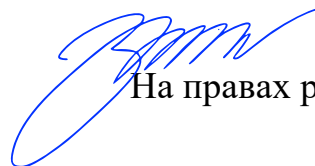


Министерство науки и высшего образования Российской Федерации

Томский государственный университет  
систем управления и радиоэлектроники (ТУСУР)



На правах рукописи

Егошин Николай Сергеевич

**МОДЕЛИ УГРОЗ НАРУШЕНИЯ БЕЗОПАСНОСТИ  
ИНФОРМАЦИОННЫХ ПОТОКОВ В КИБЕРПРОСТРАНСТВЕ**

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 2021

## Содержание

<b>Введение</b> .....	3
<b>1 Обзор текущего состояния предметной области</b> .....	10
<b>1.1 Применимость модели информационных потоков</b> .....	10
<b>1.2 Модели угроз информации</b> .....	13
<b>1.3 Модель нарушителя</b> .....	22
<b>1.4 Методики формирования политики разграничения доступа</b> .....	26
<b>1.5 Выводы по главе</b> .....	29
<b>2 Модель элементарных информационных потоков</b> .....	32
<b>2.1 Построение модели элементарных информационных потоков</b> ....	32
<b>2.2 Пример использования модели</b> .....	36
<b>2.3 Выводы по главе</b> .....	40
<b>3 Модель угроз информации</b> .....	41
<b>3.1 Описание несанкционированных потоков</b> .....	41
<b>3.2 Модель угроз целостности и доступности</b> .....	44
<b>3.3 Модель угроз конфиденциальности</b> .....	57
<b>3.4 Комплексированная модель угроз и сравнение с аналогами</b> .....	67
<b>3.5 Выводы по главе</b> .....	74
<b>4 Модель нарушителя информационной безопасности</b> .....	75
<b>4.1 Формирование модели нарушителя</b> .....	75
<b>4.2 Соотнесение модели нарушителя и модели угроз</b> .....	80
<b>4.3 Выводы по главе</b> .....	81
<b>5 Методика формирования политики разграничения доступа</b> .....	82
<b>5.1 Общее описание методики</b> .....	82
<b>5.2 Пример применения методики</b> .....	84
<b>5.3 Выводы по главе</b> .....	90
<b>Заключение</b> .....	92
<b>Список использованной литературы</b> .....	94
<b>Приложение А – Акты внедрения</b> .....	111

## Введение

С развитием и становлением информационного общества проблема обеспечения информационной безопасности становится все более актуальной. Любые современные организации стремятся увеличить интеграцию информационных технологий во сферы своей деятельности, ведь это позволяет перейти на качественно другой уровень хранения, обработки и передачи информации.

В связи с непрерывным ростом объемов обрабатываемой информации возникла необходимость перехода к электронному документообороту. Повсеместное внедрение информационных технологий позволило отказаться от бумажных носителей, снизить затраты на обработку и хранение документов, а также обеспечить быстрый поиск.

Если подойти к проблеме с точки зрения системного анализа, то можно постараться абстрагироваться и обобщить до единого понятия все способы взаимодействия между любыми объектами, выполняющими хранение, обработку и передачу информации. Любой случай передачи информации, можно представить, как некий информационный поток между источником и получателем. Оперируя этим понятием, всю суть защиты информации можно свести к одной цели – необходимо обеспечить безопасность всех элементов любого элементарного информационного потока в каждый момент времени.

Основная проблема с современным правовом поле – это отсутствие должной унификации. Закрепленные законодательно методики часто носят исключительно рекомендательный характер и при этом содержат в себе пространные формулировки. В связи с этим, специалисты по защите информации вынуждены разрабатывать свои собственные локальные нормативные акты. В такой ситуации профессионализм эксперта и его субъективное мнение существенно влияют на итоговый результат.

Важно понимать, что появление новых технологий не только порождает новые способы атак, но и расширяет существующий перечень угроз, а, как известно, каждая угроза может быть осуществлена большим

количеством различных атак [1]. Появление новых технологий нелинейно снижает уровень защищенности существующих систем. В связи с этим на первый план выходит необходимость формирования полного перечня угроз информации, однако данная проблема не имеет простого решения. Для решения этой задачи создаются различные модели угроз, в основе которых лежат всевозможные математические аппараты и информационные модели.

При этом множественность различных моделей обуславливается не только различием взглядов исследователей и их подходов к решению проблемы. Используемые решения задач защиты информации зависят от аспекта информационной безопасности [2]. Мы не можем использовать одни и те же модели для обеспечения защиты конфиденциальности и целостности или доступности, так же как мы не можем использовать одинаковые модели для предсказания атак на информацию и на систему в виду того, что объекты принципиально отличаются друг от друга [3]. Всем вышесказанным определяется **актуальность** темы диссертационного исследования.

Значительный вклад в развитие теории и практики защиты информации в информационных системах, в том числе при рассмотрении проблем построения моделей угроз, внесли А.А. Грушо, В.В. Меньших, Н.А. Гайдамакин, В.А. Герасименко, П.Д. Зегжда, А.М. Ивашко, С.М. Климов, И.Д. Королев, А.И. Костогрызов, А.С. Кузьмин, А.И. Куприянов, О.Б. Макаревич, В.Ф. Макаров, А. М. Сычев, А.А. Стрельцов, Л.М. Ухлинов, А.В. Черемушкин, В.Ф. Шаньгин, А.А. Шелупанов, В.П. Шерстюк, И.Б. Шубинский, А.Ю. Щербаков, Ю.К. Язов, W. Burr, M.A. Burrows, J. Clark, W. Diffie, D.F. Dodson, C. Kaufman, J. Kjaersgaard, A. Lensrta, G. Lowe, J. Myers, R.M. Needham, N. Pole, W.T. Polk, K. Rannenber, B. Schneier, G. Stoneburner, S.B. Wilson, T.Y.C. Woo и др. В их исследованиях разработана концепция защиты информации, обоснованы принципы обеспечения информационной безопасности и построения систем защиты информации объектов информатизации, а также сформулированы основы построения моделей угроз и нарушителей безопасности информации.

Диссертационная работа посвящена исследованию механизмов моделирования и описания процессов передачи информации внутри системы с целью обоснования и создания полной модели угроз информации.

**Целью исследования** является развитие подхода к формированию актуального перечня угроз и политики разграничения доступа за счет применения моделей информационных потоков и угроз безопасности информации.

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

1. выполнить анализ текущего состояния предметной области;
2. сформировать модель описания информационных процессов системы с учетом гетерогенности каналов передачи информации;
3. классифицировать угрозы конфиденциальности, целостности и доступности информации, применительно к процессам ее хранения и передачи;
4. создать модель угроз конфиденциальности информации на основе определенной ранее классификации угроз;
5. создать модель угроз целостности и доступности информации на основе определенной ранее классификации угроз;
6. разработать методику формирования политики разграничения доступа;
7. создать модель нарушителя;
8. апробировать методику и предложенные модели в процессе формирования политики разграничения доступа.

**Объектом исследования** данной работы является информация защищаемая и обрабатываемая в информационной системе при условии существования внутренних и внешних угроз этой информации.

**Предметом исследования** являются модели и методика, применяемые при формировании политики информационной безопасности организации.

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

**Научная новизна** результатов работы и проведенных исследований:

1. предложена мультиграфовая модель элементарных информационных потоков в информационной системе, учитывающая гетерогенность каналов взаимодействия;

2. разработана модель угроз конфиденциальности информации, отличающаяся от аналогов полнотой учета всех типовых угроз элементам системы и каналам передачи информации;

3. предложена модель угроз целостности и доступности информации, отличающаяся от аналогов учетом угроз доступности как подмножество угроз целостности информации, направленных на канал передачи информации.

**Достоверность** и обоснованность предлагаемых научных положений, результатов и выводов работы подкрепляется разносторонним изучением современного состояния предметной области, системным обоснованием предложенных моделей, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также практикой внедрения результатов исследования.

**Научная значимость** работы состоит в развитии теории и методологии обеспечения информационной безопасности в части создания новых моделей угроз информации, нарушителя, описания информационных потоков в системе и методики формирования политики разграничения доступа с применением математического аппарата теории графов для моделирования процессов взаимодействия в системе.

**Практическая значимость** результатов исследования состоит в следующем:

1. Модель нарушителя позволила расширить количество учитываемых типов нарушителя за счет комбинирования его характеристик;
2. Методика формирования политики разграничения доступа, основанная на модели элементарных информационных потоков, позволила разграничить доступ к каналам передачи информации как к самостоятельным структурным элементам системы.

**Реализация результатов работы.** 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) и в рамках базовой части государственного задания ТУСУРа на 2020–2022 гг. (проект № FEWM-2020-0037).

**Положения, выносимые на защиту:**

1. Модель элементарных информационных потоков позволяет описать гетерогенную информационную систему объекта защиты, находящегося под воздействием угроз, с помощью конечного множества элементарных информационных потоков;

Паспорт специальности, пункт 1: теория и методология обеспечения информационной безопасности и защиты информации.

2. Модель угроз конфиденциальности информации позволяет определить полное множество типовых угроз конфиденциальности с учетом процессов передачи, хранения и обработки информации;

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

3. Комплексированная модель угроз конфиденциальности и целостности/доступности информации позволила выявить 13 дополнительных угроз в сравнении с аналогом – «Банк данных угроз безопасности информации ФСТЭК».

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

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

— XI Международной научно-практической конференции «Электронные средства и системы управления» (Томск, 2018);

— XIII Международной конференции студентов, аспирантов и молодых ученых «Перспективы развития фундаментальных наук» (Томск, 2018);

— II Российско-Тихоокеанской конференция по компьютерным технологиям и приложениям «RPC 2017» (Владивосток, 2017)

— Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO-2019» (Томск, 2019)

— XVI Международная научно-практическая конференция «Проблемы информационной безопасности государства, общества и личности» (Томск, 2018)

Результаты исследования докладывались и обсуждались на заседаниях IEEE семинаров «Интеллектуальные системы моделирования, проектирования и управления» Института системной интеграции и безопасности (ИСИБ ТУСУР) в г. Томске.

**Внедрение результатов.** Результаты диссертационной работы внедрены в деятельность «Удостоверяющего Центра Сибири» и НПФ «Информационные системы безопасности», а также в учебный процесс Томского Государственного Университета Систем Управления и Радиоэлектроники.

**Личный вклад.** В диссертационной работе использованы результаты, в которых автору принадлежит определяющая роль. Постановка задачи исследования и верификация результатов в процессе выполнения работы



осуществлялась научным руководителем д.т.н., профессором Шелупановым А.А. Консультативное содействие оказывалось к.т.н., доцентом Коневым А.А.

**Публикации по теме диссертации.** По материалам исследования опубликовано 11 работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, и 2 в изданиях WoS и Scopus.

**Структура и объем работы.** Диссертация содержит введение, 5 глав, заключение и список источников из 120 наименований. Объем работы: 113 страниц, в том числе 31 таблица и 29 рисунков.

## **1 Обзор текущего состояния предметной области**

Метод формальной разработки системы защиты информации опирается на различные модели (модель управления доступом, модель политики безопасности, модель нарушителя, модель угроз и т.д.). Целью любой модели является выражение сути определенных требований к системе, она определяет потоки информации и правила управления доступом к ним [4].

Формирование политики безопасности организации опирается на большое количество различных частных моделей и методик. В данной работе рассмотрены следующие направления:

- определение типовых угроз информации;
- построение модели нарушителя;
- формирование политики разграничения доступа.

### **1.1 Применимость модели информационных потоков**

В различных научных трудах не раз поднималась тема о необходимости применения модели информационных потоков при решении вопросов информационной безопасности, например, при построении модели угроз или формировании политики разграничения доступа.

Теория информационных потоков применима к обширному спектру типов систем: киберфизическим (CPS), системам телемедицины, SCADA, IoT, системам разработки программного обеспечения. Разберем подробнее все виды систем.

Говоря о киберфизических системах, можно выделить следующие публикации: в работе [5] авторы сообщают что, информационный поток – это концептуально фундаментальная основа системы безопасности, а конфиденциальность информации в системе может быть нарушена при возникновении несанкционированного потока, данное высказывание совпадает с идеями автора, высказанными в введении текущей работы; в свою очередь авторы [6] не уделяют такого большого внимания конкретно информационным потокам, больше говоря о физических потоках, однако при

этом упоминая, что необходимо обеспечить контроль за разграничением доступа к информационным потокам.

