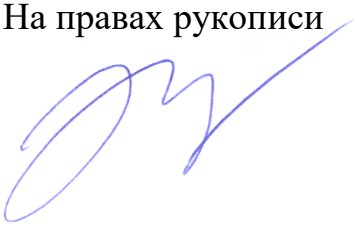
Министерство науки и высшего образования Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники (ТУСУР)

На правах рукописи



Новохрестов Алексей Константинович

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ АТРИБУТИВНЫХ МЕТАГРАФОВ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук,
профессор, А.А. Шелупанов

Томск 2018

Содержание

Введение

Проблема обеспечения безопасности компьютерных сетей не теряет актуальности с момента их появления и широкого распространения до наших дней. Так, согласно исследованию [1] к концу 2017 года сложность преодоления защищенного сетевого периметра в 56% случаев оценивалась как тривиальная. Вместе с этим, технологии постоянно развиваются: появляются новые виды угроз [2, 3], и обеспечение безопасности компьютерных сетей эволюционирует в обеспечение безопасности системы «Интернет вещей» [4, 5].

Неотъемлемым этапом процесса обеспечения безопасности является определение перечня актуальных угроз. Однако до определения актуальности необходимо составить как можно более обширный перечень угроз [6], т.е. осуществить идентификацию угроз.

При этом вопросы обеспечения сетевой безопасности актуальны как для крупных компаний [7], так и для небольших организаций [8]. При этом очевидно, что ресурсы, которые могут быть выделены на обеспечение безопасности, будут отличаться. Это влияет не только на возможные затраты на техническое оснащение, но и на квалификацию специалистов, которых организация может нанять.

Профессиональный уровень, а также субъективное мнение эксперта при использовании существующих подходов к построению перечней угроз информационных систем существенно влияет на итоговый результат.

Актуальной является задача по разработке эффективной методики составления перечня угроз информационной безопасности компьютерных сетей, при использовании которой будет минимизировано влияние профессионального уровня и субъективного мнения эксперта.

Целью исследования является повышение объективности составления перечня угроз информационной безопасности компьютерных сетей.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. выполнить анализ текущего состояния предметной области: использующихся при составлении перечней угроз моделей компьютерных сетей и подходов к построению моделей угроз;
2. разработать модель компьютерной сети, позволяющую описать структуру системы на достаточном для составления перечня угроз уровне детализации;
3. разработать модель угроз компьютерной сети, учитывающую максимально возможное количество угроз;
4. разработать методику составления перечня угроз информационной безопасности компьютерных сетей;
5. апробировать методику и модели на практике.

Объектом исследования данной работы является информационная безопасность компьютерных сетей в условиях существования угроз системе и обрабатываемой в ней информации.

Под рассматриваемыми компьютерными сетями подразумеваются локальные вычислительные сети (ЛВС), представляющие собой систему, обеспечивающую обмен данными между подсетями, узлами сети и установленным на них программным обеспечением.

Предметом исследования является модель угроз информационной безопасности компьютерных сетей.

Основные **методы исследования**, примененные в диссертационной работе – это методы моделирования, системного анализа, теории графов и теории защиты информации.

Научная новизна результатов работы и проведенных исследований заключается в следующем:

1. Предложена модель компьютерной сети, основанная на атрибутивных метаграфах, отличающаяся наличием связей между различными уровнями программного обеспечения компьютерных систем.

2. Предложена модель угроз информационной безопасности компьютерных сетей, отличающаяся формированием типов угроз на основе элементарных операций над метаграфами.

3. Разработана новая методика составления перечня угроз информационной безопасности компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами.

Практическая значимость результатов исследования состоит в следующем:

1. Представлены методические рекомендации по формированию перечня угроз, направленных на нарушение конфиденциальности и целостности информационной системы.

2. Разработана и внедрена методика составления перечня угроз информационной безопасности, использующая разработанные модели компьютерной сети и угроз. Внедрение методики позволило при применении к разрабатываемой системе коммерческого учета энергоресурсов обнаружить на 18% больше угроз, чем ранее было обнаружено экспертами.

Теоретическая значимость результатов исследования заключается в том, что:

1. Применительно к разработке модели угроз информационной безопасности компьютерной сети результативно использован математический аппарат теории графов для моделирования компьютерных сетей.

2. Изучена связь между типами угроз и базовыми операциями над метаграфами.

Положения, выносимые на защиту:

1. Модель компьютерной сети, основанная на атрибутивных метаграфах, позволяет описать компоненты программного обеспечения компьютерных сетей (прикладное, системное и сетевое программное обеспечение) и все возможные связи между ними (сетевые протоколы, драйверы, и т.п.) для построения модели угроз.

Соответствует пункту 3 паспорта специальности: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

2. Модель угроз информационной безопасности компьютерных сетей позволяет описать угрозы более полно относительно существующих решений: в банке данных угроз ФСТЭК России представлено 25 из 36 типов угроз безопасности информационной системы, выделенных в данной работе.

Соответствует пункту 3 паспорта специальности: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

3. Методика составления перечня угроз информационной безопасности компьютерных сетей позволила увеличить на 18% количество учтенных угроз при разработке автоматизированной системы коммерческого учета энергоресурсов.

Соответствует пункту 15 паспорта специальности: модели и методы управления информационной безопасностью.

Обоснованность и достоверность результатов работы подтверждается их внутренней непротиворечивостью и положительным эффектом от внедрения научных исследований в работу действующего предприятия, о чем свидетельствует соответствующий Акт о внедрении. Использовано сравнение авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Внедрение результатов. Результаты диссертационной работы внедрены в деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов, а также в учебный процесс Томского государственного университета систем управления и радиоэлектроники.

Личный вклад. В работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных работ написана в соавторстве с сотрудниками научной группы. Постановка задачи

исследования осуществлялась научным руководителем д.т.н., профессором Шелупановым А.А.

Апробация работы. Основные и промежуточные результаты исследования докладывались и обсуждались на следующих конференциях:

— VI Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных: Проблемы и пути их решения» (Брянск, 2014);

— Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2014» (Томск, 2014),

— Российской научно-технической конференции «Инновации и научно-техническое творчество молодежи» (Новосибирск, 2014);

— XV Всероссийской научно-практической конференции «Проблемы информационной безопасности государства, общества, личности» (Иркутск, 2014);

— XI Международной научно-технической конференции «Динамика систем, механизмов и машин» (Омск, 2014);

— Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2015» (Томск, 2015),

— XI Международной научно-практической конференции «Электронные средства и системы управления» (Томск, 2015);

— XIII Международной конференции студентов, аспирантов и молодых ученых «Перспективы развития фундаментальных наук» (Томск, 2016);

— Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2016» (Томск, 2016);

— XII Международной научно-практической конференции «Электронные средства и системы управления» (Томск, 2016);

— V всероссийской научно-технической конференции «Студенческая наука для развития информационного общества» (Ставрополь, 2016);

— Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности» (Самара, 2017);

— XIII Международной научно-практической конференции «Электронные средства и системы управления» (Томск, 2017).

А также на заседаниях кафедры Комплексной информационной безопасности электронно-вычислительных систем ТУСУР и IEEE семинарах «Интеллектуальные системы моделирования, проектирования и управления» в г. Томске.

Результаты настоящей работы использовались в реализации комплексного проекта по созданию высокотехнологичного производства интеллектуальных приборов энергоучета, разработанных и изготовленных на базе отечественных микроэлектронных компонентов, и гетерогенной автоматизированной системы мониторинга потребляемых энергоресурсов на их основе (контракт № 02.G25.31.0107 от 14 августа 2014 г).

Работа выполнена при поддержке Министерства образования и науки РФ в соответствии с государственным заданием ТУСУР на 2017–2019 гг. Проект № 2.8172.2017/8.9 «Метод и модели определения уровня защищенности информационных систем».

Публикации по теме диссертации. По материалам исследования опубликовано 16 работ, в том числе 2 работы в изданиях, рекомендованных ВАК РФ.

Структура и объем диссертации. Диссертация содержит введение, три главы, заключение, 1 приложение и список источников из 108 наименований. Объем диссертационной работы: 114 страниц, в том числе 14 таблиц и 14 рисунков.

1 Обзор подходов к построению моделей компьютерных сетей и моделей угроз компьютерным сетям

В настоящее время известно множество подходов к построению моделей угроз информационных систем. Эти подходы описаны в нормативных актах и стандартах, документах различных компаний и научных исследованиях, результаты которых могут, как и уже применяться на практике, так и оставаться пока только теоретическими исследованиями.

При решении задач построения модели угроз, построения модели нарушителя и оценки защищенности систем требуется максимально точное описание системы [9], другими словами требуется наличие модели информационной системы, или, если рассматривать данную работу, модель компьютерной сети.

В данной главе рассматриваются подходы к построению моделей компьютерных сетей, применяемые при идентификации угроз и оценке защищенности, а также непосредственно подходы к описанию и идентификации угроз и построению моделей угроз компьютерных сетей и информационных систем.

1.1 Модели компьютерных сетей

Модели информационных систем и, в частности, компьютерных сетей могут быть поделены на классы в зависимости от решаемой задачи [10, 11]. Один из примеров такого деления приведен далее:

— концептуальные модели [12, 13];
— функциональные модели [14];
— математические модели [15].

Концептуальные модели определяют структуру описываемой системы, свойства её элементов, причинно-следственные связи, важные для достижения целей моделирования на неформальном языке. Для этого обычно

используются графики, таблицы, диаграммы и т.д. Описание модели на неформальном языке как правило используется для взаимопонимания специалистов разных профилей.

Функциональные модели с помощью набора взаимодействующих и взаимосвязанных блоков показывают, что, как и кем делается в рамках функционирования организации. Являются описательными графическими моделями.

Математические модели используются в общественных, технических и естественных науках, также при решении различных задач проектирования. Описываются с помощью формул, графов, примеров и т.д.

В работе [16] автор делает вывод, что для моделирования угроз компьютерной сети необходимо представлять саму компьютерную сеть в виде модели ее отдельных элементов и взаимосвязей между ними, так как модели сравнимые с «черным ящиком» не будут отображать функционирование системы в достаточной мере. Наиболее точно отразить структуру системы, схожей с компьютерной сетью, можно с использованием теории графов.

Математические, а именно, графовые модели могут быть построены с помощью следующих инструментов:

— ориентированного графа;
— системы массового обслуживания;
— многодольного графа.

Данные модели и подлежат рассмотрению.

1.1.1 Система массового обслуживания

В работе [17] информационная система представляется, как система массового обслуживания, в которую поступают угрозы (заявки). На вход системы поступают угрозы одного типа. При этом предполагают, что данная угроза не может быть реализована или не может наступить несколько раз в

один и тот же момент времени. Если эта ситуация соблюдена, то система может находиться в трех состояниях:

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

Также в работе отмечается, что у данной системы отсутствуют поглощающие состояния. Это значит, что реализация угрозы либо не повлияет на работу системы, либо выведет из строя на недолгий промежуток времени один из ее сегментов.

На рисунке 1.1 представлен переход из состояния в состояние, в системе, который осуществляется согласно ориентированному графу.

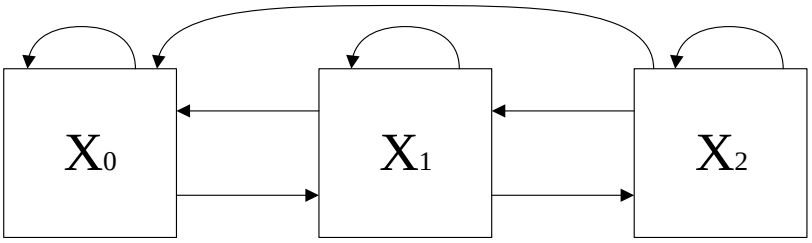


Рисунок 1.1 – Ориентированный граф

Недостаток данной модели заключается в том, что неизвестно, чем являются объекты информационной системы, как они взаимодействуют друг с другом, так как модель представлена в виде черного ящика.

1.1.2 Модель взаимодействия объектов распределенной вычислительной системы

В работе [18] описывается модель взаимодействия объектов распределенной вычислительной системы в проекции на физический, канальный и сетевой уровень модели OSI. На вход модели подается адрес объекта, с которого идет передача сообщения, и адрес, на который идет передача сообщения. На выходе получаем результат, а именно доставлено или

нет передаваемое сообщение. Главная задача модели PBC состоит в том, чтобы сформировать путь между заданными входными параметрами модели.

Модель в проекции на физический уровень OSI определяет физическую связь между объектами распределенной вычислительной системы. Устанавливает взаимодействие объектов на уровне аппаратных адресов сетевых адаптеров в проекции на канальный уровень OSI. В проекции на сетевой уровень OSI определяет связь объектов на уровне логических адресов. В работе вводится универсальная линия *KS*, под которой понимается линия связи либо физического, либо канального уровня OSI, так как модель в проекции на физический и канальный уровень ничем не отличаются. Объектами на физическом уровне являются сетевой адаптер хоста или роутера, на канальном – аппаратный адрес сетевого адаптера.

Данная распределенная вычислительная система включает N связанных между собой KS (линиями связи на физическом и канальном уровне) и LS (линиями связи на сетевом уровне) объектов и роутеров:

$$X = \{x_i | i = 1..M\}$$ – множество хостов,

где $i = 1..M$ – количество хостов.

$$G = \{g_i | j = M + 1..N\}$$ – множество роутеров,

где $j = M + 1..N$ – количество роутеров.

На физическом или канальном уровнен каждый хост связан только с одним ближайшим роутером. Все объекты взаимодействуют между собой с помощью двунаправленных линий связи ks_{KL}, которые соединяют объект K с объектом L.

$$KS = \{ks_{KL} | k = 1..N, L = 1..N\},$$

где KS – множество линий связи на физическом или канальном уровне OSI.

Модель информационной системы в проекции на канальный или физический уровень, представленная с помощью графа, изображена на рисунке 1.2.

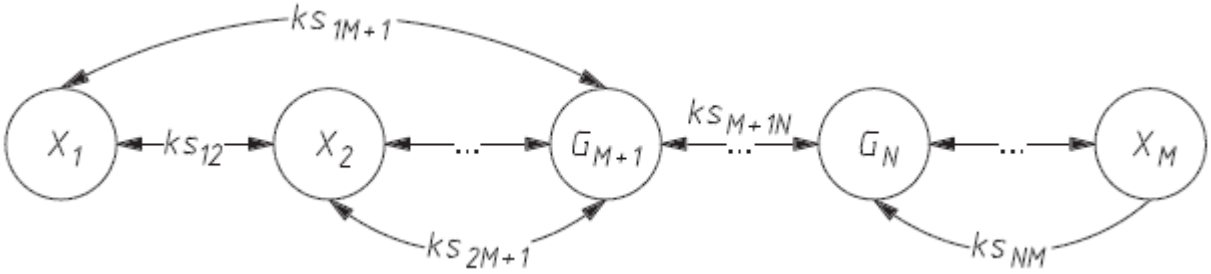


Рисунок 1.2 – Графовая модель в проекции на физический или канальный уровень OSI

На сетевом уровне каждый объект может взаимодействовать с другим объектом (любым) с помощью одно-двунаправленной линии связи ls_{KL}, которая соединяет объект K с объектом L. На данном уровне под объектом имеется в виду сетевой адрес хоста или роутера.

$$LS = \{ls_{KL} | k = 1..N, L = 1..N\},$$

где LS – множество линий связи объектов на сетевом уровне.

Модель информационной системы в проекции на сетевой уровень, представленная с помощью графа, изображена на рисунке 1.3.

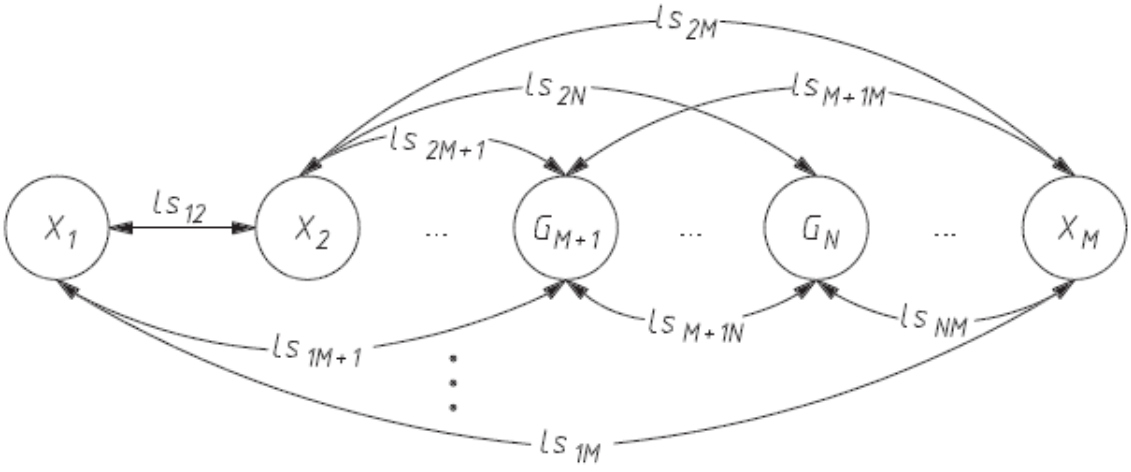


Рисунок 1.3 – Графовая модель в проекции на сетевой уровень OSI

Модель взаимодействия объектов в проекции на физический (или канальный) и сетевой уровни модели OSI изображена на рисунке 1.4.

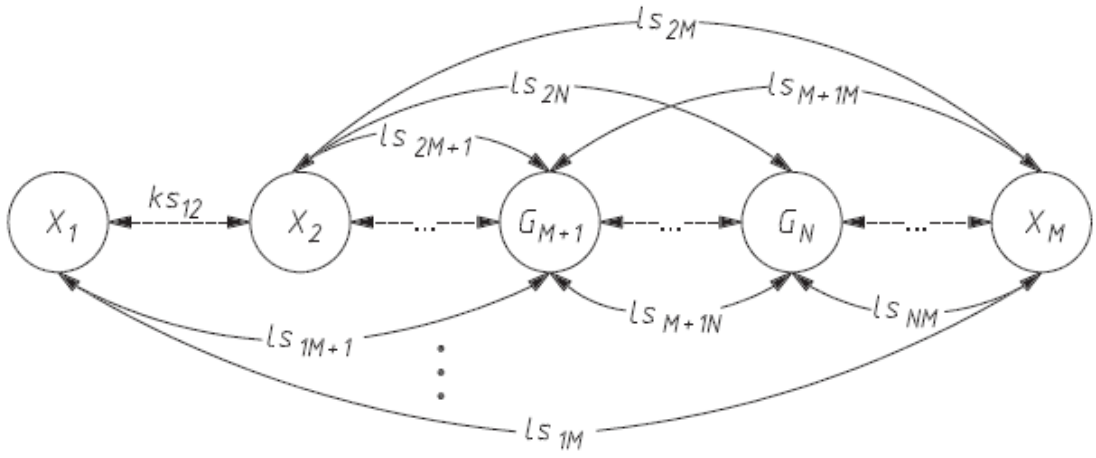


Рисунок 1.4 – Графовая модель в проекции на физический (или канальный) и сетевой уровни OSI

Описанная выше модель информационной системы построена при помощи ориентированного графа, в котором описывается взаимодействие объектов распределенной вычислительной системы на физическом, канальном и сетевом уровне модели OSI. В рассмотренной модели учтены не все уровни эталонной модели OSI, так как в ней не рассматривается взаимодействие между программным обеспечение и операционными системами в сети.

1.1.3 Графовая модель системы обеспечения информационной безопасности

В работе [19] для описания системы обеспечения информационной безопасности используется графовая модель, описанная с помощью трехдольного графа, представленная на рисунке 1.5. Множество отношений угроза-объект образует двудольный граф *{T, O}*. Введение третьего набора M перекрывает все возможные ребра в графе. В результате получается трехдольный граф *S= {T, M, O}*.

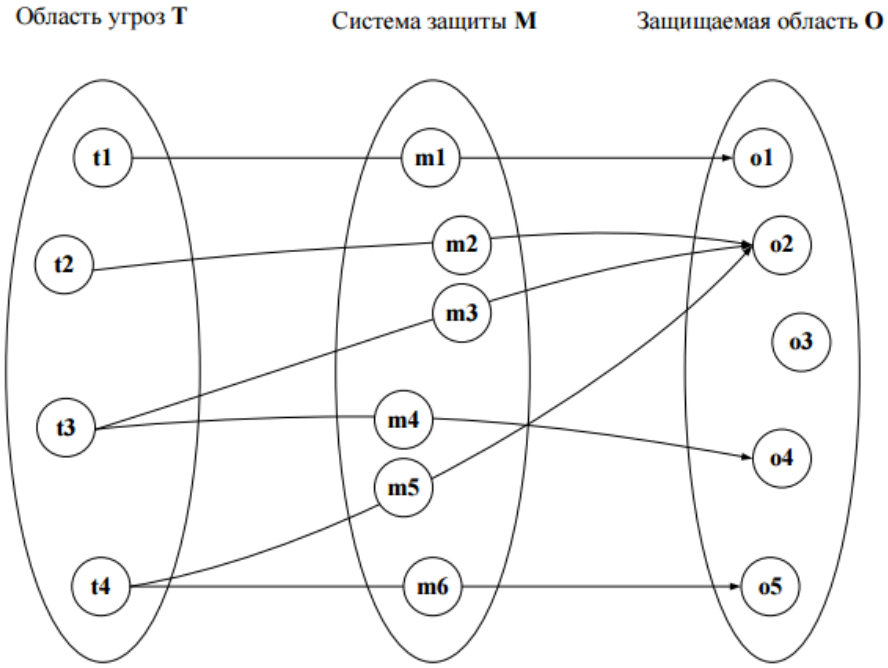


Рисунок 1.5 – Графовая модель системы обеспечения информационной безопасности

Данная модель описывает взаимодействие между «областью угроз», «областью системы защиты» и «защищаемой областью». В этой модели нет конкретного описания взаимодействия объектов в защищаемой области, также отсутствует описание самих объектов.

