0.01
Хищение, модификация, удаление информации	0.1	0.01	0.01
Нейтрализация средств защиты	0.1	0.01	0.1
Действия вредоносного ПО (вирусов)	0.25	0.1	0.01
Установка ПО, не связанного со служебной деятельностью	0.1	0.1	0.01
Случайное изменение (удаление) персональных данных сотрудниками, допущенными к ее обработке	0.1	0.01	0.01
Случайный вывод из строя средств защиты	0.1	0.01	0.01
Сбой аппаратных и программных средств обработки информации	0.1	0.1	0.5
Нарушение подачи электропитания	0.1	0.25	0.1
Катаклизмы / катастрофы	0.1	0.25	0.5
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0.1	0.25	0.01
Разглашение персональных данных, модификация, удаление сотрудниками, допущенными к ее обработке	0.25	0.01	0.01
Угрозы несанкционированного удаленного запуска ПО	0.25	0.5	0.01

Так как процесс построения имитационной модели не отличается от описанных выше процессов построения имитационных моделей других сегментов, опустим этапы построения имитационной модели наступления и реализации угроз и представим сразу Q-схему (Рисунок 19) и схему

имитационной модели реализации угроз при наличии дополнительной системы защиты (Рисунок 20):

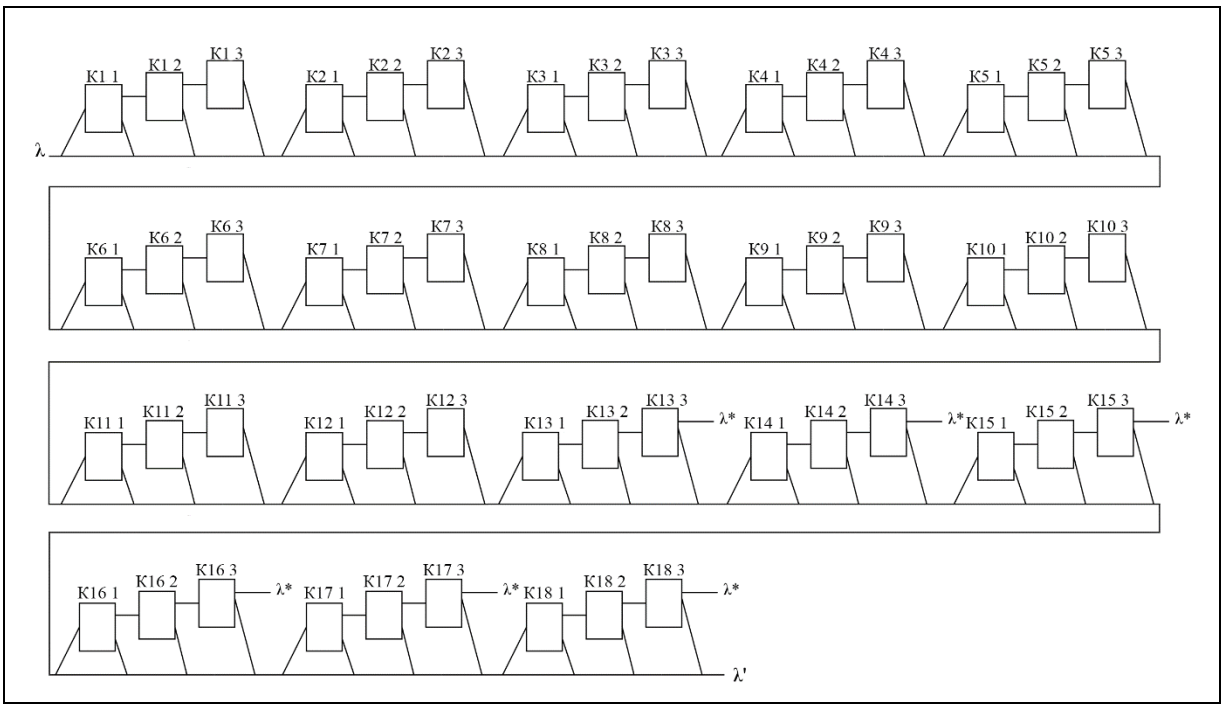

Рисунок 19 - Q-схема имитационной модели реализации угроз при наличии дополнительной защиты на сегменте «Оператор - ЭВМ»

где λ – входной поток, λ´ - выходной поток, λ* - поток заявок, прервавших 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 … 18 – угрозы, которые могут наступить на рассматриваемом сегменте по мнению группы экспертов.

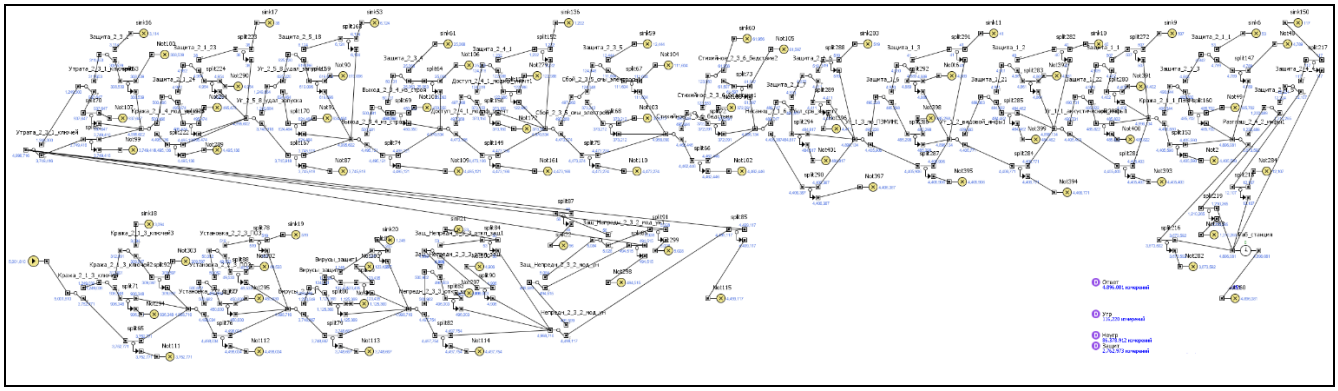

Рисунок 20 – Схема имитационной модели реализации угроз при наличии дополнительной защиты на сегменте «Оператор - ЭВМ» (скриншот компьютерной реализации модели)

В результате проведенных экспериментов с имитационной моделью установлено, что движение по сегменту завершают 97,9% сгенерированных запросов. Процент реализованных угроз от общего количества реализованных, нереализованных и не наступивших угроз составил 0,12.

Для определения угроз, наиболее значимо влияющих на конечный результат, результаты реализации каждого типа угроз рассмотрены отдельно от остальных результатов измерений (Таблица 28).

Таблица 28 –Процент количества реализованных угроз на сегменте «Оператор – ЭВМ»

Наименование угрозы	Количество угроз с защитой	% от кол-ва угроз с защ. от общ. кол-ва
Угрозы перехвата акустической информации	507	0.436
Угрозы перехвата видовой информации	40	0.034
Угрозы перехвата информации по каналам побочных электромагнитных излучений и наводок	41	0.035
Хищение ЭВМ	53	0.046
Потеря ключей и атрибутов доступа	3114	2.679
Хищение ключей и атрибутов доступа	3094	2.662
Хищение, удаление, модификация информации	38	0.033
Нейтрализация средств защиты	519	0.447
Действия вредоносного ПО (вирусов)	1245	1.071
Установка ПО, не связанного со служебной деятельностью	519	0.447
Случайное изменение (удаление) персональных данных сотрудниками	56	0.048
Случайный вывод из строя средств защиты	53	0.046
Сбой аппаратных и программных средств обработки информации	25068	21.569
Нарушение подачи электропитания	12444	10.707
Катаклизмы / катастрофы	61956	53.309
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	1232	1.060
Разглашение персональных данных, модификация, удаление сотрудниками, допущенными к ее обработке	117	0.101
Угрозы несанкционированного удаленного запуска ПО	6124	5.269

Проведенные эксперименты с моделью показали, что вероятность реализации является наиболее высокой у следующих угроз:

Катаклизмы / катастрофы – 53,31% от общего количества реализовавшихся угроз;

Сбой аппаратных и программных средств – 21,57%;

Нарушение подачи электропитания – 10,71%;

Угрозы несанкционированного удаленного запуска ПО – 5,27%.

Отдельно по данному сегменту проведены расчеты качества и значимости защиты от каждой угрозы. Результаты, аналогично предыдущим моделям, позволяют сделать вывод о том, в целом система защиты на данном сегменте позволяет минимизировать количество реализованных угроз и повысить вероятность успешного завершения прохождения запроса практически до ста процентов.

2.5 Построение имитационной модели сегмента «Коммутатор - маршрутизатор»

Теперь рассмотрим сегмент, на котором запрос поступает от коммутатора, объединяющего несколько ЭВМ, до маршрутизатора подразделения, либо управляемого коммутатора, объединяющего несколько других коммутаторов, в случае к ЭВМ от оператора. Для данного сегмента экспертной комиссией выделены угрозы, представленные в Таблица 29.

Общая схема данной имитационной модели аналогична общим схемам, описанным выше, за исключением пути продвижения запроса (в рассматриваемом случае запрос движется от коммутатора до маршрутизатора).

Вероятности наступления угроз, реализации и реализации при наличии дополнительной системы защиты, использованные при построении имитационной модели, представлены в Таблица 29.

Так как процесс построения имитационной модели не отличается от описанных выше процессов построения имитационных моделей других сегментов, опустим этапы построения имитационной модели наступления и реализации угроз и представим сразу Q-схему (Рисунок 21) и схему имитационной модели реализации угроз при наличии дополнительной системы защиты (Рисунок 22).

Таблица 29 – Значения вероятностей наступления и реализации угроз на сегменте «Коммутатор - маршрутизатор»

Наименование угрозы	Вероятность наступления угрозы	Вероятность реализации угрозы	Реализ с защитой
Вывод из строя частей ЭВМ, каналов передачи информации	0.1	0.1	0.01
Сбой аппаратных и программных средств	0.1	0.1	0.5
Нарушение подачи электропитания	0.1	0.25	0.1
Катаклизмы / катастрофы	0.1	0.25	0.5
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, вне контролируемой зоны)	0.25	0.5	0.01
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, сторонними нарушителями в пределах КЗ)	0.1	0.25	0.01
Угроза «Анализ потока информации в сети» (перехват сотрудниками в пределах контролируемой зоны информации)	0.1	0.25	0.01
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др.	0.1	0.25	0.1
Нейтрализация средств защиты	0.1	0.01	0.1
Угрозы выявления по сети учетных данных	0.25	0.5	0.01
Угрозы навязывания неверной маршрутизации в сети	0.1	0.1	0.01
Угрозы замены доверенного объекта в сети	0.1	0.1	0.01
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	0.1	0.1	0.01
Угрозы типа «Отклонение запроса»	0.1	0.25	0.01

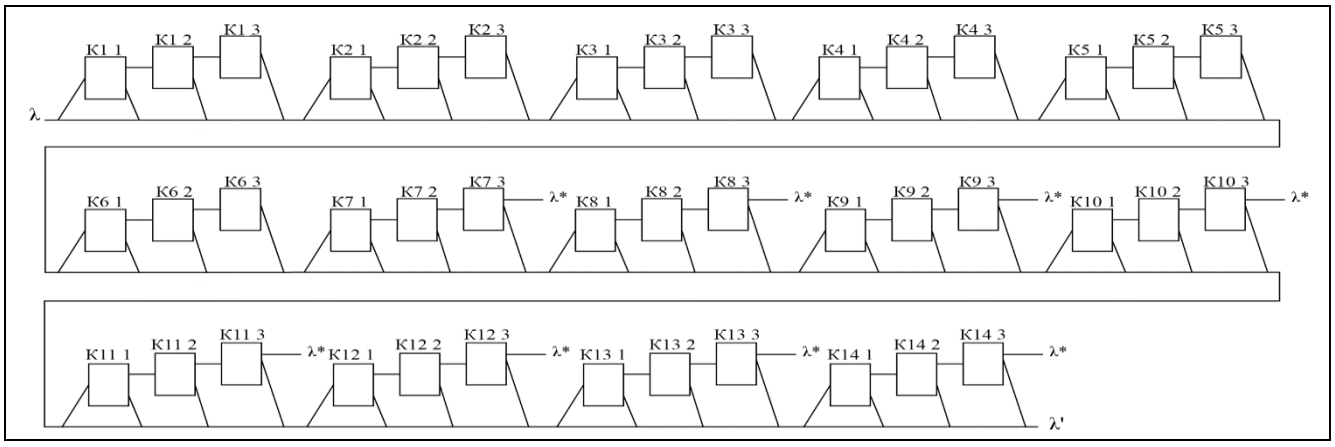

Рисунок 21 - Q-схема имитационной модели реализации угроз при наличии дополнительной защиты на сегменте «Коммутатор - маршрутизатор»

где λ – входной поток, λ´ - выходной поток, λ* - поток заявок, прервавших 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 … 14 – угрозы, которые могут наступить на рассматриваемом сегменте по мнению группы экспертов.

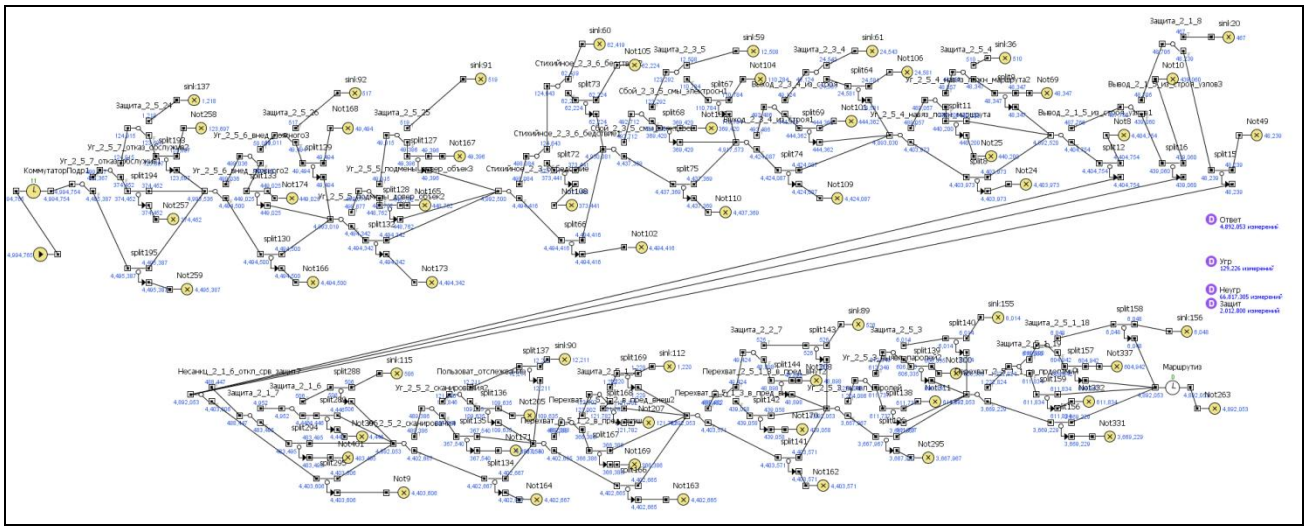

Рисунок 22 –Схема имитационной модели реализации угроз при наличии дополнительной защиты на сегменте «Коммутатор - маршрутизатор» (скриншот компьютерной реализации модели)

Численные расчеты результатов экспериментов показали, что количество запросов, завершивших движение, составляет 97,94% от количества сгенерированных. Процент реализованных угроз от общего количества реализованных, нереализованных и не наступивших угроз составил 0,19.

Для выявления типов угроз, которые наиболее значимо влияют на конечный результат, результаты реализации угроз, полученные в ходе экспериментов рассмотрены отдельно от остальных результатов измерений (Таблица 30).

Проведенные эксперименты с моделью показали, что на данном сегменте наиболее вероятными угрозами являются следующие:

Катаклизмы / катастрофы – 48,3% от общего количества реализовавшихся угроз;

Сбой аппаратных и программных средств – 18,99%;

Нарушение подачи электропитания – 9,68%;

Угрозы анализа сети – 9,45%.

Таблица 30 –Процент количества реализованных угроз на сегменте «Коммутатор - маршрутизатор»

Наименование угрозы	Количество угроз с защитой	% от кол-ва угроз с защ. от общ. кол-ва
Вывод из строя частей ЭВМ, каналов передачи информации	467	0.361
Сбой аппаратных и программных средств обработки информации	24 543	18.992
Нарушение подачи электропитания	12 508	9.679
Катаклизмы / катастрофы	62 419	48.302
Анализ потока информации в сети (перехват информации вне КЗ)	6 048	4.68
Анализ потока информации в сети (перехват информации сторонними нарушителями в пределах КЗ)	1 220	0.944
Анализ потока информации в сети (перехват информации сотрудниками в пределах контролируемой зоны)	526	0.407
Нейтрализация средств защиты	506	0.392
Угрозы анализа сети, нацеленные на выявление сетевых адресов и т.д.	12 211	9.449
Угрозы выявления по сети учетных данных	6 014	4.654
Угрозы навязывания неверной маршрутизации в сети	510	0.395
Угрозы замены доверенного объекта в сети	519	0.402
Угрозы внедрения неверного объекта как в пределах информационной системы, так и во внешних сетях	517	0.4
Угрозы типа «Отклонение запроса»	1 218	0.943

Для проведения оценки уровня влияния наличия средств защиты от каждого типа угроз в отдельности на конечный результат из имитационной модели поочередно убиралась защита от каждой угрозы, после чего проводились эксперименты. В связи с тем, что процесс определения значимости защиты сопоставим с процессам, описанными выше, а результаты отличаются незначительно, можно сделать вывод о том, что в целом система защиты ИСПДн на сегменте «Коммутатор – маршрутизатор» является эффективной.

Полученные результаты полностью совпадают с опытом использования информационной системы на протяжении длительного промежутка времени.

Для упрощения процедуры запуска имитационной модели, а также возможности просмотра процесса моделирования без необходимости применения дополнительного программного обеспечения разработана с использованием языка программирования Visual Basic (в среде Visual Studio) и зарегистрирована в государственном реестре программ для ЭВМ программа «Автоматизация запуска имитационных моделей». Данная программа предназначена для автоматизации запуска имитационных моделей наступления

и реализации угроз безопасности персональных данных сегментов информационной системы, позволяет без запуска среды моделирования произвести выполнение эксперимента с имитационной моделью, разработанной в среде моделирования на языке программирования Java (Рисунок 23). Программа предназначена для сокращения времени запуска моделей, и наглядности их представления.