Всё более востребованными становятся системы телемедицины, и по данной тематике также существуют публикации с аналогичными взглядами: если авторы [7] и [8] предлагают использовать методологию DFD совместно с STRIDE или DREAD, то авторы [9] не вводят отдельного понятия информационной потока, но говорят, что сеть является важной частью системы наравне с клиентами и серверами.

В работе [10] информационный поток также упоминается только один раз в контексте того, что он может быть объектом атаки, однако в разработанной методике определяются только угрозы, направленные на элементы системы, при этом сам поток к таковым не отнесён.

Всё чаще модели угроз начинают применяться уже на ранних этапах разработки программных средств. Есть работы, которые придерживаются методологии STRIDE, как например [11-13], но при этом и есть работы, которые полностью игнорируют данную тему, например [14].

Начав говорить о программном обеспечении, ни в коем случае нельзя обойти стороной и SCADA-системы, ведь по количеству каналов передачи информации они вполне вероятно обходят все другие системы, а уже нарушение режима защищенности информации в этих каналах может привести к катастрофическим последствиям (экономическим потерям или даже техногенным катастрофам). Авторы статей [15] и [16] используют примерно одинаковый подход: в их моделях присутствуют угрозы, направленные на канал, однако сам канал не рассматривается в виде значимой части системы, а без всестороннего анализа трудно говорить о полноте самой модели.

Переходя к вопросу о больших и распределённых системах, необходимо обязательно упомянуть уже такие, ставшие обыденностью, вещи как облачные технологии и IoT. Как и ожидалось, с увеличением системы значимость линий связи также возрастает. Для IoT системы канал передачи

информации уже является не просто обязательным элементом, но становится полноценной рабочей единицей [17]. Соответственно и работы по данной теме обладают большим единодушием. Авторы работы [18] хоть и не говорят ничего об информационных потоках, но всё же считают, что при использовании облачных технологий или мобильных устройств определение угроз информации и оценка рисков становятся значительно сложнее. Авторы работ [19-22] обозначают важность учета информационных потоков и предлагают использование методологии DFD и STRIDE.

Если отойти от прикладных решений, которые были рассмотрены выше, и посмотреть на предметную область в целом, то станет понятно, что публикации на данную тему выходят с завидной регулярностью уже больше десятилетия.

Совместно с вышеуказанными работами присутствуют и труды, которые относятся к уникальным предметным областям или же вообще имеют общее назначение, но всё же так или иначе упоминают информационные потоки при построении модели угроз. Часть из них [23-25], даже используют аналогичный термин – поток. А в ряде работ [26-34] используют термин *network*, хотя из контекста становится понятно, что имеется в виду не сетевое соединение, а именно информационный поток.

Данные понятия необходимо строго разграничивать, т. к. их смешение и подмена вызывает только большую путаницу. Не каждый информационный поток реализуется сетевым каналом, но всё же каждый сетевой канал является информационным потоком. Сетевое соединение – это только частный вид информационного потока. Само понятие потока гораздо более обширно и определяет все возможные каналы передачи информации.

При рассмотрении схемы информационных потоков большинство работ использует методологию DFD, однако у неё есть ряд критически значимых недостатков:

— модель имеет две отдельные нотации для построения схем внутреннего и внешнего взаимодействия;

— модель не описывает каналы передачи информации и образующиеся информационные потоки.

В работе [35] предлагается использование Скрытых Марковских Цепей для асимметричного моделирования угроз. Однако, такой подход не является верным, т. к. Цепи Маркова целесообразнее использовать при определении атак, которые в отличие от угроз носят вероятностный характер.

В конце обзора литературы стоит упомянуть очень интересный вариант решения проблемы, а именно использование Сетей Петри [36-37]. Определенно сети Петри удобно использовать при моделировании дискретных автоматов как конечных, так и бесконечных. Однако, в контексте текущего исследования в этом нет смысла, так как Сети Петри позволяют описать процесс передачи информации, а точнее сам факт перемещения информации с одной вершины в канал и далее, но не позволяют описать отдельно канал передачи информации. Нет смысла моделировать систему при различных местонахождениях информации в ней. Необходим более высокий уровень абстракции, когда информация может находиться как во всех элементах одновременно, так и в любой другой комбинации, вплоть до полного её отсутствия.

Резюмируя обзорную часть, необходимо обозначить одну важную деталь. Проблема в том, что STRIDE позволяет смоделировать не угрозы, а атаки. Эти термины, несомненно, являются смежными, однако их всё же не надо смешивать. Угрозы – более обширное понятие нежели атаки, и при этом каждая угроза может быть реализована множеством различных атак. Комплексные меры по борьбе с угрозами носят превентивный характер. Перекрытие угрозы обеспечивает защиту от большого пласта атак. Потому формирование модели угроз имеет первоочередной характер.

## **1.2 Модели угроз информации**

Большое количество компаний используют компьютерные сети (в частности, Интернет) для передачи и обработки информации. Для того чтобы

построить некую систему защиты информации, необходимо определить все возможные угрозы безопасности информации [38], том числе и на каналы передачи информации.

Модель угроз носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой [39]. Вследствие чего возможны ситуации, когда специалисты по информационной безопасности вынуждены составлять специальные нормативно-методические документы, так как существующие модели не удовлетворяют всем особенностям работы организации [40-51].

Переработка общей модели для частного случая не всегда может быть корректно осуществлена по различным причинам (будь то недостаточный профессионализм сотрудника, либо банальная нехватка времени). Возможная избыточность итоговой модели не нанесёт вреда, в то время как пробелы могут оставить «дыры» в системе безопасности.

В данном пункте рассматриваются подходы к описанию и идентификации угроз и построению моделей угроз безопасности информации, обрабатываемой в информационной системе.

### **1.2.1 Банк данных угроз безопасности информации ФСТЭК России**

Первым и очевиднейшим способом является полный перебор всех возможных угроз с выделением именно тех, что относятся к системе обработки информации, безопасность которой необходимо обеспечить. Хорошим помощником в данном деле послужит [52], в котором приведены сведения об основных угрозах безопасности информации. На момент использования источника [52] база содержала в себе 213 актуальных угроз, к каждой угрозе есть описание, также приведен объект воздействия. Несмотря на несомненную результативность данного метода, сложно говорить о его эффективности.

Основная проблема заключается в том, что эффективность данного метода полностью основывается на компетентности эксперта, составляющего список.

Предположительно, данная проблема решается при помощи документа [53], который определяет такие вещи как, формирование экспертной группы и определение актуального списка угроз. Однако, документ не содержит в себе никаких практических рекомендаций и примеров.

### **1.2.2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных**

В результате анализа [54] было установлено, что по данному документу модель угроз имеет следующую структуру:

- полный перечень угроз;
- общая характеристика информационной системы;
- классы уязвимостей;
- виды деструктивных воздействий на объект доступа;
- способы реализации деструктивных воздействий.

Пункты 3–5 не должны фигурировать при описании модели угроз. Данные параметры основываются на угрозе, а не наоборот, и, следовательно, результирующие угрозы от них не зависят.

### **1.2.3 Рекомендации в области стандартизации банка России РС БР ИББС-2.4-2010**

Источник [55] предоставляет следующий вид модели угроз:

- источники угроз информационной безопасности (ИБ) (внешний нарушитель и внутренний нарушитель);
- методы реализации угроз ИБ;
- объекты, пригодные для реализации угроз ИБ;
- уязвимости, используемые источниками угроз ИБ;
- типы возможных потерь;

– масштабы потенциального ущерба.

Пункт 1 представляет список источников угроз, в качестве которого выделяется тип нарушителя (внешний или внутренний). Но, так как тип нарушителя характеризуется при построении модели нарушителя, следовательно, данный пункт не относится к модели угроз.

Пункт 2 включает в себя описание механизмов воздействия, которые нарушитель использует для реализации какой-либо угрозы. То есть, данный пункт относится к модели нарушителя.

Пункт 3 применим к модели угроз, так как является входным параметром модели угроз.

Пункты 4–6 не являются частью модели угроз. Данные параметры основываются на угрозе, а не наоборот, и, следовательно, они не являются входными параметрами, от которых зависят результирующие угрозы.

#### **1.2.4 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:

- 1) угрозы от действий вредоносных программ (вирусов);
- 2) угрозы утраты ключей и атрибутов доступа;
- 3) угрозы выявления паролей по сети;
- 4) угрозы внедрения по сети вредоносных программ;



- 5) угрозы наличия не декларированных возможностей системного программного обеспечения (далее ПО) и ПО для обработки персональных данных;
- 6) угрозы перехвата за пределами контролируемой зоны;
- 7) угрозы сканирования;
- 8) угрозы подмены доверенного объекта в сети;
- 9) угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.
- 10) угрозы типа «отказ в обслуживании»;
- 11) угрозы удаленного запуска приложений.

### **1.2.5 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, случайная, природная.

Перечень рассматриваемых угроз информационной безопасности в [57]:

- 1) поиск повторно используемых или забракованных носителей;
- 2) раскрытие;
- 3) данные из ненадежных источников;
- 4) преступное использование аппаратных средств;
- 5) преступное использование программного обеспечения;
- 6) определение местонахождения;
- 7) перехват компрометирующих сигналов помех;
- 8) дистанционный шпионаж;
- 9) прослушивание;
- 10) кража носителей или документов;
- 11) кража оборудования;
- 12) отказ оборудования;
- 13) неисправная работа оборудования;
- 14) насыщение информационной системы;

- 15) нарушение функционирования программного обеспечения;
- 16) нарушение сопровождения информационной системы;
- 17) несанкционированное использование оборудования;
- 18) мошенническое копирование программного обеспечения;
- 19) использование контрафактного или скопированного программного обеспечения;
- 20) искажение данных;
- 21) незаконная обработка данных;
- 22) ошибка при использовании;
- 23) злоупотребление правами;
- 24) фальсификация прав;
- 25) отказ в осуществлении действий;
- 26) нарушение работоспособности персонала.

Стандарт [57] содержит в себе обобщенный список угроз информационной безопасности.

### **1.2.6 The STRIDE Threat Model**

Методология компании Microsoft – STRIDE [58], в которой используется подход к созданию защищенных систем на основе моделирования угроз. Ее использование предполагается при разработке программного обеспечения. Согласно [58] моделирование угроз проводится на этапе проектирования (согласно документации, этап назван «Дизайн (design)») программного средства.

Первое, на что необходимо прямо указать, это неверное применение терминов в данной методологии. Само название методологии – это аббревиатура из первых букв названий угроз: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege. Проблема в том, что в строгом понимании данные термины являются не угрозами, а атаками. Причем каждая из них направлена на определенный аспект информационной безопасности, однако же аспекты, описываемые в

методологии, расширяют классическую CIA triad, но не совпадают с Parkerian Hexad.

В STRIDE нет разделения угроз по объекту воздействия и нет описания типовых угроз. Вернёмся к нашему примеру с передачей электронной почты. К какому объекту системы применима угроза «Information disclosure»? К каналам? Хранилищам? К СЗИ? Данное определение является очень общим из-за чего специалист по защите информации вынужден сам определять к каким узлам системы применять каждую из угроз.

Например, взаимодействие пользователя и почтового клиента с помощью мобильного устройства. К какой из частей данной локальной системы взаимодействия применима каждая из угроз? В STRIDE выходит на первый план распространённая проблема – отсутствие типизации и формализации. Специалисту не предоставлен инструмент, согласно которому он должен описать систему, чтобы потом определить угрозы информации.

### **1.2.7 NIST Special Publication 800-37**

Документ [59] является руководством по управлению рисками для ИТ-систем и ориентирован на менеджмент 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 [59] и заключаются в существенном влиянии субъективного мнения и профессионального уровня эксперта.

### **1.2.8 Авторефераты по теме исследования**

Исходя из [60], автор Лукинова О.В. выделяет следующую структуру модели угроз:

- класс уязвимостей (содержит представление понятий, связанных с уязвимостями среды бизнес-процесса);
- класс нарушителя (объекты, характеризующие возможности потенциального нарушителя);
- класс атак (потенциально-опасные атаки).

Пункт 1 и 3 не должны использоваться при построении модели угроз. Так как при формировании данных двух классов (уязвимостей, атак) базисом является сама угроза, которая в свою очередь это конечный результат модели угроз. Другими словами, сначала выявляют угрозу, затем используя данную угрозу, получают возможные уязвимости и атаки, а не наоборот. Следовательно, уязвимости и потенциально-опасные атаки не являются элементами модели угроз.