1.2 Модели угроз компьютерным сетям

Предполагается, что сведения о существующих угрозах должны быть получены специалистом из нормативных документов, таких как [20, 21, 22], каталогов угроз (примером являются банк данных ФСТЭК России [23] и матрица ATT&CK [24]), а также исследований и отчетов компаний, занимающихся вопросами защиты информации [1], [3].

Для построения модели угроз недостаточно только сведений об угрозах из перечисленных источников, так как специалист физически не в состоянии запомнить все угрозы. Если предположить, что существует полный перечень угроз, то процесс работы с ним окажется крайне трудоемким. Поэтому для

составления моделей угроз используются различные подходы к классификации и идентификации угроз.

Об актуальности вопроса построения модели угроз информационных систем говорят такие работы как [25]. В работе утверждается, что модель позволяет сформировать основу для разработки владельцами объектов информационной безопасности правовых и организационных, технических и иных решений в целях создания комплексной системы обеспечения безопасности. Кроме того, модель позволяет субъектам обеспечения безопасности оперативно реагировать на возникающие, реализуемые или реализованные угрозы и предпринимать соответствующие меры противодействия для ликвидации последствий реализации угроз на различных этапах их возможного проявления. В работе [26] приводятся модели идентифицируемости признаков распознавания угроз конфиденциальности информационных ресурсов компьютерных систем и обосновываются варианты их представления. Исследование [27] посвящено структурным модели и содержит в себе алгоритм моделирования информационных процессов АСБ. В работе [28] на основе обобщенных требований формулируется постановка и порядок решения задачи разработки алгоритмов и моделей для оценки защищенности информации в интегрированных системах безопасности.

В работах [29] и [30] авторы разделяют методы классификации угроз на две группы:

— основанные на способе реализации атаки [31, 32, 33];

— основанные на способе воздействия [34, 35].

Классификация по способу реализации атаки предполагает использование в качестве критериев параметры, определяющие каким образом реализуются атаки на активы организации: источник, мотивация, частота, используемая уязвимость.

Классификация по способу воздействия как правило использует в качестве критерия нарушаемые свойства информации.

Часть работ посвящена рассмотрению применимости типовых моделей угроз безопасности к каким-то конкретным объектам. Так в [36] авторами рассмотрена применимость к информационным системам автоматизации учебного процесса подразделений вуза, в результате чего были выявлены типовые уязвимости и угрозы, сопряженные с обработкой персональных данных в рассмотренных информационных системах, выбраны методы борьбы с ними, указаны зоны ответственности. В [37] рассматривается аналитическая модель комплексной оценки эффективности защиты данных от угроз их искажения преднамеренного и непреднамеренного характера, для которой рассматривается применимость для обоснования направлений совершенствования мер защиты информации от искажения на объектах информатизации сферы страхования. В статье [38] рассмотрены причины возникновения такого явления, как преступления в сфере информационных технологий. Работа [39] рассматривает подход к решению задачи формализации критериев выбора средств защиты информационных систем на основе оценки количественных показателей дестабилизирующих факторов и уязвимостей информационных систем при автоматизированном проектировании систем защиты информации. Статья [40] рассматривает угрозы информационным системам в организациях, а также способы их устранения посредством стратегических решений и программ осведомленности, чтобы гарантировать информационную безопасность. А в [41] представлена модель прогнозирования, которая может направлять менеджеров ИС для инициативного смягчения внутренних угроз. Работа, представленная в [42], включает исследование различных методов, поддерживающих безопасное поддержание состояний компьютерной сети, ее ресурсов и информации, которую она передает. Исследуются методы заключения компромисса информационной системы, ворвавшись в систему без санкционированного доступа, различные фазы цифрового анализа уже поставившей под угрозу системы, и затем исследуются инструменты и методы

для того, чтобы в цифровой форме проанализировать поставившую под угрозу систему, чтобы вернуть её к безопасному состоянию.

Среди моделей угроз информационных систем можно выделить вербальные. Так в статье [43] рассматривается модель угроз, реализуемых в информационной системе, где описывается необходимость построения структурной вербальной модели угроз, формат которой определяет сведения об объектах атак (источниках информации), источниках угроз, о структуре угрозы, путях их распространения в виртуальных средах. Модель из статьи [44] предполагает, что любая модель может быть обоснованно скорректирована экспертом и все полученные модели могут быть представлены в текстовом виде с использованием генератора документов по шаблону. Предложенный метод разработки модели угроз может быть использован вне зависимости от информации, обрабатываемой в информационной системе (персональные данные, коммерческая тайна, государственная тайна, иные сведения ограниченного доступа, общедоступная информация). В работе [45] проведен анализ вербального описания методов реализации полного множества угроз информационной безопасности автоматизированных систем, содержащейся в специализированной литературе. Что позволило построить формальную модель полного множества угроз информационной безопасности с использованием логических деревьев атак Б. Шнайера и присвоением дугам дерева числовых коэффициентов, имеющих временной смысл. В статье [46] описывается процесс функционально-информационного моделирования угроз и действий по защите информации в интегрированных системах безопасности, приводится функционально-информационная модель исследуемых процессов в логико-лингвистической форме. В [47] рассмотрен используемый при автоматизированном анализе способ реализации экспертных оценок защищенности информационной системы персональных данных для последующего применения показателей при построении системы защиты и предлагается рассчитывать вербальный показатель на основе анализа оценок,

полученных от сотрудника организации, которому будет предложен ряд вопросов, заранее «взвешенных» по важности экспертами.

Другим вариантом построения модели угроз информационных систем служит графическая модель. В статье [48] ведется разработка формализованного подхода к угрозам информационной безопасности с помощью логических деревьев, с сопоставлением дугам графа параметра времени реализации сопоставленного с дугой шага. По реализации угрозы позволяет моделировать сложные сценарии информационных атак и оценивать их временные характеристики. Исследование, представленное в [49], содержит модель на основе графа атаки, созданного на основе отношения эксплуатации уязвимостей.

Не редко, при построении модели угроз информационных систем – прибегают в математической модели. Так в работе [50] рассматривается математическая модель угроз безопасности защищенных информационных систем и вводятся ряд ограничений для оценки угроз безопасности информационным ресурсам защищенных информационных систем. Авторами работы [51] приведены плотности вероятности основных одно-, двух- и трёхпараметрических распределений с возможными значениями на положительной полуоси и имеющими максимум плотности вероятности, которые целесообразно использовать для математического моделирования рисков возникновения угроз в информационно-технических системах. В работе [52] предложена математическая модель воздействия внутренних и внешних угроз на информационную систему обработки персональных данных. С помощью марковской цепи проводится расчет вероятностей нахождения математической модели информационной системы в одном из трех рассматриваемых состояний (угроза не наступила, угроза наступила, но не была реализована, и угроза реализована). Работа, представленная в [53] посвящена разработке и анализу параметров математической модели изменения риска, позволяющих в расчетах на организационно-технические мероприятия, направленные на создание или модификацию системы защиты

информационно-технических систем, определить приемлемое отношение суммы затрат на систему защиты и уровень риска угроз, который может считаться приемлемым для конкретной информационно-технической системы. В статье [54] предложены математические модели и методический подход для описания динамики возникновения и реализации угроз информационной безопасности, которые позволяют учесть влияние мер технической ЗИ.

1.2.1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее ПДн) представляет собой классификацию угроз информационной безопасности. Угрозы, представленные в [55], ведут к ущербу интересов личности, общества и государства.

Базовая модель угроз ПДн содержит информацию по угрозам безопасности персональных данных, связанных с перехватом персональных данных по техническим каналам, с целью их незаконного использования, а также с несанкционированным доступом к информационной системе персональных данных с использованием программных и программно – аппаратных средств с целью их модификациях.

Угрозы, рассматриваемые в [55]:

а) угрозы утечки акустической (речевой) информации;

б) угрозы утечки видовой информации;

в) угрозы утечки информации по каналу побочных электромагнитных излучений и наводок (далее ПЭМИН);

г) угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

д) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения несанкционированного доступа (далее НДС) программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах);

е) угрозы внедрения вредоносных программ;

ж) угрозы «анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

з) угрозы сканирования, направленные на выявление типа операционной системы автоматизированного рабочего места (далее АРМ), открытых портов и служб, открытых соединений;

и) угрозы выявления паролей;

к) угрозы получения НСД путем подмены доверенного объекта;

л) угрозы типа «отказ в обслуживании»;

м) угрозы удаленного запуска приложений;

н) угрозы «анализа сетевого трафика» с перехватом передаваемой по сети информации;

о) угрозы внедрения по сети вредоносных программ;

п) угрозы сканирования, направленные на выявление типа операционной системы информационной системы персональных данных (далее ИСПДн), сетевых адресов рабочих станций, открытых портов и служб, открытых соединений;

р) угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений;

с) угрозы внедрения ложного объекта сети;

т) угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

у) угрозы «анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

ф) угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений;

х) угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

ц) угрозы подмены доверенного объекта.

Модель представляет собой описание возможных источников угрозы безопасности персональных данных. Угрозы информационной безопасности персональных данных, содержащиеся в [55], могут дополняться по мере выявления новых источников угроз. В разделе 3.1 настоящей работы показано, что все угрозы, описанные в модели, присутствуют в [23].

1.2.2 Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости

Источник [56] содержит перечень угроз безопасности данных при их обработке в информационных системах персональных данных. Угрозы безопасности вызваны преднамеренными или непреднамеренными

действиями лиц, служб, организаций, которые ведут к ущербу интересам личности, общества и государства.

В ходе анализа методики [56], был составлен перечень актуальных угроз безопасности ПДн:

а) угрозы от действий вредоносных программ (вирусов);

б) угрозы утраты ключей и атрибутов доступа;

в) угрозы выявления паролей по сети;

г) угрозы внедрения по сети вредоносных программ;

д) угрозы наличия недекларированных возможностей системного программного обеспечения (далее ПО) и ПО для обработки персональных данных;

е) угрозы перехвата за переделами с контролируемой зоны;

ж) угрозы сканирования;

з) угрозы подмены доверенного объекта в сети;

и) угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

к) угрозы типа «отказ в обслуживании»;

л) угрозы удаленного запуска приложений.

В разделе 3.1 настоящей работы показано, что все угрозы, описанные в рассматриваемом перечне, присутствуют в [23].

1.2.3 ГОСТ Р ИСО/МЭК 27005 – 2010. Методы и средства обеспечения безопасности

Стандарт [57] содержит в себе перечень типичных угроз, а также происхождение каждой угрозы: умышленная – все умышленные действия направленны на информационные активы, случайная – действия персонала, которые могут случайно нанести ущерб информационным активам, природная – инциденты, не основанные на действиях персонала.

Ниже приведен перечень угроз информационной безопасности, представленный в [57].

Перечень рассматриваемых угроз информационной безопасности в [57]:

а) поиск повторно используемых или забракованных носителей;

б) раскрытие;

в) данные из ненадежных источников;

г) преступное использование аппаратных средств;

д) преступное использование программного обеспечения;

е) определение местонахождения;

ж) перехват компрометирующих сигналов помех;

з) дистанционный шпионаж;

и) прослушивание;

к) кража носителей или документов;

л) кража оборудования;

м) отказ оборудования;

н) неисправная работа оборудования;

о) насыщение информационной системы;

п) нарушение функционирования программного обеспечения;

р) нарушение сопровождения информационной системы;

с) несанкционированное использование оборудования;

т) мошенническое копирование программного обеспечения;

у) использование контрафактного или скопированного программного обеспечения;

ф) искажение данных;

х) незаконная обработка данных;

ц) ошибка при использовании;

ч) злоупотребление правами;

ш) фальсификация прав;

щ) отказ в осуществлении действий;

ы) нарушение работоспособности персонала.

Стандарт [57] содержит в себе обобщенный список угроз информационной безопасности, однако весь это список угроз содержится в [23], что показано в разделе 3.1 настоящей работы.

1.2.4 Банк данных угроз безопасности информации ФСТЭК России

В банке приведены сведения об основных угрозах безопасности информации. На момент использования банк данных угроз безопасности информации содержит 209 актуальных угроз, к каждой угрозе есть описание, также приведен объект воздействия и даты включения угроз в банк данных угроз.

В разделе 3.1 показано что, угрозы из [55], [56] и [57] более детально описаны в [23], следовательно, ключевые недостатки банка данных можно распространить и на представленные выше подходы к описанию угроз.

Одним из недостатков [23] отсутствие системности в описании угроз.

Так, в банке представлены угрозы, описание которых подразумевает множество способов их реализации. Примером такой угрозы является угроза под номером 67 – «Угроза неправомерного ознакомления с защищаемой информацией», в описании которой обозначено, что она может быть осуществлена путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др. В качестве дополнительных примеров можно привести угрозы 104 – «Угроза определения топологии вычислительной сети» и 179 – «Угроза несанкционированной модификации защищаемой информации».

Одновременно с этим описаны угрозы, являющиеся по своей сути частными случаями одной угрозы. Примером являются угрозы 167 – «Угроза заражения компьютера при посещении неблагонадёжных сайтов», 171 – «Угроза скрытного включения вычислительного устройства в состав бот-сети», 172 – «Угроза распространения «почтовых червей», 186 – «Угроза внедрения вредоносного кода через рекламу, сервисы и контент», 190 – «Угроза внедрения вредоносного кода за счет посещения зараженных сайтов

в сети Интернет» и 191 – «Угроза внедрения вредоносного кода в дистрибутив программного обеспечения». Все эти угрозы подразумевают внедрение в атакуемую систему вредоносного кода или программного обеспечения и, если провести аналогию с описанием угроз 67 и 179 могли быть представлены не отдельными угрозами, а в рамках описания одной.

Такой разброс в описании угроз затрудняет экспертам работу с перечнем при составлении модели угроз для реальной системы.

Следующим недостатком модели является то, что она содержит модель нарушителя. Таким примером является угроза злоупотребления доверием потребителей облачных услуг. В данной работе модель нарушителя не учитывается, так как, изначально исходим от того, что модель угроз должна описывать сами угрозы, не должна включать описание нарушителя, например, мотив нарушителя [61].

Еще одним недостатком является отсутствие разделения угроз на угрозы информации и угрозы системе. Отказ от такой классификации угроз затрудняет в дальнейшем выбор необходимых средств защиты и в итоге построение системы защиты [62].

1.2.5 The STRIDE Threat Model

Методология компании Microsoft [34], в которой используется подход к созданию защищенных систем на основе моделирования угроз. Ее использование предполагается при разработке программного обеспечения. Согласно [63] моделирование угроз проводится на этапе проектирования (согласно документации этап назван «Дизайн (design)») программного средства. Методология представляет собой классификационную схему для описания атак в зависимости от типа используемых для их реализации уязвимостей или мотивации нарушителя:

— подмена личности;

— подделка данных;

— отказ (пользователь отказывается от того, что выполнял какие-либо действия, и никаким способом обратное доказать невозможно);

— раскрытие информации (доступ к информации, к которой пользователь не должен иметь прав);

— отказ в обслуживании (ddos атаки и т.д.);

— высота привилегий (не имеющий привилегий пользователь получает доступ к информации).

[34] является вариантом определения безопасности информационных систем на ряду с триадой конфиденциальность-целостность доступность [64] и гексадой Паркера [65]. Вопрос о характеризующем безопасность системы и информации наборе свойств остается дискуссионным [66]. Так в [67] информационная безопасность определяется на основе свойств из гексады Паркера, однако в документах ФСТЭК России используются конфиденциальность, целостность и доступность. В настоящей работе применяется «классическая» триада свойств системы и информации.

Хотя данный подход и ориентирован на разработку программного обеспечения, его можно применить и при определении угроз информации и системе при проектировании таких систем, как компьютерные сети. Его недостатком является отсутствие формализации и существенное влияние субъективного мнения и профессионального уровня эксперта.

1.2.6 NIST Special Publication 800-30

Документ [68] является руководством по управлению рисками для IT-систем. Он ориентирован на вопросы управления рисками уровня менеджмента организации. В данном руководстве на этапе идентификации угроз предоставляется только описание злоумышленников (источников угроз) и их вероятных действий. В рамках данного подхода на этапе идентификации угроз формируется перечень классов угроз, который в дальнейшем

ранжируется по вероятности реализации. Основной акцент делается на уязвимостях.

Таким образом, недостатки подхода аналогичны недостаткам модели [34] и заключаются существенном влиянии субъективного мнения и профессионального уровня эксперта.

1.3 Выводы по главе

В результате обзора подходов к построению моделей компьютерных сетей можно сказать, что с их помощью невозможно подробно описать, чем являются объекты в информационной системе, а также, как они между собой взаимодействуют. Не представляется возможным описать многоуровневую информационную систему, которая бы включала в себя взаимодействие на всех уровнях модели OSI.

В ходе анализа рассмотренных моделей угроз информационной безопасности, были обнаружены недостатки:

1) в моделях угроз присутствует модель нарушителя, либо оказывает непосредственное влияние на их формирование;

2) отсутствие системности – в рамках одной модели описываются как обобщенные угрозы, так и частные случаи;

3) построение перечней угроз основывается на субъективном мнении эксперта;

4) отсутствует разделение на угрозы, направленные на систему и информацию.

Ключевой недостаток всех моделей заключается в том, что ни в одной из них нет описания угроз информационной системе в явном виде. Все внимание уделяется угрозам информации, обрабатываемой в определенной информационной системе, например в информационной системе персональных данных.

Каждая из рассмотренных моделей может учитывать те или иные угрозы, которые не описаны в другой.

Также во многих рассмотренных моделях нет математической формализации, т.е. все модели описаны посредством словесных перечней и указаний, что может привести к тому, что каждый из экспертов может трактовать одну и ту же методику по-разному, более того эксперты, зачастую, не имеют прямого отношения к организации, что вносит дополнительные неточности в формирование моделей угроз.

2 Методика составления перечня угроз информационной безопасности компьютерных сетей

Исходя из результатов анализа подходов к построению модели угроз, а также подходов к анализу рисков безопасности информационных систем, этапами которых в той или иной степени является определение угроз информационной безопасности информации или системы, можно сделать вывод, что для получения перечня угроз необходимо:

1. описать систему, т.е. определить перечень ее компонентов подлежащих защите;
2. непосредственно определить угрозы для каждого из элементов определенного на шаге 1 перечня.

Далее предлагается методика составления перечня угроз, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами. Также описываются используемые в методике модель компьютерной сети и подход к классификации угроз.

2.1 Функциональная схема методики

Методика составления перечня угроз информационной безопасности компьютерных сетей представляется 3 этапами:

1. классификация элементов компьютерной сети;
2. формирование матрицы взаимосвязей;
3. составление перечня угроз.

Схема методики, представленная в графической нотации IDEF0 представлена на рисунке 2.1.

Входными данными для методики являются:

1. перечни прикладного и системного программного обеспечения;
2. логическая структура компьютерной сети;
3. перечень используемых протоколов передачи данных;

4. требования по учету угроз конфиденциальности и целостности в итоговом перечне угроз.

На выходе методики получаем перечень угроз информационной безопасности рассматриваемой компьютерной сети.

Механизмами управления являются модель компьютерной сети и модель угроз, описание которых представлено в следующих разделах.

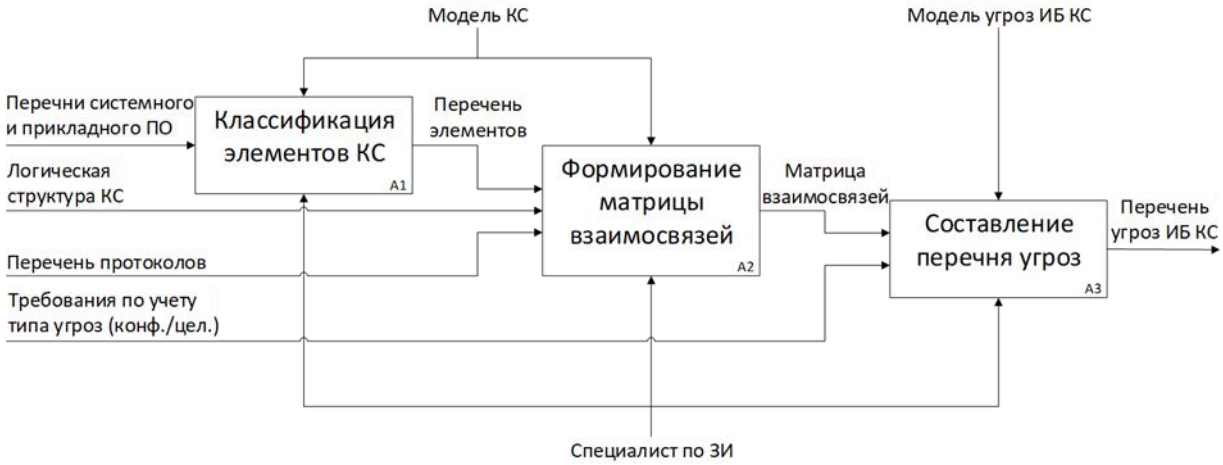


Рисунок 2.1 – Методика составления перечня угроз ИБ КС

Необходимо внести уточнения по входным данным. В методике компьютерная сеть рассматривается как структура из взаимодействующих элементов (вершины графа) и связей между ними (ребра графа).