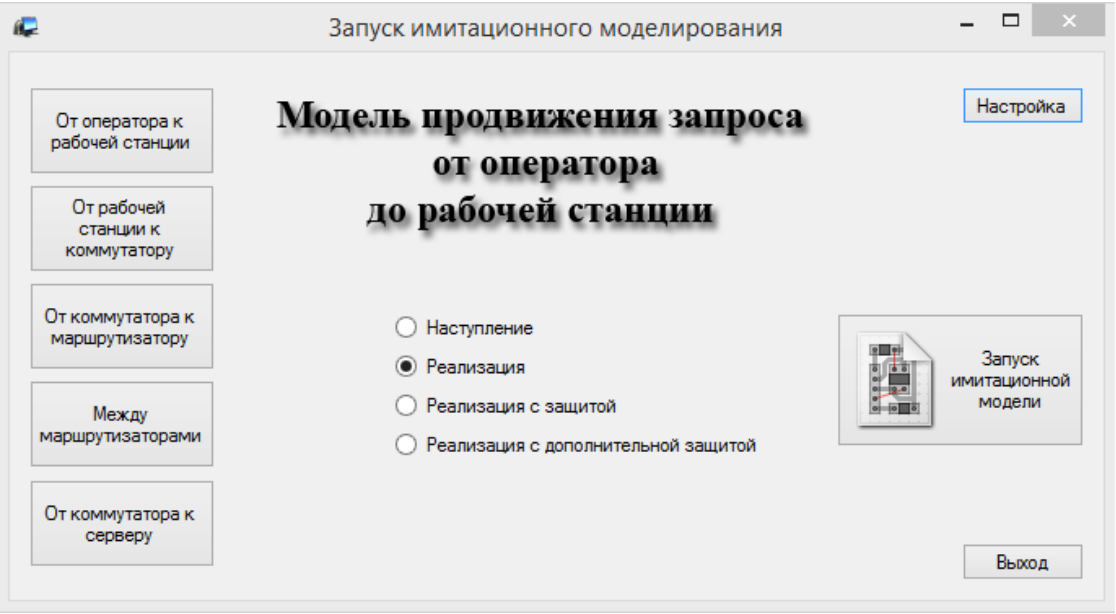

Рисунок 23 - Главное диалоговое окно программы для ЭВМ "Автоматизация запуска имитационных процессов"

В целях обеспечения более гибкого применения разработанной программы разными пользователями предусмотрена возможность оперативного редактирования запускного кода имитационной модели непосредственно из интерфейса программы.

2.6 Выводы

Как показывают результаты проведенных экспериментов, предложенные имитационные модели могут быть использованы для изучения воздействия угроз безопасности ПДн на информационную систему. Модели полностью соответствуют заданной блок-схеме и позволяют получить следующие данные: количество фактов наступления и не наступления угроз, сколько раз

наступившие угрозы были парированы первоначальной системой защиты, количество угроз, которые были парированы имеющимися дополнительными СЗПДн, количество реализованных угроз, количество запросов, поступивших в систему, сколько из них успешно завершили движение и движение скольких было прекращено вследствие реализации угроз. Все перечисленные данные могут быть получены как отдельно по угрозам каждого типа, так и обобщенные по всем типам угроз

Построение отдельной имитационной модели для каждого сегмента информационной системы позволяет детально изучить воздействие каждого типа угроз на определенном этапе прохождения запроса от оператора до сервера и обратно. Это также позволяет определить, какие СЗПДн и на каком сегменте являются эффективными, а какие нуждаются в замене или дополнении иными средствами защиты.

Проведенные расчеты также показывают, что для информационной системы «Информационные ресурсы УГИБДД» угрозы безопасности ПДн, которые можно выделить как актуальные, для всех рассматриваемых сегментов практически не отличаются. Это косвенно говорит об эффективной защите от основного количества типов угроз, и слабой защищенности от выделенных типов угроз. Однако, как показали результаты оценки эффективности используемых средств защиты информации, в целом система защиты является эффективной, а высокий уровень реализации имеют угрозы таких типов как сбой аппаратно-программных средств или катаклизмы / катастрофы, от которых не существует эффективных средств защиты, либо их внедрение потребует значительных финансовых затрат.

ГЛАВА 3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ И НЕОБХОДИМОСТИ ДОПОЛНИТЕЛЬНОЙ ЗАЩИТЫ

3.1 Построение модели воздействия угроз безопасности на информационную систему в целом

Проанализировав сегменты в отдельности, построим имитационную модель продвижения запроса от момента поступления в систему до момента получения ответа оператором. Однако, в связи с тем, что ограничения программного обеспечения не позволяют запустить имитацию модели продвижения запроса [1, 65], результаты получены путем сложения результатов, полученных на сегментах модели.

Для передачи запроса на сервер и получения ответа используется один из шести каналов связи:

1 – операторы работают с базой данных посредством локальной сети в пределах Управления ГИБДД. В данном случае запросы поступают к серверу, проходя на своем пути коммутатор, находящийся в кабинете, коммутатор, расположенный на этаже и объединяющий все коммутаторы, установленные в кабинетах, коммутатор, объединяющий все межэтажные коммутаторы, и коммутатор, объединяющий сервер и локальную сеть.

2 – операторы связываются с сервером посредством GPRS/3G каналов связи. В большинстве случаев для организации такого канала связи используется 3G модем, установленный прямо на ЭВМ оператора. В этом случае запрос от ЭВМ попадает на маршрутизатор оператора сотовой связи, после чего по шифрованному виртуальному тоннелю – на маршрутизатор Управления, оттуда на коммутатор, объединяющий сервер и маршрутизаторы. GPRS/3G соединение используется в основном для мобильного доступа (в патрульных автомобилях) и ранее, при отсутствии иных видов связи, использовались в подразделениях. Данная схема может расширяется: добавляется дополнительный маршрутизатор, в качестве которого выступает

сервер подразделения, на котором установлен 3G модем. В случае расширения схемы запрос изначально от ЭВМ будет попадать на коммутатор подразделения, потом на маршрутизатор подразделения, в качестве которого выступает сервер или другая ЭВМ, а потом уже на маршрутизатор оператора сотовой связи и маршрутизатор и коммутатор Управления. Данный вид связи практически не использовался и не используется в настоящее время, так как требует стабильного 3G соединения. В связи с тем, что лишь малое количество районов Краснодарского края находится в зоне уверенного приема 3G сигнала, происходит переключение на более медленные стандарты EDGE или GPRS, что, при одновременной работе нескольких пользователей, приводит к невозможности использования данного вида соединения из-за отключений или зависания.

3 – операторы устанавливают соединение с сервером посредством коммутируемого удаленного доступа. При таком виде связи для соединения с сервером используется dial-up модем, установленный непосредственно на ЭВМ оператора, поэтому запрос поступает сразу на маршрутизатор Управления, а оттуда на коммутатор, объединяющий сервер и маршрутизаторы. Данный вид связи в настое время сильно устарел, так как является дорогостоящим, ненадежным и низкоскоростным, что не позволяет использовать данный вид соединения для повседневной деятельности. Данный вид соединения используется в качестве резервного на случай сбоя в работе основного используемого типа соединения.

4 – операторы работают с базой данных используя спутниковые каналы связи. При таком соединении запрос от ЭВМ попадает на коммутатор подразделения, затем на маршрутизатор, установленный в здании подразделения, оттуда поочередно на 2 маршрутизатора оператора спутниковых линий связи, маршрутизатор Управления, коммутатор, объединяющий маршрутизаторы, файловый и иные серверы и локальную сеть и коммутатор, объединяющий сервер и локальную сеть.

5 – операторы устанавливают соединение с базой данных по технологии VPN-MPLS посредством xDSL соединения. При таком способе соединения запрос от ЭВМ попадает на коммутатор подразделения, оттуда на маршрутизатор, в качестве которого выступают xDSL модем и коммутатор оператора связи, поочередно на два маршрутизатора операторов связи, маршрутизатор Управления, коммутатор, объединяющий маршрутизаторы, файловый и иные серверы и локальную сеть Управления и коммутатор, объединяющий сервер и локальную сеть.

6 – операторы устанавливают соединение с базой данных, используя Единую информационную телекоммуникационную систему (ЕИТКС) МВД РФ. В связи с тем, что ЕИТКС по сути представляет собой локальную сеть, конечное количество маршрутизаторов и коммутаторов, через которые происходит связь с сервером, зависит от конкретного местоположения оператора. В большинстве случаев запрос на своем пути проходит коммутатор и маршрутизатор подразделения, маршрутизатор ГУ МВД РФ, маршрутизатор Управления, коммутатор, объединяющий маршрутизаторы, файловый и иные серверы и локальную сеть Управления и коммутатор, объединяющий сервер и локальную сеть.

Рассмотрев все виды связи, с помощью которых запрос поступает на сервер и возвращается обратно, принято решение о рассмотрении четырех моделей:

1. При прохождении запроса по спутниковым линиям связи (VSAT), с использованием оптоволоконных линий связи и с использованием технологии xDSL;

2. При прохождении запроса по коммутируемым линиям связи и по сотовым канал связи (GPRS/3G);

3. При прохождении запроса по сотовым линиям связи по технологии GPRS/3G с использованием промежуточного сервера;

4. При прохождении запроса от ЭВМ, находящейся непосредственно в Управлении ГИБДД.

Для анализа вероятности наступления угроз при использовании спутниковых линий связи, волоконно-оптических или VPN-MPLS соединения по технологии xDSL рассмотрены следующие сегменты:

1. Поступление запроса от пользователя к ЭВМ;
2. Передача запроса от ЭВМ до коммутатора подразделения;
3. Передача запроса от коммутатора подразделения до маршрутизатора (в качестве которого выступает ADSL модем, спутниковый ресивер и т.п.), устанавливающего связь с маршрутизатором Управления;
4. Поступление запроса от маршрутизатора подразделения на маршрутизатор Управления по внешним линиям связи (ведомственным или арендуемым);
5. От маршрутизатора Управления до коммутатора, объединяющего серверы Управления;
6. От коммутатора до сервера;

7.-12. Запрос поступает обратно к пользователю в качестве ответа.

При передачи запроса в базу данных пользователями, находящимися в пределах локальной сети, выделены следующие сегменты имитационной модели:

1. Поступление запроса от пользователя к ЭВМ;
2. Передача запроса от ЭВМ к коммутатору, установленному в каждом кабинете и объединяющего ЭВМ данного кабинета с межэтажным коммутатором;
3. От коммутатора, расположенного в кабинете, до управляемого коммутатора (маршрутизатора), объединяющего все коммутаторы, расположенные в кабинетах на этаже и коммутатор, объединяющий серверы Управления;
4. От управляемого коммутатора (маршрутизатора) до коммутатора, объединяющего все межэтажные коммутаторы и серверы Управления;
5. От коммутатора до сервера;
6. - 10. Запрос поступает обратно к пользователю в качестве ответа.

Для анализа вероятности наступления угроз при установке связи с сервером с использованиемGPRS/3G линий связи или коммутируемого соединения использованы следующие сегменты:

1. Поступление запроса от пользователя к ЭВМ;
2. Передача запроса от ЭВМ по коммутируемым линиям связи к маршрутизатору Управления;
3. От маршрутизатора до коммутатора, объединяющего все межэтажные коммутаторы и серверы Управления;
4. От коммутатора до сервера;
5.-8. Запрос поступает обратно к пользователю в качестве ответа.

При использования GPRS/3G модема для установления соединения с сервером Управления с использованием сервера в качестве маршрутизатора подразделения, выделены следующие сегменты:

1. Поступление запроса от пользователя к ЭВМ;
2. Передача запроса от ЭВМ до коммутатора подразделения;
3. Передача запроса от коммутатора подразделения до сервера подразделения, который также выступает в качестве маршрутизатора, устанавливающего связь с маршрутизатором Управления;
4. Поступление запроса от сервера подразделения на маршрутизатор Управления по сотовым линиям связи;
5. Поступление запроса от маршрутизатора Управления до коммутатора, объединяющего серверы Управления;
6. Поступление запроса от коммутатора до сервера;
7.-12. Запрос поступает обратно к пользователю в качестве ответа, проходя все перечисленные сегменты в обратном порядке.

В результате расчетов получены следующие результаты (Таблица 31, Таблица 32):

Таблица 31 –Результаты расчетов по каналам без защиты

Тип связи, без защиты	% полученных ответов от количества поступивших запросов	% угроз от общ кол-ва угр и неугр	% угроз от кол-ва запросов
Спутниковая, оптоволоконная	86,12	1,72	26,2
Dial-Up, GPRS/3G	86,3	1,29	20,29
GPRS/3G с промежуточным сервером	86,12	1,6	26,86
В одной подсети	85,56	1,82	28,91

Таблица 32 –Результаты расчетов по каналам с дополнительными СЗПДн

Тип связи, с защитой	% полученных ответов от количества поступивших запросов	% угроз от общ 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	2,7
В одной подсети	97,91	0,16	2,65

Как видно из проведенных расчетов конечные результаты для разных моделей при наличии дополнительных средств защиты практически не отличаются. Процент завершенных запросов от количества поступивших в систему для всех моделей оказался практически одинаковым, составив 97,91%. Процент реализованных угроз от количества реализованных, нереализованных и не наступивших угроз также отличается лишь в 0,01% и составляют 0,16%. Небольшое различие в конечных результатах наблюдается в расчетах процента реализованных угроз от количества поступивших запросов. Если рассматривать эффективность защиты с точки зрения данного параметра, то наиболее безопасным является способ связи с сервером посредством GPRS/3G модема или коммутируемого соединения (процент реализованных угроз составляет 2,61% от общего количества угроз), наименее безопасным является тип связи посредством GPRS/3G модема и промежуточного сервера (2,7%). Однако разница в показателях настолько невелика, что может возникнуть из-за погрешности измерений.

3.2 Определение актуальных угроз безопасности информационной системы в целом

Рассмотрим детально результаты проведенных расчетов для выделения угроз, вероятность реализации которых является наиболее актуальной.

Изначально рассмотрим и проанализируем данные, полученные для модели продвижения запроса по каналам сотовой связи и с использованием коммутируемого подключения. Результаты расчетов представлены в Таблица 33.

Таблица 33 –Результаты расчетов по каналам сотовой связи

Наименование угрозы	Кол-во реализ. угроз без защиты	Кол-во реализ. угроз с защитой	% от кол-ва угроз без защиты	% от кол-ва угроз с защитой
Потеря ключей и атрибутов	634578	12504	7,81806	1,19718
Установка ПО, не связанного со служебной деятельностью	87582	1038	1,07902	0,09938
Угроза перехвата информации по каналам ПЭМИН	7716	82	0,09506	0,00785
Угроза перехвата видовой информации	7870	80	0,09696	0,00766
Угроза перехвата акустической информации	78758	1014	0,97031	0,09708
Несанкционированный удаленный запуск ПО	1125604	24854	13,86754	2,37962
Угроза анализа сети	276966	73576	3,41225	7,04445
Катаклизмы / катастрофы	1881018	497698	23,17431	47,65150
Нарушение подачи электропитания	363338	99062	4,47636	9,48457
Разглашение перс. данных, модификац., удаление	44772	512	0,55160	0,04902
Замена доверенного объекта в сети	29894	3130	0,36830	0,29968
Перехват вне КЗ	69650	36974	0,85809	3,54003
Перехват в пред КЗ сотрудниками	18032	3534	0,22216	0,33836
Перехват в пред КЗ внешн. нарушителями	27794	7328	0,34242	0,70161
Отклонение запроса	30014	7440	0,36978	0,71233
Нейтрализация средств защиты	26840	3018	0,33067	0,28895
Случайный вывод из строя средств защиты	8660	106	0,10669	0,01015
Случайное изменение (удаление) персональных данных сотрудниками, допущенными к обработке	8776	112	0,10812	0,01072
Скрытый функционал системного ПО и ПО для обработки персональных данных	10016	108	0,12340	0,01034
Навязывание неверной маршрутизации в сети	27938	2984	0,34420	0,28570
Хищение ЭВМ	17834	216	0,21972	0,02068
Хищение носителей информации	9922	100	0,12224	0,00957
Хищение, модификай. информации	19126	182	0,23563	0,01743
Хищение ключей и атрибутов доступа	586142	6188	7,22132	0,59246
Доступ, модификация информации	220282	5068	2,71389	0,48523
Действие вирусов и вредоносного ПО	470444	4988	5,79591	0,47757
Угрозы выявления по сети учетных данных	69498	36398	0,85622	3,48488
Сбой аппаратных и программных средств	1875692	197890	23,10869	18,94674
Вывод из строя частей ЭВМ, каналов связи	26804	2912	0,33023	0,27881
Распространение по сети вредоносного ПО	24976	12270	0,30771	1,17478
Внедрение неверного объекта в сетях	30288	3088	0,37315	0,29566

Как показали расчеты, наличие дополнительных средств защиты информации наиболее заметно влияет на вероятность реализации угрозы несанкционированного удаленного запуска ПО (процент реализации которой от общего количества реализованных угроз снизился с 13,87 до 2,38), угрозу хищения ключей и атрибутов доступа (с 7,22% до 0,59%), угрозу потери ключей и атрибутов доступа (с 7,82% до 1,19%), действия вирусов и вредоносного ПО (с 5,8% до 0,48%) и угроза сбоя аппаратных и программных средств обработки информации (с 23,11% до 18,95%). В свою очередь, увеличился процент реализации следующих угроз: катаклизмы / катастрофы – с 23,17% до 47,65%, нарушение подачи электропитания – с 4,48% до 9,48% угроза анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов электронных вычислительных машин ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др.– с 3,41% до 7,04%, угроза перехвата за пределами контролируемой зоны – с 0,86% до 3,54% и угроза выявления по сети учетных данных – с 0,86% до 3,48%.

В качестве угроз, вероятность реализации которых является наиболее высокой при наличии дополнительных СЗПДн, можно выделить следующие:

1. катаклизмы / катастрофы – 47,65% от общего количества реализованных угроз;
2. Сбой аппаратных и программных средств – 18,95%;
3. Нарушение подачи электропитания – 9,48%.

В данной модели наиболее вероятными являются угрозы стихийного характера (катаклизмы / катастрофы), способов защиты от которых программными средствами не существует. Далее по убыванию вероятности идут угроза анализа сети – 7,044%, перехват данных вне контролируемой зоны – 3,54%, выявление по сети учетных данных – 3,48%, угроза несанкционированного удаленного запуска ПО – 2,38%, угроза потери ключей и атрибутов доступа – 1,2%, распространение по сети вредоносного ПО – 1,17%. Реализация остальных угроз составляет не более 1%.

При отсутствии дополнительной защиты от наступления угроз наиболее вероятными являются следующие угрозы: катаклизмы или катастрофы – 23,17%, угроза сбоя аппаратных и программных средств обработки информации – 23,11%, угрозы несанкционированного удаленного запуска ПО – 13,87%, угроза потери ключей и атрибутов доступа – 7,82% и угроза хищения ключей и атрибутов доступа – 7,22%. Однако в связи с тем, что результаты, полученные в результате экспериментов с моделью реализации угроз безопасности ИСПДн без наличия защиты, не представляют практического интереса и рассматриваются только в качестве статистических данных, позволяющих проследить изменения процента реализации, проводить подробный анализ поведения модели при отсутствии защиты является нецелесообразным.

Рассмотрим результаты расчетов вероятностей реализации угроз безопасности ИСПДн для остальных моделей. Результаты расчетов для модели продвижения запроса по оптоволоконным/спутниковым каналам связи представлены в Таблица 34.