Пункт 2 описывает тип нарушителя. Данный пункт не должен фигурировать при описании модели угроз. Все, что касается нарушителей (источников угроз), относится к понятию «Модель нарушителя».

Автор Дунин В.С. в с [61] представил модель угроз как канал несанкционированного доступа, который содержит:

- субъект доступа;
- путь распространения угрозы;
- информационный объект (объект доступа).

Далее, автор, конкретизируя определение, переходит к понятию «кортежей» и представляет модель угроз в виде формулы.

$$U=(S, K, B_c, B_x, П, ИО(C) ),$$

где  $S$  – субъект доступа (процесс или человек);

$K$ – оборудование в канале связи (коммутаторы, маршрутизаторы и др.);

$B_c, B_x$  – сервисы безопасности на пути распространения угрозы (журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и др.);

$П$  – протоколы и пакеты;

$ИО$  – информационный объект доступа.

Субъект доступа (S) и информационный объект доступа (ИО) являются входными характеристиками модели угроз. Эти параметры нужны при формировании модели угроз.

Оборудование в канале связи (К) не влияет на специфику самой угрозы, этот параметр не является входными данными в функции модели угроз. Например, при реализации угрозы, как анализ сетевого трафика, относительно различных устройств (коммутатор, маршрутизатор, сервер) суть самой угрозы как таковой не меняется. Следовательно, готовая угроза на выходе функции модели угроз никак не зависит от данного параметра на входе. Не требуется.

Сервисы безопасности (Бс, Бх) не требуются в модели угроз, так как сама специфика угрозы не меняется в зависимости от инструмента защиты. Следовательно, от данного параметра (Бс, Бх) модель угроз как функция не зависит.

В [62] автор Ерохин С.С. представляет два основных понятия: «Модель нарушителя» и «Модель угроз». Идея заключается в том, что сначала формируется модель нарушителя, затем на вход модели угроз поступают данные из модели нарушителей. На выходе формируются деструктивные воздействия по каждому объекту для каждого нарушителя. Из всех возможных деструктивных воздействий образуется множество актуальных угроз информационной безопасности.

Параметр «нарушитель» использует понятие «тип нарушителя», что, как ранее было сказано, относится только к модели нарушителя. Не требуется.

Параметр «объект атаки» (объект доступа) является входным параметром модели угроз, то есть влияет на результирующую угрозу. Требуется.

Параметр «цель атаки» описывает мотив самого нарушителя. Данный параметр относится к модели нарушителя, следовательно, не является параметром модели угроз. Не требуется.

Значение параметров «информация об объекте атаки», «средства атаки», «способы реализации угроз», «структура объекта исследования» в работе автора не представлено.

Параметр «права доступа пользователей к информации ограниченного доступа» характеризует инструменты безопасности, значение которого не влияет на результирующую угрозу на выходе модели угроз.

### **1.3 Модель нарушителя**

Неотъемлемым от процесса разграничения доступа является определение модели нарушителя. Пользователи системы и ее персонал, являются необходимым элементом информационной системы, но они же являются и основной причиной нарушений и преступлений.

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства [63].

Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Важно понимать, что игнорирование или недобросовестное построение модели может серьезно отразиться на сохранности конфиденциальной информации. Исходя из этого, решение проблемных вопросов формирования модели нарушителя является одним из первоочередных направлений обеспечения информационной безопасности.

В данном пункте рассматриваются подходы к описанию и построению модели нарушителя безопасности информации.

### **1.3.1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных**

Документ [54] определяет нарушителя как один из источников угроз НСД в ИСПДн наравне с носителями вредоносных программ и аппаратным закладками.

Нарушители делятся на два типа по наличию права постоянного или разового доступа в контролируемую зону ИСПДн. В свою очередь внутренние нарушители делятся ещё на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

В документе приводится описание возможностей и уровня знаний нарушителя. Минусом модели является неочевидность градации нарушителей по уровням полномочий. Модель не разбирает внешних нарушителей, а только даёт их общее описание. Часть внутренних нарушителей является таковыми только при определенных условиях, во многих случаях их можно отнести именно к внешним нарушителям. Отсутствует математическая формализация.

### **1.3.2 Методические рекомендации ФСБ по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации**

Согласно [64] нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредств и СФК).

Документ подразумевает наличие шести основных типов нарушителей:  $H_1$ ,  $H_2$ ,  $H_3$ ,  $H_4$ ,  $H_5$ ,  $H_6$ . Возможности нарушителя более высокого уровня включают в себя возможности нарушителей предыдущих типов.

Сначала все физические делятся сначала на две категории по наличию или отсутствию права доступа в контролируемую зону информационной

системы. Далее все потенциальные нарушители подразделяются на внутренних и внешних. Приводится описание привилегированных пользователей информационной системы. Обосновываются исключения тех или иных типов лиц из числа потенциальных нарушителей. Как правило, привилегированные пользователи информационной системы исключаются из числа потенциальных нарушителей. И, наконец, рассматривается вопрос о возможном сговоре нарушителей.

На следующем этапе делаются предположения об имеющейся у нарушителя информации об объектах атак и об имеющихся у нарушителя средствах атак. На основе этих предположений определяется непосредственно тип нарушителя  $H_i$ .

Также данная методика подразумевает определение и описание каналов атак, указывается, что с практической точки зрения этот раздел является одним из важнейших в модели нарушителя.

Плюсом методики является акцентирование внимания на определении каналов атак. Методика имеет четкую градацию нарушителей и подробное описание предположений о его уровне. Основным недостатком методики является её структура: нет четкой математической модели, из-за чего может случиться путаница.

### **1.3.3 Руководящий документ: концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации**

Согласно [65] в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами автоматизированной системы. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами.

Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего. В своем уровне нарушитель



является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

Как и следует из названия документа, модель нарушителя носит исключительно концептуальный характер, однако данная модель даже на своём концептуальном уровне не подразумевает разделение нарушителей на внутренних и внешних.

#### **1.3.4 Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли**

Модель нарушителя из [66] представляет из себя довольно грубое смешение моделей [53] и [64]. Как результат данная модель наследует минусы предыдущих моделей, при этом создавая новые неопределенности.

В модели присутствует разбиение внутренних нарушителей на 8 уровней, тип нарушителя определяется только на основе таблицы соответствия.

При таком подходе не ясно зачем вообще определять тип нарушителя, если достаточно знать его группу, а также не ясно зачем делать предположения о степени информирования нарушителя и о имеющихся у него средствах атак.

Стоит добавить, что разработчики данной модели косвенно подтвердили тезис автора из пункта 1.3.1 данной работы о том, что модель [66] имеет неочевидную градацию, т. к. группе 7 соответствует более высокий тип нарушителя и класс СКЗИ чем группе 8.

#### **1.3.5 Модель угроз типовой медицинской информационной системы (МИС) типового лечебного профилактического учреждения (ЛПУ)**

Модель нарушителя из [67] построена основе рекомендаций из документа [53]. В виду того, что данная модель разработана для конкретной предметной области, в ней были учтены некоторые минусы прототипа, несмотря на этой они всё же есть: модель не имеет математической

формализации и не учитывает вероятность случайных действий или стихийных факторов.

#### **1.4 Методики формирования политики разграничения доступа**

Информационные системы представляют собой сложные системы, способные работать с большими объемами разнородных данных из территориально удаленных источников, количество которых может сильно варьироваться. В работе такой системы неизбежно встают вопросы о контроле целостности данных, обеспечении их доступности, а также конфиденциальности в случае секретных данных. Разрешение этих вопросов достигается путём осуществления комплекса мер по защите информации сразу на нескольких уровнях. Эти уровни можно объединить в два крупных блока – физический и информационный уровень. На физическом уровне меры защиты направлены на ограничение доступа к зданиям, помещениям, сейфам, сетевому оборудованию, кабельному хозяйству, к серверам и рабочим станциям. На информационном уровне меры защиты направлены на ограничение доступа к информации в сетях и операционных системах [68-75]. Многоуровневый подход позволяет разделить ответственность за защиту информации между участниками обмена данными на разных этапах процессов приема, обработки и передачи данных [76].

Как правило, для разграничения доступа к информации применяется дискреционный или мандатный принцип разграничения доступа, но они применимы в чистом виде только для узкого класса задач [77]. Поэтому существует потребность в создании универсальной методики по разграничению доступа информации и создание нормативного документа по разграничению доступа.

Нормативный документ по разграничению доступа необходим любой организации для разработки локальной нормативной базы в области информационной безопасности при внедрении системы управления информационной безопасностью, документировании процессов и требований

безопасности, распределении ролей, прав доступа и назначении ответственных за безопасность [78].

Используя методику, можно внести изменения в систему защиты информации для более эффективной ее работы, снизив угрозы утечки ценной информации и ущерб от атак нарушителей.

Важной особенностью является то, что часто никакими средствами нельзя ограничить утечку информации, кроме как использования ограничительных мер в организационной документации. Именно поэтому этой документации надо уделить особое внимание [79].

В данном пункте проводится анализ подходов к формированию политики разграничения доступа.

#### **1.4.1 Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

В документе [80] представлены рекомендации по разработке положения о разграничении прав доступа к обрабатываемым персональным данным.

Согласно рекомендациям, разграничение прав должно осуществляться на основании отчета по результатам проведения внутренней проверки, а также исходя из характера и режима обработки персональных данных в информационной системе [80].

Для каждой информационной системы должен быть представлен поименованный список сотрудников ответственный за обработку персональных данных. Список групп пользователей берется из отчета по результатам проведения внутренней проверки [84].

#### **1.4.2 ГОСТ Р 50739–95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования**

Согласно требованиям [81], система защиты информации должна осуществлять разграничение доступа субъектов к данным, которое производится в соответствии с политикой безопасности.

Ограничения должны осуществляться по следующим признакам:

- роль субъекта;
- домен безопасности субъекта;
- право доступа к объекту;
- организационная принадлежность субъекта.

Таким образом, для получения доступа субъект должен подать системе защиты запрос, включающий идентификатор субъекта, аутентификационные параметры и содержание запроса.

В зависимости от требований к разграничению прав доступа в информационных системах реализуют различные модели разграничения прав доступа. В [81] говорится о дискреционной и мандатной моделях разграничения прав доступа.

### **1.4.3 СТО БР ИББС-1.0-2010 Обеспечение информационной безопасности организаций банковской системы Российской Федерации.**

#### **Общие положения.**

В стандарте [82], предлагается разграничить доступ к информационной инфраструктуре банка на несколько уровней. Для каждого уровня определить права доступа.

Должен быть документально определен перечень информационных активов (их типов) организации банковской системы РФ. Права доступа работников и клиентов организации БС РФ к данным активам должны быть документально зафиксированы [82].

#### **1.4.4 PCI DSS**

Согласно стандарту безопасности данных индустрии платежных карт (PCI DSS), при разграничении доступа необходимо руководствоваться

принципом минимальных привилегий. То есть запретить пользователю все, а затем предоставить только права, необходимые для выполнения должностных обязанностей. При назначении привилегий необходимо руководствоваться правилом предоставления привилегий только по ролям. То есть права назначать только для роли, а не для конкретного пользователя, затем присвоить роль конкретному пользователю.

Для гарантии того, что доступ к критичным данным есть только у авторизованного персонала, системы и приложения должны ограничивать доступ к данным в соответствии с принципом служебной необходимости. Принцип служебной необходимости – права доступа предоставляются только к тем данным, которые необходимы для выполнения должностных или договорных обязанностей [83].

#### **1.4.5 Концепция защиты средств вычислительной техники от несанкционированного доступа к информации**

В [65] говорится, что в средствах вычислительной техники (СВТ) должен применяться дискреционный или мандатный принцип контроля доступа.

Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т.е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).

### **1.5 Выводы по главе**

По итогам анализа предметной области было установлено, что для описания информационной системы чаще всего используются три следующих подхода:

- Цепи Маркова;
- Сети Петри;

— Диаграммы потоков данных – DFD.

Однако, ни один из подходов не описывает канал передачи как структурный элемент системы, не описывает его характеристики и, следовательно, не учитывают гетерогенность канала в компьютерной сети.

В ходе анализа рассмотренных моделей угроз информации, были обнаружены следующие недостатки:

— отсутствие единого подхода, каждая модель удовлетворяет только требованиям своей предметной области;

— в некоторых моделях угроз учитывается модель нарушителя, что по мнению автора не является корректным;

— модели основываются на субъективном мнении эксперта.