Под угрозами понимается несанкционированное изменение структуры компьютерной сети (графа). Т.е. рассматриваются угрозы безопасности системы, а не информации. Хотя подход и может быть расширен для определения угроз безопасности информации.

Исходя из того, что рассматриваются угрозы системе, а не информации из перечня угроз удалены угрозы доступности, так как рассмотрение свойства доступности для информационной системы находится под вопросом. В настоящее время если речь заходит о доступности, то понимается доступность информации в информационной системе, а не доступность самой системы для пользователя. Если бы угрозы доступности системы были бы включены в

модель, то на этапе обобщения угроз безопасности информации и системы в единый перечень происходило бы дублирование угроз доступности.

Также необходимо обозначить следующее ограничение - на данном этапе работы рассматривается взаимодействие только программных элементов, хотя подход может быть применен и на аппаратном уровне (что рассмотрено в главе 3).

Таким образом классификация элементов компьютерной сети, которые могут быть представлены в виде вершины графа, включает в себя:

1. программное обеспечение;
2. операционные системы;
3. подсети.

Предполагается следующее соответствие протоколов и элементов компьютерной сети согласно уровням модели OSI:

- программное обеспечение – взаимодействует с помощью протоколов прикладного уровня и связей на уровне операционной системы;
- операционные системы – взаимодействует посредством протоколов транспортного, сетевого и канального уровней;
- подсети – взаимодействует посредством протоколов сетевого и канального уровней.

Матрица взаимосвязей, использование которой является ключевой особенностью настоящей методики формируется следующим образом:

1. определяется перечень элементов компьютерной сети в соответствии с логической структурой сети;
2. определяется перечень использующихся протоколов;
3. сопоставляются перечни элементов и протоколов.

По сути, определение перечень элементов подается на вход методики, однако в данном случае имеется в виду что необходимо определить принадлежность элементов относительно иерархии: подсеть включает

операционные системы, а операционные системы, в свою очередь, включают программное обеспечение.

Перечень использующихся протоколов формируется из протоколов, с помощью которых осуществляется взаимодействие элементов в рамках рассматриваемой компьютерной сети.

Сопоставление перечней подразумевает определение того, с помощью каких протоколов взаимодействует каждая пара элементов. Все этапы формирования матрицы взаимосвязей могут осуществляться параллельно, однако для удобства разделены на последовательные шаги.

Таким образом формируется матрица взаимосвязей. Пример матрицы приведен в таблице 2.1

Таблица 2.1 - Пример матрицы взаимосвязей:

	ПО1	ПО2	ОС1	ОС2
ПО1		Протокол 1 Протокол 2	-	-
ПО2	Протокол 1 Протокол 2		-	-
ОС1	-	-		Протокол 3 Протокол 4
ОС2	-	-	Протокол 3 Протокол 4	

По таблице можно судить, что все элементы главной диагонали матрицы равны нулю, так как связь элемента с самим собой не рассматривается. Также можно рассматривать матрицу взаимосвязей как треугольную, так как она является симметричной и рассматривать взаимодействие между элементами дважды не имеет смысла.

Согласно описанию методики можно сделать вывод, что к используемой в ней модели компьютерной сети представляются следующие требования:

— необходимо учитывать иерархичность программного обеспечения компьютерных сетей.
— необходимо учитывать возможность существования нескольких связей между двумя элементами.
— необходимо учитывать, что элементы и связи между ними имеют параметры.

2.2 Метаграфы

В основу моделей угроз и компьютерных сетей, применяемых в методике составления перечня угроз информационной безопасности компьютерных сетей, был положен математический аппарат метаграфов. Обобщенно, о целесообразности применения теории графов при выявлении угроз безопасности информации говорится в работе [69, 70].

Метаграф содержит и согласует между собой два основных свойства системы: единство (совокупность взаимосвязанных элементов) и делимость (каждый элемент системы – тоже система). В связи с этим из системы можно выделить подсистемы, что позволяет в определенной ситуации сосредоточить внимание на системе или ее подсистеме, в зависимости от того, что в данный момент интересует аналитика.

В работах [71] и [72], в которых введено и используется данное понятие, метаграф представляет из себя обобщение обычных графов и гиперграфов. В исследовании [73] рассмотрены проблемы, возникающие при визуализации метаграфов без участия человека. Также предложены пути решения этих проблем и алгоритм, который может быть применен при реализации программного средства для построения моделей компьютерных сетей.

Также следует отметить, что гиперребро, которое рассматривается в теории гиперграфов является отношением (свойством), определенным на множестве объектов. В связи с этим невозможно связывать отношение с другим отношением или объектом этого отношения. Поэтому для метаграфа

вводится понятие метавершины, которое имеет не смысл отношения, а смысл обобщения порождающего множества вершин.

Ребро метаграфа соединяет две вершины (метавершины) в отличие от гиперребра гиперграфа, которое может охватывать множество вершин. На число ребер между двумя вершинами не накладывается ограничений, ребра могут различаться набором атрибутов, следовательно, метаграф также является разновидностью мультиграфа. Ребро может соединять как вершины, так и метавершины метаграфа (рисунок 2.2).

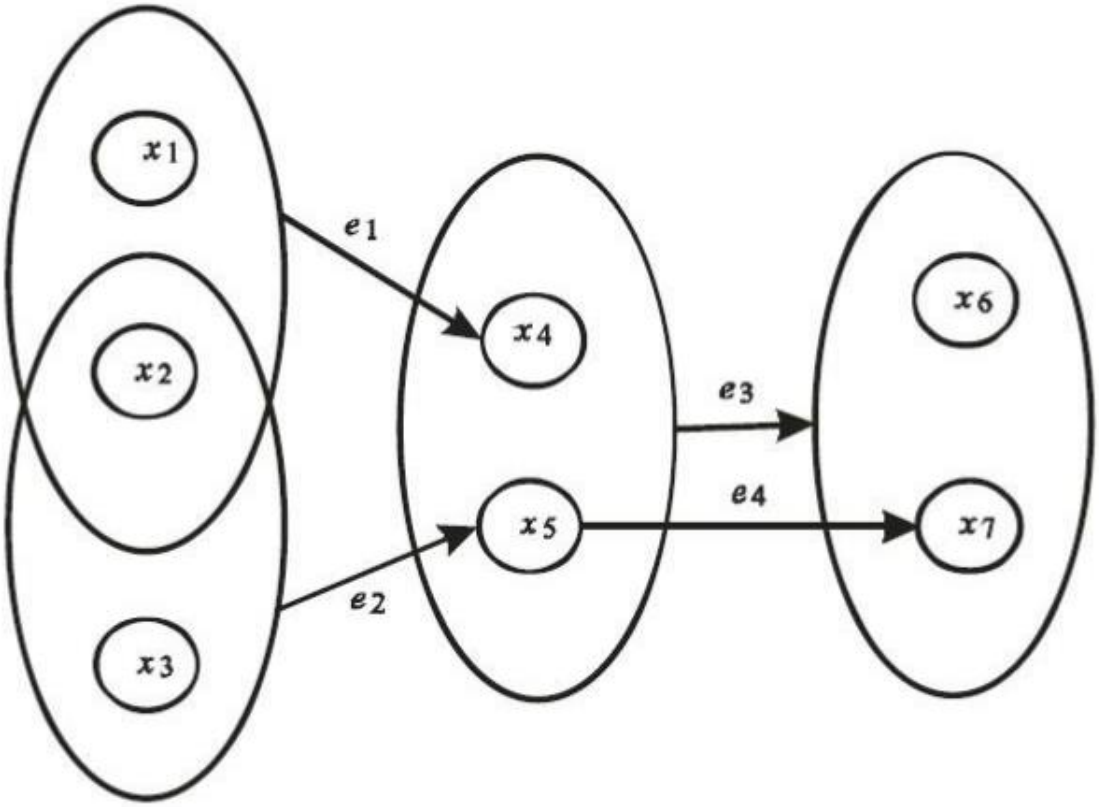


Рисунок 2.2 – Метаграф

В работе [70] вводится понятие метаграфа вложенности n.

Метаграф вложенности n (рисунок 2.3) представляется как упорядоченная пара:

$$G = (X, E),$$

где G – метаграф вложенности n;

$X = \{x_i\}, i = \overline{1,n}$ – непустое конечное множество вершин;

$E = \{e_k\}, k = \overline{1,m}$ – множество ребер графа.

Каждое ребро n-мерного графа соединяет два подмножества множества вершин:

$$e_k = (V_i, W_i),$$

где $V_i, W_i \subseteq X$;

$V_i \cup W_i \neq \emptyset$;

i – уровень вложенности.

Также существуют функции:

$$f_1^l: g_1^l(x_1^l, e_1^l) \to x_2^p, f_2^p: g_2^p(x_2^p, e_2^p) \to x_3^m, \dots, f_{n-1}^t: g_{n-1}^t(x_{n-1}^t, e_{n-1}^t) \to x_n\ ,$$

где $l, p, r, \dots, t$ – номер вершин и ребер на соответствующем уровне.

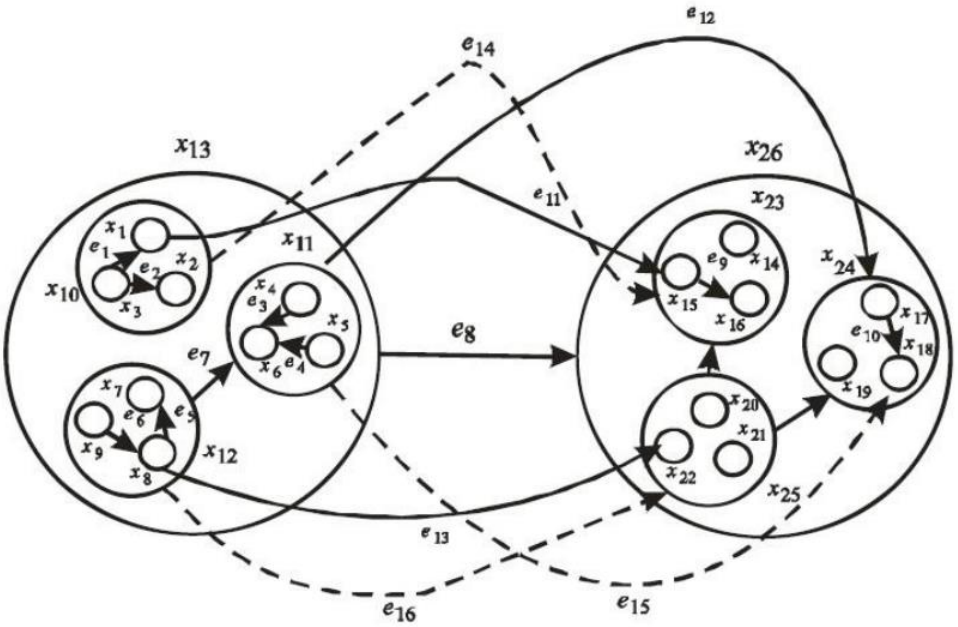


Рисунок 2.3 – Метаграф вложенности n

В работе [72] описывается атрибутивный метаграф, в котором каждому ребру или вершине может быть присвоено любое количество атрибутов (характеристик). В настоящей работе используются только метаграфы, однако в настоящий момент времени существуют исследования, еще больше расширяющие теорию графов. Так в работах [74] и [75] предлагаются и описываются виды обобщения графов, в частности протографы и архиграфы.

Атрибутивный метаграф представляет упорядоченную четверку:

$$MG = (V, MV, E, ME),$$

где MG – метаграф;

V – множество вершин метаграфа;

MV – множество метавершин метаграфа;

E – множество ребер метаграфа;

ME – множество метаребер метаграфа.

Вершина метаграфа характеризуется множеством атрибутов:

$$v_i = \{atr_k\},$$

где v_i– вершина метаграфа, $v_i \in V$;

atr_k – атрибут.

Ребро метаграфа характеризуется множеством атрибутов, исходной и конечной вершиной, признаком направленности:

$$e_j = (V_s, V_E, eo, \{atr_k\}),$$

где e_j – ребро метаграфа, $e_j \in E$;

V_s– исходная вершина (метавершина) ребра;

V_E – конечная вершина (метавершина) ребра;

eo – признак направленности ребра;

atr_k– атрибут.

Признак направленности ребра может принимать следующие значения:

$$eo = true|\text{false},$$

где $eo = true$ – направленное ребро;

$eo = \text{false}$ – ненаправленное ребро.

2.3 Модель компьютерной сети

На сегодняшний день практически любая информационная система состоит из нескольких рабочих станций, объединенных в локальную вычислительную сеть (ЛВС). На каждой рабочей станции в локальной сети установлена операционная система (ОС). Каждая операционная система в свою очередь включает в себя множество прикладного программного обеспечения (ПО) [76]. Модель информационной системы основана на подходе, описанном в [77].

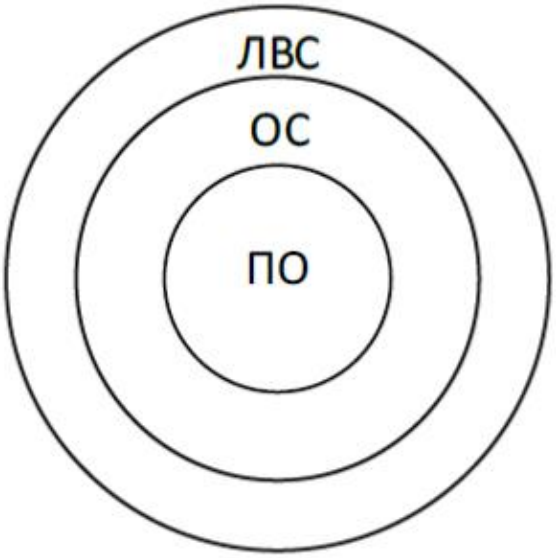


Рисунок 2.4 – Структура системы

На входе у модели находятся множества ПО, ОС и ЛВС. Основными задачами данной модели являются описание информационной системы, структура которой изображена на рисунке 2.4 с помощью структуры атрибутивного метаграфа вложенности 3 и формирование связей между заданными входными элементами (между программным обеспечением, операционными системами и локальными вычислительными сетями). Связи будут описываться в соответствии с эталонной моделью OSI изображенной на рисунке 2.5.

Рисунок 2.5 – Эталонная модель OSI

Согласно модели OSI, данные между объектами сети на разных уровнях передаются в соответствии с работающими на них протоколами.

Прикладной, представительский и сеансовый уровни OSI ориентированы на работу с ПО, следовательно, связи между ПО будут описаны с помощью протоколов, работающих на перечисленных уровнях OSI. Но следует отметить, что не всегда используемые в ПО протоколы строго соответствуют модели OSI, и зачастую функции сеансового и представительского уровней объединены с прикладным [78].

Протоколы транспортного уровня реализуются программными средствами конечных узлов сети - компонентами ОС, соответственно связи между ОС будут описаны с помощью протоколов, работающих на транспортном уровне OSI.

Связи между ЛВС осуществляют маршрутизаторы с помощью протоколов, работающих на сетевом уровне OSI, соответственно связи между ЛВС будут описаны с помощью протоколов, работающих на данном уровне OSI [79].

Канальный и физический уровни не рассматриваются, так как в работе рассматривается информационная система в виртуальной среде, а данные уровни отвечают за взаимодействие объектов в физической среде.

Уровни взаимодействия между элементами информационной системы в соответствии с моделью OSI изображены на рисунке 2.6.

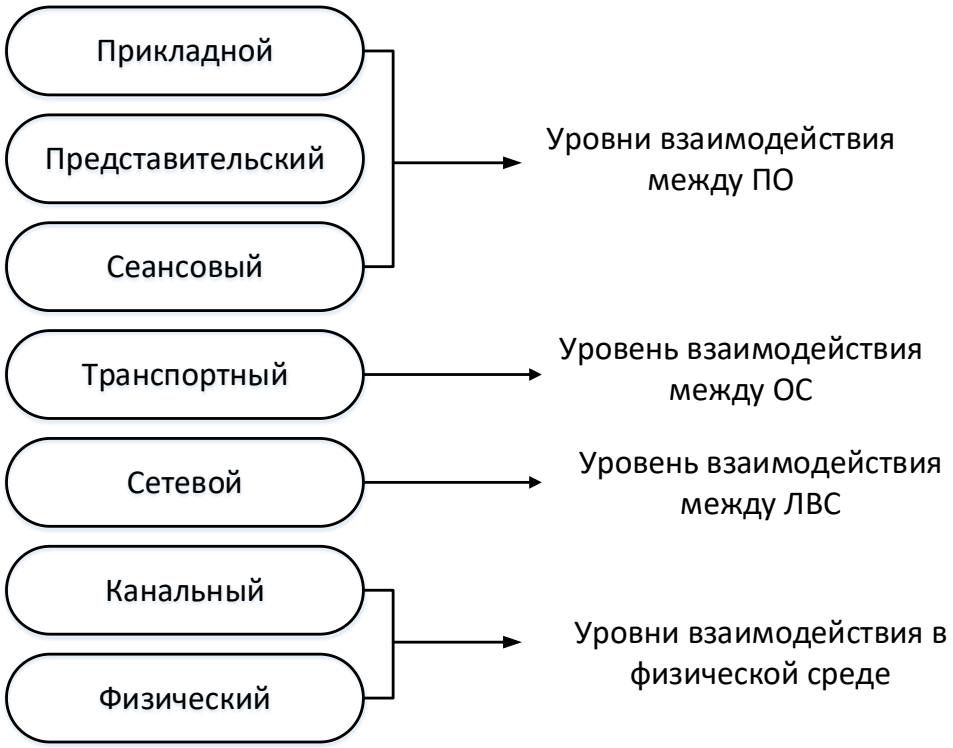


Рисунок 2.6 – Уровни взаимодействия между элементами информационной системы

Информационная система представляет из себя совокупность взаимосвязанных и взаимодействующих между собой элементов. Система является составным элементом для систем более высокого уровня, а ее элементы выступают в роли систем более низкого уровня [80].

Информационная система, структура которой изображена на рисунке 3.1, описывается с помощью атрибутивного метаграфа вложенности 3 построенного на основе работ [72] и [71].

Так как в настоящей работе рассматривается только программная составляющая компьютерной сети, то возникает коллизия понятий «операционная система» и «программное обеспечение». Корректными

формулировками в данном контексте являлись бы «системное программное обеспечение» и «прикладное программное обеспечение». Таким образом в настоящей работе для разделения структуры программного обеспечения компьютерной сети принимаются следующие обозначения:

— уровень прикладного программного обеспечения – уровень программного обеспечения (уровень ПО);
— уровень системного программного обеспечения – уровень операционных систем (уровень ОС);
— уровень программного обеспечения передачи данных в компьютерных сетях – уровень подсетей (уровень ЛВС).

Атрибутивный метаграф вложенности 3 представляется как упорядоченная шестерка:

$$G = (X_1, X_2, X_3, E_1, E_2, E_3),$$

где G – атрибутивный метаграф вложенности 3;

$X_1 = \{x_1^k\}$, $k = \overline{1,q}$ – множество программного обеспечения;

$X_2 = \{x_2^l\}$, $l = \overline{1,r}$ – множество операционных систем, $x_2^l \subset X_1$;

$X_3 = \{x_3^m\}$, $m = \overline{1,s}$ – множество ЛВС, $x_3^m \subset X_2$;

$E_1 = \{e_1^n\}$, $n = \overline{1,t}$ – множество связей между программным обеспечением, определенных на множестве X_1;

$E_2 = \{e_2^o\}$, $o = \overline{1,u}$ – множество связей между операционными системами, определенных на множестве X_2;

$E_3 = \{e_3^p\}$, $p = \overline{1,v}$ – множество связей между локальными вычислительными сетями, определенных на множестве X_3.

Причем существуют функции:

$$f_1^w : g_1^w(x_1^k, e_1^n) \to x_2^l,$$

где x_1^k – элемент из множества программного обеспечения;

e_1^n – элемент из множества связей между программным обеспечением;

x_2^l – элемент из множества операционных систем.

$$f_2^y : g_2^y\left(x_2^l, e_2^o\right) \rightarrow x_3^m,$$

где x_2^l– элемент из множества операционных систем;

e_2^o – элемент из множества связей между операционными системами;

x_3^m – элемент из множества локальных вычислительных сетей.

Вершина характеризуется множеством атрибутов:

$$x_i^b = \{atr_a\},$$

где $i = \overline{1,3}$ – уровень вложенности вершины;

b – номер вершины на соответствующем уровне i;

atr_a – атрибуты вершины (числовые, строковые и др).

Ребро характеризуется множеством атрибутов:

$$e_i^h = (x_i^s, x_i^e, \{atr_z\}),$$

где x_i^c – исходная вершина ребра;

x_i^d – конечная вершина ребра;

$j = \overline{1,3}$ – уровень вложенности ребра;

atr_z – атрибуты ребра (числовые, строковые и т.д.);

h – номер ребра на соответствующем уровне j;

c, d – номера вершин на соответствующем уровне i.