Проведенные расчеты показали, что наивысшую вероятность реализации имеют следующие угрозы:

1. Катаклизмы / катастрофы – 47,2%;
2. Угроза сбой аппаратных и программных средств -18,72%;
3. Нарушение подачи электропитания – 9,41%.

Также высокую вероятность реализации можно выделить у угроз анализа сети, нацеленных на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др. – 7,78%, угрозы выявления по сети учетных данных – 3,84%, угрозы несанкционированного удаленного запуска ПО – 2,35% и угрозы перехвата за пределами контролируемой зоны – 2,34%.

Добавление в модель имеющихся средств защиты наиболее заметно повлияло на процент количества реализованных угроз от количества всех реализованных угроз для следующих видов угроз:

- Катаклизмы / катастрофы – с 16,58% до 47,2%;
- Несанкционированный удаленный запуск ПО – с 15,1% до 2,35%;
- Угроза распространения по сети вредоносного ПО – с 8,1% до 1,57%;
- Угроза потери ключей и атрибутов доступа – с 8,1% до 1,95%;
- Нарушение подачи электропитания – с 4,31% до 9,41%.

Таблица 34 –Результаты расчетов по оптоволоконным/спутниковым каналам связи

Угроза	Кол-во угроз без защиты	Кол-во угроз с защитой	% от колва угроз без защ	% от колва угроз с защ
Отклонение запроса	254336	12408	1,61769	0,78406
Внедрение неверного объекта в сетях	133626	5048	0,84992	0,31898
Замена довер объект	131346	5096	0,83542	0,32201
Катаклизмы / катастрофы	2606810	747036	16,58044	47,20481
Нарушение подачи электропитания	677252	148864	4,30762	9,40664
Сбой аппаратных и программных средств обработки информации	2434418	296204	15,48395	18,71698
Навязывание неверной маршрутизации	137340	4914	0,87354	0,31051
Вывод из строя частей ЭВМ, линий передачи	119018	4812	0,75701	0,30407
Нейтрализация средств защиты	35814	4030	0,22779	0,25465
Угроза анализа сети	616016	123142	3,91813	7,78128
Перехват в пределах КЗ внешними нар.	136884	12428	0,87064	0,78532
Перехват в пределах КЗ сотрудниками.	278306	5608	1,77015	0,35437
Выявление по сети учетных данных	1341962	60812	8,53546	3,84268
Перехват за пределами КЗ	69650	36974	0,44300	2,33637
Потеря ключей и атрибутов доступа	1274196	30910	8,10444	1,95319
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	469420	7564	2,98571	0,47797
Хищение, удаление модификация информации	19126	182	0,12165	0,01150
Несанкционированный удаленный запуск ПО	2374272	37174	15,10140	2,34901
Распространение по сети вредоносного ПО	1273914	24792	8,10265	1,56659
Хищение ЭВМ	17834	216	0,11343	0,01365
Хищение носителей информации	9922	100	0,06311	0,00632
Угроза разглашения персональных данных	44772	512	0,28477	0,03235
Угроза перехвата по каналам побочных наводок	7716	82	0,04908	0,00518
Угроза перехвата видовой информации	7870	80	0,05006	0,00506
Угроза перехвата акустической информации	78758	1014	0,50094	0,06407
Хищение ключей и атрибутов доступа	586142	6188	3,72812	0,39102
Установка ПО, не связанного со службой	87582	1038	0,55706	0,06559
Действие вирусов и вредоносного ПО	470444	4988	2,99223	0,31519
Случайный вывод из строя средств защиты	8660	106	0,05508	0,00670
Случайное изменение ПДн сотрудниками	8776	112	0,05582	0,00708
Скрытый функционал системного ПО и ПО для обработки персональных данных	10016	108	0,06371	0,00682

Результаты расчетов вероятностей реализации угроз безопасности ИСПДн для модели продвижения запроса по GPRS/3G каналам связи с использованием промежуточного сервера представлены в Таблица 35.

Таблица 35 –Результаты расчетов по каналам сотовой связи с промежуточным сервером

3G с сервером	Кол-во угроз без защиты	Кол-во угроз с защитой	% от колва угроз без защ	% от колва угроз с защ
Отклонение запроса	254554	12516	1,57934	0,77303
Внедрение неверного объекта в сетях	133892	5084	0,83071	0,31400
Замена довер объект	131218	5136	0,81412	0,31722
Катаклизмы / катастрофы	2606490	747220	16,17158	46,15067
Нарушение подачи электропитания	678792	148384	4,21147	9,16467
Сбой аппаратных и программных средств	2432590	295866	15,09265	18,27362
Навязывание неверной маршрутизации в сети	138156	4856	0,85717	0,29992
Вывод из строя частей ЭВМ, линий передачи	119300	4912	0,74018	0,30338
Нейтрализация средств защиты	36922	3986	0,22908	0,24619
Угроза анализа сети	626406	123628	3,88644	7,63566
Перехват в пределах КЗ внешними нар.	138202	12428	0,85745	0,76759
Перехват в пределах КЗ сотрудниками.	269236	4556	1,67044	0,28139
Выявление по сети учетных данных	1344700	61018	8,34299	3,76866
Перехват за пределами КЗ	94672	49472	0,58738	3,05555
Потеря ключей и атрибутов доступа	1262204	25090	7,83116	1,54964
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	479076	10168	2,97236	0,62801
Хищение, удаление, модификация информации	29332	288	0,18199	0,01779
Несанкционированный удаленный запуск ПО	2399400	49780	14,88672	3,07457
Распространение по сети вредоносного ПО	1298890	37062	8,05877	2,28907
Хищение ЭВМ	27706	326	0,17190	0,02013
Хищение носителей информации	19844	200	0,12312	0,01235
Угроза разглашения персональных данных	69738	790	0,43268	0,04879
Угроза перехвата по каналам наводок	7716	82	0,04787	0,00506
Угроза перехвата видовой информации	7870	80	0,04883	0,00494
Угроза перехвата акустической информации	78758	1014	0,48864	0,06263
Хищение ключей и атрибутов доступа	586142	6188	3,63663	0,38219
Установка ПО, не связанного со служеб. деят.	87582	1038	0,54339	0,06411
Действие вирусов и вредоносного ПО	720860	7486	4,47247	0,46236
Случайный вывод из строя средств защиты	8660	106	0,05373	0,00655
Случайное изменение ПДн сотрудниками	8776	112	0,05445	0,00692
Скрытый функционал системного ПО и ПО для обработки персональных данных	20032	216	0,12429	0,01334

Как видно из таблицы, наличие защиты наиболее заметно влияет на вероятность реализации Угрозы несанкционированного удаленного запуска ПО (процент реализации которой от общего количества реализованных угроз снизился с 14,89 до 3,07), угрозу распространения по сети вредоносного ПО (с 8,06% до 2,3%), угрозу потери ключей и атрибутов доступа (с 7,83% до 1,55%), выявление по сети учетных данных (с 8,34% до 3,77%) и действие вирусов и вредоносного ПО (с 4,48% до 0,46%). В свою очередь, увеличился процент реализации следующих угроз: катаклизмы или катастрофы – с 16,17% до

46,15%, нарушение подачи электропитания – с 4,21% до 9,16% угроза анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др.– с 3,89% до 7,64% и угроза сбоя аппаратных и программных средств обработки информации – с 15,09% до 18,27%.

В качестве угроз, вероятность реализации которых является наиболее высокой при наличии защиты, можно выделить следующие:

1. Катаклизмы или катастрофы – 46,15% от общего количества реализованных угроз;
2. Сбой аппаратных и программных средств – 18,27%;
3. Нарушение подачи электропитания – 9,16%;
4. Угроза анализа сети – 7,64%.

Также высокую вероятность реализации имеют угроза выявления по сети учетных данных – 3,77%, угроза несанкционированного удаленного запуска ПО – 3,07%, угроза перехвата за пределами контролируемой зоны – 3,06% и угроза распространения по сети вредоносного ПО – 2,29%.

Результаты расчетов вероятностей реализации угроз безопасности ИСПДн для модели продвижения запроса в пределах локальной сети представлены в Таблица 36.

В данной модели наибольшую вероятность реализации имеют следующие угрозы:

1. Катаклизмы или катастрофы – 47,06% от общего количества реализованных угроз;
2. Сбой аппаратных и программных средств – 18,6%;
3. Нарушение подачи электропитания – 9,38%;
4. Угроза анализа сети – 7,47%.

Таблица 36 –Результаты расчетов по каналам ЛВС

Угрозы	Кол-во угроз без защиты	Кол-во угроз с защитой	% от колва угроз без защ	% от колва угроз с защ
Отклонение запроса	244512	9948	1,69067	0,75137
Внедрение неверного объекта в сетях	123544	4064	0,85424	0,30695
Замена довер объекта	121484	4082	0,84000	0,30831
Катаклизмы / катастрофы	2134272	623110	14,75735	47,06347
Нарушение подачи электропитания	587490	124242	4,06218	9,38399
Сбой аппаратных и программных средств	1935978	246284	13,38625	18,60182
Навязывание неверной маршрутизации в сети	128242	3912	0,88672	0,29547
Вывод из строя частей ЭВМ, линий передачи инф.	110152	3868	0,76164	0,29215
Нейтрализация средств защиты	35814	4030	0,24763	0,30439
Угроза анализа сети	527164	98896	3,64506	7,46961
Перехват в пределах КЗ внешними нар.	127900	9980	0,88436	0,75379
Перехват в пределах КЗ сотрудниками	269344	3126	1,86237	0,23611
Выявление по сети учетных данных	1319878	48676	9,12625	3,67650
Перехват за пределами КЗ	47238	24594	0,32663	1,85758
Потеря ключей и атрибутов доступа	1274196	30910	8,81039	2,33463
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	469420	7564	3,24579	0,57131
Хищение, удаление, модификация информации	19126	182	0,13225	0,01375
Несанкционированный удаленный запуск ПО	2374272	37174	16,41682	2,80775
Распространение по сети вредоносного ПО	1273914	24792	8,80844	1,87254
Хищение ЭВМ	17834	216	0,12331	0,01631
Хищение носителей информации	9922	100	0,06861	0,00755
Угроза разглашения персональных данных	44772	512	0,30957	0,03867
Угроза перехвата по каналам наводок	7716	82	0,05335	0,00619
Угроза перехвата видовой информации	7870	80	0,05442	0,00604
Угроза перехвата акустической информации	78758	1014	0,54457	0,07659
Хищение ключей и атрибутов доступа	586142	6188	4,05286	0,46738
Установка ПО, не связанного со служеб. деят.	87582	1038	0,60558	0,07840
Действие вирусов и вредоносного ПО	470444	4988	3,25287	0,37674
Случайный вывод из строя средств защиты	8660	106	0,05988	0,00801
Случайное изменение ПДн сотрудниками	8776	112	0,06068	0,00846
Скрытый функционал системного ПО и ПО для обработки персональных данных	10016	108	0,06926	0,00816

Также высокую вероятность реализации имеют угроза выявления по сети учетных данных – 3,68%, угрозы несанкционированного удаленного запуска ПО – 2,81% и угроза потери ключей и атрибутов доступа – 2,33%.

Добавление в модель имеющихся средств защиты наиболее заметно повлияло на процент количества реализованных угроз от количества всех реализованных угроз для следующих видов угроз:

- Катаклизмы / катастрофы – с 14,76% до 47,06%;
- Несанкционированный удаленный запуск ПО – с 16,42% до 2,33%;
- Угроза распространения по сети вредоносного ПО – с 8,81% до 1,87%;
- Угроза потери ключей и атрибутов доступа – с 8,81% до 1,87%;

- Нарушение подачи электропитания – с 4,06% до 9,38%.

В целях выявления угроз, вероятность реализации которых является высокой для всех построенных моделей, рассмотрим обобщенные результаты, представленные в Таблица 37.

Таблица 37 –Сводные результаты по моделям

№ п/п	Модель продв. запроса по 3G каналам	Модель продв. запроса по VSAT каналам	Модель продв. запроса по лок. сети	Модель продв. запроса по 3G каналам с доп. сервером	Сегмент продв. отопреатора до раб. станции	Сегмент продв. от раб. станции до коммут.	Сегмент продв. от комм. до маршр.	Сегмент продв. по каналу связи	Сегмент продв. от комм. до сервера
1.	Катастр. 47,65%	Катастр 47,2%	Катастр 47,06%	Катастр 46,15%	Катастр 53,31%	Катастр 44,52%	Катастр 48,3%	Катастр 47,93%	Катастр 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.	Наруш. электр. 9,48%	Наруш. электр. 9,41	Наруш. электр. 9,38%	Наруш. электр. 9,16%	Наруш. электр. 10,71%	Угр.скан 8,99%	Наруш. электр. 9,68%	Наруш. электр. 9,52%	Угр.скан 8,44%
4.	Угр.скан 7,04%	Угр.скан 7,78%	Угр.скан. 7,47%	Угр.скан 7,64%	Несан. уд. зап. ПО. 5,27%	Наруш. электр. 8,86%	Угр.скан 9,45%	Угр.скан 9,38%	Наруш. электр. 8,32%
5.	Перехват вне КЗ 3,54%	Выявл. учет. данных 3,84%	Выявл. учет. данных 3,68%	Выявл. учет. данных 3,77%	Потеря ключей 2,68	Угр. внедр. вред. прог. 4,48%	Перехват вне КЗ 4,68%	Перехват вне КЗ 4,79%	Удал. зап. ПО 4,27%
6.	Выявл. уч. данн. 3,68	Удал. зап. ПО. 2,35%	Удал. зап. ПО. 2,81%	Удал. зап. ПО. 3,07%	Хищение ключей 2,66%	Выявл. уч. данных 4,43%	Выявл. уч. дан. 4,65%	Выявл. уч. дан. 4,69%	Перехват вне КЗ 4,24%
7.	Удал. зап. ПО 2,38	Перехват за КЗ 2,34%	Потеря ключей 2,33%	Перехват за КЗ 3,06%	Вирусы 1,07%	Удал. зап. ПО 4,41%	Перехв в КЗ внеш. 0,94%	Перехв в КЗ внеш. 0,96%	Внедр. по сети 4,16%

Как видно из представленных результатов (Таблица 37), вероятности реализации угроз типа «катаклизмы / катастрофы» и «сбой аппаратных и программных средств обработки информации» являются самыми высокими как в моделях в целом, так и в отдельных её сегментах. Причем на эти две угрозы приходится более 60% от всех реализованных угроз. Угрозы, следующие дальше по убыванию вероятности реализации, различаются для моделей в целом и их сегментов. Так для всех четырех моделей за угрозой сбоя аппаратных и программных средств обработки информации следуют нарушение подачи электропитания и угроза анализа сети. Для сегментов системы также далее следуют эти же две угрозы, однако процент реализации

является практически одинаковым, в отличии от общих моделей, где разница процентов реализации данных угроз составляет около двух процентов. Помимо этого для сегмента, на котором запрос проходит от пользователя к ЭВМ угроза анализа сети в принципе не может наступить. Угроза перехвата за пределами контролируемой зоны также является актуальной не для всех моделей. Например, для сегмента поступления запроса от оператора к ЭВМ и модели системы поступления запроса к серверу в пределах локальной сети данная угроза не актуальна.

В целях организации систематизированного хранения полученных результатов разработана и зарегистрирована в государственном реестре программ для ЭВМ программа «Результаты моделирования». Данная программа содержит численные данные, используемые при построении имитационной модели информационной системы «Информационные ресурсы УГИБДД», и результаты экспериментов, проведенных с построенными моделями. В программе также содержатся результаты расчетов качества и значимости защиты от угроз безопасности, применяемой в информационной системе, промежуточные вычисления значений вероятностей наступления и реализации угроз безопасности и определение угроз, вероятность реализации которых является наиболее высокой по сравнению с остальными (Рисунок 24).

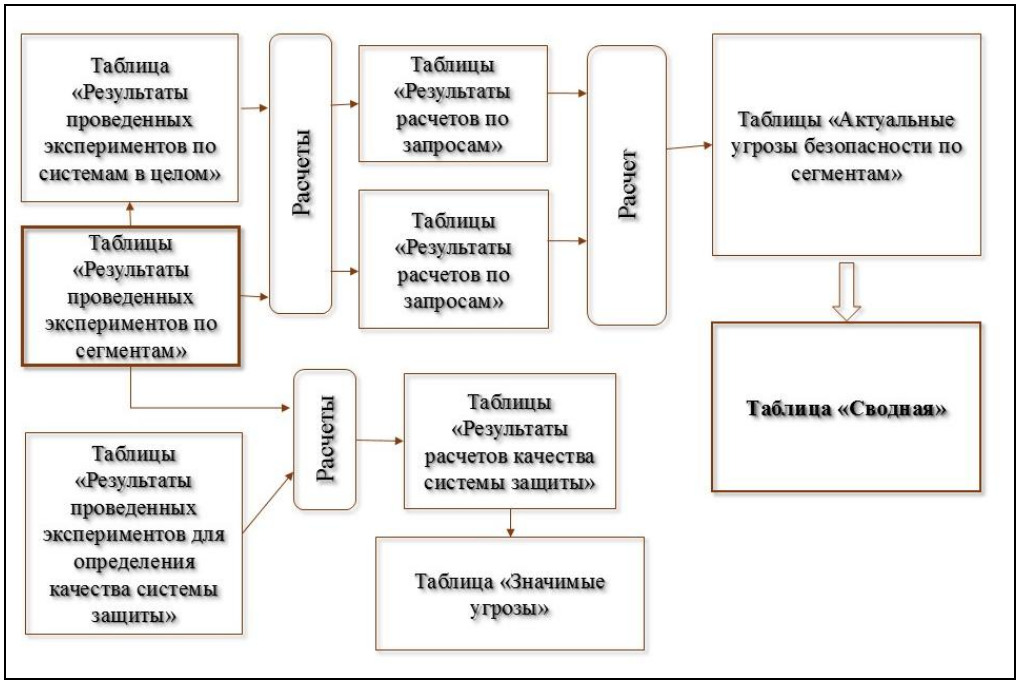

Рисунок 24 - Структура программы для ЭВМ "Результаты моделирования"

В данную программу заносятся все численные значения, полученные в результате проведения экспериментов с имитационными моделями сегментов информационной системы. Как видно из структуры программы (Рисунок 24), используя введенные данные заполняется таблица с результатами расчетов качества и значимости защиты от угроз безопасности, применяемой в информационной системе, промежуточные вычисления значений вероятностей наступления и реализации угроз безопасности и определение угроз, вероятность реализации которых является наиболее высокой по сравнению с остальными, проводятся расчёты по каждой угрозе на каждом сегменте в отдельности и в результате выводятся окончательные результаты.

В целях обеспечения универсальности применения разработанных программ для ЭВМ, повышения удобства доступа к базам данных и повышения наглядности представления полученной информации, разработана и зарегистрирована в государственном реестре программ для ЭВМ программа «Обработка данных имитационной модели (ОДИМ)». Программа объединяет в себе функционал описанных ранее разработанных программ и предназначена для работы со значениями от момента получения первоначальных данных до вывода окончательных результатов. Данная программа позволяет использовать внешние базы данных, что позволит в одном программном продукте обрабатывать сведения о разных информационных системах Программа позволяет вводить и редактировать данные, находящиеся в базах данных, в однопользовательском режиме.