В результате анализа упомянутых моделей нарушителя были выявлены их недостатки и определены сложности, на которые следует обратить внимание при разработке собственной модели нарушителя:

— некоторые модели рассматривают нарушителя исключительно как злоумышленника, как следствие в моделях мало упоминаний случайных ошибок, действий стихийного характера и природных явлений;

— модели представляют из себя описание примеров действий нарушителя, формулировки нередко многословны и сложны для восприятия;

— отсутствует универсальность разработанных моделей, например, модель нельзя применить к системе, описываемой в работе и наоборот;

— обширное использование лингвистических шкал оценок, что недопустимо для корректной оценки возможностей нарушителя.

На основании обзора способов формирования политик разграничения доступа было установлено, что в них:

— отсутствие методики как таковой, присутствуют только краткие методические рекомендации;

— когда заходит речь о разграничении доступа, говорится, что оно должно основываться на политике разграничения доступа, однако, нигде не

указано как именно она должна быть сформирована и что должна в себя включать.

В связи с тем, что в каждом из затронутых вопросов обзор аналогов выявил определенные недостатки, было принято решение разработать собственный набор моделей, каждая из которых учитывала бы недостатки существующих решений.

## 2 Модель элементарных информационных потоков

Информация сегодня – важный ресурс, потеря которого чревата неприятными последствиями. Документооборот – движение документов в организации с момента их создания или получения до завершения исполнения или отправления, юбую схему документооборота можно представить, как совокупность информационных потоков [85].

Информационный поток – это совокупность циркулирующих в рамках системы, а также между системой и внешней средой сообщений, необходимых для контроля и управления действиями. Необходимость применения модели информационных потоков не раз подчеркивалась в различных исследованиях [86-98]. Однако, как и во многих других случаях, касающихся вопроса обеспечения информационной безопасности, данная тема остаётся открытой ввиду отсутствия типизации [99]. В данной работе предлагается своя версия применения модели информационных потоков для обеспечения информационной безопасности.

### 2.1 Построение модели элементарных информационных потоков

Любую схему обмена информацией можно представить, как совокупность элементарных информационных потоков. Элементарный информационный поток включает в себя три элемента: две вершины и канал взаимодействия.

Данное понятие можно продемонстрировать, применив теорию графов [100]. Введём следующие обозначения:  $V$  – множество носителей информации (множество вершин графа),  $E$  – множество каналов взаимодействия (множество рёбер графа). Сопоставив любые два элемента из  $V$  и один из  $E$ , мы получим элементарный информационный поток в виде неориентированного графа с двумя вершинами (рис. 2.1).



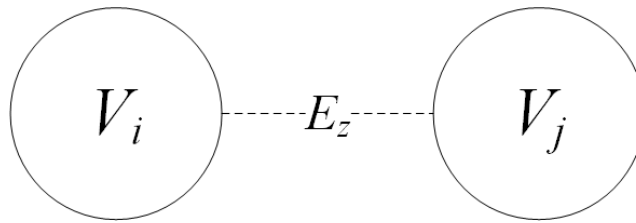


Рисунок 2.1 – Элементарный информационный поток.

Нотация информационных потоков основана на нотации теории графов [101]. Указанный выше информационный поток описывается тройкой:

$$g = \{V_i, E_z, V_j\},$$

где  $V_i, V_j$  – возможный носитель информации;

$E_z$  – возможный канал передачи информации.

Множество носителей информации было разделено на три подмножества и приобрело вид:

$$V = \{V_1, V_2, V_3\},$$

где  $V_1$  – множество пользователей,

$V_2$  – множество программного обеспечения,

$V_3$  – множество устройств хранения информации

Так как рамки исследования ограничены взаимодействием в киберпространстве, считается, что пользователь осуществляет взаимодействие с ПО средствами операционной системы. А каналы взаимодействия между пользователем и ПО являются каналами взаимодействия между операционной системой и ПО. Чтобы конкретизировать множество каналов передачи информации, следует обратиться к модели OSI [102].

Изучив все уровни взаимодействия и используемые протоколы, можно разделить их на определенные группы. Первая классификация следует из определения самих уровней – каналы связи можно разделить на локальные и удаленные. Вторая классификация вытекает из особенностей работы протоколов и устройств на различных уровнях – каналы можно разделить на работающие в виртуальной и электромагнитной среде. Тогда множество каналов взаимодействия приобретет следующий вид:

$$E = \{E_1, E_2, E_3, E_4\},$$

где  $E_1$  – множеств каналов взаимодействия в электромагнитной среде (поле передачи данных),

$E_2$  – множеств каналов взаимодействия в виртуальной среде (виртуальное адресное пространство),

$E_3$  – множество каналов удаленного взаимодействия в электромагнитной среде,

$E_4$  – множество каналов удаленного взаимодействия в виртуальной среде.

Также необходимо ввести дополнительные ограничения:

— элементы множества  $V_1$  не могут напрямую взаимодействовать с другими элементами этого же множества;

— элементы множества  $V_3$  не могут напрямую взаимодействовать с другими элементами этого же множества;

— элементы множества  $V_1$  не могут напрямую взаимодействовать с элементами множества  $V_3$  и наоборот;

— удаленные каналы доступны только при взаимодействии элементов множества  $V_2$  с элементами этого же множества.

Учитывая всё вышесказанное, множество всех элементарных потоков будет иметь следующий вид

$$G = \{g_i \mid g \in G\}, i = \overline{1, 8}$$

$$g_1 = \{V_1, e_1, V_2\},$$

$$g_2 = \{V_1, e_2, V_2\},$$

$$g_3 = \{V_2, e_1, V_2\},$$

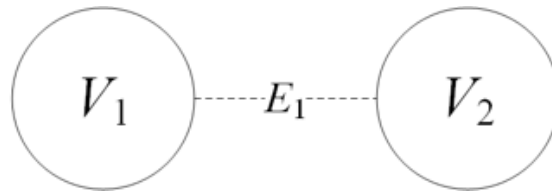
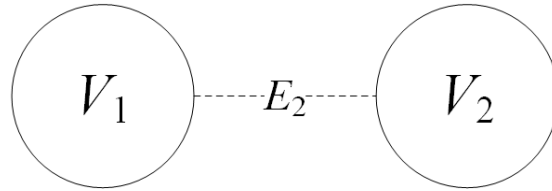
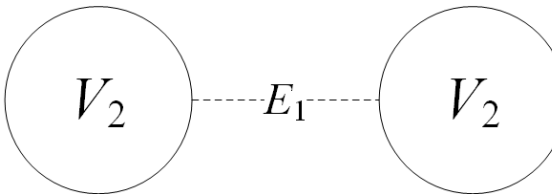
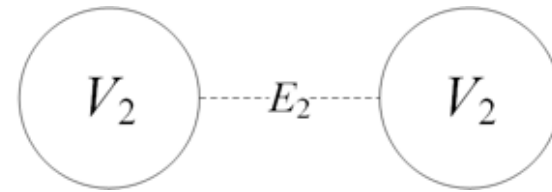
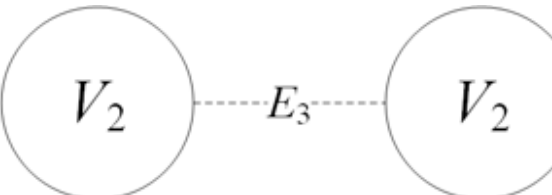
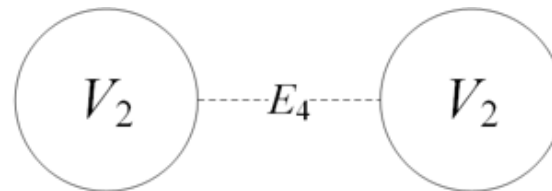
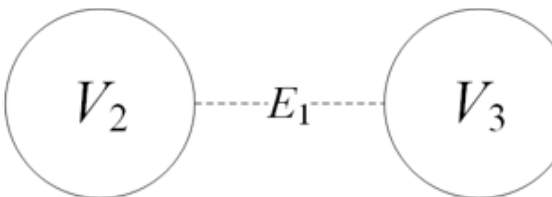
$$g_4 = \{V_2, e_2, V_2\},$$

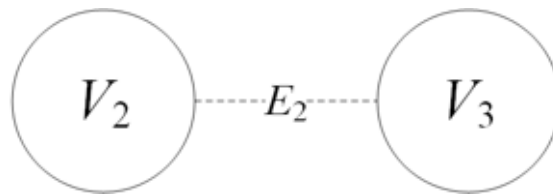
$$g_5 = \{V_2, e_3, V_2\},$$

$$g_6 = \{V_2, e_4, V_2\},$$

$$g_7 = \{V_2, e_1, V_3\},$$

$$g_8 = \{V_2, e_2, V_3\}.$$

Рисунок 2.2 – Поток  $g_1 = \{V_1, E_1, V_2\}$ Рисунок 2.3 – Поток  $g_3 = \{V_1, E_2, V_2\}$ Рисунок 2.4 – Поток  $g_3 = \{V_2, E_1, V_2\}$ Рисунок 2.5 – Поток  $g_4 = \{V_2, E_2, V_2\}$ Рисунок 2.6 – Поток  $g_5 = \{V_2, E_3, V_2\}$ Рисунок 2.7 – Поток  $g_6 = \{V_2, E_4, V_2\}$ Рисунок 2.8 – Поток  $g_7 = \{V_2, E_1, V_3\}$

Рисунок 2.9 – Поток  $g_8 = \{V_2, E_2, V_3\}$ 

Результатом объединения всех указанных выше графов будет являться ненаправленный мультипликативный граф (рис. 2.10), который и будет представлять из себя модель элементарных информационных потоков при осуществлении доступа к электронными информационным ресурсам [103].

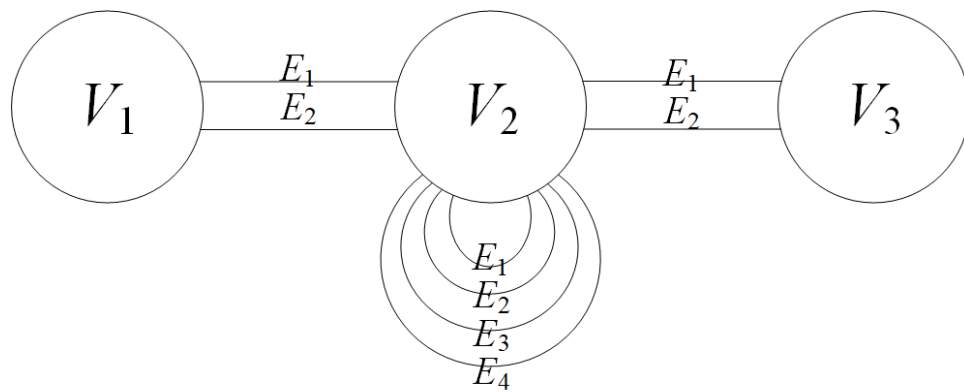


Рисунок 2.10 – Ненаправленный мультипликативный граф.

Данная модель позволяет построить схему информационных потоков в информационной системе, используя конечное множество элементарных информационных потоков  $G$ .

## 2.2 Пример использования модели

Продемонстрируем применение модели элементарных информационных потоков на примере процесса передачи/получения электронной почты. Переписка осуществляется между двумя пользователями с их мобильных устройств, которые подключены к сети Интернет беспроводным соединением (общая схема описываемого процесса представлена на рисунке 2.11).