Возможные атрибуты для элементов данных множеств представлены в таблице 2.2.

Таблица 2.2 – Атрибуты для элементов множеств

Элементы множеств	Атрибуты
X_1 (множество ПО)	1 Название ПО 2 Номер версии драйвера ПО 3 Расположение ПО 4 Номер порта, который использует ПО
X_2 (множество ОС)	1 Название ОС 2 ip-адрес, который использует ОС 3 Настройки ОС
X_3 (множество ЛВС)	1 Название ЛВС 2 MAC–адрес сетевого оборудования 3 Название протоколов, по которым осуществляется взаимодействие в ЛВС 4 Настройки протоколов, работающих в сети
E_1 (множество связей между ПО)	Названия протоколов прикладного, представительского и сеансового уровней OSI
E_2 (множество связей между ПО)	Названия протоколов транспортного уровня OSI
E_3 (множество связей между ПО)	Названия протоколов сетевого уровня OSI

Дополнительно вводится правило, что связь между двумя элементами на *i*-ом уровне существует тогда и только тогда, когда связь существует между всеми элементами, находящихся на более высоких уровнях, которым принадлежат объекты *i*-го уровня. Это означает что программное обеспечение, находящееся на разных операционных системах связано между собой только в том случае, если соответствующие операционные системы также связаны между собой.

Также операционные системы, находящиеся в разных локальных вычислительных сетях, могут быть связаны между собой только при условии того, что соответствующие локальные вычислительные сети также связаны между собой.

Другими словами, взаимодействие между двумя элементами на i-ом уровне существует тогда и только тогда, когда связь существует на всех уровнях взаимодействия объектов в виртуальной среде модели OSI.

Для удобства формирование связей между объектами начинается со связи объектов 1-го уровня и выше, т.е. сначала формируются связи между ПО, затем между ОС и только потом между ЛВС.

2.4 Модель угроз информационной безопасности компьютерной сети

2.4.1 Модель угроз целостности компьютерной сети

В данной модели приводится перечень угроз целостности элементов информационной системы [6].

В ней выделяется две группы типов угроз:

— типы угроз для множеств элементов (вершин метаграфа);

— типы угроз для множеств связей между элементами (ребер метарафа).

Каждый из этих типов атак, в свою очередь, содержит по три ключевые атаки.

Типы угроз для множеств элементов:

1) подмена элемента (вершины);
2) удаление элемента (вершины);
3) добавление элемента (вершины).

Типы угроз для множеств связей:

1) подмена связи (ребра);
2) удаление связи (ребра);
3) добавление связи (ребра).

Моделью угроз целостности элементов информационной системы будет являться совокупность всех C_{si}:

$$C_s := \Big(C_{s1}\big(x_1^k x_2^l x_3^m\big) \cup C_{s1}\big(e_1^n e_2^o e_3^p\big) \cup C_{s2}\big(x_1^k x_2^l x_3^m\big) \cup C_{s2}\big(e_1^n e_2^o e_3^p\big) \cup$$
$$C_{s3}\big(x_1^k x_2^l x_3^m\big) \cup C_{s3}\big(e_1^n e_2^o e_3^p\big) \cup C_{s4}(atr_a) \cup C_{s4}(atr_z)\Big),$$

где C_{s1} – класс угроз подмены элемента или связи:

$C_{s1}\left(x_1^k x_2^l x_3^m\right)$ – угроза подмены элемента (вершины) на соответствующем уровне;

$C_{s1}\left(e_1^n e_2^o e_3^p\right)$ – угроза подмены связи (ребра) на соответствующем уровне;

C_{s2} – класс угроз удаления элемента или связи:

$C_{s2}\left(x_1^k x_2^l x_3^m\right)$ – угроза удаления элемента (вершины) на соответствующем уровне;

$C_{s2}\left(e_1^n e_2^o e_3^p\right)$ – угроза удаления связи (ребра) на соответствующем уровне;

C_{s3} – класс угроз добавления элемента или связи:

$C_{s3}\left(x_1^k x_2^l x_3^m\right)$ – угроза добавления элемента (вершины) на соответствующем уровне;

$C_{s3}\left(e_1^n e_2^o e_3^p\right)$ – угроза добавления связи (ребра) на соответствующем уровне;

C_{s4} – класс угроз изменения настроек элемента или связи:

$C_{s4}(atr_a)$ – угроза изменения настроек (атрибутов) элемента (вершины).

$C_{s4}(atr_z)$ – угроза изменения настроек (атрибутов) связи (ребра)

Характеристики связи задаются в атрибутах вершин. Характеристикой связи для множества программного обеспечения будет номер порта, используемого программным обеспечением, а для множества операционных систем – ip-адрес, используемый операционной системой. Характеристикой связи для множества локальных вычислительных сетей является ip-адрес сети и таблица маршрутизации, используемая для взаимодействия элементов входящих в сеть.

Угрозы целостности элементов информационной системы сведены в таблицу 2.3, которая представлена ниже.

Таблица 2.3 – Угрозы целостности информационной системы

	Множество ЛВС	Множество ОС	Множество ПО
Угрозы множества вершин	Подмена, выведение из строя, добавление		Подмена, удаление, установка
Угрозы множества атрибутов вершин	Изменение таблицы маршрутизации или ip-адреса сети	Изменение ip-адреса, который использует ОС	Изменение номера порта, который использует ПО
Угрозы множества ребер	Подмена, удаление, добавление протокола		
	Работающего на уровне ЛВС	Работающего на уровне ОС	Работающего на уровне ПО

Множества программного обеспечения, операционных систем и локальных вычислительных сетей обозначаются X_1, X_2, X_3, соответственно.

Множества связей между ПО, ОС и ЛВС обозначаются E_1, E_2, E_3.

Множества атрибутов программного обеспечения, операционных систем и локально-вычислительных сетей обозначаются atr_a. Причем, $atr_a \in x_1^k$ – на уровне ПО, $atr_a \in x_2^l$ – на уровне ОС, $atr_a \in x_3^m$ – на уровне ЛВС.

2.4.1.1 Угрозы на уровне программного обеспечения

Угроза подмены ПО характеризуется удалением вершины из множества X_1 и добавлением в него новой вершины [81]:

$$G' = \left(X_1 \setminus x_1^k, X_2, X_3, E_1, E_2, E_3\right), \quad (2.1)$$

где X_1 – множество программного обеспечения;

x_1^k – удаляемое программное обеспечение, причем $x_1^k \in X_1$.

$$G'' = \left(X_1 \cup x_1^{k\prime}, X_2, X_3, E_1, E_2, E_3\right), \quad (2.2)$$

где x_1^{q+1} – добавляемое программное обеспечение.

Угроза удаления программного обеспечения характеризуется удалением вершины из множества X_1, осуществляется по формуле (2.1).

Угроза установки программного обеспечения характеризуется добавлением во множество X_1 новой вершины, осуществляется по формуле (2.2).

Угроза подмены, удаления и добавления протоколов реализуются на прикладном, представительском или сеансовом уровне OSI.

Угроза подмены протокола характеризуется удалением ребра из множества E_1 и добавлением в него нового:

$$G' = (X_1, X_2, X_3, E_1 \setminus e_1^n, E_2, E_3), \tag{2.3}$$

где E_1 – множество связей между программным обеспечением;

e_1^n – удаляемая связь между программным обеспечением, причем $e_1^n \in E_1$.

$$G'' = (X_1, X_2, X_3, E_1 \cup e_1^{t+1}, E_2, E_3), \tag{2.4}$$

где e_1^{t+1} – добавляемая связь между программным обеспечением, t – количество ребер множества E_1.

Угроза удаления протокола осуществляется по формуле (2.3), а угроза добавления протокола, по которому взаимодействует программное обеспечение – по формуле (2.4).

Угроза подмены api-функции, которая связывает между собой программное обеспечение в соответствующей операционной системе, возможна согласно формулам (2.3) и (2.4), если существуют следующие функции:

$$f_1^w : g_1^w(e_1^n) \to x_2^1 \tag{2.5}$$

$$f_1^w : g_1^w(e_1^{t+1}) \to x_2^1 \tag{2.6}$$

где e_1^n – удаляемая связь между программным обеспечением;

e_1^{t+1} – добавляемая связь между программным обеспечением;

x_2^1 – элемент множества операционных систем.

Угроза удаления api-функции осуществляется по формуле (2.3), при условии, что существует функция (2.5).

Угроза добавления api-функции осуществляется по формуле (2.4), при условии, что существует функция (2.6).

Угроза изменения номера порта, используемого программным обеспечением, осуществляется изменением атрибута вершины:

$$atr_a := atr'_a,$$

где $atr_a \in x_1^k$, x_1^k – элемент множества ПО, $x_1^k \in X_1$;

atr_a – начальный номер порта;

atr'_a - измененный номер порта.

2.4.1.2 Угрозы на уровне операционных систем

Угроза подмены ОС характеризуется удалением вершины из множества X_2 и добавлением в него новой вершины:

$$G' = \left(X_1, X_2 \setminus x_2^l, X_3, E_1, E_2, E_3\right), \quad (2.7)$$

где X_2 – множество операционных систем;

x_2^l – удаляемая операционная система, причем $x_2^l \in X_2$.

$$G'' = (X_1, X_2 \cup x_2^{r+1}, X_3, E_1, E_2, E_3), \quad (2.8)$$

где x_2^{r+1} – добавляемое программное обеспечение.

Угроза намеренного повреждения (выведение из строя) операционной системы обеспечения характеризуется удалением вершины из множества X_2, осуществляется по формуле (2.7).

Угроза установки дополнительной операционной системы характеризуется добавлением во множество X_2 новой вершины, осуществляется по формуле (2.8).

Угрозы подмены, удаления и добавления протоколов реализуются на транспортном уровне OSI.

Угроза подмены протокола характеризуется удалением ребра из множества E_2 и добавлением в него нового:

$$G' = (X_1, X_2, X_3, E_1, E_2 \setminus e_2^o, E_3), \quad (2.9)$$

где E_2 – множество связей между операционными системами;

e_2^o – удаляемая связь между операционными системами, причем $e_2^o \in E_2$.

$$G'' = (X_1, X_2, X_3, E_1, E_2 \cup e_2^{u+1}, E_3), \quad (2.10)$$

где e_2^{u+1} – добавляемая связь между операционными системами;

u – количество ребер множества E_2.

Угроза удаления протокола осуществляется по формуле (2.9), а угроза добавления протокола, по которому взаимодействуют операционные системы – по формуле (2.10).

Угроза изменения ip-адреса, используемого операционной системой, осуществляется изменением атрибута вершины:

$$atr_a := atr'_a,$$

где $atr_a \in x_2^l$, x_2^l– элемент множества ПО, $x_2^l \in X_2$;

atr_a – начальный номер порта;

atr'_a - измененный номер порта.

2.4.1.3 Угрозы на уровне локальных вычислительных сетей

Угроза подмены локально-вычислительной сети осуществляется удалением вершины из множества X_3 и добавлением в него новой вершины:

$$G' = (X_1, X_2, X_3 \setminus x_3^m, E_1, E_2, E_3), \quad (2.11)$$

где X_3 – множество ЛВС;

x_3^m – удаляемая ЛВС, причем $x_3^m \in X_3$.

$$G'' = (X_1, X_2, X_3 \cup x_3^{s+1}, E_1, E_2, E_3), \quad (2.12)$$

где x_3^{s+1} – добавляемая локально-вычислительная сеть.

Угроза намеренного повреждения (выведение из строя) локально-вычислительной сети характеризуется удалением вершины из множества X_3, осуществляется по формуле (2.11).

Угроза установки дополнительной локально-вычислительной сети характеризуется добавлением во множество X_3 новой вершины, осуществляется по формуле (2.12).

Угрозы подмены, удаления и добавления протоколов реализуются на сетевом уровне OSI.

Угроза подмены протокола характеризуется удалением ребра из множества E_3 и добавлением в него нового:

$$G' = \left(X_1, X_2, X_3, E_1, E_2, E_3 \setminus e_2^p\right), \quad (2.13)$$

где E_3– множество связей между операционными системами;

e_2^p – удаляемая связь между операционными системами, причем $e_2^o \in E_3$.

$$G'' = (X_1, X_2, X_3, E_1, E_2, E_3 \cup e_2^{v+1}), \quad (2.14)$$

где e_2^{v+1} – добавляемая связь между операционными системами;

v – количество ребер множества E_3.

Угроза удаления протокола осуществляется по формуле (2.13), а угроза добавления протокола, по которому взаимодействуют локальные вычислительные сети – по формуле (2.14).

Угроза изменения ip-адреса сети осуществляется изменением параметров атрибута вершины x_3^m:

$$atr_a := atr'_a,$$

где $atr_a \in x_3^m$, x_3^m– элемент множества ЛВС, $x_3^m \in X_3$;

atr_a – правильный ip-адрес сети;

atr'_a – измененный ip-адрес сети.

Угроза изменения таблицы маршрутизации, используемая локально-вычислительной сетью, осуществляется изменением параметров атрибута вершины x_3^m, который содержит таблицу маршрутизации:

$$atr_a := atr'_a,$$

где $atr_a \in x_3^m$, x_3^m– элемент множества ЛВС, $x_3^m \in X_3$;

atr_a – изначальная таблица маршрутизации;

atr'_a – измененный таблица маршрутизации.

2.4.2 Модель угроз конфиденциальности компьютерной сети

В рамках исследовательской работы был разработан подход к построению модели угроз конфиденциальности элементам информационной системы, основанный на [6]. При разработке подхода использовалась структура информационной системы, построенная с помощью метаграфа, описанного в разделе 2.2.

Имея информационную систему, состоящую из локально-вычислительной сети, рабочей станции (операционной системы) и программного обеспечения, были описаны угрозы, применимые к вершинам (ЛВС, ОС, ПО) и ребрам метаграфа (связи между ЛВС, ОС, ПО). Также описаны угрозы на атрибуты метаграфа.

Атрибутами метаграфа могут быть, например:

— номер версии операционной системы;

— версия протокола, по которому передаются данные;

— имя рабочей станции;

— ip-адрес;

— длина ключа шифрования

— и т.д.

Пример угроз:

— разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие операционных систем, в соответствующей локальной сети;

— разглашение (утечка) информации о названии программного обеспечения, установленного в рамках операционной системы;

— разглашение информации о портах, использующихся для передачи данных между рабочими станциями;

— и т.д.

В разработанной модели угроз описываются угрозы конфиденциальности элементам информационной системы.

В общем случае под конфиденциальностью понимают свойство информации, которое состоит в том, что данная информация не будет доступна пользователям, которые не имеют к ней отношения.

В Федеральном Законе «Об информации, информационных технологиях и защите информации» [60], дается понятие конфиденциальности информации. В соответствии с данным законом, конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

С точки зрения конфиденциальности в локально-вычислительной сети нарушителю (злоумышленнику) интересна вся информация о операционной системе (рабочих станциях), программном обеспечении, которое установлено в рамках операционной системы, а также протоколы, по которым взаимодействую элементы сети, а также о их настройках. Если злоумышленник соберет всю информацию о локальной сети, то с помощью полученных данных может, в дальнейшем, нанести ущерб данной сети.

Разработанная модель является дополнением к модели угроз целостности элементов информационной системы, рассмотренной в разделе 2.4.1.

Угрозами для каждого множество атрибутов вершин является разглашение (утечка) информации о данных вершинах.

Угрозами для каждого множества ребер, соответственно, является разглашение (утечка) информации о данных ребрах.

Моделью угроз конфиденциальности всей системы K_s будет являться совокупность всех K_{si}:

$$K_s := \left(K_{s1}\left(x_1^k\ x_2^l\ x_3^m\right) \cup K_{s1}\left(e_1^n\ e_2^o\ e_3^p\right) \cup K_{s2}(atr_a) \cup K_{s2}(atr_z)\right),$$

где K_{s1} – класс угроз разглашения (утечки) информации о имени элементов и связей:

$K_{s1}\left(x_1^k\ x_2^l\ x_3^m\right)$ – угроза разглашения (утечки) информации о имени элементов (вершины);

$K_{s1}\left(e_1^n\ e_2^o\ e_3^p\right)$ – угроза разглашения (утечки) информации о имени элементов (ребра);

K_{s2} – класс угроз разглашения (утечки) информации о настройках элементов и связей:

$K_{s2}(atr_a)$ – угроза разглашения (утечки) информации о настройках (атрибутах) элементов (вершин);

$K_{s2}(atr_z)$ – угроза разглашения (утечки) информации о настройках (атрибутах) связей (ребер).

Настройки системы задаются в атрибутах вершин. Настройки связи задаются в атрибутах ребер. Настройками системы, в данном случае, будет являться вся информация о версии программного обеспечения, версии операционных системы, о драйверах, которые использует программное обеспечение и прочее. Настройками сети будет являться вся информация о протоколах, например длина ключа шифрования, версия протокола, набор

правил, mac-адреса сетевого оборудования, ip-адреса сетевых устройств и прочее.

Степень ущерба будет напрямую зависеть от того, какой важности информация обрабатывается в информационной системе.

Все угрозы разглашения (утечки) информации можно разбить на группы, в зависимости от того, что рассматривается: вершины, ребра или атрибуты метаграфа.

Под именем программного обеспечения, операционной системы и локальной вычислительной сети, будем понимать полный адрес расположения элемента в системе, включающий названия ПО, ОС и ЛВС.

Угрозы для множества вершин описаны в таблице 2.4, представленной далее.

Таблица 2.4 – Угрозы конфиденциальности для множества элементов

Множество	Угрозы конфиденциальности компьютерной сети
X_3 (множество ЛВС)	Разглашение (утечка) информации о имени ЛВС
X_2 (множество ОС)	Разглашение (утечка) информации о имени ОС
X_1 (множество ПО)	Разглашение (утечка) информации о имени ПО

В таблице 2.5 представлены угрозы для множества ребер.

Таблица 2.5 – Угрозы конфиденциальности для множества связей

Множество	Угрозы конфиденциальности компьютерной сети
E_3 (множество связей между ЛВС)	Разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ЛВС
E_2 (множество связей между ОС)	Разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ОС
E_1 (множество связей между ПО)	Разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ПО

Угрозы для множеств атрибутов вершин описаны в таблице 2.6.

Таблица 2.6 – Угрозы конфиденциальности для настроек

Множество	Угрозы конфиденциальности информационной системы
$\{atr_a\} \in x_1^m$ (множество атрибутов ЛВС)	Разглашение (утечка) информации о настройках ЛВС
$\{atr_a\} \in x_1^l$ (множество атрибутов ОС)	Разглашение (утечка) информации о настройках ОС
$\{atr_a\} \in x_1^k$(множество атрибутов ПО)	Разглашение (утечка) информации о настройках ПО

Угрозы разглашения информации о настройках сети для множеств вершин представлены в таблице 2.7.

Таблица 2.7 – Угрозы конфиденциальности для множеств атрибутов ребер (настройки сети)

Множество	Угрозы конфиденциальности информационной системы
$\{atr_z\} \in e_3^p$ (множество атрибутов связей между ЛВС)	Разглашение (утечка) информации о настройках протокола на уровне ЛВС
$\{atr_z\} \in e_2^o$ (множество атрибутов связей между ЛВС)	Разглашение (утечка) информации о настройках протокола на уровне ОС
$\{atr_z\} \in e_1^n$ (множество атрибутов связей между ЛВС)	Разглашение (утечка) информации о настройках протокола на уровне ПО

2.4.2.1 Угрозы на уровне программного обеспечения

Угрозы конфиденциальности на уровне программного обеспечения:

— разглашение (утечка) информации о имени ПО;

— разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ПО;

— разглашение (утечка) информации о настройках ПО;

— разглашение (утечка) информации о настройках протокола на уровне ПО.

Угроза разглашения (утечки) информации о имени программного обеспечения характеризуется пересечением множества X_1 с множеством J_1:

$$G' = (X_1 \cap J_1, X_2, X_3, E_1, E_2, E_3),$$

где $X_1 \cap J_1 = \{x_1^k | x_1^k \in X_1 \wedge x_1^k \in J_1\}$;

x_1^k – элемент, принадлежащий множеству X_1;

X_1 – множество ПО, которое необходимо защитить;

J_1 – множество ПО, элементы которого известны всем.

Пересечением множеств называется множество, которое состоит из тех и только тех элементов, которые принадлежат как первому множеству, так и второму [82].

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие программного обеспечения характеризуется пересечением множества E_1с множеством D_1:

$$G' = (X_1, X_2, X_3, E_1 \cap D_1, E_2, E_3),$$

где $E_1 \cap D_1 = \{e_1^n | e_1^n \in E_1 \wedge e_1^n \in D_1\}$;

e_1^n – элемент, принадлежащий множеству E_1;

E_1 – множество связей между программным обеспечением;

D_1 – множество связей между ПО, элементы которого известны.

Угроза разглашения (утечки) информации о настройках программного обеспечения, характеризуется пересечением вершины x_1^k, содержащей атрибут, который описывает настройки ПО, с множеством J_1:

$$atr_a := atr_a',$$

где $atr_a \in x_1^k$,

x_1^k – элемент множества ПО, $x_1^k \in X_1$;

atr_a – атрибут вершины x_1^k, содержащий настройки ПО;

atr'_a – атрибут вершины из множества J_1.