3.3 Расчет необходимости применения дополнительных мер защиты ИСПДн

В целях повышения качества системы защиты предложено дополнительно использовать сертифицированное Федеральной службой по техническому и экспортному контролю программное обеспечение.

Использование программного обеспечения в качестве дополнительной защиты не позволяет защититься от всех угроз сразу, в особенности от угроз стихийного характера или сбоев оборудования, но практически полностью исключает реализацию угроз, связанных с действием нарушителей на программном уровне [26, 37,47, 48, 62, 101].

Для получения информации о состоянии защиты при добавлении еще одной системы защиты в имеющиеся сегменты модели Система защиты добавлена так же, как и на предыдущих этапах построения модели, в виде точки, расположенной на пути реализации угрозы. Вероятности реализации угроз при наличии дополнительной защиты также получены экспертным путем (Таблица 38).

Таблица 38 –Вероятность реализации с системой дополнительной защиты

Наименование угрозы	Вер-тьреализ с доп. защитой
Хищение, удаление, модификация информации	0,005
Действия вредоносного ПО (вирусов)	0,1
Доступ, изменение, удаление ПДн лицами, не допущенными к их обработке	0,005
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей вне контролируемой зоны)	0,005
Угроза «Анализ потока информации в сети» (перехват информации, передаваемой из ИСПДн и принимаемой из внешних сетей, сторонними нарушителями в пределах КЗ)	0,005
Угроза «Анализ потока информации в сети» (перехват информации сотрудниками в пределах контролируемой зоны)	0,005
Угрозы анализа сети, нацеленные на выявление типа системного ПО, сетевых адресов ЭВМ ИСПДн, топологии сети, незаблокированных портов и служб, активных соединений и др.	0,005
Угрозы выявления по сети учетных данных	0,005
Угрозы навязывания неверной маршрутизации в сети	0,005
Угрозы замены доверенного объекта в сети	0,005
Угрозы внедрения неверного объекта как в пределах инф. системы, так и во внешних сетях	0,005
Угрозы распространения по сети вредоносного ПО	0,005

После добавления указанных вероятностей модели приняли следующий вид (Рисунок 25–Рисунок 29):

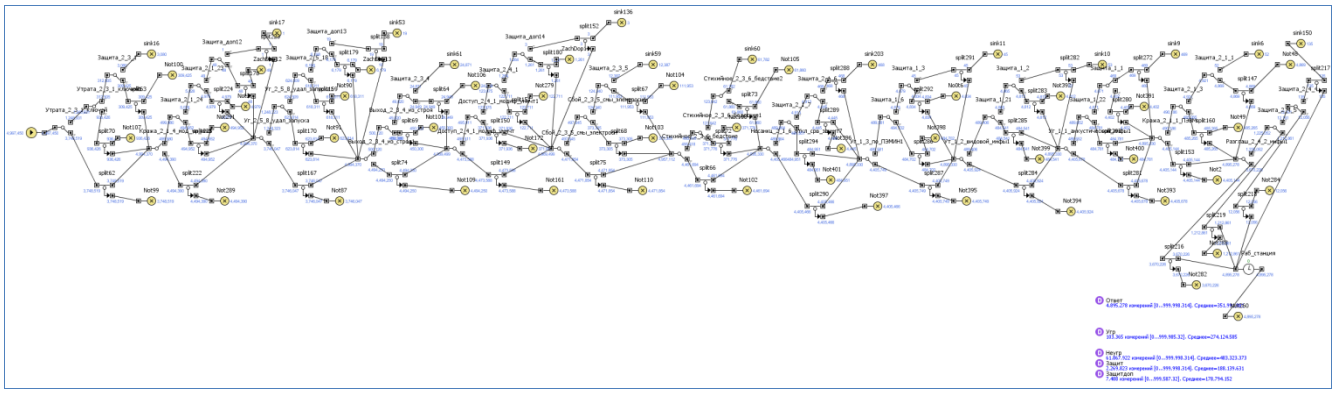

Рисунок 25 – Схема реализации с дополнительной защитой на сегменте «Пользователь - ЭВМ» (скриншот компьютерной реализации модели)

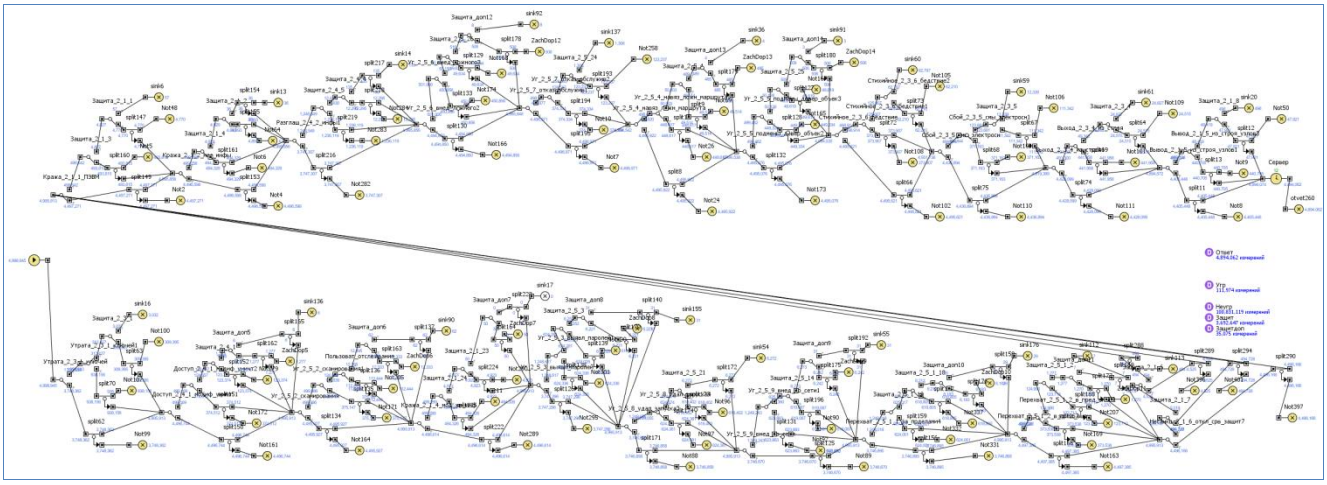

Рисунок 26 – Схема реализации с дополнительной защитой на сегменте «Коммутатор – сервер» (скриншот компьютерной реализации модели)

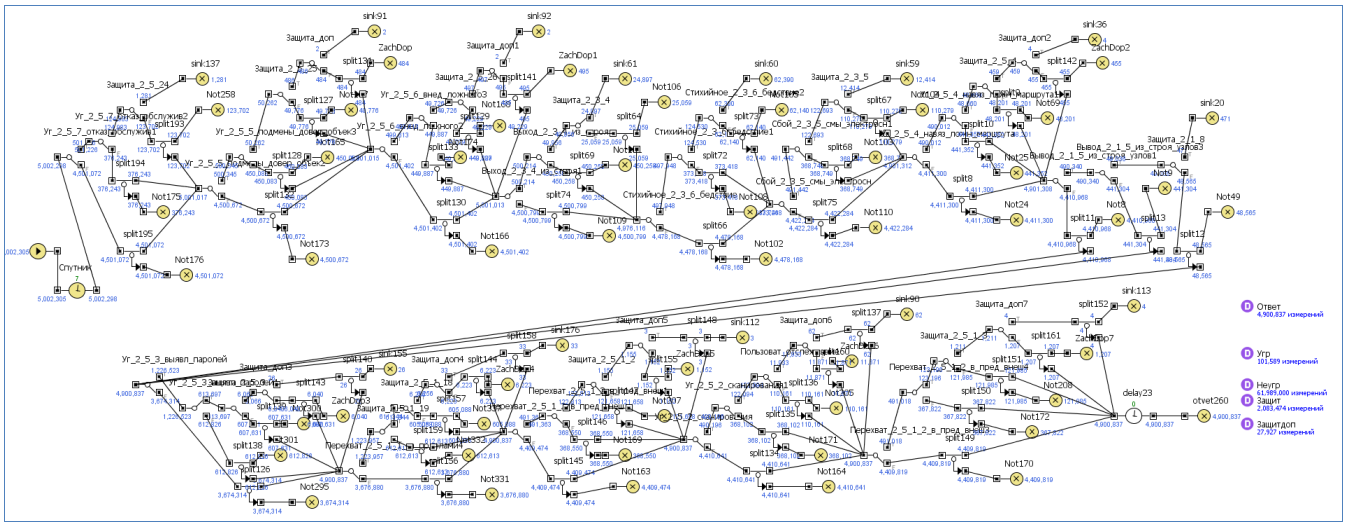

Рисунок 27 –Схема реализации с дополнительной защитой на сегменте «Маршрутизатор – маршрутизатор» (скриншот компьютерной реализации модели)

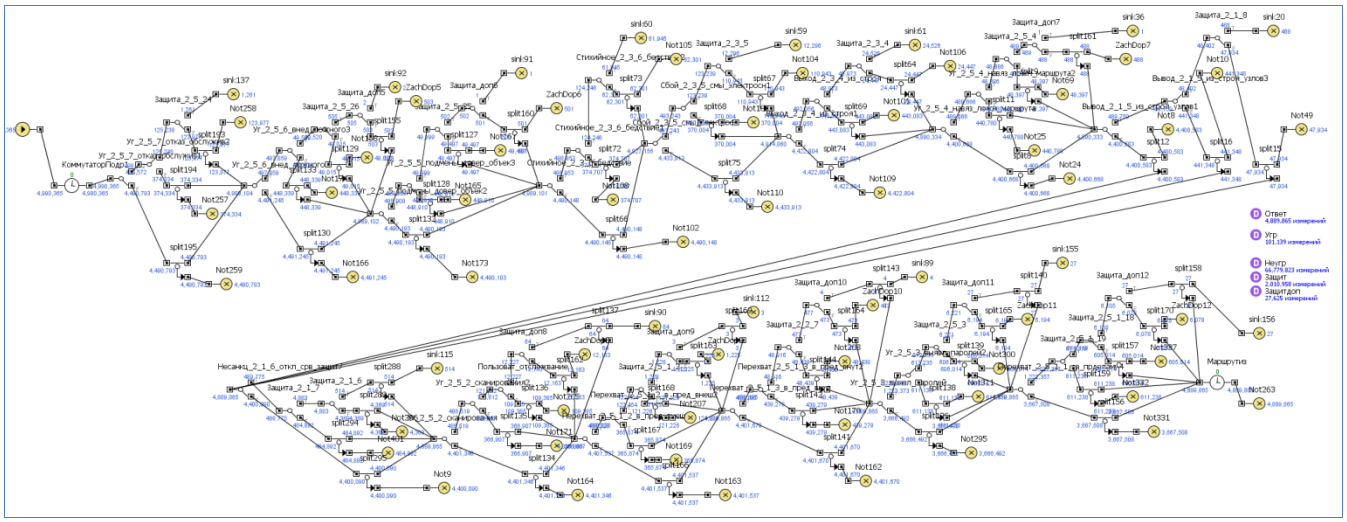

Рисунок 28 – Схема реализации с дополнительной защитой на сегменте «Коммутатор – маршрутизатор» (скриншот компьютерной реализации модели)

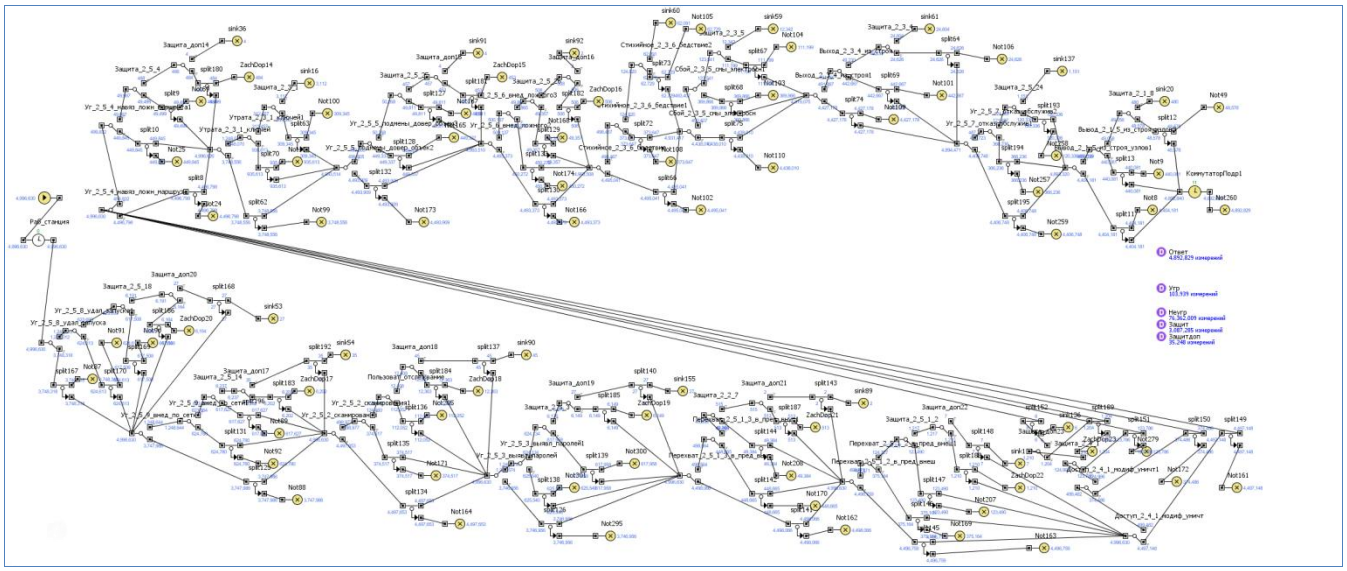

Рисунок 29 – Схема реализации с дополнительной защитой на сегменте «ЭВМ – коммутатор» (скриншот компьютерной реализации модели)

Результаты, полученные в ходе экспериментов с моделью, представлены в Таблица 39.

Таблица 39 –Результаты, полученные в ходе экспериментов с дополненной моделью

Сегмент прохождения запроса	Кол-во запросов поступило	Кол-во запросов окончило	Кол-во реализ. угроз	Кол-во ненаст. угроз	Кол-во угроз, нереализ. с-мой защиты	Кол-во угроз, нереализ. с-мой доп. защиты
От оператора	4999990	4894770	107034	86349871	2762760	8703
От ЭВМ до коммутатора	4996630	4892829	103939	76362009	3087285	35248
От коммутатора к маршрутизатору	4990365	4889865	101139	66779823	2010958	27625
По каналу связи	5002298	4900837	101589	61989000	2077087	27927
От коммутатора до сервера	4991965	4887711	111467	110537437	3814835	36305

Используя полученные данные, проведены расчеты, результаты которых представлены в Таблица 40.

Таблица 40 –Результаты расчетов значений

Сегмент прохождения запроса	Кол-во реализ и нереализ угроз	% заверш. запросов от кол-ва поступивших	% угроз от кол-ва реали и нереализ угроз	% угроз от кол-ва запросов
От оператора до ЭВМ	89228368	97,90%	0,12%	2,14%
От ЭВМ до коммутатора	79588481	97,92%	0,13%	2,08%
От коммутатора к маршрутизатору	68919545	97,99%	0,15%	2,03%
По каналу связи	64195603	97,97%	0,16%	2,03%
От коммутатора до сервера	114500044	97,91%	0,10%	2,23%

Как показали расчеты процент количества завершенных запросов от количества поступивших практически не изменился по сравнению с данным параметром для моделей без дополнительной защиты. Это объясняется тем, что среди угроз, от которых защищает предлагаемая система защиты, нет угроз, препятствующих дальнейшему продвижению запроса. Однако такие параметры, как процент реализованных угроз от количества реализованных, нереализованных и не наступивших и процент реализованных угроз от количества поступивших запросов, уменьшились.

При рассмотрении поведения каждой угрозы в отдельности выделено, что для каждого сегмента более девяноста процентов реализованных угроз являются катаклизмы или катастрофы (составляющая в среднем более 57% от всех реализованных угроз), сбой аппаратных и программных средств обработки информации (в среднем более 22%) и нарушение подачи электропитания (более 11%). Так, для сегмента продвижения запроса между двумя маршрутизаторами по арендуемым или ведомственным каналам связи указанные три угрозы составляют более 98%.

Далее, используя имеющиеся данные, проведем расчеты результатов для моделей продвижения запроса от оператора до сервера и обратно. Результаты расчетов представлены в Таблица 41.

Таблица 41 –Результаты расчетов количества завершенных запросов

Тип связи	% полученных ответов от количества поступивших запросов	% реализ.угроз от общ кол-ва реализованных и нереализованных угроз	% угроз от кол-ва запросов
Спутниковая, оптоволоконная	97,95	0,13	2,09
Dial-Up, GPRS/3G	97,94	0,13	2,11
GPRS/3G с промежуточным сервером	97,93	0,12	2,12
В одной подсети	97,94	0,13	2,1

Как видно из результатов расчетов наличие дополнительной защиты позволяет добиться снижения количества реализованных угроз на единицу запроса. Данный параметр с одной угрозы на 40 запросов уменьшился до одной угрозы на 50 запросов.

Для выявления актуальных угроз представим результаты, полученные для каждой угрозы в отдельности, в сводной таблице (Таблица 42).