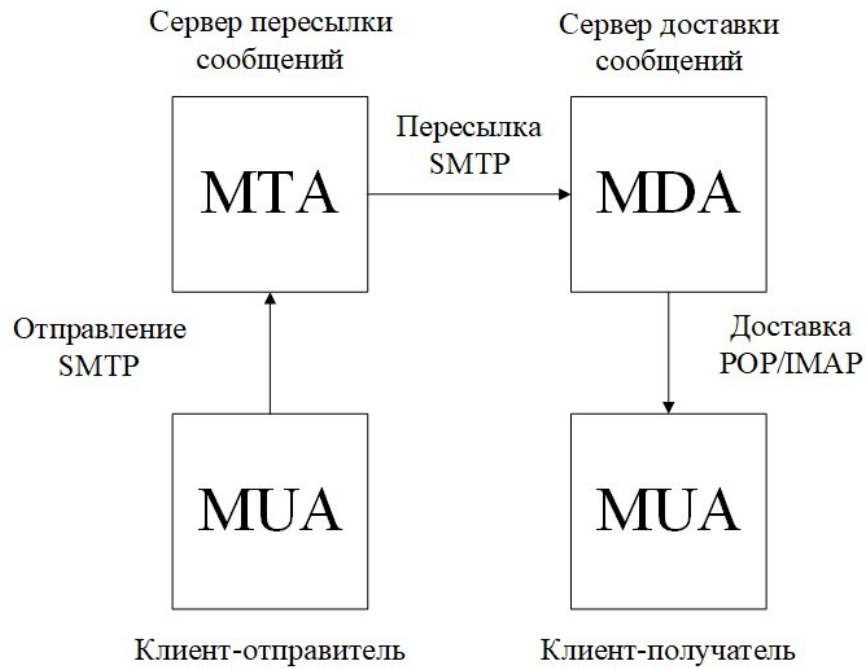


Рисунок 2.11 – Общая схема процесса передачи электронной почты

Общее описание процесса передачи/получения электронной почты:

- первый пользователь отправляет письмо на почтовый сервер своего провайдера;
- почтовый провайдер отправляет письмо на сервер провайдера получателя;
- сервер провайдера получателя передает письмо получателю.

Чтобы составить полный перечень информационных потоков, добавим еще несколько пояснений к описанию процесса:

- письмо имеет только текстовую составляющую и набирается пользователем;
- Mail Transfer Agent (MTA) не хранит сообщения у себя, он только передает их на Mail Delivery Agent (MDA);
- MDA (как и MTA) – это некий программно-аппаратный комплекс, который состоит из программного средства пересылки сообщений и хранилища данных; в нашем случае осуществляется взаимодействие между

мобильным почтовым клиентом и серверным ПО, которое уже взаимодействует с серверным хранилищем;

— взаимодействие между почтовым клиентом получателя и MDA осуществляется по протоколу IMAP.

Из всего сказанного выше, следует следующий перечень информационных потоков:

1. Отправитель – Mail User Agent (MUA);
2. MUA – MTA;
3. MTA – MDA;
4. MDA – Серверное хранилище;
5. Серверное хранилище – MDA;
6. MDA – MUA;
7. MUA – Получатель.

Основываясь на перечне информационных потоков и учитывая, что MDA и MTA – это разные устройства, построим полный перечень элементарных информационных потоков. Каждый поток разбивается на два элементарных, так как модель подразумевает разделение канала передачи данных на электромагнитный и виртуальный. Дополнительно введем обозначения всех участников процесса согласно модели элементарных информационных потоков.

Множество пользователей:

$$V_1 = \{ v_1^1, v_1^2 \}, \quad (5)$$

где  $v_1^1$  – отправитель;  $v_1^2$  – получатель.

Множество процессов:

$$V_2 = \{ v_2^1, v_2^2, v_2^3, v_2^4 \}, \quad (6)$$

где  $v_2^1$  – MUA отправителя;  $v_2^2$  – MTA;  $v_2^3$  – MDA;  $v_2^4$  – MUA получателя.

Множество хранилищ информации:

$$V_3 = \{ v_3^1 \}, \quad (7)$$

где  $v_3^1$  – серверное хранилище (база данных).

Множества каналов взаимодействия:

$$E_1 = \{e_1^1\}, E_2 = \{e_2^1\}, E_3 = \{e_3^1\}, E_4 = \{e_4^1\}.$$

Итоговое множество элементарных информационных потоков будет иметь следующий вид:

$$S = \{s_i | s \in S\}, i = \overline{1, 14} \quad (8)$$

$$\begin{aligned} \text{где } s_1 = (v_1^1, e_1^1, v_2^1), s_2 = (v_1^1, e_1^1, v_2^1), s_3 = (v_2^1, e_3^3, v_2^2), s_4 = (v_2^1, e_4^4, v_2^2), s_5 = (v_2^2, e_3^3, v_2^3), \\ s_6 = (v_2^2, e_3^3, v_2^3), s_7 = (v_2^3, e_1^1, v_3^1), s_8 = (v_2^3, e_2^2, v_3^1), s_9 = (v_3^1, e_1^1, v_2^3), s_{10} = (v_3^1, e_2^2, v_2^3), \\ s_{11} = (v_2^3, e_3^3, v_2^4), s_{12} = (v_2^3, e_4^4, v_2^4), s_{13} = (v_2^4, e_1^1, v_1^2), s_{14} = (v_2^4, e_2^2, v_1^2). \end{aligned}$$

Весь процесс передачи информации можно описать с помощью набора элементарных информационных потоков, которые в совокупности и формируют полную схему информационных потоков.

Так, на примере процесса отправки/получения электронной почты была проиллюстрирована работа модели элементарных информационных потоков. Данный разбор показывает, что применение модели позволяет разбить любой процесс передачи информации на конечное множество элементарных информационных потоков, при этом единственная сложность заключается в правильном описании множеств элементов системы. Чем полнее и точнее описаны множества элементов, тем более подробной будет и схема потоков. Из этого следует ещё один тезис, связанный с применением разработанной модели: эксперт в любом случае субъективен, полностью избавиться от субъективизма не представляется возможным, но можно сместить его в относительно менее критичную сторону – правильное и полное описание системы с учетом всех её элементов вместо бессистемного определения вероятных угроз.

Необходимо отметить следующее: можно заметить, что в рассматриваемом примере присутствует четырнадцать информационных потоков, в то время как в модели элементарных информационных потоков их только восемь. Дело в том, что модель по определению носит абстрактный характер, а каждый её информационный поток может быть представлен бесконечным множеством примеров из реальной жизни.

Учитывая симметричность потоков и принадлежность вершин к одним и тем же множествам, можно однозначно сопоставить все элементы множества  $S$  элементам множества  $G$ :

—  $g_1 \sim s_1, s_{13}$ ;

—  $g_2 \sim s_2, s_{14}$ ;

—  $g_5 \sim s_3, s_5, s_6, s_{11}$ ;

—  $g_6 \sim s_4, s_{12}$ ;

—  $g_7 \sim s_7, s_9$ ;

—  $g_8 \sim s_8, s_{10}$ .

Из этого следует, что любой процесс передачи информации в системе можно свести к конечному множеству элементарных информационных потоков. Мощность этого множества равна восьми, т. е. все каналы любой системы передачи электронной информации можно описать с помощью конечного множества элементов. Несомненно, такого описания не хватит для большинства нужд, связанных с использованием информационных систем, однако в контексте защиты информации и определения перечня типовых угроз информации такого описания будет более чем достаточно.

### 2.3 Выводы по главе

Результаты работы, представленные в настоящей главе:

— предложена мультиграфовая модель элементарных информационных потоков в информационной системе, отличающаяся учетом гетерогенности каналов взаимодействия;

— модель элементарных информационных потоков позволяет описать гетерогенную компьютерную систему с помощью конечного множества элементов;

— схема элементарных информационных потоков включает в себя все возможные потоки, которые могут возникнуть в системе.



### 3 Модель угроз информации

Защита информации требует комплексный подход. Необходимо затронуть все возможные аспекты в области защиты информации, в частности, определить полный перечень угроз и в будущем использовать данный перечень угроз с конкретной системой. Модель угроз является основой для проектирования систем защиты информационных систем. Важна именно полнота перечня угроз, так как при отсутствии какого-либо элемента вероятность реализации угрозы резко возрастает [104]. Таким образом, необходимо формирование модели угроз, способной предоставить полноценный перечень угроз.

Основной проблемой является то, что на сегодняшний день все имеющиеся модели носят весьма условный характер. Нет единого принципа построения модели угроз. Существует множество подходов и каждый из них трактуется по-своему: отсутствие четкого понятия «модели угроз», разительное отличие структур и принципов функционирования моделей, способов применения модели, избыточность модели в виде слияния с моделью нарушителя и многое другое. Наличие в совокупности рассмотренных недостатков отрицательно сказывается на эффективности работы эксперта с самой моделью и на конечном результате, обусловленном отсутствием стандартизованных итоговых оценок одной модели угроз относительно другой.

Вследствие всего вышесказанного была поставлена задача создания собственной модели угроз информации.

#### 3.1 Описание несанкционированных потоков

Принцип построения модели угроз основан на разработанной модели элементарных информационных потоков, а именно на понятии элементарного информационного потока. Снова обратимся к определению элементарного информационного потока, который описывается тройкой:

$$g = \{V_i, E_z, V_j\}, \quad (9)$$

где  $V_i$ ,  $V_j$  – множества носителей информации;  $E_z$  – множество каналов передачи информации.

Канал передачи информации – это не какой-то абстрактный объект, а вполне реальный элемент системы, который обладает некоторыми физическими и/или виртуальными свойствами. Из этого следует, что к нему возможен такой же доступ, как и к двум другим элементам потока.

Обозначим и классифицируем виды воздействия. Согласно [105] несанкционированное воздействие на информацию – это воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Само определение несанкционированного доступа подразумевает появление в системе нового элемента, который будет осуществлять этот самый доступ.

Используя обозначенную ранее нотацию, данную ситуацию можно изобразить следующим образом (рис. 3.1).

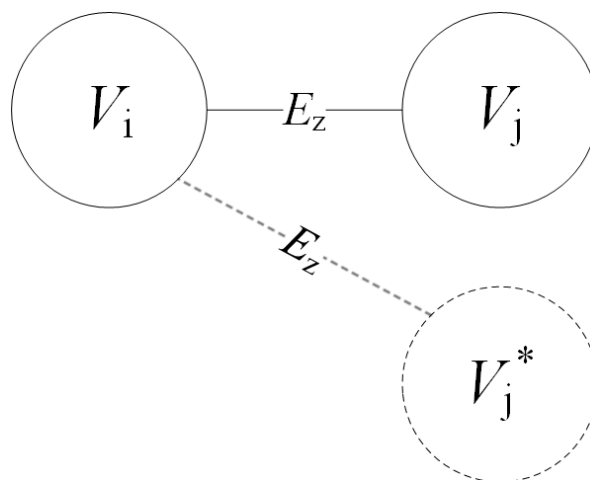


Рисунок 3.1 – Возникновение несанкционированного элемента  $V_j^*$ , который получает информацию из элемента  $V_i$

Аналогичная ситуация возможна для любого элемента информационного потока. По аналогии с описанной выше ситуацией (рис. 3.1) доступ может быть осуществлен как к элементу множества  $V_j$  (рис. 3.2), так и к  $E_z$  (рис. 3.3).

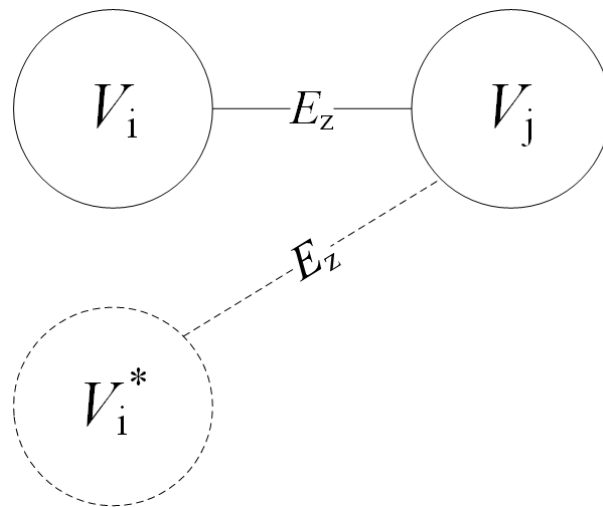


Рисунок 3.2 – Возникновение несанкционированного элемента  $V_i^*$ , который получает информацию из элемента  $V_j$

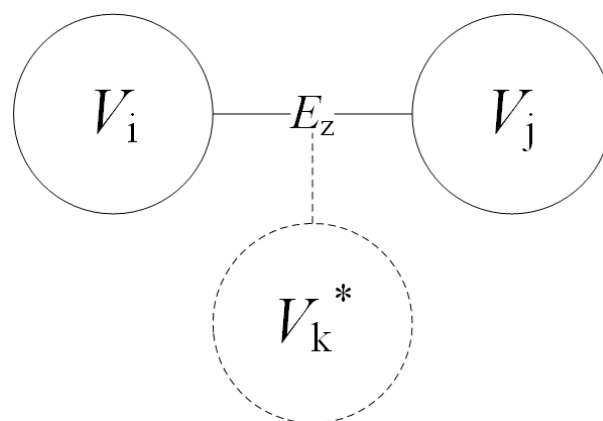


Рисунок 3.3 – Возникновение несанкционированного элемента  $V_k^*$ , который получает информацию из элемента  $E_z$

На данном этапе необходимо внести определенную ясность: взаимодействие с элементами элементарного информационного потока приводит к угрозам нарушения целостности и доступности, а взаимодействие с информацией, циркулирующей в этом потоке, к угрозам нарушения конфиденциальности [106].