Угроза разглашения (утечки) информации о настройках протокола на уровне ПО характеризуется пересечением вершины e_1^n, содержащей атрибут, который описывает настройки связи на уровне ПО, с множеством J_1:

$$atr_z := atr'_z,$$

где $atr_z \in e_1^n$,

e_1^n– элемент множества связей между ПО, $e_1^n \in E_1$;

atr_z – атрибут ребра e_1^n, в котором содержится описание настроек связи на уровне ПО;

atr'_z – атрибут ребра из множества J_1.

2.4.2.2 Угрозы на уровне операционных систем

Угрозы конфиденциальности на уровне операционных систем:

— разглашение (утечка) информации о имени ОС;

— разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ОС;

— разглашение (утечка) информации о настройках ОС;

— разглашение (утечка) информации о настройках протокола на уровне ОС.

Угроза разглашения (утечки) информации о имени операционной системы характеризуется пересечением множества X_2 с множеством J_2:

$$G' = (X_1, X_2 \cap J_2, X_3, E_1, E_2, E_3),$$

где $X_2 \cap J_2 = \{x_2^l | x_2^l \in X_2 \wedge x_2^l \in J_2\}$;

x_2^l – элемент, принадлежащий множеству X_2;

X_2 – множество ОС, которое необходимо защитить;

J_2 – множество ОС, элементы которого известны всем.

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие операционных систем характеризуется пересечением множества E_2с множеством D_2:

$$G' = (X_1, X_2, X_3, E_1, E_2 \cap D_2, E_3),$$

где $E_2 \cap D_2 = \{e_2^o | e_2^o \in E_2 \wedge e_2^o \in D_2\}$;

e_2^o – элемент, принадлежащий множеству E_2;

E_2 – множество связей между операционными системами;

D_2 – множество связей между ОС, элементы которого известны.

Угроза разглашения (утечки) информации о настройках операционных систем, характеризуется пересечением вершины x_2^l, содержащей атрибут, который описывает настройки ОС, с множеством J_2:

$$atr_a := atr_a',$$

где $atr_a \in x_2^l$,

x_2^l– элемент множества ОС, $x_2^l \in X_2$;

atr_a – атрибут вершины x_2^l, содержащий настройки ОС;

atr_a' – атрибут вершины из множества J_2.

Угроза разглашения (утечки) информации о настройках протокола на уровне ОС характеризуется пересечением ребра e_2^o, содержащей атрибут, который описывает настройки связи на уровне ОС, с множеством J_2:

$$atr_z := atr_z',$$

где $atr_z \in e_2^o$,

e_2^o– элемент множества ОС $e_2^o \in E_2$;

atr_z – атрибут ребра e_2^o , в котором содержится описание настроек связи на уровне ОС;

atr_z' – атрибут ребра из множества J_2.

2.4.2.3 Угрозы на уровне локальных вычислительных сетей

Угрозы конфиденциальности на уровне локальных вычислительных сетей:

— разглашение (утечка) информации о имени ЛВС;

— разглашение (утечка) информации о протоколе, по которому осуществляется взаимодействие ЛВС;

— разглашение (утечка) информации о настройках ЛВС;

— разглашение (утечка) информации о настройках протокола на уровне ЛВС.

Угроза разглашения (утечки) информации о имени локально-вычислительной сети характеризуется пересечением множества X_3 с множеством J_3:

$$G' = (X_1, X_2, X_3 \cap J_3, E_1, E_2, E_3),$$

где $X_3 \cap J_3 = \{x_3^m | x_3^m \in X_3 \wedge x_3^m \in J_3\}$;

x_3^m – элемент, принадлежащий множеству X_3;

X_3 – множество ЛВС, которое необходимо защитить;

J_3 – множество ЛВС, элементы которого известны всем.

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие локально – вычислительных сетей характеризуется пересечением множества E_3с множеством D_3:

$$G' = (X_1, X_2, X_3, E_1, E_2, E_3 \cap D_3),$$

где $E_3 \cap D_3 = \{e_3^p | e_3^p \in E_3 \wedge e_3^p \in D_3\}$;

e_3^p – элемент, принадлежащий множеству E_3;

E_3 – множество связей между операционными системами;

D_3 – множество связей между ОС, элементы которого известны.

Угроза разглашения (утечки) информации о настройках ЛВС, характеризуется пересечением вершины x_3^m, содержащей атрибут, который описывает настройки ЛВС, с множеством J_3:

$$atr_a := atr'_a,$$

где $atr_a \in x_3^m$,

x_3^m– элемент множества ЛВС, $x_3^m \in X_3$;

atr_a – атрибут вершины x_3^m, который содержит настройки ЛВС;

atr'_a – атрибут вершины из множества J_3.

Угроза разглашения (утечки) информации о настройках протокола на уровне ЛВС характеризуется пересечением ребра e_3^p, содержащей атрибут, который описывает настройки связи на уровне ЛВС, с множеством D_3:

$$atr_z := atr'_z,$$

где $atr_z \in e_3^p$,

e_3^p– элемент множества ЛВС, $e_3^p \in E_3$;

atr_z – атрибут ребра e_3^p, в котором содержится описание настроек связи на уровне ЛВС;

atr'_z – атрибут ребра из множества J_3.

2.4.3 Модель угроз целостности и конфиденциальности компьютерной сети

Безопасностью всей системы T_S будет являться объединение K_S и C_S:

$$T_S = K_S \cup C_S;$$

где K_S – модель угроз конфиденциальности элементов информационной системы;

C_S – модель угроз целостности элементов информационной системы.

Объединением множеств называется множество, состоящее из всех элементов, принадлежащих или первому, или второму множеству [82].

Следовательно, безопасность всей системы можно представить формулой:

$$T_S := (C_{s1}(x_1^k x_2^l x_3^m) \cup C_{s1}(e_1^n e_2^o e_3^p) \cup C_{s2}(x_1^k x_2^l x_3^m) \cup C_{s2}(e_1^n e_2^o e_3^p) \cup C_{s3}(x_1^k x_2^l x_3^m) \cup C_{s3}(e_1^n e_2^o e_3^p) \cup C_{s4}(atr_a) \cup K_{s1}(x_1^k\ x_2^l\ x_3^m) \cup K_{s1}(e_1^n\ e_2^o\ e_3^p) \cup K_{s2}(atr_a) \cup K_{s2}(atr_z)).$$

2.4.3.1 Угрозы на уровне программного обеспечения

Угроза разглашения (утечки) информации о имени программного обеспечения характеризуется пересечением множества X_1 с множеством J_1:

$$G' = (X_1 \cap J_1, X_2, X_3, E_1, E_2, E_3),$$

где $X_1 \cap J_1 = \{x_1^k | x_1^k \in X_1 \wedge x_1^k \in J_1\}$;

X_1 – множество ПО, элементы которого необходимо защитить;

x_1^k – элемент, принадлежащий множеству X_1;

J_1 – множество ПО, элементы которого известны всем.

Угроза подмены программного обеспечения характеризуется удалением вершины из множества X_1 и добавлением в него новой вершины:

$$G' = (X_1 \setminus x_1^k, X_2, X_3, E_1, E_2, E_3), \quad (2.15)$$

где X_1 – множество ПО, элементы которого необходимо защитить;

x_1^k – удаляемое программное обеспечение, причем $x_1^k \in X_1$.

$$G'' = (X_1 \cup x_1^{q+1}, X_2, X_3, E_1, E_2, E_3), \quad (2.16)$$

где x_1^{q+1} – добавляемое программное обеспечение.

Угроза удаления программного обеспечения характеризуется удалением вершины из множества X_1, осуществляется по формуле (2.15).

Угроза установки программного обеспечения характеризуется добавлением во множество X_1 новой вершины, осуществляется по формуле (2.16).

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие программного обеспечения характеризуется пересечением множества E_1с множеством D_1:

$$G' = (X_1, X_2, X_3, E_1 \cap D_1, E_2, E_3),$$

где $E_1 \cap D_1 = \{e_1^n | e_1^n \in E_1 \wedge e_1^n \in D_1\}$;

E_1 – множество связей между ПО, которые необходимо защитить;

e_1^n – элемент, принадлежащий множеству E_1;

D_1 – множество связей между ПО, элементы которого известны.

Угроза подмены протокола характеризуется удалением ребра из множества E_1 и добавлением в него нового:

$$G' = (X_1, X_2, X_3, E_1 \setminus e_1^n, E_2, E_3), \quad (2.17)$$

где E_1 – множество связей между программным обеспечением, которые необходимо защитить;

e_1^n – удаляемая связь между программным обеспечением, причем $e_1^n \in E_1$.

$$G'' = (X_1, X_2, X_3, E_1 \cup e_1^{t+1}, E_2, E_3), \quad (2.18)$$

где e_1^{t+1} – добавляемая связь между программным обеспечением, t – количество ребер множества E_1.

Угроза удаления протокола, по которому взаимодействует программное обеспечение осуществляется по формуле (2.17).

Угроза добавления протокола, по которому взаимодействует программное обеспечение – по формуле (2.18).

Угроза подмены api-функции, которая связывает между собой программное обеспечение в соответствующей операционной системе, возможна согласно формулам (2.17) и (2.18).

Угроза удаления api-функции осуществляется по формуле (2.17).

Угроза добавления api-функции осуществляется по формуле (2.18).

Угроза изменения номера порта, используемого программным обеспечением, осуществляется изменением атрибута вершины x_1^k:

$$atr_a := atr_a',$$

где $atr_a \in x_1^k$, x_1^k – элемент множества ПО, $x_1^k \in X_1$;

atr_a – начальный номер порта;

atr_a' – измененный номер порта.

Угроза разглашения (утечки) информации о настройках программного обеспечения, характеризуется пересечением вершины x_1^k, содержащей атрибут, который описывает настройки ПО, с множеством J_1:

$$atr_a := atr_a',$$

где $atr_a \in x_1^k$,

x_1^k – элемент множества ПО, $x_1^k \in R_1$;

atr_a – атрибут вершины x_1^k, содержащий настройки ПО;

atr_a' – атрибут вершины из множества J_1.

Угроза разглашения (утечки) информации о настройках протокола на уровне ПО характеризуется пересечением вершины e_1^n, содержащей атрибут, который описывает настройки связи на уровне ПО, с множеством J_1:

$$atr_z := atr_z',$$

где $atr_z \in e_1^n$,

e_1^n – элемент множества связей между ПО, $e_1^n \in E_1$;

atr_z – атрибут ребра e_1^n, в котором содержится описание настроек связи на уровне ПО;

atr_z' – атрибут ребра из множества J_1.

2.4.3.2 Угрозы на уровне операционных систем

Угроза подмены ОС характеризуется удалением вершины из множества X_2 и добавлением в него новой вершины:

$$G' = \left(X_1, X_2 \setminus x_2^l, X_3, E_1, E_2, E_3\right), \quad (2.19)$$

где X_2 – множество ОС, элементы которого необходимо защитить;

x_2^l – удаляемая операционная система, причем $x_2^l \in X_2$.

$$G'' = (X_1, X_2 \cup x_2^{r+1}, X_3, E_1, E_2, E_3), \quad (2.20)$$

где x_2^{r+1} – добавляемое программное обеспечение.

Угроза удаления операционной системы характеризуется удалением вершины из множества X_2, осуществляется по формуле (2.19).

Угроза установки программного обеспечения характеризуется добавлением во множество X_2 новой вершины, осуществляется по формуле (2.20).

Угроза разглашения (утечки) информации о имени операционной системы характеризуется пересечением множества X_2 с множеством J_2:

$$G' = (X_1, X_2 \cap J_2, X_3, E_1, E_2, E_3),$$

где $X_2 \cap J_2 = \{x_2^l | x_2^l \in X_2 \wedge x_2^l \in J_2\}$;

X_2 – множество ОС, элементы которого необходимо защитить;

x_2^l – элемент, принадлежащий множеству X_2;

J_2 – множество ОС, элементы которого известны всем.

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие операционных систем характеризуется пересечением множества E_2с множеством D_2:

$$G' = (X_1, X_2, X_3, E_1, E_2 \cap D_2, E_3),$$

где $E_2 \cap D_2 = \{e_2^o | e_2^o \in E_2 \wedge e_2^o \in D_2\}$;

E_2 – множество связей между ОС, элементы которого необходимо защитить;

e_2^o – элемент, принадлежащий множеству E_2;

D_2 – множество связей между ОС, элементы которого известны.

Угроза подмены протокола характеризуется удалением ребра из множества E_2 и добавлением в него нового:

$$G' = (X_1, X_2, X_3, E_1, E_2 \setminus e_2^o, E_3), \quad (2.21)$$

где E_2 – множество связей между операционными системами;

e_2^o – удаляемая связь между операционными системами, причем $e_2^o \in E_2$.

$$G'' = (X_1, X_2, X_3, E_1, E_2 \cup e_2^{u+1}, E_3), \quad (2.22)$$

где e_2^{u+1} – добавляемая связь между операционными системами;

u – количество ребер множества E_2.

Угроза удаления протокола, по которому взаимодействуют операционные системы осуществляется по формуле (2.21).

Угроза добавления протокола, по которому операционные системы – по формуле (2.22).

Угроза изменения ip-адреса, используемого операционной системой, осуществляется изменением атрибута вершины x_2^l:

$$atr_a := atr_a',$$

где $atr_a \in x_2^l$, x_2^l– элемент множества ПО, $x_2^l \in X_2$;

atr_a – начальный номер порта;

atr_a' – измененный номер порта.

Угроза разглашения (утечки) информации о настройках операционных систем, характеризуется пересечением вершины x_2^l, содержащей атрибут, который описывает настройки ОС, с множеством J_2:

$$atr_a := atr'_a,$$

где $atr_a \in x_2^l$,

x_2^l– элемент множества ОС, $x_2^l \in X_2$;

atr_a – атрибут вершины x_2^l, содержащий настройки ОС;

atr'_a – атрибут вершины из множества J_2.

Угроза разглашения (утечки) информации о настройках протокола на уровне ОС характеризуется пересечением вершины e_2^o, содержащей атрибут, который описывает настройки связи на уровне ОС, с множеством D_2:

$$atr_z := atr'_z,$$

где $atr_z \in e_2^o$,

e_2^o – элемент множества связей между ПО, $e_2^o \in E_2$;

atr_z – атрибут ребра e_2^o, в котором содержится описание настроек связи на уровне ПО;

atr'_z – атрибут ребра из множества D_2.

2.4.3.3 Угрозы на уровне локальных вычислительных сетей

Угроза подмены локально-вычислительной сети осуществляется удалением вершины из множества X_3 и добавлением в него новой вершины:

$$G' = (X_1, X_2, X_3 \setminus x_3^m, E_1, E_2, E_3), \quad (2.23)$$

где X_3 – множество ЛВС, элементы которого необходимо защитить;

x_3^m – удаляемая ЛВС, причем $x_3^m \in X_3$.

$$G'' = (X_1, X_2, X_3 \cup x_3^{s+1}, E_1, E_2, E_3), \quad (2.24)$$

где x_3^{s+1} – добавляемая локально-вычислительная сеть.

Угроза намеренного повреждения (выведение из строя) локально-вычислительной сети характеризуется удалением вершины из множества X_3, осуществляется по формуле (2.23).

Угроза добавления локальной вычислительной сети характеризуется добавление новой вершины в множество X_3, которая осуществляется по формуле (2.24).

Угроза разглашения (утечки) информации о имени локально-вычислительной сети характеризуется пересечением множества X_3 с множеством J_3:

$$G' = (X_1, X_2, X_3 \cap J_3, E_1, E_2, E_3),$$

где $X_3 \cap J_3 = \{x_3^m | x_3^m \in X_3 \wedge x_3^m \in J_3\}$;

X_3 – множество ЛВС, элементы которого необходимо защитить;

x_3^m – элемент, принадлежащий множеству X_3;

J_3 – множество ЛВС, элементы которого известны всем.

Угроза разглашения (утечки) информации о протоколе, по которому осуществляется взаимодействие локально – вычислительных сетей характеризуется пересечением множества E_3с множеством D_3:

$$G' = (X_1, X_2, X_3, E_1, E_2, E_3 \cap D_3),$$

где $E_3 \cap D_3 = \{e_3^p | e_3^p \in E_3 \wedge e_3^p \in D_3\}$;

E_3 – множество связей между ЛВС;

e_3^p – элемент, принадлежащий множеству E_3;

D_3 – множество связей между ОС, элементы которого известны.

Угроза подмены протокола характеризуется удалением ребра из множества E_3 и добавлением в него нового:

$$G' = \left(X_1, X_2, X_3, E_1, E_2, E_3 \setminus e_3^p\right), \quad (2.25)$$

где E_3 – множество связей между ЛВС;

e_3^p – удаляемая связь между операционными системами, причем $e_3^p \in E_3$.

$$G'' = (X_1, X_2, X_3, E_1, E_2, E_3 \cup e_3^{v+1}), \quad (2.26)$$

где e_3^{v+1} – добавляемая связь между операционными системами;

v – количество ребер множества E_3.

Угроза удаления протокола взаимодействия локальных вычислительных сетей осуществляется по формуле (2.25).

Угроза добавления протокола, по которому взаимодействуют локальные вычислительные сети – по формуле (2.26).

Угроза изменения ip-адреса сети осуществляется изменением параметров атрибута вершины x_3^m:

$$atr_a := atr_a',$$

где $atr_a \in x_3^m$, x_3^m– элемент множества ЛВС, $x_3^m \in X_3$;

atr_a – правильный ip-адрес сети;

atr_a' – измененный ip-адрес сети.

Угроза изменения таблицы маршрутизации, используемая локально-вычислительной сетью, осуществляется изменением параметров атрибута вершины x_3^m аналогичным образом.

Угроза разглашения (утечки) информации о настройках операционных систем, характеризуется пересечением вершины x_3^m, содержащей атрибут, который описывает настройки ОС, с множеством J_2:

$$atr_a := atr_a',$$

где $atr_a \in x_3^m$,

x_3^m– элемент множества ОС, $x_3^m \in X_3$;

atr_a – атрибут вершины x_3^m, содержащий настройки ЛВС;

atr'_a – атрибут вершины из множества J_2.

Угроза разглашения (утечки) информации о настройках протокола на уровне ЛВС характеризуется пересечением вершины e_3^p из множества E_3, содержащей атрибут, который описывает настройки связи на уровне ЛВС, с множеством D_3:

$$atr_z := atr'_z,$$

где $atr_z \in e_3^p$,

e_3^p – элемент множества ЛВС, $e_3^p \in E_3$;

atr_z – атрибут ребра e_3^p, в котором содержится описание настроек связи на уровне ЛВС;

atr'_z – атрибут ребра из множества J_3.

Таким образом совмещаются две, разработанные по отдельности, модели: модель угроз целостности и модель угроз конфиденциальности элементов информационной системы, в одну, которая носит название модель угроз безопасности компьютерной сети.

2.5 Выводы по главе

Результатами работы, представленными в настоящей главе, являются методика определения перечня угроз, а также модели компьютерной сети и угроз безопасности компьютерной сети.

Модель компьютерной сети на основе атрибутивных метаграфов позволяет описывать компоненты программного обеспечения компьютерных сетей и все возможные связи между ними. К компонентам программного обеспечения в данном случае относится прикладное, системное и сетевое программное обеспечение. Связи подразумеваются не только между элементами, находящимися на одном уровне, но и обозначающие вложенность одних элементов в другие. С использованием разработанной модели возможно

на этапе проектирования структуры систем учитывать характеристики элементов и взаимосвязи между ними для формирования требований к функциям средств защиты информации.

Модель угроз, основанная на элементарных операциях над метаграфами, позволяет составлять полные перечни угроз целостности и конфиденциальности компьютерных сетей. Далее, в главе 3, показано, что разработанная модель угроз выигрывает сравнение с наиболее полным аналогом, существующим на данный момент – банком данных угроз ФСТЭК России. Недостатки моделей угроз, рассмотренных в главе 1, были учтены и по возможности устранены:

1) элементы модели нарушителя полностью устранены из модели угроз;

2) все угрозы описаны однотипно, и присутствует строгое их разделение на классы;

3) угрозы были разделены на угрозы информации и системе, в настоящей рассмотрен подход к описанию угроз системе, т.е. компьютерной сети;

4) субъективность и влияние профессионального уровня эксперта при построении перечня угроз сведены к минимуму, благодаря формализации подхода к определению угроз.

Разработанная методика составления перечня угроз информационной безопасности компьютерных сетей, использующая вышеупомянутые модели, позволяет увеличить количество идентифицируемых угроз при формировании моделей угроз информационных систем и, в частности компьютерных сетей. Ее преимуществом является повторяемость: разные эксперты, используя ее, получат одинаковый перечень угроз для одной системы в независимости от их профессионального уровня. Однако, условием в данном случае будет правильное формирование перечня элементов рассматриваемой системы.

Также методика может быть применена как один из этапов оценки защищенности компьютерных сетей [83, 84, 85, 86].

3 Внедрение результатов исследования

3.1 Сравнение перечня угроз с банком данных угроз ФСТЭК России

В результате анализа представленных в разделе 1.2 источников, было отмечено, что обобщенные угрозы информационной безопасности, содержащиеся в [55], [56] и [57] более детально описаны в источнике [23].

Так, например, угроза из [55] (перечисление о) соответствует угрозе из [56] (перечисление г), что в свою очередь соответствует угрозе 167. Угроза из [55] V соответствует угрозе из [56] Н, что совпадает с угрозой 32. Угроза из [55] (перечисление л) соответствует угрозе из [56] (перечисление к), что соответствует угрозе из [57] (перечисление м), и в итоге соответствует угрозе 140 из [23]. В таблице 3.1 представлены соответствия угроз информационной безопасности из источников [55], [56], [57] источнику [23].