Таблица 42 –Сводная таблица полученных вероятностей реализации угроз

Тип угрозы	3G с сервером	ЛВС	VSAT, VPN	Модем
Отклонение запроса	0,96837%	0,93555%	0,98833%	0,89690%
Внедрение неверного объекта в сетях	0,00094%	0,00114%	0,00128%	0,00095%
Замены довер объект	0,00236%	0,00191%	0,00192%	0,00166%
Катаклизмы / катастрофы	58,53056%	59,07154%	59,45151%	58,94964%
Нарушение подачи электропитания	11,59267%	11,71010%	11,79278%	11,68509%
Сбой аппаратных и программных средств обработки информации	23,29906%	23,48271%	23,64895%	23,49909%
Навязывание неверной маршрутизации в сети	0,00204%	0,00152%	0,00192%	0,00166%
Вывод из строя частей ЭВМ, каналов передачи информации	0,38342%	0,36724%	0,38288%	0,34423%
Нейтрализация средств защиты	0,30598%	0,37754%	0,31630%	0,34827%
Угроза анализа сети	0,04351%	0,04307%	0,04598%	0,04249%
Перехват в пределах КЗ внешними нар.	0,00377%	0,00305%	0,00303%	0,00332%
Перехват в пределах КЗ сотрудниками	0,00236%	0,00286%	0,00303%	0,00190%
Выявление по сети учетных данных	0,02450%	0,02268%	0,02315%	0,02160%
Перехват за пределами КЗ	0,01885%	0,01086%	0,01437%	0,02137%
Потеря ключей и атрибутов доступа	2,00837%	1,82327%	1,52753%	1,52601%
Доступ, изменение, удаление персональных данных лицами, не допущенными к их обработке	0,00408%	0,00362%	0,00303%	0,00309%
Хищение, удаление, модификация информации	0,00000%	0,00000%	0,00000%	0,00000%
Несанкционированный удаленный запуск ПО	2,00633%	1,22256%	1,02426%	1,51651%
Распространение по сети вредоносного ПО	0,01586%	0,01296%	0,01086%	0,00783%
Хищение ЭВМ	0,02058%	0,01715%	0,01437%	0,02137%
Хищение носителей информации	0,01288%	0,00781%	0,00655%	0,00973%
Угроза разглашения персональных данных	0,05513%	0,04517%	0,03784%	0,05626%

Продолжение таблицы 42

Тип угрозы	3G с сервером	ЛВС	VSAT, VPN	Модем
Угроза перехвата по каналам наводок	0,00927%	0,01124%	0,00942%	0,01401%
Угроза перехвата видовой информации	0,00723%	0,00877%	0,00734%	0,01092%
Угроза перехвата акустической информации	0,07524%	0,09129%	0,07648%	0,11371%
Хищение ключей и атрибутов доступа	0,49338%	0,59861%	0,50151%	0,74568%
Установка ПО, не связанного со служеб. деят.	0,07555%	0,09167%	0,07680%	0,11419%
Действие вирусов и вредоносного ПО	0,00565%	0,00457%	0,00383%	0,00570%
Случайный вывод из строя средств защиты	0,00848%	0,01029%	0,00862%	0,01282%
Случайное изменение ПДн сотрудниками	0,00817%	0,00991%	0,00830%	0,01234%
Скрытый функционал системного ПО и ПО для обработки персональных данных	0,01539%	0,00934%	0,00782%	0,01163%

Из приведенных расчетов видно, что преобладающее количество угроз для каждого вида модели составляют так же, как и для отдельных сегментов, три угрозы: катаклизмы / катастрофы, сбой аппаратных и программных средств обработки информации и нарушение подачи электропитания. Также вероятность реализации около одного процента от количества реализованных угроз имеют угрозы несанкционированного удаленного запуска ПО, отклонение запроса и угроза потери ключей и атрибутов доступа.

Проанализировав выделенные угрозы и имеющиеся средства борьбы с ними, сделаны следующие выводы:

1. Для защиты от угроз «Катаклизмы / катастрофы», сбой аппаратных и программных средств обработки информации и отклонение запроса принимаются всевозможные меры и добиться снижения вероятности их реализации без значительных финансовых затрат в настоящее время не представляется возможным;

2. Защита от угрозы нарушения подачи электропитания является эффективной, однако, так как при расчете вероятностей реализации угроз учитывались реальные составляющие, которые часто встречаются в подразделениях (например, для запуска генератора необходимо получить ключ, дойти до места установки генератора, заправить и потом уже запустить его, на что тратится время, превышающее время работы источников бесперебойного питания), данная угроза по сравнению с остальными имеет высокий уровень реализации;

3. Угроза несанкционированного удаленного запуска ПО имеет вероятность реализации выше, чем у большинства угроз, так как для удобства управления серверами и ЭВМ используется программное обеспечение для удаленного доступа к ЭВМ. Несмотря на то, что данное программное обеспечение имеет разграничение прав доступа и для подключения требует введения необходимых установок и авторизации пользователя, вероятность доступа к ЭВМ нарушителя возрастет. Однако отказ от использования программного обеспечения для удаленного доступа приводит к возрастанию угроз таких типов, как, например, отклонение запроса, действия вирусов и вредоносного ПО. Это связано с тем, что пропадает возможность оперативного доступа к серверу или ЭВМ для устранения одной из реализованных угроз, особенно это актуально, когда требуется оперативное вмешательство администратора в нерабочее время, во время нахождения от серверной на удаленном расстоянии;

4. Защититься полностью от угрозы потери ключей и атрибутов доступа не представляется возможным, так как данная угроза полностью зависит от человеческого фактора: рассеянности или забывчивости.

Как показали проведенные расчеты, наличие дополнительных программных средств защиты практически не влияет на процент запросов, которые вернулись к пользователю в качестве ответов, однако позволяет исключить угрозы, связанные с действиями внешних или внутренних нарушителей. Исключение наступления указанных угроз с помощью сертифицированного программного обеспечения позволяет использовать информационную систему для обработки персональных данных 2 категории, которой является информационная система «Информационные ресурсы Управления ГИБДД». Несмотря на то, что внедрение дополнительного программного обеспечения в масштабах всего Краснодарского края потребует более 35 миллионов рублей, для обеспечения заданного уровня безопасности и соблюдений требований Российского законодательства это является необходимым.

3.4 Выводы

В результате проведенных вычислений выделены угрозы, которые являются актуальными для рассматриваемой информационной системы. В качестве актуальных выделены угрозы типа «Катаклизмы / катастрофы» и «сбой аппаратных и программных средств обработки информации», причём данные угрозы выделены в качестве актуальных как для информационной системы в целом, так и для отдельных её сегментов. Численные расчёты, проведенные с результатами экспериментов с имитационными моделями, показывают, что процент реализации этих двух типов угроз составил более шестидесяти процентов от общего количества реализованных угроз. Помимо этого в качестве актуальной выделена угроза нарушения подачи электропитания, а также угроза анализа сети, несанкционированного удаленного запуска ПО и угроза потери ключей и атрибутов доступа, процент реализации которых составляет около одного процента от общего количества реализованных угроз, но является высоким по сравнению с другими типами угрозами.

Проанализировав угрозы безопасности, выделенные в качестве актуальных для рассматриваемой информационной системы, и имеющиеся средства защиты от них, сделаны следующие выводы:

1. Используемые средства защиты от таких типов угроз как катаклизмы или катастрофы, сбой аппаратных и программных средств обработки информации и отклонение запроса являются максимально возможными на данный момент и добиться снижения вероятности их реализации без значительных финансовых вложений не представляется возможным;
2. Защита от угрозы нарушения подачи электропитания является эффективной, однако, так как при расчете вероятностей реализации угроз учитывались реальные составляющие, которые часто встречаются в подразделениях (например, неисправность генератора), данная угроза выделена в качестве актуальной;

3. Актуальность угрозы несанкционированного удаленного запуска ПО обусловлена применением в подразделениях программного обеспечения для удаленного доступа к ЭВМ. Несмотря на то, что данное программное обеспечение имеет разграничение прав доступа и для подключения требует введения необходимых установок и авторизации пользователя, вероятность доступа к ЭВМ нарушителем возрастет. Однако отказ от использования данного программного обеспечения приведёт к возрастанию угроз других типов, что в первую очередь, связано с тем, что пропадёт возможность оперативного доступа к серверу или ЭВМ для устранения одной из реализованных угроз, особенно это актуально, когда требуется оперативное вмешательство системного администратора в нерабочее время;

4. Защититься полностью от угрозы потери ключей и атрибутов доступа не представляется возможным, так как данная угроза полностью зависит от человеческого фактора: рассеянности или забывчивости.

Полученные данные также доказывают, что для выделения актуальных угроз вместе со всей информационной системой необходимо рассматривать и её отдельные сегменты. Это связано с тем, что некоторые угрозы, актуальные для какого-либо сегмента, могут не оказывать сколь-нибудь значительного воздействия на систему в целом и наоборот. Для рассматриваемой информационной системы разница в результатах заметная при рассмотрении угроз с низкой вероятностью реализации, а основные три угрозы выделены в качестве актуальных при изучении всех предложенных моделей.

Проведенный анализ прогноза использования дополнительного программного средства защиты информации показал, что его внедрение практически не повлияет на процент запросов, которые вернулись к пользователю в качестве ответов, однако позволит исключить угрозы, связанные с действиями внешних или внутренних нарушителей. Вместе с тем исключение наступления указанных угроз с помощью сертифицированного программного обеспечения позволяет использовать информационную систему для обработки персональных данных 2 категории, которой является

информационная система «Информационные ресурсы Управления ГИБДД». Несмотря на то, что внедрение дополнительного программного обеспечения потребует значительных финансовых затрат, для обеспечения заданного уровня безопасности и соблюдений требований Российского законодательства это является необходимым.

ГЛАВА 4. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

4.1 Применение аналитической модели для выявления актуальных угроз безопасности

С помощью предложенных имитационных моделей можно определить (выявить) угрозы, которые представляют реальную опасность для информационной системы. Однако, используя статистические данные, можно определить такие угрозы также методами математического моделирования.

Рассмотрим аналитическую математическую модель воздействия угроз на указанную информационную систему и на основе этой модели разработать методику их выявления.

Рассматриваемую информационную систему можно интерпретировать как систему массового обслуживания, в которую поступают угрозы (заявки). Вначале рассмотрим ситуацию, когда на вход системы поступает угрозы одного типа, предполагая при этом, что данная угроза не может быть реализована или наступить несколько раз в один и тот же момент времени. Если выполнены указанные предположения, то система может находиться в трёх различных состояниях (Рисунок 30):

1) угроза не поступала, и, соответственно, не была реализована;
2) угроза поступала, но не была реализована;
3) угроза поступала и была реализована.

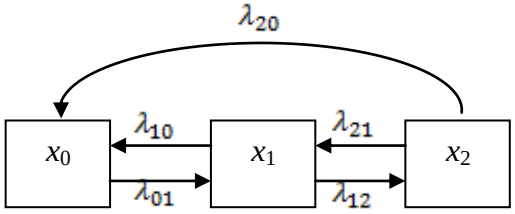

Рисунок 30 –Ориентированный граф переходов из состояния x_i в состояние x_j, $i, j = 0, 1, 2$

Похожая модель информационной системы, которая также может находиться в указанных состояниях, предложена в работах А.П. Росенко [89, 98]. В данных работах допускалось наличие поглощающих состояний системы и выполнение требования, что система не может находиться в одном состоянии в течении некоторого отрезка времени. Указанные допущения не позволяют применить предложенную в [89, 98] математическую модель для анализа реально функционирующих информационных систем, таких как «Информационные ресурсы УГИБДД», потому что у них отсутствуют поглощающие состояния. Это связано с тем, что реализация угрозы либо никак не влияет на работоспособность системы в целом, либо может вывести из строя на непродолжительный промежуток времени только один из её многочисленных сегментов. Если же учитывать возможность возврата системы в исходное состояние, то можно будет изучить её поведение на протяжении длительного промежутка времени.

Рассматриваемая система является системой с восстановлением, так как состояние x_2 не является поглощающим, а значит система может вернуться из x_2 в исходное состояние x_0. Переход системы из состояния x_i в состояние x_j, $i, j = 0, 1, 2$, осуществляется согласно ориентированному графу, представленному на Рисунок 30. Для описания процесса перехода из состояния x_i в состояние x_j, $i, j = 0, 1, 2$, за промежуток времени Δt на основе интенсивностей поступления действующих на нее событий, построена следующая матрица вероятностей перехода системы из состояния в состояние [14]:

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

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

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

Кроме того необходимо учитывать нормированное условие:

$$p_0(t) + p_1(t) + p_2(t) = 1 \quad (3)$$

Элементы матрицы интенсивностей переходов могут быть найдены (вычислены) с помощью предложенных выше имитационных моделей. Опишем вероятностно-аналитический способ их определения. Согласно [14] найти вероятности нахождения системы в каждом из состояний в определенный момент времени можно построив систему дифференциальных уравнений, для чего зафиксируем момент времени $t+\Delta t$ и рассмотрим вероятность пребывания системы в каждом состоянии в отдельности.

Определим вероятность нахождения системы в состоянии x_0 равную $p_0(t+\Delta t)$. В данное состояние система может перейти из следующих состояний:

A. В момент времени t система находилась в состоянии x_0 и за время Δt не перешла в состояние x_1.

B. В момент времени t система находилась в состоянии x_1 и за время Δt перешла в состояние x_0.

C. В момент времени t система находилась в состоянии x_2 и за время Δt перешла в состояние x_0.

Основываясь на вышеизложенном можно найти вероятность нахождения системы в состоянии x_0 в момент времени $(t+\Delta t)$ по теореме сложения вероятностей:

$$p_0(t+\Delta t) = P_0^{(A)} + P_0^{(B)} + P_0^{(C)}$$

где $P_0^{(A)}$ – вероятность того, что за время Δt не перешла в состояние x_1,

$P_0^{(B)}$ – вероятность того, что за время Δt система перешла из состояния x_1 в состояние x_0,

$P_0^{(C)}$ – вероятность того, что за время Δt система перешла из состояния x_2 в состояние x_0.

Вероятность $P^{(A)}(t+\Delta t)$ выразим как произведение вероятности $p_0(t)$ того, что в момент времени t система находилась в состоянии x_0, на вероятность того, что за время Δt не перейдет в другое состояние, равную $e^{-\lambda_{10}\Delta t}$ [14, 34, 98]. С точностью до величин высшего порядка малости получим:

$$e^{-\lambda_{10}\Delta t} \approx 1 - \lambda_{10}\Delta t$$

Следовательно,

$$P_0^{(A)}(t+\Delta t) = p_0(\mathrm{t})(1-\lambda_{10}\Delta t)$$

Найдем вероятность $P_0^{(B)}(t+\Delta t)$ и по аналогии с ней вероятность $P_0^{(C)}(t+\Delta t)$.

Вероятность $P_0^{(B)}(t+\Delta t)$ равна вероятности $p_1(t)$ того, что в момент времени t система находилась в состоянии x_1, умноженная на вероятность перехода за время Δt в состояние x_0:

$$P_0^{(B)}(t+\Delta t) = p_1(\mathrm{t})\lambda_{10}\Delta t$$

И, следовательно:

$$P_0^{(C)}(t+\Delta t) = p_2(\mathrm{t})\lambda_{20}\Delta t$$

Применив правила сложения вероятностей, получим вероятность нахождения системы в состоянии x_0 в момент времени $(t+\Delta t)$:

$$p_0(t+\Delta t) = p_0(\mathrm{t})(1-\lambda_{00}\Delta t) + p_1(\mathrm{t})\lambda_{10}\Delta t + p_2(\mathrm{t})\lambda_{20}\Delta t \Longrightarrow$$
$$p_0(t+\Delta t) - p_0(\mathrm{t}) = -p_0(\mathrm{t})\lambda_{10}\Delta t + p_1(\mathrm{t})\lambda_{10}\Delta t + p_2(\mathrm{t})\lambda_{20}\Delta t$$

Разделим обе части уравнения на Δt и перейдем к пределу при $\Delta t \longrightarrow 0$:

$$\lim_{\Delta t \to 0} \frac{p_0(t+\Delta t) - p_0(\mathrm{t})}{\Delta t} = -p_0(\mathrm{t})\lambda_{10} + p_1(\mathrm{t})\lambda_{10} + p_2(\mathrm{t})\lambda_{20}$$

Из формулы видно, что левая часть уравнения представляет собой производную по времени от функции $p_0(\mathrm{t})$:

$$\frac{dp_0(\mathrm{t})}{dt} = -p_0(\mathrm{t})\lambda_{10} + p_1(\mathrm{t})\lambda_{10} + p_2(\mathrm{t})\lambda_{20}$$

Аналогично определим вероятность нахождения системы в состоянии x_1 равную $p_1(t+\Delta t)$. В данное состояние система может перейти из следующих состояний:

A. В момент времени t система находилась в состоянии x_1 и за время Δt не перешла в другое состояние

B. В момент времени t система находилась в состоянии x_0 и за время Δt перешла в состояние x_1

C. В момент времени t система находилась в состоянии x_2 и за время Δt перешла в состояние x_1

$$p_1(t+\Delta t) = P_1^{(A)} + P_1^{(B)} + P_1^{(C)}$$

где $P_1^{(A)}$ – вероятность того, что за время Δt не перешла в иное состояние,

$P_1^{(B)}$– вероятность того, что за время Δt система перешла из состояния x_0 в состояние x_1,

$P_1^{(C)}$ – вероятность того, что за время Δt система перешла из состояния x_2 в состояние x_1.

Откуда

$$\frac{dp_1(\mathrm{t})}{dt} = p_0(\mathrm{t})\lambda_{01} - p_1(\mathrm{t})(\lambda_{10} + \lambda_{12}) + p_2(\mathrm{t})\lambda_{21}$$

По аналогии с нахождением вероятности пребывания системы в состояниях x_0 и x_1, определим вероятность нахождения системы в состоянии x_2. В данном состоянии система может оказаться двумя способами: перейти из состояния x_1 или оставаться в состоянии x_2.

$$p_2(t + \Delta t) = P_2^{(A)} + P_2^{(B)}$$

где $P_2^{(A)}$ – вероятность того, что за время Δt система не перешла в иное состояние,

$P_2^{(B)}$ – вероятность того, что за время Δt система перешла из состояния x_1 в состояние x_2,

В результате вероятность нахождения системы в x_2 приняло вид:

$$p_2(t + \Delta t) = p_1(\mathrm{t})\lambda_{12}\Delta t - p_2(\mathrm{t})(\lambda_{20} + \lambda_{21})\Delta t$$

Следовательно,

$$\frac{dp_2(\mathrm{t})}{dt} = p_1(\mathrm{t})\lambda_{12} - p_2(\mathrm{t})(\lambda_{20} + \lambda_{21})$$

Таким образом, согласно [14], в соответствии с видом информационной системы (см. Рисунок 30), для определения вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$, где $p_0(t)$ – вероятность нахождения системы в состоянии x_0 в момент времени t, $p_1(t)$ – вероятность нахождения системы в состоянии x_1 в момент времени t, $p_2(t)$ – вероятность нахождения системы в состоянии x_2 в момент времени t, имеем систему дифференциальных уравнений

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

с начальными условиями

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

Полученная система уравнений позволяет найти финальные вероятности нахождения системы в одном из состояний. Задачу Коши (3), (4), представляющую собой математическую модель рассматриваемой информационной системы, можно решить численно, если воспользоваться известными пакетами прикладных программ (например, программой «Mathcad», разработанным фирмой Parametric Technology Corporation).