Не все авторы уделяют внимание этому обстоятельству в своих работах. В большинстве случаев говорится о состоянии безопасности

информационного потока [107-109], без классификации возможных воздействий и последствий, что является необходимым ввиду разной природы происхождения воздействия [110-112].

### **3.2 Модель угроз целостности и доступности**

Три вышеуказанные модели описывают ситуации, при которых оказывается непосредственное воздействие на один из элементов информационного потока, что может привести к искажению информации или её уничтожению.

Из всего вышесказанного следует, что на любой из элементов элементарного информационного потока, а значит и на информацию, может быть оказано любой из трёх видов несанкционированного воздействия:

- уничтожение;
- искажение;
- подмена.

Снова обратимся к понятию элементарного информационного потока и разберём взаимосвязь между видами воздействия на элементы потока с классическими аспектами информационной безопасности: целостностью и доступностью.

Применительно к вершинам потока:

- уничтожение информации на одной из вершин приводит к нарушению целостности информации;
- искажение информации на одной из вершин приводит к нарушению целостности информации;
- подмена информации на одной из вершин приводит к нарушению целостности информации.

Применительно к каналу передачи информации:

- уничтожение информации в канале приводит к нарушению доступности;

— искажение информации в канале приводит к нарушению целостности;

— подмена информации в канале приводит к нарушению доступности.

Итого: четыре угрозы целостности и две – доступности. Необходимо обратить внимание, что информационный поток имеет две симметричные вершины, и воздействие может быть оказано на любую из них, что приводит к тому, что количество угроз целостности, направленных на вершины, вырастает вдвое, а значит итоговое их число становится равно семи. Таким образом, разобрав все возможные виды воздействия на информационный поток, можно построить полное множество типовых угроз целостности и доступности информации

Обозначим множество угроз целостности:

$$C = \{c_i | c \in C\}, i = \overline{1, 7}, \text{ где} \quad (10)$$

где  $c_1, c_2, c_3, c_4, c_5, c_6, c_7$  – типовые угрозы целостности информации.

Разберём каждую из них подробнее:

$c_1$  – подмена источника  $V_i$  (передача искаженной информации элементу  $V_j$ ), рисунок 3.4;

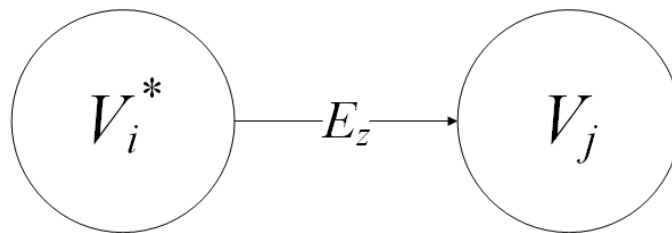


Рисунок 3.4 – Вид информационного потока при подмене источника  $V_i$

$c_2$  – подмена источника  $V_j$  (передача искаженной информации элементу  $V_i$ ), рисунок 3.5;

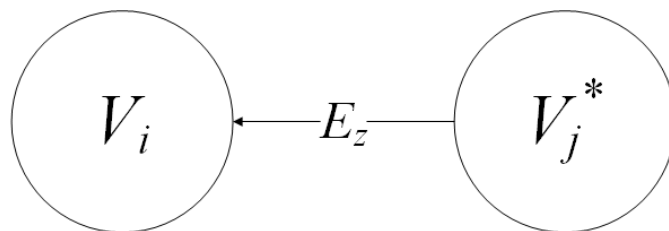


Рисунок 3.5 – Вид информационного потока при подмене источника  $V_j$

$c_3$  – подмена источника  $V_i$  (уничтожение информации в элементе  $V_j$ ),  
 рисунок 3.6;

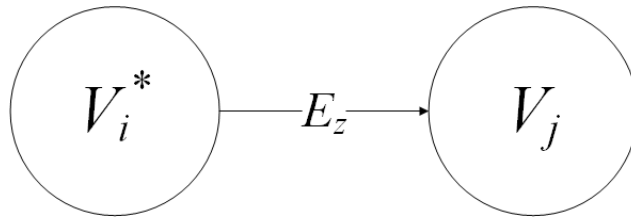


Рисунок 3.6 – Вид информационного потока при подмене источника  $V_i$

$c_4$  – подмена источника  $V_j$  (уничтожение информации в элементе  $V_i$ ),  
 рисунок 3.7;

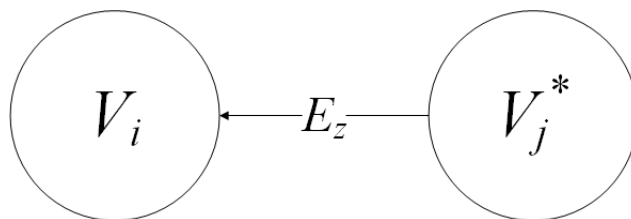


Рисунок 3.7 – Вид информационного потока при подмене источника  $V_j$

$c_5$  – подмена источника  $V_i$  (подмена информации в элементе  $V_j$ ), рисунок  
 3.8;

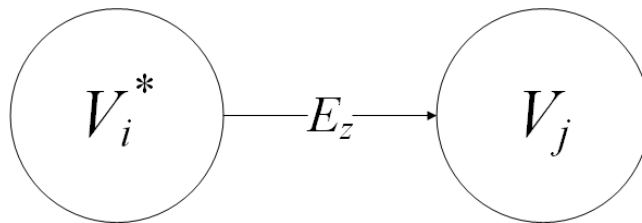


Рисунок 3.8 – Вид информационного потока при подмене источника  $V_i$

$c_6$  – подмена источника  $V_j$  (подмена информации в элементе  $V_i$ ), рисунок  
 3.9;

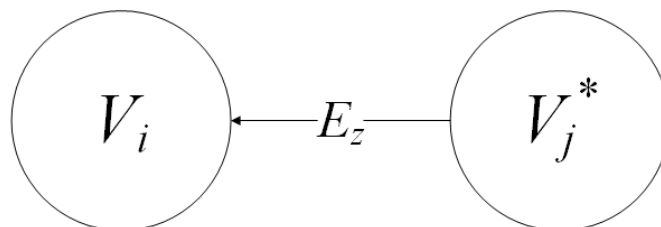


Рисунок 3.9 – Вид информационного потока при подмене источника  $V_j$

$c_7$  – воздействие на информацию при передаче по каналу  $E_z$  (искажение  
 информации в канале), рисунок 3.10;

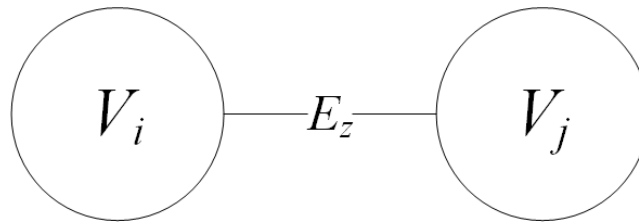


Рисунок 3.10 – Вид информационного потока при воздействии на информацию в канале  $E_z$

Обозначим множество угроз доступности:

$$D = \{d_1, d_2\},$$

где  $d_1, d_2$  – типовые угрозы конфиденциальности информации.

Разберём каждую из них подробнее:

$d_1$  – неработоспособность канала  $E_z$  - перегрузка, уничтожение, невозможность установить связь с носителем информации (полное отсутствие доступа к информации санкционированным лицом), рисунок 3.11;



Рисунок 3.11 – Вид информационного потока при неработоспособном канале  $E_z$

$d_2$  – «зашумленность» канала  $E_z$  - помехи (частичный доступ к информации санкционированным лицом), рисунок 3.12.

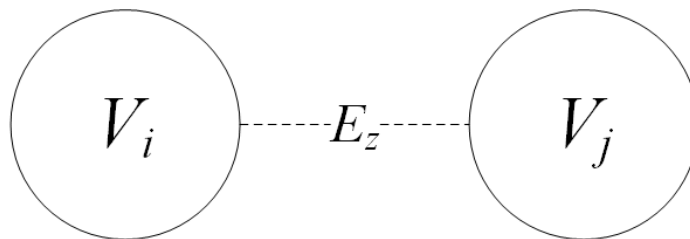


Рисунок 3.12 – Вид информационного потока при «зашумленном» канале  $E_z$

Снова обратимся к примеру с отправлением электронной почты и посмотрим, как можно применить к нему типовые угрозы, обозначенные выше.

Рассмотрим первый поток  $s_1 = (v_1^1, e_1^1, v_2^1)$ . Напомним:  $v_1^1$  – пользователь-отправитель,  $e_1^1$  – электромагнитный канал,  $v_2^1$  – Mail User Agent (MUA).

Применим каждую из четырех угроз к данному потоку. Опять же вспомним, что соединительный канал в потоке симметричен и соответственно двунаправлен.

При реализации угрозы  $c_1$  осуществляется подмена пользователя  $v_1^1$  несанкционированным пользователем  $v_1^{1*}$ , в результате чего этот элемент может внести искажения в информацию, которая хранится в элементе  $v_2^1$ . Примером реализации угрозы может служить передача телефона третьему лицу. Несанкционированный пользователь может от лица санкционированного отправить письмо с измененной информацией.

При реализации угрозы  $c_2$  осуществляется подмена почтового клиента  $v_2^1$  несанкционированным софтом  $v_2^{1*}$ , в результате чего санкционированный пользователь  $v_1^1$  может получить искаженную информацию. Примером может служить установка приложения из непроверенного источника.

При реализации угрозы  $c_3$  осуществляется подмена пользователя  $v_1^1$  несанкционированным пользователем  $v_1^{1*}$ , в результате чего этот элемент может уничтожить информацию, которая хранится в элементе  $v_2^1$ . Примером реализации угрозы может служить передача телефона третьему лицу. Несанкционированный пользователь с помощью почтового клиента может удалить важные письма.

При реализации угрозы  $c_4$  осуществляется подмена почтового клиента  $v_2^1$  несанкционированным софтом  $v_2^{1*}$ , в результате чего будет уничтожена информация, с которой пользователь непосредственно взаимодействует. Примером может служить установка приложения из непроверенного источника.

При реализации угрозы  $c_5$  осуществляется подмена пользователя  $v_1^1$  несанкционированным пользователем  $v_1^{1*}$ , в результате чего этот элемент может подменить информацию, которая хранится в элементе  $v_2^1$ . Примером реализации угрозы может служить передача телефона третьему лицу.



Несанкционированный пользователь может от лица санкционированного отправить письмо с полностью измененной информацией.

При реализации угрозы  $c_6$  осуществляется подмена почтового клиента  $v_2^1$  несанкционированным софтом  $v_2^{1*}$ , в результате чего санкционированный пользователь  $v_1^1$  может получить полностью неверную информацию. Примером может служить установка приложения из непроверенного источника.

При реализации угрозы  $c_7$  осуществляется воздействие на информацию в канале связи  $e_1^1$ . В данном случае каналом связи является устройство ввода/вывода, которое, учитывая нынешние реалии, вероятнее всего является сенсорным экраном. Примером может служить аппаратная закладка, которая искажает вывод информации на экран, например, меняет отображаемый цвет.

При реализации угрозы  $d_1$  осуществляется воздействие на канале связи  $e_1^1$ , в результате чего санкционированный пользователь не может получить доступ к этой информации. Если в качестве примера снова взять экран мобильного устройства, то примером реализации угрозы может послужить банальная неработоспособность экрана. Информация не скомпрометирована, но пользователь не может получить к ней доступ.

При реализации угрозы  $d_2$  осуществляется воздействие на канале связи  $e_1^1$ , в результате чего санкционированный пользователь не может получить доступ к в полном объеме информации. Возвращаясь всё к тому же примеру с экраном, примером реализации угрозы может являться частичная неработоспособность устройства вывода в результате действия закладок.

Аналогичный подбор примеров реализации угроз можно подобрать и для любого другого потока и его элементов, однако мы не будем приводить здесь данные разборы, т. к. этот процесс однообразен и при этом уже не позволит глубже отразить суть работы модели угроз.