Таблица 3.1 – Сопоставление угроз информационной безопасности

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн	Частная модель угроз безопасности ПДн учреждений здравоохранения…	ГОСТ Р ИСО/МЭК 27005 – 2010	Банк данных угроз безопасности информации ФСТЭК России
а		и	199
б		ж, з	203
в			126
г			154
д			18
е	а		145
ж			98
з, п, ф	ж	т	98
и	в		74
к			32

Окончание таблицы 3.1 – Сопоставление угроз информационной безопасности

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн	Частная модель угроз безопасности ПДн учреждений здравоохранения…	ГОСТ Р ИСО/МЭК 27005 – 2010	Банк данных угроз безопасности информации ФСТЭК России
л	к	м, н, п, ц, щ	140
м	л		195
н			99
о	г		167
р			98
с	и		12
т			174
у			99
х			12
ц	з		32
	б		39
	е		126
		а	71
		б	17
		в	186
		г	143
		д	188
		е	133
		к	156
		л	139
		о	22
		р	23
		с	203
		у	44
		ф	27
		х	127
		ч	20
		щ	128
		ы	139

При этом, по итогам сопоставления следует заметить, что перечень угроз из [23] перекрывает все угрозы, обозначенные в [55], [56] и [57]. Следовательно, дальнейшее сравнение результатов настоящего исследования будет производиться именно с [23].

В ходе анализа угроз в [23], была составлена таблица 3.2, в которой представлена классификация угроз информационной безопасности. Классификация включает три группы: информация, информационная система, система защиты информации, рассматриваются только технические меры, то есть те меры, которые направлены на защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев [58].

На данном этапе, для установления однозначности, необходимо обозначить определения информационной системе и информации.

Под информационной системой понимается система, предназначенная для сбора, передачи, обработки, хранения и выдачи информации потребителям [59].

Информация – это сведения, которые можно собирать, хранить, передавать, обрабатывать и использовать [60].

Стоит отметить, что возникает трудность при распределении угроз информационной безопасности между информационной системой и системой защиты информации, так как существуют встроенные механизмы защиты в информационную систему, которые не значительно могут отличаться от системы защиты информации.

При рассмотрении угрозы 134, был сделан вывод о том, что, исходя из описания предоставленного ФСТЭК России, угроза имеет организационные меры, поэтому она не рассматривается. Угроза 40 относится к организационным мерам, так как угроза подразумевает возможность отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства

стран, резиденты которых участвуют в оказании облачных услуг. Поэтому угроза 40 не рассматривается. Так же угроза 52 относится к организационным мерам, так как по представленному описанию ФСТЭК России, данная угроза возможна в случае несовместимости стандартных программных интерфейсов обмена данными для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Угрозы 54, 65, 66, 137 и 138 относятся к организационным мерам, так как заключаются в возникновении разногласий между поставщиком и потребителем облачных услуг. Угрозы 56 и 96 заключаются в возможности ошибок при работе специалистов, и недостаточной проработке некоторых аспектов реализации системы или системы безопасности. Угроза 70 также не будет рассматриваться из-за того, что она относится к организационным мерам, так как реализация угрозы возможна при занесении в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. Угрозы 127 и 175 реализуются методами социальной инженерии и вследствие невозможности противопоставления им технических средств защиты не рассматриваются. Угроза 141 относится к организационным мерам, так из описания ФСТЭК России, следует, что угроза возникает из-за трудно решаемых проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Поэтому угроза 141 не будет рассматриваться.

В результате распределения угроз информационной безопасности составлена таблица 3.2, в которой отражается классификация угроз информационной безопасности из банка данных угроз ФСТЭК России относительно объекта воздействия. Так как банк данных определяет угрозы конфиденциальности, целостности и доступности для информации, возникают трудности при выделении среди них угроз информационной системе и системе защиты. Угрозы относились к классу угроз системе в случае однозначного обозначения в описании угрозы, что она нарушает какое-либо из свойств

системы. Угрозы, в описании которых значилось нарушение свойств информации вследствие получения доступа к системе считались угрозами информации. В итоге было выделено 68 угроз безопасности информационной системы, с этими угрозами была продолжена дальнейшая работа.

Таблица 3.2 – Классификация угроз информационной безопасности по объекту воздействия

Информация	Информационная система	Система защиты информации
13, 14, 15, 16, 17, 21, 22, 29, 34, 35, 38, 39, 43, 44, 47, 50, 51, 57, 59, 60, 63, 64, 67, 68, 75, 77, 80, 81, 82, 84, 85, 87, 88, 91, 93, 97, 101, 105, 106, 110, 113, 115, 116, 117, 118, 119, 120, 121, 122, 124, 130, 135, 136, 140, 142, 143, 147, 148, 149, 152, 153, 155, 156, 161, 163, 166, 175, 179, 192, 199, 200, 201, 203, 205, 209	1, 2, 5, 9, 10, 11, 12, 18, 20, 23, 24, 25, 26, 32, 36, 37, 45, 48, 49, 53, 55, 58, 62, 69, 73, 74, 78, 79, 83, 89, 90, 92, 94, 95, 104, 107, 108, 111, 112, 114, 125, 129, 131, 132, 133, 145, 146, 150, 151, 154, 160, 164, 165, 171, 174, 178, 180, 182, 184, 188, 190, 191, 198, 200, 201, 202, 206, 207, 208	3, 4, 6, 7, 8, 19, 27, 28, 30, 31, 33, 41, 42, 46, 61, 71, 72, 86, 98, 99, 100, 102, 103, 109, 123, 126, 128, 139, 144, 157, 158, 159, 162, 167, 168, 169, 170, 172, 173, 177, 181, 183, 185, 186, 187, 189, 193, 194, 195, 196, 197, 204

Угрозы системе, представленные в таблице 3.2, были разделены на угрозы целостности и конфиденциальности. Как уже было обозначено ранее в главе 2, свойство доступности рассматривается только применительно к информации, соответственно угрозы, нарушающие доступность, также относятся к угрозам информации. Таким образом, направленные на систему угрозы, представленные в таблице 3.3, делятся только на 2 группы – угрозы целостности и конфиденциальности.

Далее приведено сопоставление выделенных из [23] угроз конфиденциальности и целостности системы угрозам, обозначенным в главе 2 настоящей работы. При этом, из перечня угроз не удалялись угрозы, направленные на аппаратную часть информационных систем, а также угрозы, не относящиеся к компьютерным сетям. Поэтому для корректности при

сравнении угрозы не делились по уровням (ПО, ОС, ЛВС), а рассматривались как классы угроз информационной системе.

Таблица 3.3 – Классификация угроз безопасности системы по нарушаемому свойству

Угрозы конфиденциальности системы	Угрозы целостности системы
2, 36, 37, 55, 74, 104, 132, 133, 146, 151, 174, 184, 207	1, 5, 9, 10, 11, 12, 18, 20, 23, 24, 25, 26, 32, 45, 48, 49, 53, 58, 62, 69, 73, 78, 79, 83, 89, 90, 92, 94, 95, 107, 108, 111, 112, 114, 125, 129, 131, 145, 150, 154, 160, 164, 165, 171, 178, 180, 182, 188, 190, 191, 198, 202, 206, 208

Для сопоставления используется следующий перечень:

— K_{s1X} – угрозы разглашения (утечки) информации о имени элемента (вершины);

— K_{s1E} – угрозы разглашения (утечки) информации о имени связи (ребра);

— K_{s2X} – угрозы разглашения (утечки) информации о настройках (атрибутах) элементов (вершин);

— K_{s2E} – угрозы разглашения (утечки) информации о настройках (атрибутах) связей (ребер);

— C_{s1X} – угрозы подмены элемента (вершины);

— C_{s1E} – угрозы подмены связи (ребра);

— C_{s2X} – угрозы удаления элемента (вершины);

— C_{s2E} – угрозы удаления связи (ребра);

— C_{s3X} – угрозы добавления элемента (вершины);

— C_{s3E} – угрозы добавления связи (ребра);

— C_{s4X} – угрозы изменения настроек (атрибутов) элемента (вершины);

— C_{s4E} – угрозы изменения настроек (атрибутов) связи (ребра).

Для сравнения результатов настоящей работы с использующимся специалистами по защите информации на практики банком данных угроз

ФСТЭК России составлена таблица 3.4. Необходимо отметить, что из-за отсутствия в банке данных угроз системности возникли сложности в однозначном сопоставлении угроз. Для разрешения этой проблемы было решено при сравнении обозначать однозначное соответствие угроз, хотя на практике по описанию некоторых угроз из банка данных им будут соответствовать несколько угроз из авторской модели.

Таблица 3.4 – Сопоставление банка данных угроз ФСТЭК России с классами угроз из авторской модели

БДУ	Авторская модель	БДУ	Авторская модель	БДУ	Авторская модель
Угрозы конфиденциальности					
2	K_{s1X}	104	K_{s1E}	174	K_{s2X}
36	K_{s2X}	132	K_{s2X}	184	K_{s2X}
37	K_{s2X}	133	K_{s2X}	207	K_{s2X}
55	K_{s2X}	146	K_{s2X}		
74	K_{s2X}	151	K_{s2X}		
Угрозы целостности					
1	C_{s3X}	62	C_{s1E}	131	C_{s1X}
5	C_{s3X}	69	C_{s4E}	145	C_{s3X}
9	C_{s1X}	73	C_{s4X}	150	C_{s4X}
10	C_{s3X}	78	C_{s4X}	154	C_{s1X}
11	C_{s1X}	79	C_{s4X}	160	C_{s2X}
12	C_{s4X}	83	C_{s3X}	164	C_{s2X}
18	C_{s1X}	89	C_{s4X}	165	C_{s1X}
20	C_{s3X}	90	C_{s3X}	171	C_{s3X}
23	C_{s1X}	92	C_{s3E}	178	C_{s3X}
24	C_{s4X}	94	C_{s4X}	180	C_{s2X}
25	C_{s4X}	95	C_{s4X}	182	C_{s2X}
26	C_{s4E}	107	C_{s2E}	188	C_{s1X}
32	C_{s1X}	108	C_{s4X}	190	C_{s3X}
45	C_{s4X}	111	C_{s3E}	191	C_{s1X}
48	C_{s4X}	112	C_{s4X}	198	C_{s4X}

Окончание таблицы 3.4 – Сопоставление банка данных угроз ФСТЭК России с классами угроз из авторской модели

БДУ	Авторская модель	БДУ	Авторская модель	БДУ	Авторская модель
Угрозы целостности					
49	C_{s4X}	114	C_{s4X}	202	C_{s3X}
53	C_{s4X}	125	C_{s3X}	206	C_{s4X}
58	C_{s3X}	129	C_{s1X}	208	C_{s3X}

Таким образом, всем угрозам, которые согласно описанию из [23] удалось определить как угрозы информационной системе, были поставлены в соответствие классы угроз, представленные в авторской модели угроз.

Распределение угроз из [23] по классам угроз авторской модели получилось следующим:

— K_{s1X} – угрозы разглашения (утечки) информации о имени элемента (вершины): 2;

— K_{s1E} – угрозы разглашения (утечки) информации о имени связи (ребра): 104;

— K_{s2X} – угрозы разглашения (утечки) информации о настройках (атрибутах) элементов (вершин): 36, 37, 55, 132, 133, 146, 151, 174, 184, 207;

— K_{s2E} – угрозы разглашения (утечки) информации о настройках (атрибутах) связей (ребер): 104;

— C_{s1X} – угрозы подмены элемента (вершины): 9, 11, 18, 23, 32, 129, 131, 154, 165, 188, 191;

— C_{s1E} – угрозы подмены связи (ребра): 62;

— C_{s2X} – угрозы удаления элемента (вершины): 160, 164, 180, 182;

— C_{s2E} – угрозы удаления связи (ребра): 107;

— C_{s3X} – угрозы добавления элемента (вершины): 1, 5, 10, 20, 58, 83, 90, 125, 145, 171, 178, 190, 202, 208;

— C_{s3E} – угрозы добавления связи (ребра): 92, 111;

— C_{s4X} – угрозы изменения настроек (атрибутов) элемента (вершины): 12, 24, 25, 45, 48, 49, 53, 73, 78, 79, 89, 94, 95, 108, 112, 114, 150, 198, 206;

— C_{s4E} – угрозы изменения настроек (атрибутов) связи (ребра): 26, 69.

Необходимо заметить, в данном случае угрозам из банка данных в соответствие ставились классы угроз без разделения их по уровням инфраструктуры компьютерной сети: уровень подсетей, уровень ОС и уровень ПО. Рассмотрим распределение угроз при разделении класса угроз авторской модели на уровни. Показательным в данном случае будет разделение классов, к которым было отнесено наименьшее количество угроз из банка данных ФСТЭК России.

Так, при разделении K_{s1X} угроза 2 «Угроза агрегирования данных, передаваемых в грид-системе» согласно ее описанию, а именно «заключается нув возможности . . . выявления задействованных в её обработке узлов . . .» будет отнесена к угрозам на уровне операционных систем. Так как данная угроза оказалось единственной отнесенной к классу K_{s1X}, то получаем, что в [23] не учтены угрозы утечки информации о программном обеспечении и подсетях.

В качестве примера для угроз целостности возьмем C_{s1E}, угроза 62 «Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера» будет отнесена к угрозам на уровне программного обеспечения. Так как это единственная угроза, которую можно отнести к данному классу, получится что в [23] не учтены угрозы подмены связей между операционными системами и подсетями.

Полное сравнение с разделением угроз по уровням представлено в таблице 3.5.

Таблица 3.5 – Сопоставление угроз из банка данных угроз ФСТЭК России с типами угроз авторской модели угроз

Банк данных угроз ФСТЭК России	Уровни программного обеспечения компьютерной сети		
	Уровень ПО	Уровень ОС	Уровень ЛВС
K_{s1X} – угроза разглашения (утечки) информации о имени элемента			
2		+	
K_{s1E} – угрозы разглашения (утечки) информации о имени связи			
104		+	+
K_{s2X} – угрозы разглашения (утечки) информации о настройках элементов			
36	+	+	
37	+	+	+
55		+	+
132	+	+	+
133		+	
146	+	+	+
151	+		+
174	+		+
184	+	+	
207		+	
K_{s2E} – угрозы разглашения (утечки) информации о настройках связей			
104		+	+
C_{s1X} – угрозы подмены элемента			
9		+	
11		+	
18		+	
23	+	+	
32		+	
129		+	
131	+	+	+
154		+	
165	+	+	+
188	+		
191	+		

Продолжение таблицы 3.5 – Сопоставление угроз из банка данных угроз ФСТЭК России с типами угроз авторской модели угроз

Банк данных угроз ФСТЭК России	Уровни программного обеспечения компьютерной сети		
	Уровень ПО	Уровень ОС	Уровень ЛВС
C_{s1E} – угрозы подмены связи			
62	+		
C_{s2X} – угрозы удаления элемента			
160		+	+
164	+	+	+
180	+	+	+
182	+	+	+
C_{s2E} – угрозы удаления связи			
107		+	
C_{s3X} – угрозы добавления элемента			
1	+		
5		+	
10	+	+	
20	+		
58		+	
83	+	+	
90	+		
125		+	
145	+		
171	+		
178	+	+	
190	+		
202	+		
208	+	+	
C_{s3E} – угрозы добавления связи			
92	+	+	
111		+	

Окончание таблицы 3.5 – Сопоставление угроз из банка данных угроз ФСТЭК России с типами угроз авторской модели угроз

Банк данных угроз ФСТЭК России	Уровни программного обеспечения компьютерной сети		
	Уровень ПО	Уровень ОС	Уровень ЛВС
C_{s4X} – угрозы изменения настроек элемента			
12	+	+	+
24		+	
25	+	+	+
45		+	
48		+	+
49	+	+	+
53		+	
73			+
78	+	+	
79		+	
89		+	
94	+	+	+
95	+	+	+
108		+	
112	+	+	
114	+	+	+
150		+	
198	+		
206	+	+	
C_{s4E} – угрозы изменения настроек связи			
26	+		
69	+	+	

При разделении 12 классов угроз авторской модели на угрозы по уровням инфраструктуры компьютерной сети получается 36 типов угроз. По итогам сопоставления угроз их банка данных ФСТЭК России, представленного в таблице 3.5, получился следующий результат сравнения: из 36 типов угроз в банке представлены 25, т.е. при предложенной

классификации угроз появляется 11 неучтенных ранее в нормативных документах типов угроз.

Неучтенными оказались следующие типы угроз на уровне программного обеспечения:

— угрозы разглашения (утечки) информации о имени элемента;

— угрозы разглашения (утечки) информации о имени связи;

— угрозы разглашения (утечки) информации о настройках связей;

— угрозы удаления связи.

На уровне операционных систем:

— угрозы подмены связи.

На уровне подсетей:

— угроза разглашения (утечки) информации о имени элемента;

— угрозы подмены связи;

— угрозы добавления элемента;

— угрозы добавления связи;

— угрозы изменения настроек связи.

Может вызывать сомнение актуальность некоторых из представленных выше типов угроз, так, например, угроза несанкционированного добавления в рассматриваемую систему целой подсети как отдельного элемента видится маловероятной. Но, как оговорено ранее в главе 1, вопросы актуальности выходят за рамки данной работы и должны рассматриваться на следующем после идентификации угроз этапе обеспечения информационной безопасности информационных систем – на этапе оценки рисков.

При этом эти типы угроз не являются принципиально новыми и обнаруженными впервые, но из-за того, что они в явном виде не учтены в нормативных документах, то при обеспечении безопасности компьютерных сетей организации у специалистов по защите информации могут возникнуть сложности при идентификации этих угроз и, соответственно, при учете этих угроз в создании системы защиты информации.

Таким образом, предложенный в главе 2 подход к построению моделей угроз позволяет специалистам по защите информации учесть при построении системы защиты информации на 11 типов угроз информационной безопасности системы больше, чем использование банка данных угроз ФСТЭК России.

В результате можно судить о полноте разработанной модели угроз относительно банка данных угроз ФСТЭК России и документов [55], [56], [57].

3.2 Модель угроз целостности автоматизированной системы коммерческого учета энергоресурсов

Методика составления перечня угроз информационной безопасности компьютерных сетей, описанная в настоящей работе, была применена для составления перечня угроз разрабатываемой автоматизированной системы коммерческого учета энергоресурсов (АСКУЭ).

Хотя АСКУЭ и не является компьютерной сетью при первом приближении [87], модели, разработанные в ходе работы могут быть применены практически к любой информационной системе, в которой осуществляется передача информации [88].

Актуальность составления перечня угроз АСКУЭ заключается в том, что изначально подобные системы не имели надежных механизмов защиты, так как использовались на промышленных объектах [89, 90] и не использовались для коммерческого учета ресурсов [91]. Отсутствие механизмов защиты, требуемых для безопасной передачи информации через каналы связи общего пользования, затрудняло внедрение промышленных систем в сферу жилищно-коммунальных услуг. Такое внедрение потребовало серьезной переработки системы, в том числе и подсистемы защиты информации [92, 93].

Общую структуру АСКУЭ можно описать как множество трех основных типов объектов:

- устройство учета энергоресурсов (УУЭ);
- устройство сбора и передачи данных (УСПД);
- центральный сервер (ЦС).

Структура системы представлена на рисунке 3.1. Под пользователем понимается не оператор или клиент, а устройство, при помощи которого происходит взаимодействие. Множество пользователей также можно разбить на подмножества разных типов с разными правами. Т.е. как часть системы могут рассматриваться устройства пользователей, работающих с АСКУЭ, применяемые для настройки и обслуживания системы.

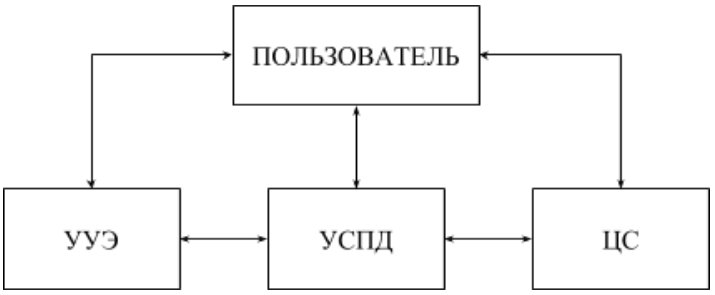


Рисунок 3.1 – Представление системы

Все устройства, составляющие систему, можно расположить в виде древовидной структуры, корнем которой будет центральный сервер. С ЦС работает несколько УСПД, к каждому УСПД в свою очередь подключено некоторое количество УУЭ. Очевидно, что чем дальше от корневого сервера находится устройство, тем более низкоуровневым оно является.

Взаимодействие между всеми компонентами системы может быть описано с помощью терминов модели OSI.

Далее, на рисунке 3.2 представлена структура системы на настоящий момент времени.