Рассмотрим возможность расчета вероятностей нахождения системы в одном из возможных состояний через несколько шагов, т.е. переходов из состояния в состояние. В данном случае матрица вероятностей перехода из состояния в состояние имеет вид (1), матрица вероятностей перехода за n шагов (в момент $t = n$) – следующий вид [35, 98]:

$$\|p_{ij}(n)\| = \begin{vmatrix} p_0(t)(1-\lambda_{01})\Delta t & p_0(t)\lambda_{01}\Delta t & 0 \\ p_1(t)\lambda_{10}\Delta t & p_1(t)(1-(\lambda_{10}+\lambda_{12}))\Delta t & p_1(t)\lambda_{12}\Delta t \\ p_2(t)\lambda_{20}\Delta t & p_2(t)\lambda_{21}\Delta t & p_2(t)(1-(\lambda_{20}+\lambda_{21}))\Delta t \end{vmatrix}^n. \quad (5)$$

Так как $p(0) = (1, 0, 0)$ (см. 4) задан, то вектор абсолютных вероятностей $p(n) = (p_0(n), p_1(n), p_2(n))$ определяется соотношением

$$p(n) = p(0)\|p_{ij}(n)\|. \qquad (6)$$

Рассчитать значения вероятностей $p_0(n)$, $p_1(n)$, $p_2(n)$ можно и другим способом [98]. Значения вероятностей $p_0(1)$, $p_1(1)$, $p_2(1)$ нахождения системы в состояниях x_0, x_1 и x_2 при имеющихся исходных данных $p_0(0) = 1,\ p_1(0) = 0,\ p_2(0) = 0$ будут следующими:

$$p_0(1) = 1 - \lambda_{01},$$

$$p_1(1) = \lambda_{01},$$

$$p_2(1) = 0$$

Для сокращения записи формул введем следующие значения:

$$\lambda_{00} = 1 - \lambda_{01},$$

$$\lambda_{11} = 1 - (\lambda_{10} + \lambda_{12}),$$

$$\lambda_{22} = 1 - (\lambda_{20} + \lambda_{21}).$$

После второго шага вероятности состояния системы примут следующий вид:

$$p_0(2) = p_0(1)\lambda_{00} + p_1(1)\lambda_{10} + p_2(1)\lambda_{20} = \lambda_{00}\lambda_{00} + \lambda_{01}\lambda_{10} + 0 \cdot \lambda_{20} = \\ = \lambda_{00}^2 + \lambda_{01}\lambda_{10},$$

$$p_1(2) = p_0(1)\lambda_{01} + p_1(1)\lambda_{11} + p_2(1)\lambda_{21} = \lambda_{01}\lambda_{00} + \lambda_{01}\lambda_{11} + 0 \cdot \lambda_{21} = \\ = \lambda_{01}\lambda_{00} + \lambda_{01}\lambda_{11},$$

$$p_2(2) = p_0(1) \cdot 0 + p_1(1)\lambda_{12} + p_2(1)\lambda_{22} = 0 + \lambda_{01}\lambda_{12} + 0 \cdot \lambda_{22} = \lambda_{01}\lambda_{12}$$

Аналогичным образом определим вероятности нахождения системы в состоянии x_j, i, = 0, 1, 2, после третьего шага:

$$p_0(3) = p_0(2)\lambda_{00} + p_1(2)\lambda_{10} + p_2(2)\lambda_{20} = \\ = (\lambda_{00}^2 + \lambda_{01}\lambda_{10})\lambda_{00} + (\lambda_{01}\lambda_{00} + \lambda_{01}\lambda_{11})\lambda_{10} + \lambda_{01}\lambda_{12}\lambda_{20} = \\ = \lambda_{00}^3 + \lambda_{01}\lambda_{00}\lambda_{10} + \lambda_{01}\lambda_{00}\lambda_{10} + \lambda_{01}\lambda_{11}\lambda_{10} + \lambda_{01}\lambda_{12}\lambda_{20} = \\ = \lambda_{00}^3 + 2\lambda_{01}\lambda_{00}\lambda_{10} + \lambda_{01}\lambda_{11}\lambda_{10} + \lambda_{01}\lambda_{12}\lambda_{20},$$

$$p_1(3) = p_0(2)\lambda_{01} + p_1(2)\lambda_{11} + p_2(2)\lambda_{21} =$$
$$= (\lambda_{00}^2 + \lambda_{01}\lambda_{10})\lambda_{01} + (\lambda_{01}\lambda_{00} + \lambda_{01}\lambda_{11})\lambda_{11} + \lambda_{01}\lambda_{12}\lambda_{21} =$$
$$= \lambda_{00}^2\lambda_{01} + \lambda_{01}^2\lambda_{10} + \lambda_{01}\lambda_{00}\lambda_{11} + \lambda_{11}^2\lambda_{01} + \lambda_{01}\lambda_{12}\lambda_{21}$$

$$p_2(3) = p_0(2)\cdot 0 + p_1(2)\lambda_{12} + p_2(2)\lambda_{22} = 0 + (\lambda_{01}\lambda_{00} + \lambda_{01}\lambda_{11})\lambda_{12} + \lambda_{01}\lambda_{12}\lambda_{22}$$
$$== \lambda_{01}\lambda_{00}\lambda_{12} + \lambda_{01}\lambda_{11}\lambda_{12} + \lambda_{01}\lambda_{12}\lambda_{22}$$

Дальнейший процесс нахождения вероятностей состояний системы не представляет практического интереса, так как решение можно получить с использованием программного обеспечения.

Примеры численной реализации моделей

Пример 1. Зададим матрицу интенсивностей переходов (2):

$$\begin{vmatrix} 0{,}075 & 0{,}075 & 0 \\ 0{,}825 & 0{,}85 & 0{,}025 \\ 0{,}875 & 0 & 0{,}875 \end{vmatrix}.$$

Решим поставленную задачу методом Рунге-Кутты четвертого порядка для момента времени t = 50 с количеством шагов 4 на каждую единицу времени. Вычисления проведем воспользовавшись пакетом прикладных программ.

В результате проведенных вычислений найдены значения вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ для различных моментов времени, которые представлены в Таблица 43.

Таблица 43 –Результаты вычислений значений $p_0(t)$, $p_1(t)$, $p_2(t)$ для различных моментов времени

Значение времени t	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0,951	0,049	0
2	0,93	0,069	0,001
3	0,922	0,076	0,002
4	0,919	0,079	0,002
5	0,918	0,08	0,002
6	0,917	0,081	0,002
…	…	…	…
25	0,917	0,081	0,002
…	…	…	…
50	0,917	0,081	0,002

Следовательно, в момент времени t = 50 $p_0(t)$ = 0,917, $p_1(t)$ = 0,081, $p_2(t)$ = 0,002.

Отобразим на графике изменения значений вероятностей, приведенных в Таблица 43, в зависимости от времени t (Рисунок 31).

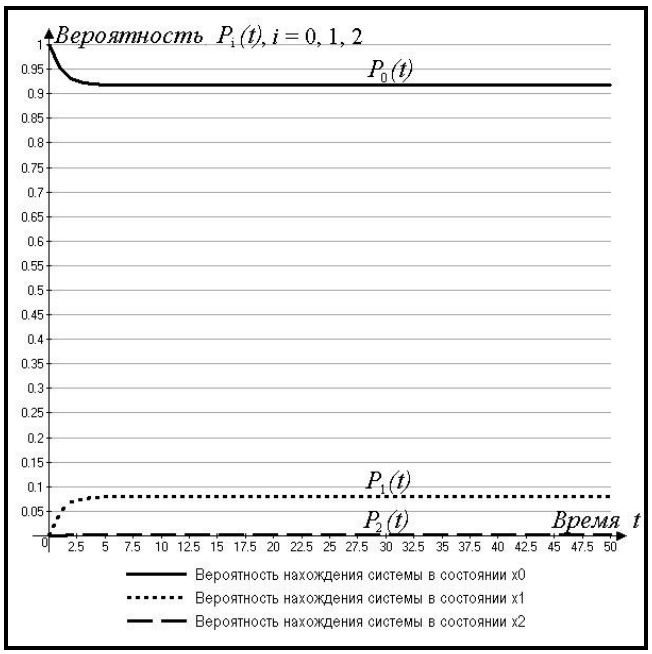

Рисунок 31 –График изменения значений вероятностей $p_i(t)$, i=0, 1, 2, в зависимости от времени t

Пример 2. Зададим матрицу вероятностей перехода:

$$\|p_{ij}\| = \begin{vmatrix} 0{,}9 & 0{,}1 & 0 \\ 0{,}9075 & 0 & 0{,}0025 \\ 1 & 0 & 0 \end{vmatrix},$$

с начальным распределением:

$$p(0) = (1,0,0).$$

Рассчитаем значения вероятностей нахождения системы в состоянии x_i, i = 0, 1, 2, через 8 шагов, также воспользовавшись пакетом прикладных программ. Результаты расчетов приведены в Таблица 44.

Таблица 44 –Результаты вычислений, полученные с использованием программного обеспечения

Шаг эксперимента	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0,9	0,1	0
2	0,88	0,1	0,02
3	0,864	0,108	0,028
4	0,856	0,111	0,033
5	0,852	0,113	0,035
6	0,849	0,114	0,037
7	0,848	0,115	0,038
8	0,847	0,115	0,038

Используя данные, представленные в Таблица 44, построен график изменения значений вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ (Рисунок 32)

Используя предложенную модель можно изучить поведение информационной системы при воздействии на неё угроз одного типа. Однако, для изучения реальной информационной системы рассматриваемую модель необходимо расширить, добавив возможность изучения поведения при воздействии угроз нескольких типов.

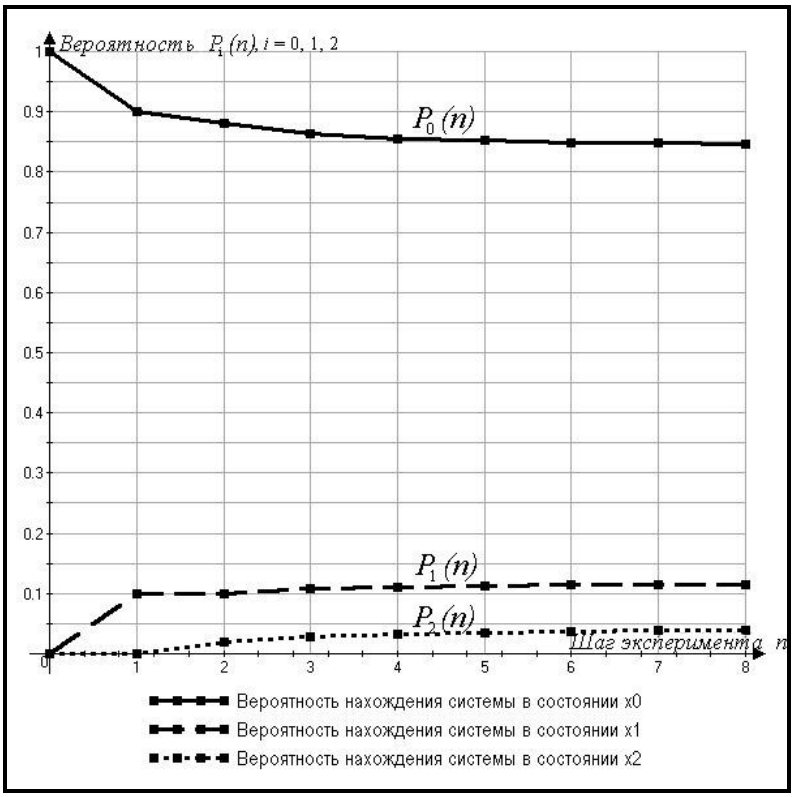

Рисунок 32 – График изменения значений вероятностей $p_i(t)$, i=0, 1, 2 в зависимости от n

4.2 Аналитическая модель воздействия на систему угроз безопасности нескольких видов

Для построения аналитической 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 в один и тот же момент времени Δt;

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

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

Таким образом, представленный ранее ориентированный граф переходов (Рисунок 30) примет следующий вид (Рисунок 33):

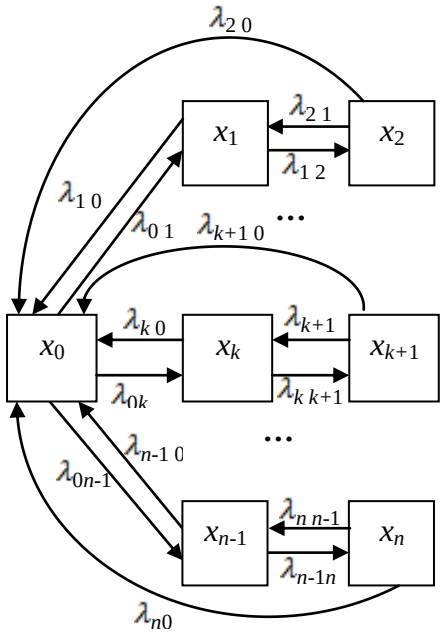

Рисунок 33 - ориентированный граф переходов системы из одного состояния в другое

Матрица интенсивностей переходов (2) примет следующий вид:

$$\|p_{ij}\| = \begin{vmatrix} \lambda_{00} & \lambda_{01} & 0 & \cdots & \lambda_{0k} & 0 & \cdots & \lambda_{0n-1} & 0 \\ \lambda_{10} & \lambda_{10}+\lambda_{12} & \lambda_{12} & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \lambda_{20} & \lambda_{21} & \lambda_{20}+\lambda_{21} & & 0 & 0 & & 0 & 0 \\ & \vdots & & \ddots & & & \iddots & \vdots & \\ \lambda_{k0} & 0 & 0 & \cdots & \lambda_{k0}+\lambda_{kk+1} & \lambda_{kk+1} & \cdots & 0 & 0 \\ \lambda_{k+10} & 0 & 0 & & \lambda_{k+1k} & \lambda_{k+10}+\lambda_{k+1k} & & 0 & 0 \\ & \vdots & & \iddots & & \vdots & \ddots & \vdots & \\ \lambda_{n-10} & 0 & 0 & \cdots & 0 & 0 & \cdots & \lambda_{n-10}+\lambda_{n-1n} & \lambda_{n-1n} \\ \lambda_{n0} & 0 & 0 & & 0 & 0 & & \lambda_{nn-1} & \lambda_{nn-1}+\lambda_{n0} \end{vmatrix}$$

Где $\lambda_0 = \lambda_{01}+\ldots+\lambda_{0\,k}+\ldots+\lambda_{0\,n-1}$

Для построения системы дифференциальных уравнений проделаем действия, описанные выше в случае с моделью воздействия на систему одного вида угроз. В итоге система дифференциальных уравнений для нахождения вероятностей $p_i(t)$, при $i \in [0,n]$, приняла следующий вид:

$$\begin{cases} \frac{dp_0(t)}{dt} = -p_0(t)\lambda_0 + p_1(t)\lambda_{10} + p_2(t)\lambda_{20} + \cdots + p_k(t)\lambda_{k0} + p_{k+1}(t)\lambda_{k+10} + \cdots + p_{n-1}(t)\lambda_{n-10} + p_n(t)\lambda_{n0}, \\ \frac{dp_1(t)}{dt} = p_0(t)\lambda_{01} - p_1(t)(\lambda_{10}+\lambda_{12}) + p_2(t)\lambda_{21}, \\ \frac{dp_2(t)}{dt} = p_1(t)\lambda_{12} - p_2(t)(\lambda_{20}+\lambda_{21}), \\ \cdots \\ \frac{dp_k(t)}{dt} = p_0(t)\lambda_{0k} - p_k(t)(\lambda_{k0}+\lambda_{kk+1}) + p_{k+1}(t)\lambda_{k+1k}, \\ \frac{dp_{k+1}(t)}{dt} = p_k(t)\lambda_{kk+1} - p_{k+1}(t)(\lambda_{k+10}+\lambda_{k+1k}), \\ \cdots \\ \frac{dp_{n-1}(t)}{dt} = p_0(t)\lambda_{0n-1} - p_{n-1}(t)(\lambda_{n-10}+\lambda_{n-1n}) + p_n(t)\lambda_{nn-1}, \\ \frac{dp_n(t)}{dt} = p_{n-1}(t)\lambda_{n-1n} - p_n(t)(\lambda_{n0}+\lambda_{nn-1}). \end{cases}$$

где $\lambda_0 = \lambda_{01}+\ldots+\lambda_{0\,k}+\ldots+\lambda_{0\,n-1}$

По аналогии с (5) также можно найти значения вероятностей нахождения системы в каждом из состояний при переходах из одного состояния в другое.

Численные расчеты, используя предложенную модель, можно осуществить воспользовавшись пакетами прикладных программ также, как и в случае с математической моделью воздействия угроз одного типа, только добавив в расчеты значения вероятностей наступления всех рассматриваемых угроз ПДн. Причем первоначальные данные можно получить используя предложенную ранее математическую модель воздействия на систему угроз одного типа.

4.3 Применение предложенной аналитической модели для изучения поведения некоторых микроэкономических систем

Предложенную выше аналитическую модель можно также использовать для изучения поведения некоторых объектов микроэкономики с помощью аппарата теории дискретных марковских процессов. Рассмотрим поведение некоторой организации на рынке в качестве микроэкономической системы, которая может находиться в каждый момент времени $t \in [0,T]$ в одном из трёх представленных состояний (Рисунок 30):

1) организация производит востребованный потребителями продукт, который не имеет аналогов на рынке, либо имеющиеся аналоги не могут конкурировать с ним по качеству или стоимости (состояние x_0);

2) на рынке имеются аналоги выпускаемой продукции, которые схожи с ней по стоимости и по качеству (состояние x_1);

3) рынок наполнен продукцией фирм-конкурентов, которая превосходит выпускаемый рассматриваемой организацией продукт по качеству, набору функций или стоимости, в связи с чем он не может конкурировать и нуждается обновлении либо полной замене (состояние x_2).

Построим модель для расчета значений вероятностей нахождения системы в состоянии i в момент времени t $p_i(t)$, $i = 0, 1, 2$, $t \in [0,T]$. При разработке модели необходимо учитывать особенность, присущую рынку товаров: значение вероятностей перехода системы из состояния x_1 в состояние

x_0 и из состояния x_2 в состояние x_0 или x_1 равно или близко к 0. Данная особенность возникает в реалиях рыночных отношений в связи с тем, что фирмы производители всегда стремятся занять нишу, востребованную потребителями, предложив замену продукту фирм-конкурентов, который был выпущен ранее. Но нельзя и полностью пренебрегать указанными вероятностями, так как вполне возможно, что представленные аналоги не будут востребованы потребителями, в связи с чем конкуренту придётся уйти с рынка.

Пусть время $t \in [0,T]$ непрерывно. Матрица интенсивностей перехода имеет представленный ранее вид (2) [14].

Согласно [14] для определения вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ получаем систему дифференциальных уравнений:

$$\begin{cases} \frac{dp_0(t)}{dt} = -p_0(t)\lambda_{01} + p_1(t)\lambda_{10} + p_2(t)\lambda_{20}, \\ \frac{dp_1(t)}{dt} = p_0(t)\lambda_{01} - p_1(t)(\lambda_{10} + \lambda_{12}) + p_2(t)\lambda_{21}, \\ \frac{dp_2(t)}{dt} = p_1(t)\lambda_{12} - p_2(t)(\lambda_{20} + \lambda_{21}) \end{cases} \quad (7)$$

Начальные условия вида $p_0(0) = 1,\ p_1(0) = 0,\ p_2(0) = 0,$ которые предложены в [14, 34], в реалиях рынка не всегда будут удовлетворять сложившимся условиям, поэтому целесообразно их задавать в каждом конкретном случае отдельно. Наиболее оптимальным решением будет использование метода экспертных оценок.