Теперь снова вернемся к множеству элементарных информационных потоков и множеству угроз целостности и доступности. Зная, что оба эти множества конечны, мы можем применить каждую из угроз к каждому потоку,

т. е. сопоставить каждый элемент множеств  $C$  и  $D$  с каждым элементом множества  $G$  и получить новое множество, которое будет состоять из всех сочетаний угроз и потоков, т. е. являться их декартовым произведением (12).

$$G \times (C \cup D) = \{ \begin{array}{l} g_1c_1, g_1c_2, g_1c_3, g_1c_4, g_1c_5, g_1c_6, g_1c_7, g_1d_1, g_1d_2, \\ g_2c_1, g_2c_2, g_2c_3, g_2c_4, g_2c_5, g_2c_6, g_2c_7, g_2d_1, g_2d_2, \\ g_3c_1, g_3c_2, g_3c_3, g_3c_4, g_3c_5, g_3c_6, g_3c_7, g_3d_1, g_3d_2, \\ g_4c_1, g_4c_2, g_4c_3, g_4c_4, g_4c_5, g_4c_6, g_4c_7, g_4d_1, g_4d_2, \\ g_5c_1, g_5c_2, g_5c_3, g_5c_4, g_5c_5, g_5c_6, g_5c_7, g_5d_1, g_5d_2, \\ g_6c_1, g_6c_2, g_6c_3, g_6c_4, g_6c_5, g_6c_6, g_6c_7, g_6d_1, g_6d_2, \\ g_7c_1, g_7c_2, g_7c_3, g_7c_4, g_7c_5, g_7c_6, g_7c_7, g_7d_1, g_7d_2, \\ g_8c_1, g_8c_2, g_8c_3, g_8c_4, g_8c_5, g_8c_6, g_8c_7, g_8d_1, g_8d_2 \end{array} \} \quad (12)$$

Посчитаем мощность итогового множества (13).

$$|G| * (|C| + |D|) = 8 * (7+2) = 72 \quad (13)$$

Из этого следует, что по аналогии с описанием множества информационных потоков мы можем свести множество угроз целостности и доступности информации в системе к конечному множеству типовых угроз, мощность которого равна семидесяти двум.

Учитывая, что множество  $V$  в модели элементарных информационных потоков из раздела 2.1 имеет три подмножества, многие конкретные типовые угрозы будут отличаться для разных информационных потоков в зависимости от фактической принадлежности вершин к различным множествам  $V$ . Потому необходимо конкретизировать описание типовых угроз для каждого из девяти возможных элементарных информационных потоков, которые описаны в модели. Так же для большего удобства в дальнейшем необходимо дать уникальное наименование для каждой типовой угрозы. Результат данных действий представлен в таблицах 3.1-3.8

Таблица 3.1 – Типовые угрозы для потока  $g_l = (V_1, e_1, V_2)$ 

	Описание угрозы	Пример	
$c_1$	Передача н/с информации санкционированному процессу	искажение электромагнитной информации в результате некорректной работы устройств ввода/вывода	$g_{1c_1}$
$c_2$	Передача н/с процессом информации санкционированному пользователю	искажение электромагнитной информации в результате некорректной работы устройств ввода/вывода	$g_{1c_2}$
$c_3$	Уничтожение информации, обрабатываемой процессом	искажение электромагнитной информации в результате некорректной работы запоминающих устройств	$g_{1c_3}$
$c_4$	Уничтожение информации, обрабатываемой пользователем		$g_{1c_4}$
$c_5$	Подмена информации, обрабатываемой процессом	передача программе заведомо ложных или некорректных данных	$g_{1c_5}$
$c_6$	Подмена информации, обрабатываемой пользователем		$g_{1c_6}$
$c_7$	Воздействие на информацию при ее передаче по каналу в электромагнитной среде	неисправность контроллера (ошибки в работе) устройств ввода/вывода; некорректная работа элементов устройств ввода/вывода	$g_{1c_7}$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	выход из строя платы контроллера устройств ввода/вывода; неисправность аппаратных интерфейсов подключения и работы устройств ввода/вывода	$g_{1d_1}$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	частичная утрата работоспособности платы контроллера устройств ввода/вывода; неполадки аппаратных интерфейсов подключения и работы устройств ввода/вывода	$g_{1d_2}$

Таблица 3.2 – Типовые угрозы для потока  $g_2 = (V_1, e_2, V_2)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Передача н/с информации санкционированному процессу	ввод некорректных данных	$g_2c_1$
$c_2$	Передача н/с процессом информации санкционированному пользователю	дезинформация санкционированного лица	$g_2c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	ошибка в работе запоминающих устройств	$g_2c_3$
$c_4$	Уничтожение информации, обрабатываемой пользователем		$g_2c_4$
$c_5$	Подмена информации, обрабатываемой процессом	передача программе заведомо ложных или некорректных данных	$g_2c_5$
$c_6$	Подмена информации, обрабатываемой пользователем	дезинформация санкционированного лица	$g_2c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в виртуальной среде	использование некачественного драйвера-нестабильная работа устройств ввода/вывода	$g_2c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	отсутствие необходимого драйвера устройств ввода/вывода	$g_2d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	неполадки в работе драйвера устройства ввода/вывода	$g_2d_2$

Таблица 3.3 – Типовые угрозы для потока  $g_3 = (V_2, e_1, V_2)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Передача н/с процессом информации санкционированному процессу	подмены адреса процесса-источника в оперативной памяти	$g_3c_1$
$c_2$	Передача н/с процессом информации санкционированному процессу	подмены адреса процесса-источника в оперативной памяти	$g_3c_2$

Таблица 3.3 (Окончание)

$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_3c_3$
$c_4$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_3c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процессор-приемника в оперативной памяти	$g_3c_5$
$c_6$	Подмена информации, обрабатываемой процессом	подмены адреса процессор-приемника в оперативной памяти	$g_3c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в электромагнитной среде	нестабильная работа элементов оперативной памяти	$g_3c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	выход из строя элементов оперативной памяти	$g_3d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	неполадки в работе оперативной памяти - появление битых секторов	$g_3d_2$

Таблица 3.4 – Типовые угрозы для потока  $g_4 = (V_2, e_2, V_2)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Передача н/с процессом информации санкционированному процессу	подмены адреса процессор-источника	$g_4c_1$
$c_2$	Передача н/с процессом информации санкционированному процессу	подмены адреса процессор-источника	$g_4c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе драйвера запоминающего устройства	$g_4c_3$
$c_4$	Уничтожение информации, обрабатываемой процессом	неполадки в работе драйвера запоминающего устройства	$g_4c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процессор-приемника	$g_4c_5$

Таблица 3.4 (Окончание)

$c_6$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника	$g_4c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в виртуальной среде	некорректная работа средств межпроцессорного взаимодействия	$g_4c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	неработоспособность средств межпроцессорного взаимодействия – разделяемая память, сигналы, каналы	$g_4d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	ошибки при распределении средств межпроцессорного взаимодействия – разделяемая память, сигналы, каналы	$g_4d_2$

Таблица 3.5 – Типовые угрозы для потока  $g_5 = (V_2, e_3, V_2)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Удаленная передача н/с процессом информации санкционированному процессу	н/с изменение рабочих параметров ПО (удаленно)	$g_5c_1$
$c_2$	Удаленная передача н/с процессом информации санкционированному процессу	н/с изменение рабочих параметров ПО (удаленно)	$g_5c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_5c_3$
$c_4$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_5c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника в оперативной памяти	$g_5c_5$
$c_6$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника в оперативной памяти	$g_5c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в электромагнитной среде	ошибки в работе аппаратных интерфейсов подключения и работы сетевых устройств	$g_5c_7$

Таблица 3.5 (Окончание)

$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	перегрузка/повреждение линии связи; неисправность аппаратных интерфейсов подключения и работы сетевых устройств	$g_5d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	возникновение помех в линии связи; ошибки в работе сетевых устройств	$g_5d_2$

Таблица 3.6 – Типовые угрозы для потока  $g_6 = (V_2, e_4, V_2)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Удаленная передача н/с процессом информации санкционированному процессу	скрытое удаленное подключение к санкционированному ПО	$g_6c_1$
$c_2$	Удаленная передача н/с процессом информации санкционированному процессу	скрытое удаленное подключение к санкционированному ПО	$g_6c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе драйвера запоминающего устройства	$g_6c_3$
$c_4$	Уничтожение информации, обрабатываемой процессом	неполадки в работе драйвера запоминающего устройства	$g_6c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника	$g_6c_5$
$c_6$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника	$g_6c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в виртуальной среде	ошибки драйвера сетевой карты; потеря сетевых пакетов	$g_6c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	неполадки драйвера сетевых устройств; отсутствие необходимого протокола	$g_6d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	частичная утрата работоспособности канала – ошибка драйвера сетевых устройств	$g_6d_2$

Таблица 3.7 – Типовые угрозы для потока  $g_7 = (V_2, e_1, V_3)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Передача н/с информации процессу	считывание некорректной информации из н/с файла (загрузка эксплойта)	$g_7c_1$
$c_2$	Запись н/с информации на носитель информации	н/с изменение защищаемого файла (вредоносные, поддельные программы)	$g_7c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_4c_3$
$c_4$	Уничтожение информации, хранящейся на носителе информации	неполадки в работе постоянного запоминающего устройства	$g_4c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника в оперативной памяти	$g_4c_5$
$c_6$	Подмена информации, хранящейся на носителе информации	н/с изменение хранящейся на носителе информации	$g_4c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в электромагнитной среде	некорректная работа элементов записи/чтения цифрового носителя	$g_7c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	выход из строя устройств считывания/записи информации цифрового носителя	$g_7d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	частичная утрата работоспособности платы контроллера; элементов записи/чтения носителя; неполадки аппаратных интерфейсов подключения и работы устройств хранения информации; неполадки считывающей головки жёсткого диска	$g_7d_2$



Таблица 3.8 – Типовые угрозы для потока  $g_8 = (V_2, e_2, V_3)$ 

	Описание угрозы	Пример угрозы	
$c_1$	Передача н/с информации процессу	считывание некорректной информации из н/с файла (подмена файла)	$g_8c_1$
$c_2$	Запись н/с информации на носитель информации	н/с изменение защищаемого файла (вредоносные, поддельные программы)	$g_8c_2$
$c_3$	Уничтожение информации, обрабатываемой процессом	неполадки в работе оперативной памяти, неожиданное завершение работы ПО	$g_4c_3$
$c_4$	Уничтожение информации, хранящейся на носителе информации	неполадки в работе постоянного запоминающего устройства	$g_4c_4$
$c_5$	Подмена информации, обрабатываемой процессом	подмены адреса процесса-приемника в оперативной памяти	$g_4c_5$
$c_6$	Подмена информации, хранящейся на носителе информации	н/с изменение хранящейся на носителе информации	$g_4c_6$
$c_7$	Воздействие на информацию при ее передаче по каналу в виртуальной среде	использование некорректного драйвера носителя информации	$g_8c_7$
$d_1$	Отсутствие санкционированного доступа к информации в связи с невозможностью установки канала связи	неработоспособность драйвера устройств хранения	$g_8d_1$
$d_2$	Отсутствие санкционированного доступа к информации в связи с помехами в канале	неполадки в работе драйвера устройства хранения	$g_8d_2$

Таким образом был составлен перечень из 72-х типовых угроз целостности и доступности информации, обрабатываемой в компьютерной системе.

### 3.3 Модель угроз конфиденциальности

Если говорить исключительно о конфиденциальности информации, то по определению её нарушение безопасности не подразумевает нарушения целостности или доступности, хотя и может к этому привести [105]. Если

снова вернуться к понятию информационного потока, становится очевидным то, что нарушение конфиденциальности происходит при подмене любого из его элементов, т. е. возможны следующие случаи:

- подмена любой из двух вершин;
- подмена канала.

При этом возможны ситуации, когда будут скомпрометированы сразу несколько элементов. Теперь, зная общее количество элементов и количество состояний этих элементов, можно посчитать общее количество состояний элементарного информационного потока.

Для этого применим формулу расчета мощности множества:

$$N = p^i, \quad (14)$$

где  $p$  – количество состояний элемента;  $i$  – количество элементов.

В нашем случае  $p = 2$ , т. к. любой элемент потока может иметь два состояния – скомпрометирован или нет, а  $i = 3$ , т. к. элементарный информационный поток состоит из трёх элементов [113]. В итоге общее количество завязанных на компрометации элементов состояний элементарного информационного потока будет равняться восьми. Все возможные комбинации представлены в таблице 3.9. В ячейки таблицы занесена информация о статусе компрометации элемента, где «1» - элемент скомпрометирован, «0» - не скомпрометирован.