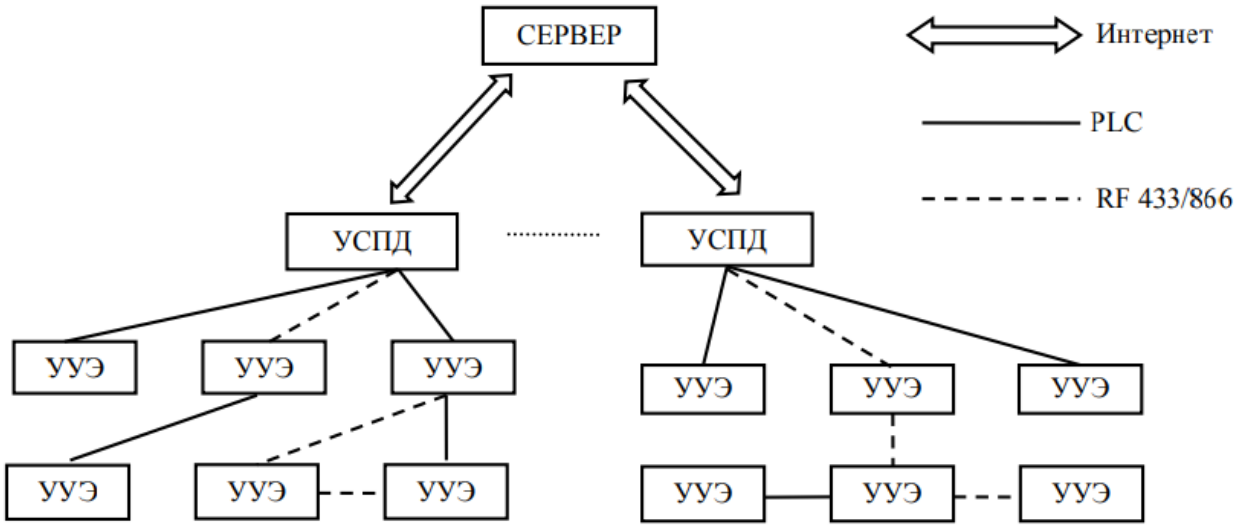


Рисунок 3.2 – Актуальная структура АСКУЭ

Ключевое отличие текущего состояния структуры системы от состояния на момент применения к ней методики заключается в наличии связей между устройствами учета энергоресурсов.

При применении методики рассматривались не уровни системы, обозначенные в главе 2 настоящей работы, а программный и аппаратный уровни системы. К программному уровню АСКУЭ были отнесены операционные системы и программное обеспечение устройств, протоколы высокого уровня, программы конфигурирования устройств. К аппаратному уровню системы отнесены все устройства системы, линии связи и протоколы низкого уровня.

Согласно [94, 95, 96] двухуровневую систему G можно представить как совокупность множества устройств X_1, в которое входят ЦС, а также все УСПД и УУЭ. Для простейшей структуры из трех устройств это множество будет выглядеть следующим образом:

$$X_2 = \{"ЦС"_2^1, "УСПД"_2^2, "УУЭ"_2^3\}.$$

Другие множества, составляющие систему – множество программного обеспечения устройств X_1, множество связей на аппаратном уровне E_2 и множества связей на программном уровне E_1.

Расположение программного обеспечения на аппаратных компонентов будет обозначаться функциями вида:

$$f_1^1 : g_1^1(\text{"ПО ЦС"}_1^1) \rightarrow \text{"ЦС"}_2^1.$$

Соответственно вся система будет представлена следующим образом:

$$G = (X_1, X_2, E_1, E_2).$$

Также у каждого элемента системы есть характеризующие его параметры, представляемые атрибутами метаграфа. Графическое представление простейшей структуры АСКУЭ, описанной в понятиях авторской модели, представлено на рисунке 3.3.

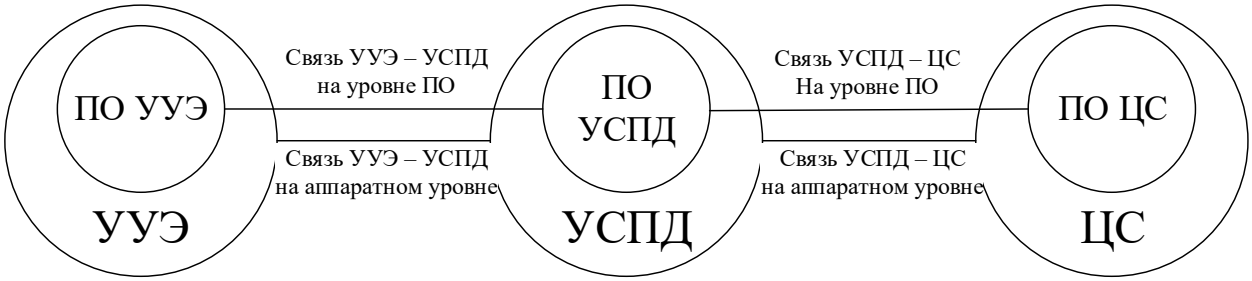


Рисунок 3.3 – Графическое представление модели АСКУЭ

После описания системы с помощью разработанной модели было осуществлено составление перечня угроз. Под угрозами безопасности системы понимаются угрозы несанкционированного изменения её состояния или структуры [97, 98]. Данную группу угроз можно разделить на две подгруппы: угрозы безопасности непосредственно системе и угрозы безопасности средствам защиты информации системы [99, 100]. Так как в рассматриваемой АСКУЭ на этапе ее рассмотрения отсутствовали механизмы защиты информации, то необходимость была только в определении угроз информационной безопасности системы.

Угрозам конфиденциальности системы являются угрозы, связанные со сбором информации о системе. Это может быть список устройств, версии программного обеспечения, данные для аутентификации, политики

разграничения доступа, сетевые адреса, протоколы взаимодействия и т.д. Но, хотя в итоговой модели угроз АСКУЭ были представлены угрозы конфиденциальности, в рамках данной работы рассмотрены только угрозы целостности

Согласно разработанной модели угроз к угрозам целостности информационной системы относятся угрозы:

— подмены объекта;
— подмены канала связи;
— удаления объекта;
— уничтожения канала связи;
— добавления объекта;
— создания канала связи;
— изменения параметров связи или объекта;

Данный перечень необходимо рассмотреть для каждой связи и объекта, представленных на рисунке 3.3.

Возможные способы реализации каждой угрозы из представленного перечня кратко расписаны для аппаратного уровня в таблице 3.6 и для программного уровня в таблице 3.7.

Всего с использованием разработанных моделей и методики было выделено 70 угроз целостности АСКУЭ на программном и аппаратном уровне [101]. До применения авторской методики для рассматриваемой системы экспертами с использованием моделей угроз [55], [30], [102] и [103] было обозначено 59 угроз информационной безопасности системы. Угрозы информации применительно к данной работе не рассматриваются, поэтому сравнения с ними не производилось.

Таблица 3.6 – Угрозы целостности системы на аппаратном уровне

Элементы системы	Добавление объекта	Удаление объекта	Подмена объекта	Создание канала связи	Уничтожение канала связи	Подмена канала связи	Изменение параметр.
Связь УУЭ - УСПД	Несанкц. добавление УУЭ или УСПД	Несанкц. удаление УУЭ или УСПД	Подмена УУЭ или УСПД	Использ. несанкц. линии связи	Повреждение линии связи, помехи на линии связи	Использ. несанкц. линии связи вместо санкционир.	Изменение MAC-адреса УУЭ или УСПД
Связь УСПД - ЦС	Несанкц. добавление УСПД или ЦС	Несанкц. удаление УСПД или ЦС	Подмена УСПД или ЦС	Использ. несанкц. линии связи	Повреждение линии связи, помехи на линии связи	Использ. несанкц. линии связи вместо санкционир.	Изменение MAC-адреса УУЭ или УСПД
УУЭ	Подключение несанкц. оборудования	Несанкц. удаление компонента УУЭ	Несанкц. замена компонента УУЭ	Создание несанкц. связей между комп. УУЭ	Уничтожение связей между комп. УУЭ	Изменение связей между комп. УУЭ	Несанкц. изменение крит. парам. УУЭ
УСПД	Подключение несанкц. оборудования	Несанкц. удаление компонента УСПД	Несанкц. замена компонента УСПД	Создание несанкц. связей между комп. УСПД	Уничтожение связей между комп. УСПД	Изменение связей между комп. УСПД	Несанкц. изменение крит. парам. УСПД
ЦС	Подключение несанкц. оборудования	Несанкц. удаление компонента ЦС	Несанкц. замена компонента ЦС	Создание несанкц. связей между комп. ЦС	Уничтожение связей между комп. ЦС	Изменение связей между комп. ЦС	Несанкц. изменение крит. парам. ЦС

Таблица 3.7 – Угрозы целостности системы на программном уровне

Элементы системы	Добавление объекта	Удаление объекта	Подмена объекта	Создание канала связи	Уничтожение канала связи	Подмена канала связи	Изменение параметр.
Связь УУЭ - УСПД	Несанкц. добавление УУЭ или УСПД (в логическую сеть)	Несанкц. удаление УУЭ или УСПД (на прогр. уровне)	Подмена УУЭ или УСПД	Использ. несанкц. драйвера или протокола	DoS-атака, удаление драйвера	Использ. несанкц. драйвера или протокола	Изменение IP-адреса УУЭ или УСПД
Связь УСПД - ЦС	Несанкц. добавление УСПД или ЦС (в логическую сеть)	Несанкц. удаление УСПД или ЦС (на прогр. уровне)	Подмена УСПД или ЦС	Использ. несанкц. драйвера или протокола	DoS-атака, удаление драйвера	Использ. несанкц. драйвера или протокола	Изменение IP-адреса УУЭ или УСПД
УУЭ	Внедрение несанкц. ПО	Несанкц. удаление ПО	Несанкц. замена ПО	Создание несанкц. связей между ПО	Уничтожение связей между ПО	Изменение связей между ПО	Несанкц. изменение крит. парам. УУЭ
УСПД	Внедрение несанкц. ПО	Несанкц. удаление ПО	Несанкц. замена ПО	Создание несанкц. связей между ПО	Уничтожение связей между ПО	Изменение связей между ПО	Несанкц. изменение крит. парам. УСПД
ЦС	Внедрение несанкц. ПО	Несанкц. удаление ПО	Несанкц. замена ПО	Создание несанкц. связей между ПО	Уничтожение связей между ПО	Изменение связей между ПО	Несанкц. изменение крит. парам. ЦС

В таблицах 3.6 и 3.7 выделено 11 угроз, которые не были учтены экспертами, в этот перечень вошло 7 угроз целостности системы на аппаратном уровне и 4 угрозы целостности системы на программном уровне:

1. несанкционированное добавление УУЭ или УСПД в систему;
2. несанкционированное добавление УСПД или ЦС в систему;

3. использование несанкционированной аппаратной линии связи между УУЭ и УСПД;
4. использование несанкционированной аппаратной линии связи между УСПД и ЦС;
5. создание несанкционированных аппаратных связей между компонентами УУЭ;
6. создание несанкционированных аппаратных связей между комп. УСПД;
7. создание несанкционированных аппаратных связей между комп. ЦС;
8. подмена УУЭ или УСПД (в логической сети);
9. подмена УСПД или ЦС (в логической сети);
10. использование несанкционированного драйвера или протокола для связи между УУЭ и УСПД;
11. использование несанкционированного драйвера или протокола для связи между УСПД и ЦС.

Актуальность угроз в рамках данной работы не рассматривается, однако необходимо заметить, что получение хотя бы одной дополнительной угрозы, для которой необходимо вводить механизмы защиты, уже является достаточным основанием для рассмотрения расширенного перечня угроз.

Применение авторской методики позволило предъявить требования к комплексу механизмов защиты [104, 105, 106] от дополнительно обнаруженных угроз, и заложить эти механизмы в структуру системы еще на этапе проектирования. Процесс разработки механизмов защиты для системы представлен в работах [107] и [108].

3.3 Выводы по главе

В данной главе представлено сравнение разработанной автором модели с перечнем угроз из банка данных угроз ФСТЭК России, а также в качестве

апробации разработанной методики и моделей рассмотрена модель угроз АСКУЭ.

Установлено, что предложенный в главе 2 подход к построению моделей угроз позволяет специалистам по защите информации учесть при построении системы защиты информации на 11 типов угроз информационной безопасности системы больше, чем использование банка данных угроз ФСТЭК России. Всего согласно авторской классификации выделено 36 типов угроз конфиденциальности и целостности системы, в банке данных угроз ФСЭК РФ представлено 25 из них.

В ходе внедрения результатов работы в деятельность АО «ПКК Миландр» при разработке автоматизированной системы коммерческого учета энергоресурсов был составлен перечень из 70 угроз целостности системы. Угрозы рассматривались на программном и аппаратном уровнях для трех основных типов элементов системы. Полученный с использованием авторской методики и моделей перечень оказался на 18% больше составленного экспертами заказчика ранее (59 угроз целостности системы). Это позволило учесть при проектировании системы защиты необходимость дополнительных механизмов защиты. Также использование авторской модели информационной системы позволило учесть при построении структуры АСКУЭ характеристики элементов и взаимосвязи между ними.

Заключение

В результате выполненного диссертационного исследования в области разработки моделей классификации угроз нарушения информационной безопасности была решена научно-техническая задача увеличения полноты перечня угроз информационной безопасности компьютерных сетей. Поставленная в начале исследования цель достигнута. Получены следующие основные результаты:

1. выполнен анализ текущего состояния предметной области: моделей компьютерных сетей, использующихся при идентификации угроз, а также подходов к построению моделей угроз компьютерных сетей. Были выделены их недостатки, требующие устранения;
2. на основе атрибутивных метаграфов разработана модель компьютерной сети, позволяющая описать компоненты программного обеспечения компьютерных сетей (прикладное, системное и сетевое программное обеспечение) и все возможные связи между ними (сетевые протоколы, драйверы, и т.п.);
3. на основе элементарных операций над метаграфами разработана модель угроз компьютерной сети, которая позволяет составлять полные перечни угроз целостности и конфиденциальности компьютерных сетей;
4. с использованием созданных моделей разработана методика составления перечня угроз информационной безопасности компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами и позволяющая увеличить количество идентифицируемых угроз при формировании моделей угроз компьютерных сетей;
5. методика и модели были апробированы на практике в процессе разработки автоматизированной системы коммерческого учета энергоресурсов, в результате чего было определено на 18% угроз целостности системы больше, чем до применения авторской методики.

Факт успешного внедрения методики составления перечня угроз информационной безопасности компьютерных сетей в деятельность АО «ПКК Миландр» в процессе разработки автоматизированной системы коммерческого учета энергоресурсов подтверждается актом внедрения, который представлен в Приложении А.

Также результаты диссертационного исследования используются в учебном процессе ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», что подтверждается актом внедрения, представленным в приложении А.

Список использованной литературы

1 Анализируем защищенность корпоративных IT-систем [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf, свободный (дата обращения: 01.09.2018 г).

2 Петренко С.А. Модель киберугроз по аналитике инноваций DARPA // Труды СПИИРАН. 2015. Вып. 39. С. 26-41.

3 2018 Internet Security Threat Report [Электронный ресурс]. – Режим доступа: https://www.symantec.com/security-center/threat-report, свободный (дата обращения: 01.09.2018 г).

4 Коробейников А.Г., Гришенцев А.Ю., Дикий Д.И., Артемьева В.Д., Сидоркина И.Г. Информационная безопасность в системе «Интернет вещей» // Вестник Чувашского университета. – 2018. – № 1. – С. 117–128.

5 Mahmoud Ammar, Giovanni Russello, Bruno Crispo. Internet of Things: A survey on the security of IoT frameworks // Journal of Information Security and Applications. Volume 38, 2018, Pages 8-27.

6 Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1-2 (25). – С. 34 –39.

7 Лысенко Е.И. Принципы обеспечения безопасности корпоративной сети. / Е.И. Лысенко, А.С. Барабошин, С.С. Черненко, В.Н. Нескромный // Современные проблемы науки и образования. – 2014. – № 4. – С. 216.

8 Суходол К.Ю. Технологии защиты информации в компьютерных сетях небольших организаций. // Теория и практика современной науки. – 2017. – № 1 (19). – С. 899–902.

9 Eran Toch. The Privacy Implications of Cyber Security Systems:A Technological Survey / Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, Bruno Lepri // ACM Computing Surveys (CSUR), Volume 51, Issue 2, 2018, Article 36.

10 E. B. Dudin, Yu. G. Smetanin. Problems and prospects of modeling computer information networks. A review [Электронный ресурс]. – Режим доступа: https://link.springer.com/article/10.3103/S0005105510060038, свободный (дата обращения: 01.05.2017 г.).

11 Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие // Ю. Н. Загинайлов. – М. Берлин: Директ-Медиа, 2015. – 253с.

12 Бова В.В. Концептуальная модель представления знаний при построении интеллектуальных информационных систем // Известия ЮФУ. Технические науки. – 2014. – № 7 (156). – С. 109–117.

13 Коломейцева А.Д., Загинайлов Ю.Н. Разработка концептуальной модели системы защиты государственной информационной системы // Анализ современных тенденций развития науки: сборник статей Международной научно - практической конференции, Волгоград, 5 июля 2017 г. – Уфа: АЭТЕРНА. В 2 частях. – Ч.1 – С. 41–44.

14 Симонова М.В., Атрощенко В.А. Особенности построения различных алгоритмов и функциональных моделей в системе мониторинга умного дома // VII международная научно-практическая конференция молодых ученых, посвященная 56-й годовщине полета Ю.А. Гагарина в космос: Сборник научных статей, Краснодар, 12-13 апреля 2017 г. - Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг". – С. 420–424.

15 Shangytbayeva G. A., Karpinski M. P., Akhmetov B. S., Yerekesheva M. M. Zhekambayeva M. N. Mathematical Model of System of Protection of Computer Networks against Attacks DOS/DDOS [Электронный ресурс]. – Режим доступа: https://doi.org/10.5539/mas.v9n8p106, свободный (дата обращения: 01.05.2017 г.).

16 Петрова Е.В. Логическая модель реализации угрозы информационной безопасности на отдельном элементе компьютерной сети // Охрана, безопасность, связь. – 2017. – № 1-2. – С. 216–220.

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

18 BugTraq.Ru: Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: https://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 01.05.2017 г.).

19 Королёва О.Ю. Модель и метод оценки эффективности системы обеспечения информационной безопасности корпоративного хранилища данных кредитных организаций Российской Федерации // Автореферат диссертации на соискание ученой степени кандидата технических наук [Электронный ресурс]. – Режим доступа: http://aspirantura.ifmo.ru/file/other/ktyaZl1TkI.pdf, свободный (дата обращения: 07.09.2018 г.).

20 Методика определения угроз безопасности информации в информационных системах. Проект. ФСТЭК России – 2015. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/812, свободный (дата обращения: 07.09.2018 г.).

21 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200057516, свободный (дата обращения: 07.09.2018 г.).

22 Рекомендации в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности" РС БР ИББС-2.2-2009 (приняты и введены в действие Распоряжением Банка России от 11.11.2009 N Р-1190) [Электронный ресурс]. – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_94789, свободный (дата обращения: 07.09.2018 г.).

23 Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru, свободный (дата обращения: 01.05.2017 г.).

24 ATT&CK Matrix [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/wiki/ATT%26CK_Matrix, свободный (дата обращения: 01.05.2017 г.).

25 Чулков Д.Н. Модель угроз информационно-технических воздействий на информационные объекты – как основа создания комплексной системы обеспечения безопасности / Д.Н. Чулков. – Санкт – Петербург: Наукоемкие технологии, 2016. – С. 82-86

26 Киселев В.В. Модели идентифицируемости признаков распознавания угроз конфиденциальности информационных ресурсов компьютерных систем / В.В. Киселев. – Воронеж: Воронежский государственный технический университет, 2011. – С. 579-582

27 Литовченко И.Н., Зарубин В.С., Савинков А.Ю. К вопросу о моделировании противоправных действий по реализации угроз информационным процессам в автоматизированных системах безопасности / И.Н. Литовченко, В.С. Зарубин, А.Ю. Савинков. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2016. – С. 179-184

28 Гайфулин В.В. Разработка математической модели противодействия информационным угрозам интегрированных систем безопасности: постановка задачи и пути решения / В.В. Гайфулин. – Воронеж: Воронежский государственный технический университет, 2009. – С. 153-154

29 Mouna Jouinia, Latifa Ben Arfa Rabaia, Anis Ben Aissab. Classification of Security Threats in Information Systems. Procedia Computer Science. Volume 32, 2014, Pages 489-496

30 Mouna Jouini, Latifa Ben Arfa - Threat classification: State of art - May 2016 - In book: Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber SecurityPublisher: igi global Editors: Brij Gupta [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art, свободный (дата обращения: 01.05.2017 г.).

31 Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Threat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, [Электронный ресурс]. – Режим доступа: https://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf, свободный (дата обращения: 01.05.2017 г.).

32 Geric S, Hutinski Z. Information system security threats classifications. Journal of Information and Organizational Sciences; 2007. 31: 51. [Электронный ресурс]. – Режим доступа: https://jios.foi.hr/index.php/jios/article/view/29, свободный (дата обращения: 01.05.2017 г.).

33 Нестерук Ф.Г., Нестерук Л.Г. Разработка модели пограничных угроз информационной безопасности // Инновации в науке. – 2017. – № 15(76). – С. 17–21.

34 The STRIDE Threat Model [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20), свободный (дата обращения: 01.05.2017 г.).

35 ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации [Электронный ресурс]. – Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=131456), свободный (дата обращения: 01.05.2017 г.).