Рассмотрим пример 1. Руководством небольшой организации принято решение выпускать бюджетный сотовый телефон. В настоящее время ниша рынка бюджетных телефонов заполнена разнообразной продукцией большого количества фирм-производителей. Продукция рассматриваемой организации является малоизвестной широкому кругу покупателей. Для задания начальных условий экспертами принято решение провести эксперимент: в популярном магазине на продажу выставлен опытный образец планируемого к выпуску телефона. В ходе эксперимента установлено, что опытным образцом телефона в

среднем заинтересовались пять покупателей из десяти, трое – параллельно выбирали между представленным телефоном и телефонами других фирм, схожими по цене и набору функций, двое – не обращая внимания на представленный телефон, делали выбор между предложениями известных фирм. Основываясь на полученные статистические данные, экспертами предложено использовать следующие начальные условия для решения системы уравнений:

$$p_0(0) = 0.5,\ p_1(0) = 0.3,\ p_2(0) = 0.2. \qquad (8)$$

Матрица интенсивностей переходов из состояния x_i в состояние x_j, $i, j = 0, 1, 2$, (за условную единицу времени принята неделя) имеет вид:

$$\begin{vmatrix} 0{,}15 & 0{,}15 & 0 \\ 0{,}05 & 0{,}75 & 0{,}7 \\ 0{,}001 & 0{,}02 & 0{,}021 \end{vmatrix}.$$

Для вычисления вероятностей $p_i(t)$, $i = 0, 1, 2$ воспользуемся пакетами прикладных программ «Mathcad», разработанным Parametric Technology Corporation. Найдем решения системы (7) при предложенных начальных условиях (8) в моменты времени $t = 1, 2, \dots, 40$ [64, 93]. Результаты численных расчетов представлены в Таблица 45.

Таблица 45 –Результаты вычисления $p_i(t)$, i=0, 1, 2, при t – непрерывно

Значение времени t	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0,442	0,195	0,363
2	0,388	0,142	0,47
3	0,34	0,112	0,547
4	0,298	0,095	0,607
5	0,261	0,083	0,656
6	0,229	0,074	0,696
7	0,201	0,068	0,731
8	0,177	0,062	0,761
9	0,156	0,058	0,786
…	…	…	…
20	0,046	0,035	0,92
…	…	…	…
30	0,023	0,03	0,947
…	…	…	…
40	0,018	0,029	0,953

Графики изменения значений этих вероятностей приведены на Рисунок 34.

Из данных, представленных в Таблица 45, и графиков, изображенных на Рисунок 34, следует, что потеря конкурентоспособности представленного телефона очень высокая на коротком промежутке времени. Используя полученные результаты, можно сделать вывод о том, что организации не следует выпускать продукцию на рынок, так как с большой долей вероятности она понесет только убытки.

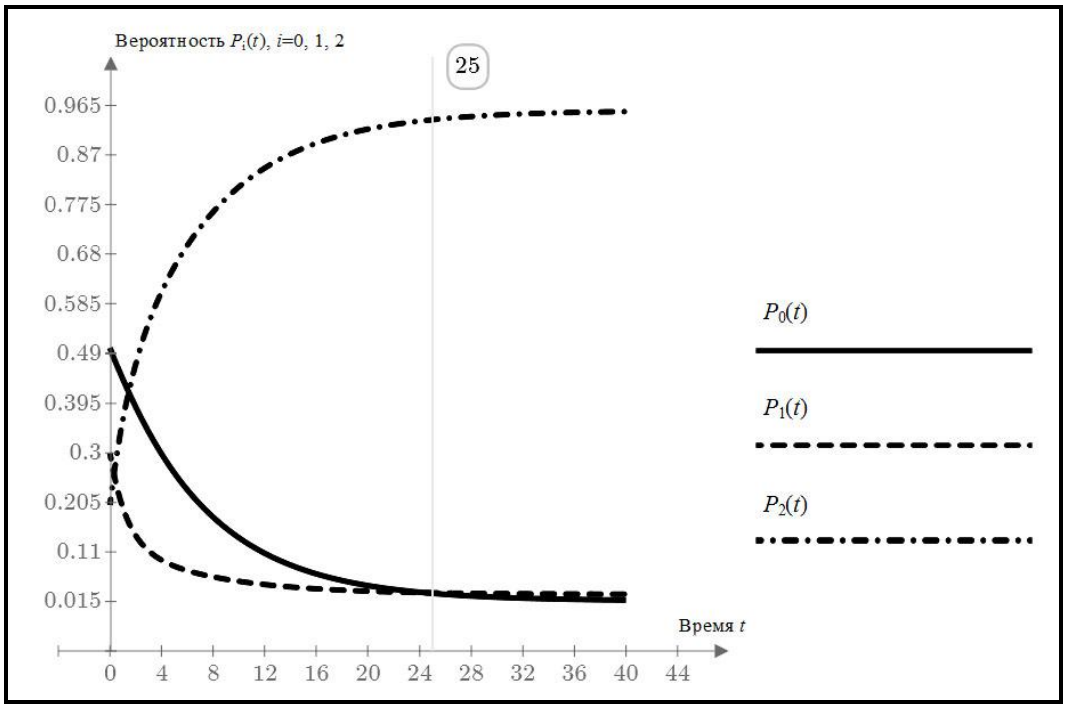

Рисунок 34 – Графики изменения $p_i(t)$, i=0, 1, 2, при

Теперь рассмотрим ситуацию, когда организация выводит на рынок абсолютно новый товар, превосходящий по своим характеристикам товары (сотовые телефоны), представленные на рынке, но с такой же стоимостью. В данном случае, очевидно, экспертами могут быть заданы следующие начальные условия:

$$p_0(0) = 1, \qquad p_1(0) = 0, \qquad p_2(0) = 0,$$

и матрица интенсивностей переходов:

$$\begin{vmatrix} 0,2 & 0,2 & 0 \\ 0,45 & 0,95 & 0,5 \\ 0,05 & 0,15 & 0,2 \end{vmatrix}.$$

Значения вероятностей $p_i(t)$, i = 0, 1, 2, рассчитанные путем решения системы (7) при указанных условиях в моменты времени $t \in [0,40]$, приведены в Таблица 46, графики их изменений – на Рисунок 35.

Таблица 46 – Полученные результаты значений $p_i(t)$, i=0, 1, 2

Значение времени t	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0.849	0.118	0.033
2	0.755	0.154	0.091
3	0.689	0.164	0.147
4	0.639	0.166	0.195
5	0.601	0.165	0.235
6	0.57	0.163	0.266
7	0.546	0.162	0.292
8	0.527	0.161	0.312
9	0.511	0.16	0.328
…	…	…	…
20	0.456	0.157	0.387
…	…	…	…
30	0.451	0.157	0.392
…	…	…	…
40	0.451	0.157	0.392

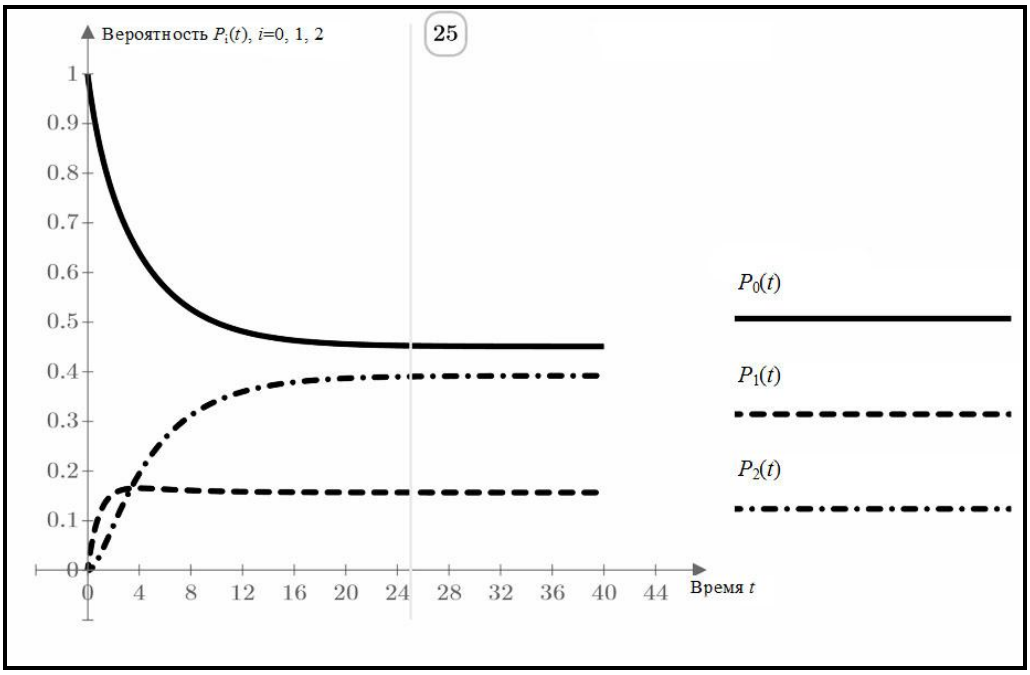

Рисунок 35 – Графики изменения значений $p_i(t)$, i=0, 1, 2

В рассмотренном случае конкурентоспособность продукции, выпускаемой организацией, является высокой, причём с течением времени её конкурентоспособность сохраняется. На основании полученных результатов можно сделать вывод о том, что организации целесообразно производить и реализовывать данный товар.

Теперь рассчитаем вероятности нахождения системы в одном из состояний через определенное количество шагов. Матрица вероятностей перехода из состояния x_i в состояние x_j, i, j = 0, 1, 2, имеет вид [14]:

$$\|p_{ij}\| = \begin{vmatrix} \lambda_{00} & \lambda_{01} & 0 \\ \lambda_{10} & \lambda_{11} & \lambda_{12} \\ \lambda_{20} & \lambda_{21} & \lambda_{22} \end{vmatrix}. \quad (9)$$

где $\lambda_{00} = 1 - \lambda_{01}, \lambda_{11} = 1 - (\lambda_{10} + \lambda_{12}), \lambda_{22} = 1 - (\lambda_{20} + \lambda_{21})$.

Вектор начальных вероятностей, как и начальные условия для математической модели с непрерывным временем, целесообразнее задавать в каждом конкретном случае используя метод экспертных оценок.

Пример 2. Организация производит телевизор с инновационным набором функций, которых не было представлено ранее. Переход системы из состояния в состояние осуществляется при появлении на рынке продукции фирм-конкурентов. Зададим матрицу вероятностей переходов:

$$\begin{vmatrix} 0,2 & 0,8 & 0 \\ 0,05 & 0,2 & 0,75 \\ 0,05 & 0,35 & 0,6 \end{vmatrix}.$$

Учитывая тот факт, что на рынке представлено большое количество моделей телевизоров в разных ценовых диапазонах с различным набором функций и по разной цене, причем выпускаемых крупными фирмами-производителями, хорошо известных широкому кругу потребителей, вектор начальных условий представим в следующем виде:

$$p_0(0) = 0.7, \qquad p_1(0) = 0.3, \qquad p_2(0) = 0.$$

Для расчетов вероятностей также воспользуемся пакетом прикладных программ «Mathcad».

Полученные результаты представлены в Таблица 47.

Таблица 47 –Результаты вычисления значений $p_i(t)$, i=0, 1, 2

Значение t	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0.155	0,62	0,225
2	0.073	0,327	0,6
3	0.061	0,334	0,605
4	0.059	0,327	0,614
5	0.059	0,327	0,614
6	0.059	0,327	0,614

По результатам, полученным в ходе проведения экспериментов с моделью построен график изменения значений $p_i(t)$, i = 0, 1, 2 (Рисунок 36).

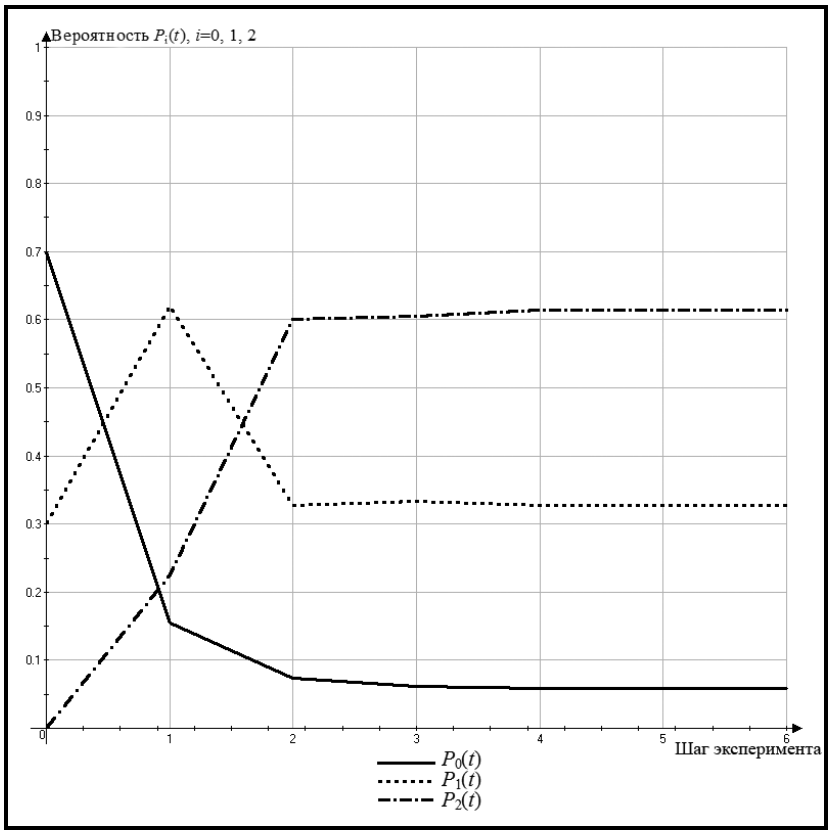

Рисунок 36 –График изменения значений вероятностей $p_i(t)$

Результаты исследования показывают, что значительное изменение конкурентоспособности выпускаемого продукта наблюдается при появлении на рынке первых двух аналогов. После второго шага конкурентоспособность продукта практически не меняется, оставаясь на очень низком уровне, что указывает на необходимость модернизации или замены.

Основываясь на полученные результаты можно сделать вывод о том, что предложенные модели поведения систем могут применяться для оценки конкурентоспособности выпускаемого продукта. При этом можно успешно применять оба типа моделей одновременно. Однако ввиду того, что на рынок товаров воздействует множество факторов, полученные результаты могут носить лишь рекомендательный характер и за непродолжительный промежуток времени полностью утратить актуальность.

4.4 Выводы

Полученные численные результаты применения предложенной методики для анализа моделей поведения информационной системы при воздействии на неё угроз одного типа показали, что их использование позволяет выделить угрозы, которые являются актуальными для рассматриваемой информационной системы и могут использоваться на практике. Недостатком данных аналитических моделей является необходимость рассмотрения воздействия каждого типа угроз в отдельности и невозможность изучения поведения при воздействии нескольких угроз одновременно. Вместе с тем, анализ поведения модели при воздействии на неё каждой угрозы в отдельности позволяет более детально изучить каждый тип угрозы и выделить те, вероятность наступления которых является наиболее высокой.

Для исключения недостатка необходимости изучения воздействия каждой угрозы в отдельности аналитическая модель доработана. Доработанная модель позволяет изучать поведение системы в реальной ситуации, когда на неё воздействуют угрозы нескольких типов, что позволяет выделить угрозы, актуальные для рассматриваемой информационной системы.

Использование обеих моделей одновременно (модели воздействия на информационную систему угроз ПДн одного типа и модель воздействия угроз нескольких типов) позволит не только рассчитать уровень воздействия угроз на систему и выделить из них угрозы, являющиеся актуальными, но и рассмотреть уровень воздействия каждого типа угроз в отдельности.

Приведенные примеры показали, что предложенную математическую модель поведения информационной системы при воздействии на неё угроз одного типа также можно использовать для прогноза конкурентоспособности продукции, выпускаемой на рынок микроэкономической системой, и анализа вопроса о целесообразности его выпуска. Причем при расчете уровня конкурентоспособности выпускаемой продукции можно успешно использовать оба типа предложенных моделей одновременно.

ЗАКЛЮЧЕНИЕ

В ходе выполнения исследования в соответствии с поставленными задачами автором получены следующие научные результаты, использование которых как в отдельности, так и совместно позволяет обеспечить эффективную защиту от угроз безопасности персональных данных, обрабатываемых в информационной системе.

1. Для формирования имитационной модели функционирования системы в реальных условиях эксплуатации и определения на этой основе условий обеспечения безопасности обработки и хранения 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 аналитическая 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.

В настоящее время предложенные модели планируется применить для исследования иных ИСПДн, использующих подразделениями МВД России по Краснодарскому краю. Для обработки и хранения результатов разработанная программа «ОДИМ» дорабатывается для возможности работы с сервером баз данных, который будет централизованным для всего края, работы в многопользовательском режиме с разграничениями прав пользователей, создания аналогичного набора таблиц в базе данных для хранения, обработки, сравнения результатов различных ИСПДн.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

3G – third generation — третье поколение, набор услуг, который объединяет как высокоскоростной мобильный доступ с услугами сети Интернет, так и технологию радиосвязи, которая создаёт канал передачи данных

EDGE – Enhanced Datarates for GSM Evolution — цифровая технология беспроводной передачи данных для мобильной связи

GPRS – General Packet Radio Service — пакетная радиосвязь общего пользования

MPLS – multi protocol label switching — многопротокольная коммутация по меткам

VPN – Virtual Private Network — виртуальная частная сеть

VSAT – Very Small Aperture Terminal — малая спутниковая наземная станция

xDSL – digital subscriber line, цифровая абонентская линия (семейство технологий)

БД – база данных

ЕИТКС – Единая информационная телекоммуникационная система

ИСПДн – информационная система обработки персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

ПДн – персональные данные

ПО – программное обеспечение

ЭВМ – электронная вычислительная машина

ПЭМИН – побочные электромагнитные излучения и наводки

СЗПДн – средства защиты персональных данных

ФСТЭК - Федеральная служба по техническому и экспортному контролю

СПИСОК ЛИТЕРАТУРЫ

1. Anylogic. Справочное руководство по Enterprise Library. –XJ Technologies Company Ltd., 2004. – 134 с.

2. Anylogic. Учебное пособие по агентному моделированию. –XJ Technologies Company Ltd., 2004. – 53 с.

3. Anylogic. Учебное пособие по системной динамике. –XJ Technologies Company Ltd., 2004. – 61 с.

4. Anylogic. Учебное пособие по Enterprise Library. –XJ Technologies Company Ltd., 2004. – 117 с.

5. Giks W.R. Markov Chain Monte Carlo in Practice / W.R. Giks, S. Richardson, D.J. Spiegelhalter. – Chapman and Hall/CRC, 1995. – 512 p.

6. Leemis L.M. Discrete–Event Simulation: A First Course / L.M. Leemis, S.K. Park. – Prentice Hall, 2004. – 538 p.

7. Liang F. Advanced Markov Chain Monte Carlo Methods: Learning from Past Samples / F. Liang, C. Liu, R.J. Carroll. – Wiley, 2010. – 378 p.

8. MacDonald M. Access 2013: The Missing Manual / M. MacDonald. – O'Reilly Media Inc., 2013. – 866 p.

9. Understanding Computer Simulation / R. Mc Haney. –Roger Mc Haney & Ventus Publishing ApS, 2009. – 172 p.

10. Microsoft Corp. Руководство по продукту Microsoft Access 2010. – Microsoft, 2010. – 60 p.

11. Microsoft Corporation. Проектирование и реализация баз данных Microsoft SQL Server 2000. Учебный курс MCAD / MCSE, MCDBA.— 2–е изд., испр. — М.: Издательско–торговый дом «Русская Редакция», 2003. – 512 с. (На русском языке.)

12. Mielke A. (Ed.) Analysis, Modeling and Simulation of Multiscale Problems / A. Mielke. – Springer, 2006. – 703 p.

13. Stewart W.J. Probability, Markov Chains, Queues, and Simulation: The Mathematical Basis of Performance Modeling / W.J. Stewart. – Princeton University Press – 2009, 776 p.

14. Алиев Т.И. Основы моделирования дискретных систем: Учебное пособие / Т.И. Алиев. – СПб: СПбГУ ИТМО, 2009. – 363 с.

15. Алтаев А.А. Имитационное моделирование на языке GPSS: Методическое пособие по дисциплине "Компьютерное моделирование" / А.А. Алтаев. – Улан–Удэ: Изд–во ВСГТУ, 2001. – 122 с.

16. Альсова О.К. Моделирование систем / О.К. Альясова. – Новосибирск: НГТУ, 2006. – 68 с.

17. Атре Ш. Структурный подход к организации баз данных / Ш. Арте. – М.: «Финансы и статистика», 2003.

18. Афонин В.В. Моделирование систем. Практикум по GPSS/PC / В.В. Афонин. –Саранск: Изд–во Мордов. университета, 2000. – 184 с.

19. Афонин В.В. Моделирование систем / В.В. Афонин, С.А. Федосин. –М.: Интернет–университет информационных технологий: Бином. Лаборатория знаний, 2010. – 231 с.: ил.

20. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утверждена заместителем директора ФСТЭК России 15 февраля 2008г. [Электронный ресурс] // Федеральная служба по техническому и экспортному контролю. – Режим доступа: http://www.fstec.ru/_spravs/ (дата обращения: 17.02.2011)

21. Бармен С. Разработка правил информационной безопасности / С. Бармен. – Вильямс, 2002. – 208 с.

22. Бахвалов Л.А. Компьютерное моделирование: долгий путь к сияющим вершинам / Л.А. Бахвалов // Компьютерра. – 1997. – № 40. – С.26–36.

23. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось. – М.: Горячая линия – Телеком, 2006. – 544 с.: ил.

24. Бен–Ган И. Microsoft SQL Server 2008. Основы T–SQL. Перевод с английского / И. Бен-Ган. — СПб.: БХВ–Петербург, 2009. – 432 с.: ил.

25. Березин Д.А. Имитационное моделирование. Учебное пособие / Д.А. Березин.–Екатеринбург 2008. – 94 с.

26. Блинов А.М. Информационная безопасность: Учебное пособие / А.М. Блинов.– СПб.: Изд–во СПбГУЭФ, 2010. – Часть 1. – 96 с.

27. Боев В.Д. Компьютерное моделирование: Пособие для курсового и дипломного проектирования / В.Д. Боев, Д.И. Кирик, Р.П. Сыпченко. — СПб.: ВАС, 2011. – 348 с.

28. Боев В.Д. Моделирование систем. Инструментальные средства GPSS World: Учебное пособие / В.Д. Боев, БХВ–Петербург, 2004. – 368 с.

29. Брайан Х. Полный справочник по Cisco = Cisco: The Complete Reference / Х. Брайн. — М.: «Вильямс». – 1088 с.

30. Бродский Ю.И. Распределенное имитационное моделирование сложных систем / Ю.И. Бродский. –М.: Вычислительный центр им. А.А. Дороницына РАН, 2010. – 156 с.

31. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г.А. Бузов. – М.: Горячая линия. – Телеком, 2010. – 240 с.

32. Введение в математическое моделирование: учебное пособие / под ред. П.В. Трусова. – изд.: Логос, 2004. – 440 с.

33. Вентцель Е.С. Исследование операций: задачи, принципы, методология / Т/С/ Вентцель. – 2–е изд., стер.– М.: Наука, Гл. ред. Физ.–мат. Лит., 1988.– 208 с.

34. Вентцель Е.С. Теория вероятностей / Е.С. Вентцель. – М.: Наука, 1969. – 576 с.

35. Волков И.К. Случайные процессы: Учебник для ВУЗов / Волков И.К., Зуев С.М., Цветкова Г.М.; под ред. В.С. Зарубина, А.П. Крищенко. – М.: МГТУ им. Баумана, 1999. – 448 с.

36. Волоха А.В. Microsoft SQL Server 2005. Новые возможности: Учебник / А.В. Волоха. –СПб.: Питер, 2006. –304 с.: ил.

37. Герасименко В.А., Основы защиты информации / В.А. Герасименко, А.А. Малюк.– М.: МИФИ, 1997. – 538 с.

38. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания / Б.В. Гнеденко, И.Н. Коваленко – М.: Наука, 1966. – 432 с.

39. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебное пособие / В.Г. Грибунин, В.В Чудовский. – М. : Издательский центр «Академия», 2009. – 416 с.

40. Доценко С.М. Комплексная информационная безопасность объекта – от теории к практике / С.М. Доценко, В.Ф. Шпак. – ООО «Издательство Полигон», 2000. – 130 с.

41. Дудин А.Н., Практикум на ЭВМ по теории массового обслуживания: Учебное пособие / А.Н. Дудин. – Мн.: "Электронная книга БГУ", 2003.

42. Духанов А.В. Имитационное моделирование сложных систем: Курс лекций / А.В. Духанов. – Изд–во Владим. гос. ун–та, 2010. – 115 с.

43. Дэвид Х. Руководство Cisco по конфигурированию коммутаторов Catalyst = Cisco Field Manual: Catalyst Switch Configuration / Х. Дэвид, Стив Мак–Квери. – М.: «Вильямс», 2004. – 560 с.

44. Евсеева О.Н. Имитационное моделирование на языке GPSS: Методические указания / О.Н. Евсеева, В.В. Шишкин. – Ульяновск: УлГТУ, 1995. – 40 с.

45. Емельянов А.А. Имитационное моделирование экономических процессов: Учеб. пособие / А.А. Емельянов, Е.А. Власова, Р.В. Дума; под ред. А.А. Емельянова. – М.: Финансы и статистика, 2002. –368 с: ил.

46. Емельянов В.В. Имитационное моделирование систем, язык и среда РДО / В.В. Емельянов, С.И. Ясиновский. – Изд–во МГТУ им. Баумана, 2009. –583 с.

47. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие / В.И. Завгородний. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. –264 с : ил.

48. Зефиров С.Л. Как измерить информационную безопасность организации? Объективно о субъективном / С.Л. Зефиров, В.Б. Голованов // Защита информации. – Инсайд. – 2006. – № 3.

49. Зибиров В.В. Visual Basic 2010 на примерах / В.В. Зибиров. — СПб.: БХВ–Петербург, 2010. – 336 с.: ил. + CD–ROM.

50. Зиновьев В.В. Компьютерная имитация и анимация: Учебное пособие / В.В. Зиновьев. – Кузбас. гос. техн. ун–т. – Кемерово, 2003. – 77 с.

51. Зыков С.В. Введение в теорию программирования. Функциональный подход / С.В. Зыков. – Учебный Центр безопасности информационных технологий Microsoft МИФИ, 2003.

52. Ивченко Г.И. Теория массового обслуживания: Учебное пособие для вузов / Г.И. Ивченко, В.А. Каштанов, И.Н. Коваленко. – М.: Высшая школа, 1982. – 256 с.

53. Имитационное моделирование // Википедия [Электронный ресурс]. — Режим доступа:http://ru.wikipedia.org/wiki/%C8%EC%E8%F2%E0%F6%E8%EE%ED%ED%EE%E5_%EC%EE%E4%E5%EB%E8%F0%EE%E2%E0%ED%E8%E5#cite_note–1 (дата обращения: 12.06.2013)

54. Имитационное моделирование // Виртуальная лаборатория [Электронный ресурс]. — Режим доступа: http://ru.vlab.wikia.com/wiki/Имитационное_моделирование (дата обращения: 13.06.2013)

55. Имитационное моделирование [Электронный ресурс]. — Режим доступа: http://финансы–кредит.рф/voprosyi–menedjmenta–obschie/imitatsionnoe–modelirovanie–20717.html (дата обращения: 12.06.2013)

56. Казарин О.В. Теория и практика защиты программ / О.В. Казарин. – М., 2004. – 450 с.

57. Калиткин Н.Н. Численные методы / Н.Н. Калиткин. – М.: Наука, 1978. – 512 с.

58. Карпов Ю.Г. Изучение современных парадигм информационного моделирования в среде AnyLogic / Ю.Г. Карпов // Компьютерные инструменты в образовании. – СПб.: Изд–во ЦПО "Информатизация образования".– 2005.– №12. – С. 03–14.

59. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5.0 / Ю.Г. Карпов. – СПб.: БХВ–Петербург, 2005. – 400 с.: ил.

60. Касперски К. Компьютерные вирусы внутри и снаружи / К. Касперски. – СПб.: Питер, 2006. – 527 с.: ил.

61. Каталевский Д.Ю. Основы имитационного моделирования и системного анализа в управлении: Учебное пособие / Д.Ю. Каталевский. — М.: Издательство Московского университета, 2011. — 304 с.: ил.

62. Каторин Ю.Ф. Защита информации техническими средствами: Учебное пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак; под редакцией Ю.Ф. Каторина.– СПб: НИУ ИТМО, 2012. – 416 с.

63. Кельтон В.Д. Имитационное моделирование / В.Д. Кельтон, А.М. Лоу. – 3–е изд. — СПб.; Питер: Киев: Издательская группа BHV, 2004. — 847 с.: ил.

64. Кирьянов Д.В. Самоучитель Mathcad 11 / Д.В. Кирьянов. – СПб.: БХВ–Петербург, 2003. – 560 с.: ил.

65. Киселева М.В. Имитационное моделирование систем в среде AnyLogic: учебно – методическое пособие / М.В. Киселёва. – Екатеринбург: УГТУ – УПИ, 2009. – 88 с.

66. Колдаев В.Д. Графовый подход к моделированию информационного образовательного пространства [Электронный ресурс] // Publishing house Educationand Science s.r.o. – 2012. – Режим доступа: http://www.rusnauka.com/10_DN_2012/Pedagogica/5_106179.doc.htm (дата обращения: 07.06.2013)

67. Королев А.Г. Моделирование систем средствами Object GPSS. Практический подход в примерах и задачах: Учеб. Пособие / А.Г. Королев. – Северодонецк, 2008. – 219 с.

68. Кудашов К.В. Руководство пользователя по GPSS World / К.В. Королев. – Казань, изд–во "Мастер Лайн", 2002. – 384 с.

69. Левин В.К. Защита информации в информационно–вычислительных системах и сетях / В.К. Левин // Программирование. – 2004. – №5. – С. 5–16.

70. Левин М. Руководство для хакеров / М. Левин. — М.: Бук_пресс, 2006. — 416 с.

71. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы / Б. Леонтьев. –М.: Познавательная книга, 1998. – 192 с.

72. Лычкина Н.Н. Имитационное моделирование экономических процессов. Учебное пособие для слушателей программы eMBI / Н.Н. Лычкина.– М.: Академия АйТи, 2005. – 96 с.

73. Мамаева З.М. Введение в моделирование / З.М. Мамаева. – Н. Новгород, ННГУ, 2005. – 120 с.

74. Мельников В. Защита информации в компьютерных системах / В. Мельников. – М.: Финансы и Статистика, 1997, – 368 с.

75. Михеев Р. MS SQL сервер 2005 для администраторов / Р. Михеев. – СПб.: БХВ–Петербург, 2007. — 519 с.

76. Моделирование [Электронный ресурс]. — Режим доступа: http://www.sportologica.ru/articles/5/Modeling.html (дата обращения: 13.06.2013)

77. Монахов А.Д. К вопросу об использовании имитационной среды Anylogic для оценки эффективности вычислительных систем / А.Д. Монахов // Науковедение. Интернет журнал. URL: http://naukovedenie.ru/index.php?id=168

78. Муха В. С. Вычислительные методы и компьютерная алгебра: учеб.–метод. Пособие / В.С. Муха. — 2–е изд., испр. и доп. — Минск: БГУИР, 2010.– 148 с.: ил.

79. О внесении изменения в статью 25 Федерального закона "О персональных данных": Федеральный закон от 23 декабря 2010 г. № 359–ФЗ: принят Государственной Думой 10 декабря 2010 г.: одобрен Советом Федерации 15 декабря 2010 г. // Российская газета. – 2010. – 27 декабря.

80. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152–ФЗ: принят Государственной Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // Российская газета. – 2006. – 29 июля.

81. Об упорядочивании прав доступа пользователей, учета, организации работы, обработки, хранении и защиты информации в автоматизированной системе (АС) УГИБДД ГУВД КК: Приказ УГИБДД ГУВД по Краснодарскому краю от 13 ноября 2006 года №149.

82. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных:

методика: утверждена заместителем директора ФСТЭК России 14 февраля 2008г. // Федеральная служба по техническому и экспортному контролю. – URL: http://www.fstec.ru/_spravs/ (дата обращения: 17.02.2011).

83. Осоргин А.Е. AnyLogic 6. Лабораторный практикум / А.Е. Осоргин. – Изд. 2–е, перераб. и доп. – Самара: ПГК, 2012. – 110 с.

84. Н. Патрик . Java 2. Наиболее полное руководство: Пер. с англ. / Патрик Н., Герберт Ш. – Спб.:ИРМПитербург, 2007.

85. Пелланд П. Переход к Microsoft Visual Studio 2010 / П. Пелланд, П. Паре. – Изд–во MicrosoftPress, 2011. – 256 с.

86. Петкович Д. Microsoft SQL Server 2008. Руководство для начинающих / Д. Петкович.– СПб.: БХВ–Петербург, 2009. – Часть 1. – 752 с.

87. Рендольф Н. Visual Studio 2010 для профессионалов / Д. Гарднер, К. Андерсон, М. Минутилло.: Изд–во Диалектика, 2011. – 1184 с.

88. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – 2–е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.: ил.

89. Росенко А.П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе / А.П. Росенко // Известия ЮФУ. Технические науки. Тематический выпуск. «Информационная безопасность». – Таганрог: Изд–во ТТИ ЮФУ. – 2008. – №8 (85).

90. Савина О.А. Имитационное моделирование экономических систем и процессов: Учебное пособие / О.А. Савина. – Орел: ОрелГТУ, 2004. – 172 с.

91. Сёмкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие / С.Н. Сёмкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. — М.: Гелиос АРВ, 2005. – 192 с.

92. Советов Б.Я. Моделирование систем: Учебник для ВУЗов / Б.Я. Советов, С.А. Яковлев.– 3–е изд., перераб. и доп. – М.: Высшая школа, 2001. – 343 с.

93. Солодов А.П. Mathcad/Дифференциальные модели / А.П. Солодов, В.Ф. Очков. – М.: Издательство МЭИ, 2002. – 239 с.: ил.

94. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А.А. Стрельцов.— М., МЦНМО, 2002. – 296 с.

95. Строгалев В.П. Имитационное моделирование: Учеб. Пособие / В.П. Строгалев, И.О. Толкачева. – М.: Изд–во МГТУ им. Н.Э. Баумана, 2008. – 280 с.: ил.

96. Сычев Ю.Н. Информационная безопасность. Учебно–практическое пособие / Ю.Н. Сычев.– М.: Изд. центр ЕАОИ, 2007. –300 с.

97. Таха. Введение в исследование операций. Пер. с англ. / Таха, А. Хемди. – 7-е издание. — М.: Издательский дом “Вильямс”, 2005. — 912 е.: ил.

98. Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: монография / А.П. Росенко. – М.: Гелиос АРВ, 2008. – 154 с.

99. Томашевский В. Имитационное моделирование в среде GPSS / В. Томашевский, Е. Жданова.– М.: Бестселлер, 2003. – 416 с.

100. Финаев В.И. Алгоритмизация и имитационное моделирование с применением аппарата систем массового обслуживания: Учебное пособие / В.И. Финаев. – Таганрог: ТГРТУ, 2003. – 72 с.

101. Фленов М.Е. Компьютер глазами хакера / М.Е. Фленов. – СПб.: БХВ–Петербург, 2005. – 336с.: ил.

102. Харин Ю.С. Основы имитационного и статистического моделирования: Учебное пособие / Ю.С. Харин. – Минск: Дизайн ПРО, 1997. – 288 с.

103. Харрингтон Джен Л. Проектирование реляционных баз данных / Джен Л. Харрингтон. – Москва, издательство "Лори", 2006. – 241 с.

104. Хендерсон К. Профессиональное руководство по SQL Server: хранимые процедуры, XML, HTML / К. Хендерсон. – СПб.: Питер, 2005. – 620 с.: ил.

105. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков; под ред. Ю.С. Ковтанюка. – К.: Издательство Юниор, 2003. – 504 с.

106. Цирлов В.Л. Основы информационной безопасности. Краткий курс / В.Л. Цирлов. – М.: Феникс, 2008. – 253 с.

107. Чернецкий В.И. Математическое моделирование динамических систем / В.И. Чернецкий. – Петрозаводск: ПГУ, 1996. – 432 с.

108. Шаньгин В.Ф Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. — М. :ИД «Форум».: ИНФРА–М, 2010. – 592 с.

109. Шелухин О.И. Моделирование информационных систем / О.И. Шелухин, А.М. Тенякшев, А.В. Осин — М.: Радиотехника, 2005. — 368 с.

110. Шеннон Р. Имитационное моделирование систем – искусство и наука. / Р. Шеннон. — М.: Мир, 1978.

111. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.

112. Шувалов И.А. Имитационная модель угроз безопасности информационной системы обработки персональных данных / Шувалов И.А. // 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. – Том 2.

113. Шувалов И.А. Моделирование сегментов информационной системы обработки персональных данных / Шувалов И.А. // 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. – Том 2.

114. Шувалов И.А. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте «коммутатор – сервер» / Шувалов И.А., Росенко А.П. // Вестник Дагестанского государственного университета. – 2013. – Вып. 1. – С. 112-123.

115. Шувалов И.А. Имитационная модель реализации внутренних и внешних угроз безопасности сегмента системы «Информационные ресурсы Управления ГИБДД» / Шувалов И.А., Росенко А.П., Семенчин Е.А. // Известия Кубанского государственного университета. Естественные науки. — 2012. — №1. — С. 32-41.

116. Шувалов И.А. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте “Маршрутизатор – маршрутизатор” / Шувалов И.А., Семенчин Е.А. // Фундаментальные исследования. – 2012. – № 9. – С. 425-431.

117. Шувалов И.А., Математическая модель воздействия угроз на информационную систему обработки персональных данных / Шувалов И.А., Семенчин Е.А. // Фундаментальные исследования. – 2013. – № 10. – Часть 3. – С. 529-533.

118. Шувалов И.А. Математическое моделирование конкурентоспособности микроэкономических систем [Электронный ресурс] / Шувалов И.А., Семенчин Е.А // Современные проблемы науки и образования. 2013. – № 4.— URL: http://www.science-education.ru/110-9889 (дата обращения: 20.08.2013).

119. Шувалов И.А. Методы определения актуальных угроз безопасности персональных данных / И.А. Шувалов // Наука, образование и культура. – 2017. – №3. – С. 7-10.

120. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин. — 2-е изд.— М.: Академический Проект; Гаудеамус, 2004. – 544 с.