36 Газизов Т.Т., Мытник А.А., Бутаков А.Н. Типовая модель угроз безопасности персональных данных для информационных систем

автоматизации учебного процесса / Т.Т. Газизов, А.А. Мытник, А.Н. Бутаков. – Томск: Томский государственный университет управления и радиоэлектроники, 2014. – С. 47-50

37 Душкин А.В., Демченков А.В. Аналитическая модель оценки эффективности обеспечения защиты данных от угроз нарушения целостности в информационных системах / А.В. Душкин, А.В. Демченков. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2015. – С. 87-95

38 Андреев Н.О. Формирование и развитие угроз в информационных системах / Н.О. Андреев. – Москва: Московский финансово-промышленный университет «Синергия», 2006. – С. 87-100

39 Рытов М.Ю., Лавров А.С. Формализация критериев выбора состава средств защиты информационных систем на основе оценки показателей угроз и уязвимостей / М.Ю. Рытов, А.С. Лавров. – Воронеж: Воронежский государственный технический университет, 2012. – С. 109-112

40 Hettiarachchi S., Wickramasinghe S. Study to identify threats to Information Systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security. – [Электронный ресурс]. – Режим доступа: http://www.academia.edu/28512865/Study_to_identify_threats_to_Information_Systems_in_organizations_and_possible_countermeasures_through_policy_decisions_and_awareness_programs_to_ensure_the_information_security

41 Nicho M., Kamoun F. Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems / M. Nicho, F. Kamoun / Communications of the Association for Information Systems. – 2014. – Vol. 35. – 18 p.

42 Samson G.L., Usman M. Securing an Information Systems from Threats: A Critical Review / G.L. Samson, M. Usman / International Journal of Computer Applications Technology and Research. – 2015. – Vol. 4 . – P. 425-434

43 Тулиганова Л.Р., Павлова И.А., Машкина И.В. Разработка моделей объекта защиты и угроз нарушения безопасности в информационной системе, базирующейся на технологии виртуализации / Л.Р. Тулиганова, И.А. Павлова, И.В. Машкина. – Ростов-на-Дону: Южный федеральный университет, 2014. – С. 32-41

44 Приезжая А.Н. Автоматизированное формирование модели угроз безопасности информационной системы / А.Н. Приезжая. – Москва: Российский государственный гуманитарный университет, 2012. – С. 240-257

45 Хвостов В.А., Багаев М.А., Кисляк А.А., Даурцев А.В., Солод Д.В. Формальная модель полного множества реализаций угроз информационной безопасности автоматизированных систем / В.А. Хвостов, М.А. Багаев, А.А. Кисляк, А.В. Даурцев, Д.В. Солод. – Воронеж: Воронежский государственный технический университет, 2011. – С. 32-35

46 Белокуров С.В., Сотников Н.В., Лунев Ю.С. Моделирование информационных угроз и действий по защите информации в интегрированных системах безопасности / С.В. Белокуров, Н.В. Сотников, Ю.С. Лунев. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2017. – С. 137-141

47 Коломиец В.В. Метод получения вербальных показателей защищенности системы / В.В. Коломиец. – Новосибирск: Новосибирский национальный исследовательский государственный университет, 2014. – С. 42-47

48 Макаров О.Ю., Хвостов В.А., Хвостова Н.В. Метод построения формальных моделей реализации угроз информационной безопасности автоматизированных систем / О.Ю. Макаров, В.А. Хвостов, Н.В. Хвостова. – Воронеж: Воронежский государственный технический университет, 2010. – С. 22-24

49 Xuezhong L., Zengliang L. Evaluating Method of Security Threat Based on Attacking-Path Graph Model / L. Xuezhong, L. Zengliang / Computer Science

and Software Engineering, 2008 International Conference on. – 2008. – December 12-14. – P. 1127-1132

50 Шимон Н.С., Кореев М.Ю., Агеев Е.С. Математическая модель угроз безопасности защищенных информационных систем / Н.С. Шимон, М.Ю. Кореев, Е.С. Агеев. – Воронеж: Воронежский государственный технический университет, 2008. – С. 561-564

51 Голубинский А.Н., Алехин И.В. О математических моделях ущербов и рисков возникновения угроз в информационно-технических системах / А.Н. Голубинский, И.В. Алехин. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2016. – С. 109-115

52 Шувалов И.А., Семенчин Е.А. Математическая модель воздействия угроз на информационную систему обработки персональных данных / И.А. Шувалов, Е.А. Семенчин. – Пенза: Издательский Дом «Академия Естествознания», 2013. – С. 529 - 533

53 Алехин И.В., Голубинский А.Н. Модели параметров оценки изменения риска возникновения угроз в информационных и технических системах / И.В. Алехин, А.Н. Голубинский. – Воронеж: ООО «Издательство «Научная книга», 2015. – С. 247-249

54 Варлатая С.К., Шаханова М.В. Математические модели динамики возникновения и реализации угроз информационной безопасности / С.К. Варлатая, М.В. Шаханова. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2012. – С. 7-11

55 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. – Режим доступа: http://fstec.ru/component/attachments/download/289, свободный (дата обращения: 10.09.2017г.).

56 Методические рекомендации по составлению Частной модели угроз безопасности персональных данных учреждений здравоохранения, социальной сферы, труда и занятости. [Электронный ресурс]. – Режим

доступа: http://www.aksimed.ru/download/ center/Model_ugroz_MIS_LPU_2009.pdf, свободный (дата обращения: 12.09.2017г.).

57 ГОСТ Р ИСО/МЭК 27005 – 2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс]. – Режим доступа: http://k504.khai.edu/attachments/article/ 1406/4293804268.pdf, свободный (дата обращения: 14.09.2017г.).

58 Студенческая библиотека онлайн. Средства защиты информации. [Электронный ресурс]. – Режим доступа: http://studbooks.net/2259831/informatika/vedenie, свободный (дата обращения: 20.09.2017г.).

59 Директор информационной службы. Информационная система. [Электронный ресурс]. – Режим доступа: https://www.osp.ru/cio/2002/06/172182, свободный (дата обращения: 21.09.2017г.).

60 Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798, свободный (дата обращения: 21.09.2017 г.).

61 Атаманов Г.А. О корректности понятий "модель угроз" и "модель нарушителя" // Эколого-мелиоративные аспекты рационального природопользования. Материалы Международной научно-практической конференции. – Волгоград: ВолГАУ, 2017. – С. 447–453.

62 Hamid B., Weber D. Engineering secure systems: Models, patterns and empirical validation / B. Hamid, D. Weber / Computers & Security. – 2018. – Vol. 77.

63 Security Development Lifecycle [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/en-us/sdl, свободный (дата обращения: 09.05.2018 г.).

64 Saltzer, H. Saltzer. The Protection of Information in Computer Systems / H. Saltzer Saltzer, Michael D. Schroeder // Proceedings of the IEEE. – USA: IEEE, 1975. – Vol. 63, no. 09. – P. 1278-1308.

65 Parker, Donn B. Fighting Computer Crime: A New Framework for Protecting Information. – N.Y.: John Wiley & Sons, 1998. – 528 p.

66 Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.

67 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электронный ресурс]. – Режим доступа: http://www.internet-law.ru/gosts/gost/271/, свободный (дата обращения: 27.05.2018).

68 NIST Special Publication 800-30 Rev.1, Guide for Conducting Risk Assessments [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, свободный (дата обращения: 21.09.2017г.).

69 Гейда А.С. Моделирование при исследовании технических систем: использование некоторых расширений теории графов // Труды СПИИРАН. – 2011. – №2 (17). – С. 234-245.

70 Попова М.С., Карпов А.П. Применение теории графов при выявлении потенциальных угроз безопасности информации // Проблемы современной науки и образования. – 2016. – №35 (77). – С. 50-52.

71 Астанин С.В., Драгныш Н.В., Жуковская Н.К. Вложенные метаграфы как модели сложных объектов // Электронный научный журнал “Инженерный вестник Дона”. – 2012. – № 4. [Электронный ресурс]. – Режим доступа: http://ivdon.ru/magazine/archive/n4p2y2012/1434, свободный (дата обращения: 01.02.2015).

72 Basu A., Blanning R. Metagraphs and their applications [Электронный ресурс]. – Режим доступа: https://www.springer.com/us/book/9780387372334, свободный (дата обращения: 01.02.2015 г.).

73 Штогринаа Е.С., Кривенко А.С. Метод визуализации метаграфа // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – №3 (91). – С. 124-130.

74 Кручинин С.В. О Некоторых обобщениях графов: мультиграфы, гиперграфы, метаграфы, потоковые и портовые графы, протографы, архиграфы // Вопросы науки. – 2017. - №3. – С. 48-67.

75 Кручинин С.В. Протографы и архиграфы как обобщение графов // Научно-исследовательские публикации. – 2017. - №3. – С. 23-33.

76 Казарин О.В. Безопасность программного обеспечения компьютерных систем. [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/articles/kazarin/, свободный (дата обращения: 21.09.2017 г.).

77 Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУРа. – 2013. – №2 (28). – С. 107-111.

78 Атаки на уровне приложений, или Новый вызов для МСЭ [Электронный ресурс]. – Режим доступа: http://www.iksmedia.ru/articles/26259-Ataki-na-urovne-prilozhenij-ili-Nov.html, свободный (дата обращения: 01.02.2015 г.).

79 Уровни эталонной модели OSI [Электронный ресурс]. – Режим доступа: http://just-networks.ru/osnovy-setej-peredachi-dannykh/model-osi, свободный (дата обращения: 01.02.2015 г.).

80 Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 343 с.

81 Берж К. Теория графов и её применения. Пер. с фр. – М.: Иностранная литература, 1962. – 319 с.

82 Ануфриенко С.А. Введение в теорию множеств и комбинаторику: учебное пособие/ С.А. Ануфриенко – Екб., 1998. – 62 с.

83 Новохрестов А.К. Оценка качества защищенности сетей / А.К. Новохрестов // Научная сессия ТУСУР-2014: Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. – Томск: В-Спектр, 2014. - В 5 частях. – Ч. 3. – С. 208-210.

84 Конев А.А. Методика оценки качества защищённости компьютерных сетей / А.А. Конев, А.К. Новохрестов // Проблемы информационной безопасности государства, общества и личности: Материалы XV всероссийской научно-практической конференции: Доклады VI Пленума СибРОУМО по образованию в области информационной безопасности и XV конференции – Томск: В-Спектр, 2014. – С. 182-187.

85 Новохрестов А.К. Оценка качества защищенности компьютерных сетей / А.К. Новохрестов, А.А. Конев // Динамика систем, механизмов и машин: Материалы XI Международной научно-технической конференции. – Омск: Издательство ОмГТУ, 2014. – №4. – С. 85-87

86 Новохрестов, А.К. Использование методов и инструментальных средств управления рисками при оценке защищенности компьютерных сетей / А.К. Новохрестов // Научная сессия ТУСУР-2015: Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых (Томск, 13–15 мая 2015г.). – В 5 ч. – Ч. 4. – Томск: В-Спектр, 2015. – С. 172-173.

87 Сапронов А.А. Требования, критерий оптимальности и функция цели АСКУЭ для бытового и мелкомоторного сектора электрических сетей напряжением 0,4 кВ // Энергосбережение и водоподготовка. – 2006. – № 6. – С. 57–58.

88 Новохрестов А.К. Обзор подходов к построению моделей информационной системы и угроз ее безопасности / А.К. Новохрестов, А.А. Конев // Актуальные проблемы обеспечения информационной безопасности: Труды Межвузовской научно-практической конференции. – Самара: Инсома-Пресс, 2017. – С. 151-155.

89 Казачков В.С., Когут С.А. Учет энергоресурсов на предприятиях железнодорожного транспорта на основе АСКУЭ // Известия Транссиба. – 2010. – №3 (3). – С. 59-65.

90 Киселев А.Н., Сеньков И.А. Опыт внедрения АСКУЭ на предприятиях тверской области. // Тверской государственный технический университет

- опорный региональный вуз в подготовке инженерных кадров. Сборник тезисов докладов внутривузовской научно-практической конференции преподавателей и сотрудников Тверского государственного технического университета. – Тверь: ТГТУ, 2015. – С. 147-149.

91 Шелупанов А. А. Актуальные направления развития методов и средств защиты информации / А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д.С. Никифоров // Доклады ТУСУРа. – 2017. – №3. – Т.20. – С. 11-24.

92 Мелких А.А. Исследование проблемы информационной безопасности АСКУЭ / А.А. Мелких, С.Ю. Микова, В.С. Оладько // Universum: Технические науки. – 2016. – №6 (27). – С. 4-16.

93 Мелких А.А. Основные угрозы информационной безопасности в АСКУЭ / А.А. Мелких, С.Ю. Микова, М.А. Нестеренко, А.А. Белозерова, В.С. Оладько // Апробация. – 2016. – №8 (47). – С. 8-10.

94 Новохрестов А.К. Многоуровневая модель информационной системы на основе атрибутивных метаграфов / А.К. Новохрестов, А.А. Конев // Электронные средства и системы управления: Сборник трудов XI Международной научно-практической конференции. – Томск: ТУСУР, 2015. – № 1-2. – С. 184–188.

95 Новохрестов А.К. Математическая модель угроз информационной системе / А.К. Новохрестов, А.А. Конев // Перспективы развития фундаментальных наук [Электронный ресурс]. – Режим доступа: http://science-persp.tpu.ru/Arch/Proceedings_2016_vol_7.pdf, свободный (дата обращения: 01.02.2017 г.).

96 Novokhrestov A. Mathematical model of threats to information systems / A. Novokhrestov, A. Konev // 13TH International conference of students and young scientists on prospects of fundamental sciences development: AIP conference proceedings (Tomsk, 26-29 April 2016). Vol. 1772. – Tomsk: AIP, 2016. – P. 060015. – DOI: 10.1063/1.4964595

97 Новохрестов А.К. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин// Вестник Иркутского государственного технического университета. – 2017. – Т. 21. – №12(131). – С. 93–104. – DOI: 10.21285/1814-3520-2017-12-93-104

98 Новохрестов А.К. Модель классификации угроз нарушения безопасности компьютерных сетей / А. К. Новохрестов, Т. С. Степанова // Электронные средства и системы управления: Материалы докладов XIII Международной научно-практической конференции (29 ноября – 1 декабря 2017 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр, 2017. – С. 76–79.

99 Новохрестов А.К. Угрозы целостности информационной системы на уровне локальных вычислительных сетей / А.К. Новохрестов // Научная сессия ТУСУР-2016: Материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых. – В 6 частях. – Ч. 5. – Томск: В-Спектр, 2016. – С. 81-83.

100 Новохрестов А.К. Модель угроз конфиденциальности информационной системы / А.К. Новохрестов // Электронные средства и системы управления: Материалы докладов XII международной научно-практической конференции (16–18 ноября 2016 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр, 2016. – №1-2. – С. 56-58.

101 Новохрестов А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2016. – Т. 19. – № 3. – С. 111-114. – DOI: 10.21293/1818-0442-2016-19-3-111-114

102 Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: http://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 01.02.2017 г.).

103 Intrusion-detection for incident-response, using a military battlefield-intelligence process / J. Yuill, F. Wu, J. Settle, F. Gong // Computer Networks. – 2000. – No. 34. – P. 671–697.

104 Новохрестов А.К. Анализ состава сетевых средств защиты информации / А.К. Новохрестов, А.А. Конев // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: Материалы VI Межрегиональной научно-практической конференции. – Брянск: Изд-во БГТУ, 2014. – С. 93-96

105 Новохрестов А.К. Классификация сетевых механизмов защиты / А.К. Новохрестов // Инновации и научно-техническое творчество молодежи: Российская научно-техническая конференция: Материалы конференции. – Новосибирск: Изд-во СибГУТИ, 2014. – С. 246-248.

106 Степанова Т.С. Механизмы защиты информации от угроз компьютерным системам / Т.С. Степанова, А.К. Новохрестов // Студенческая наука для развития информационного общества: Сборник материалов V всероссийской научно-технической конференции. – Ставрополь: Изд-во СКФУ, 2016. – С. 497-500.

107 Никифоров Д.С. Механизм защищенного взаимодействия устройства сбора и передачи данных с сервером сбора данных в автоматизированной системе коммерческого учета энергоресурсов // Электронные средства и системы управления: Сборник трудов XI Международной научно-практической конференции. – Томск: ТУСУР, 2015. – № 1-2. – С. 180–184.

108 Антонов М.М. Организация защищенной гетерогенной сети в автоматизированных системах коммерческого учета энергоресурсов / М.М. Антонов, А.А. Конев, Д.С. Никифоров, С.А. Черепанов // Доклады ТУСУРа. – 2016. – №3. – Т.29. – С. 107-110.

Приложение А – Акты внедрения

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПКК МИЛАНДР»
124498, город Москва, город Зеленоград, проспект Георгиевский, дом 5, этаж 2, помещение I, комната 38
ИНН: 7735040690 КПП: 773501001 Сайт: www.milandr.ru Тел.: +7 (495) 981-54-33
ОКПО: 29234983 ОГРН: 1027739083921 Эл. почта: info@milandr.ru Факс.: +7 (495) 981-54-36

16.10.18 № 0386/10-18 Т

На № _____ от _____

УТВЕРЖДАЮ
Генеральный директор
АО "ПКК Миландр"
_____ Павлюк М.И.
«___» _____ 2018 г.

АКТ

внедрения результатов диссертационной работы
Новохрестова Алексея Константиновича

Комиссия в составе председателя: заместителя генерального директора по стратегическому планированию и маркетингу Хафизова Р.З., членов комиссии:

- директора центра проектирования программного обеспечения Дьякова О.Н.,
- начальника отдела Мищенко И.Г.,
- начальника отдела Костромина И.С.

составили настоящий акт о том, что результаты диссертационной работы Новохрестова А.К. «Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов», представленной на соискание ученой степени кандидата технических наук, внедрены в деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов.

Для представления АСКУЭ, состоящей из трех основных типов элементов (устройство учета энергоресурсов, устройство сбора и передачи информации, центральный сервер) была использована разработанная Новохрестовым А.К. модель информационной системы на основе атрибутивных метаграфов.

Ее использование позволило учесть при построении структуры АСКУЭ характеристики элементов и взаимосвязи между ними.

Применение методики составления перечня угроз и модели угроз, разработанных Новохрестовым А.К., позволило получить максимально полный перечень угроз информационной безопасности АСКУЭ. Полученный список был учтен при определении перечня актуальных угроз и оценке рисков, которая показала необходимость внедрения в систему дополнительных механизмов защиты.

Результатом внедрения работы Новохрестова А.К. в деятельность АО «ПКК Миландр» стал перечень из 70 угроз информационной безопасности системы, что на 18 % больше, чем количество угроз, выявленных экспертами ранее.

Председатель комиссии _____ Р.З. Хафизов

Члены комиссии:

_____ О.Н. Дьяков

_____ И.Г. Мищенко

_____ Костромин И.С.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования ТУСУР
_____ П.Е. Троян
«11» ____10____ 2018 г.

АКТ
о внедрении результатов диссертационной работы
Новохрестова Алексея Константиновича в учебный процесс

Комиссия в составе:

Давыдова Е.М., к.т.н., декан факультета безопасности ТУСУР – председатель комиссии;

Конев А.А., к.т.н., доцент кафедры КИБЭВС ТУСУР;

Кручинин Д.В., к.ф.-м.н., доцент кафедры КИБЭВС ТУСУР;

Евсютин О.О., к.т.н., доцент кафедры БИС ТУСУР

составила настоящий акт о нижеследующем.

Результаты диссертационной работы Новохрестова А.К., используются в учебном процессе на факультете безопасности ТУСУР при чтении курса лекций и проведении практических занятий по дисциплинам «Безопасность сетей ЭВМ», «Управление информационной безопасностью» и «Моделирование автоматизированных информационных систем» для подготовки специалистов по защите информации, обучающихся по специальностям «10.05.03 – Информационная безопасность автоматизированных систем» и «10.05.04 – Информационно-аналитические системы безопасности».

В курсах «Безопасность сетей ЭВМ» и «Управление информационной безопасностью» используются результаты работы Новохрестова А.К. по разработке методики составления перечня угроз информационной безопасности

компьютерных сетей, позволяющие студентам ознакомиться с процессом построения моделей угроз безопасности информационных систем.

В курсе «Моделирование автоматизированных информационных систем» используется предложенная Новохрестовым А.К. модель компьютерной сети на основе атрибутивных метаграфов, позволяющая студентам ознакомиться с практическим применением теории графов.

Кроме того, студенты факультета безопасности имеют возможность ознакомиться с результатами диссертационного исследования в ходе выполнения групповых проектов, научно-исследовательских и дипломных работ и использовать их в практических работах по моделированию угроз и анализу защищенности компьютерных сетей.

Освоение студентами предложенного Новохрестовым А.К. подхода позволяет сформировать навыки составления перечней угроз информационной безопасности информационных систем, а применение методики изучить на практике особенности моделирования угроз безопасности компьютерных сетей.

Настоящий акт составлен в 3 (трех) экземплярах.

Давыдова Е.М.
к.т.н., декан факультета
безопасности ТУСУР

«10» 10 2018 г.

Конев А.А.
к.т.н., доцент кафедры
КИБЭВС ТУСУР

«10» 10 2018 г.

Кручинин Д.В.
к.ф.-м.н., доцент кафедры
КИБЭВС ТУСУР

«10» 10 2018 г.

Евсютин О.О.
к.т.н., доцент кафедры
БИС ТУСУР

«10» 10 2018 г.