Таблица 3.9 – Перечень состояний информационного потока

$V_i$	$E_z$	$V_j$
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Однако, при построении модели угроз нет необходимости рассматривать составные варианты компоновки, т. к. такой подход приведёт к высокому уровню дублирования различных угроз, потому достаточным будет рассмотрение только четырёх базовых состояний: скомпрометирован элемент  $V_i$ , элемент  $V_j$ , элемент  $E_z$ .

Необходимо отдельно разобрать ситуацию, когда ни один из элементов системы не является скомпрометированным. Дело в том, что помимо простой подмены возможна ситуация так называемой «прослушки» элемента, т. е. доступ к хранимой в нём информации из-за пределов контролируемой зоны. Однако, «прослушка» уже не будет применима ко всем трём элементам, т. к. слежение за вершиной подразумевает либо внедрение в существующий канал передачи информации, что тождественно прослушиванию канала, либо возникновение нового неразрешенного, что совпадает с подменой канала, и всё же остается вариант, когда скомпрометирована может быть уже вся система целиком.

Таким образом, разобрав все возможные виды вмешательства в информационный поток, можно построить полное множество типовых угроз конфиденциальности информации

Обозначим множество угроз конфиденциальности:

$$K = \{k_1, k_2, k_3, k_4\}, \quad (15)$$

где  $k_1, k_2, k_3, k_4$  – типовые угрозы конфиденциальности информации.

Разберём каждую из них подробнее:

$k_1$  – подмена приемника  $V_i$  (получение защищаемой информации несанкционированным элементом  $V_i^*$ ), рисунок 3.12;

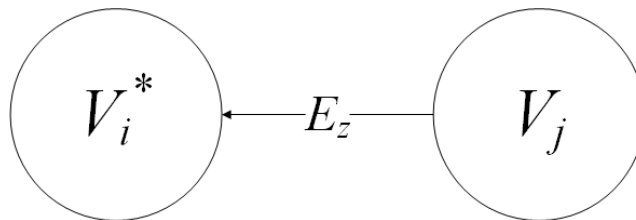


Рисунок 3.12 – Вид информационного потока при подмене приемника  $V_i$

$k_2$  – подмена приемника  $V_j$  (получение защищаемой информации несанкционированным элементом  $V_j^*$ ), рисунок 3.13;

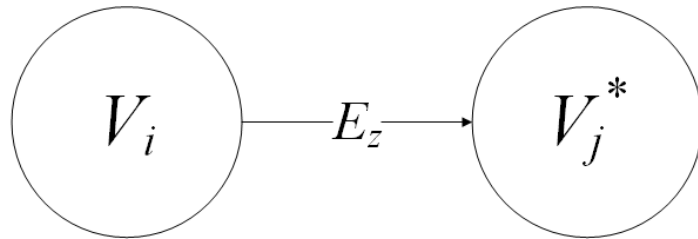


Рисунок 3.13 – Вид информационного потока при подмене приемника  $V_j$

$k_3$  – наличие несанкционированного канала  $E_z^*$  (подмена канала на н/с), рисунок 3.14;

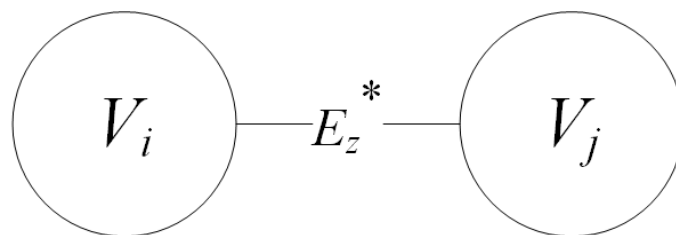


Рисунок 3.14 – Вид информационного потока при подмене канала связи  $E_z$

$k_4$  – контроль канала  $E_z$  (получение информации несанкционированным лицом из-за пределов санкционированной зоны), рисунок 3.15;

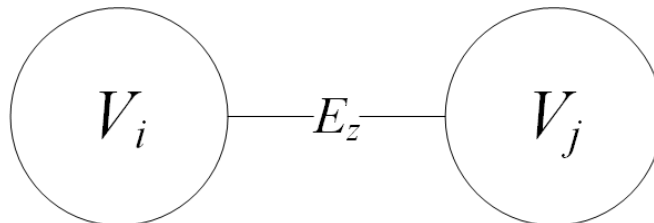


Рисунок 3.15 – Вид информационного потока при подмене канала связи  $E_z$

Снова обратимся к примеру с отправлением электронной почты и посмотрим, как можно применить к нему эти четыре типовые угрозы.

Для начала рассмотрим первый поток  $s_1 = (v_{11}, e_1, v_{21})$ . Напомним:  $v_1^1$  – это пользователь-отправитель,  $e_1$  – электромагнитный канал,  $v_2^1$  – Mail User Agent (MUA).

Применим каждую из четырех угроз к данному потоку. Опять же вспомним, что соединительный канал в потоке симметричен и соответственно двунаправлен.

При реализации угрозы  $k_1$  осуществляется подмена пользователя  $v_1^1$  несанкционированным пользователем  $v_1^{1*}$ , в результате чего этот элемент может получить доступ к конфиденциальной информации. Примером реализации угрозы может служить передача телефона третьему лицу. Несанкционированный пользователь может ознакомиться с информацией находящейся в канале передачи информации (набранный текст в интерфейсе ввода) или с помощью почтового клиента прочитать другие отправленные или полученные ранее письма.

При реализации угрозы  $k_2$  осуществляется подмена почтового клиента  $v_2^1$  несанкционированным софтом  $v_2^{1*}$ , в результате чего санкционированный пользователь  $v_1^1$  может передать конфиденциальную информацию постороннему программному средству. Примером может служить установка приложения из непроверенного источника.

При реализации угрозы  $k_3$  осуществляется подмена канала связи  $e_1$ . В данном случае каналом связи является устройство ввода/вывода, которое, учитывая нынешние реалии, вероятнее всего является сенсорным экраном. Примером реализации угрозы  $k_3$  является подмена устройства ввода/вывода: в ходе ремонта на сенсорный экран могли наложить дополнительную сенсорную панель по аналогии с накладными клавиатурами для банкоматов.

При реализации угрозы  $k_4$  не происходит непосредственное вмешательство в информационный канал, нет подмены ни одной из вершин или канала. Доступ к информации осуществляется извне. Примером реализации может служить установка аппаратной или программной закладки. Ведь по факту аппаратная закладка не подменяет ни один из элементов, она даже не вмешивается в их нормальную работу. Более того, примером реализации может послужить удаленное подглядывание, ни один из элементов элементарного информационного потока не был скомпрометирован, и всё же присутствует утечка информации за пределы системы.

По аналогии с моделью угроз целостности и доступности, ограничимся описанием угроз только для одного элементарного информационного потока.

Стоит добавить, что при реализации любой из угроз, конечно, есть вероятность и дальнейшего вмешательства в систему с последующим нарушением целостности и/или доступности, но данная модель подразумевает определение только начальных угроз, а не определение рисков или каскадного нарушения режима безопасности информации. Определение только первоочередных угроз – это не ограниченность модели, а отражение её превентивного характера.

Снова вернемся к множеству элементарных информационных потоков и множеству угроз конфиденциальности информации. Опять же по аналогии с моделью угроз целостности и доступности информации, соотнесем каждую типовую угрозу конфиденциальности с каждым элементарным информационным потоком, т.е. построим декартово произведение (16) множеств  $K$  и  $G$  и посчитаем итоговую мощность этого множества (17).

$$G \times K = \{ g_{1k_1}, g_{1k_2}, g_{1k_3}, g_{1k_4}, \\ g_{2k_1}, g_{2k_2}, g_{2k_3}, g_{2k_4}, \\ g_{3k_1}, g_{3k_2}, g_{3k_3}, g_{3k_4}, \\ g_{4k_1}, g_{4k_2}, g_{4k_3}, g_{4k_4}, \\ g_{5k_1}, g_{5k_2}, g_{5k_3}, g_{5k_4}, \\ g_{6k_1}, g_{6k_2}, g_{6k_3}, g_{6k_4}, \\ g_{7k_1}, g_{7k_2}, g_{7k_3}, g_{7k_4}, \\ g_{8k_1}, g_{8k_2}, g_{8k_3}, g_{8k_4} \} \quad (16)$$

$$|G \times K| = |G| * |K| = 8 * 4 = 32 \quad (17)$$

Из этого следует, что по аналогии с описанием множества информационных потоков мы можем свести множество угроз конфиденциальности информации в системе к конечному множеству типовых угроз, мощность которого равна тридцати двум.

Теперь классифицируем и дадим краткую характеристик определяемым типовым угрозам. Для удобства и читабельности множество типовых угроз было всё же разбито и сгруппировано по принадлежности к информационным

потокам из множества  $G$ . В следующих восьми таблицах представлена группировка и характеристики разбираемых типовых угроз.

В таблицах 3.12-3.15 первые две типовые угрозы попарно совпадают, т. к. данные потоки являются симметричными.

Таблица 3.10 – Типовые угрозы для потока  $g_1 = (V_1, e_1, V_2)$

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Передача санкционированным процессом информации н/с лицу.	Подмена учетной записи пользователя	$g_1k_1$
$k_2$	Прием н/с процессом информации от санкционированного лица	Использование н/с устройства	$g_1k_2$
$k_3$	Передача информации по н/с каналу в электромагнитной среде	Использование н/с или скомпрометированных устройств ввода/вывода;	$g_1k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Съем информации по ПЭМИН элементов аппаратных интерфейсов	$g_1k_4$

Таблица 3.11 – Типовые угрозы для потока  $g_2 = (V_1, e_2, V_2)$

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Передача санкционированным процессом информации н/с лицу.	Повышение прав учетной записи пользователя	$g_2k_1$
$k_2$	Прием н/с процессом информации от санкционированного лица	Использование н/с или скомпрометированного приложения	$g_2k_2$
$k_3$	Передача информации по н/с каналу в виртуальной среде	Использование н/с или скомпрометированных драйверов устройств ввода-вывода, аудио- и видеодрайвера	$g_2k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Чтение информации из буфера обмена	$g_2k_4$

Таблица 3.12 – Типовые угрозы для потока  $g_3 = (V_2, e_1, V_2)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Передача санкционированным процессом информации н/с процессу	Запись санкционированным процессом данных по н/с адресам в оперативной памяти	$g_3k_1$
$k_2$	Передача санкционированным процессом информации н/с процессу	Запись санкционированным процессом данных по н/с адресам в оперативной памяти	$g_3k_2$
$k_3$	Передача информации по н/с каналу в электромагнитной среде	Считывание информации с помощью аппаратных закладок	$g_3k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Съем информации по ПЭМИН с элементов оперативной памяти	$g_3k_4$

Таблица 3.13 – Типовые угрозы для потока  $g_4 = (V_2, e_2, V_2)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Передача санкционированным процессом информации н/с процессу	Получение конфиденциальной информации из-за подмены адреса процесса-источника в оперативной памяти	$g_4k_1$
$k_2$	Передача санкционированным процессом информации н/с процессу	Получение конфиденциальной информации из-за подмены адреса процесса-источника в оперативной памяти	$g_4k_2$
$k_3$	Передача информации по н/с каналу в виртуальной среде	Подмена виртуального адресного пространства	$g_4k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Съем информации по ПЭМИН с элементов оперативной памяти	$g_4k_4$



Таблица 3.14 – Типовые угрозы для потока  $g_5 = (V_2, e_3, V_2)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Удаленная передача санкционированным процессом информации н/с процессу	Скрытое перенаправление информации на н/с сетевой узел	$g_5k_1$
$k_2$	Удаленная передача санкционированным процессом информации н/с процессу	Скрытое перенаправление информации на н/с сетевой узел	$g_5k_2$
$k_3$	Передача информации по удаленному н/с каналу в электро-магнитной среде	Подмена драйвера или установка программной закладки в результате н/с перепрошивки Ethernet-контроллера	$g_5k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Съем информации по ПЭМИН с канала передачи	$g_5k_4$

Таблица 3.15 – Типовые угрозы для потока  $g_6 = (V_2, e_4, V_2)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Удаленная передача санкционированным процессом информации н/с процессу	Скрытое перенаправление информации на н/с адрес	$g_6k_1$
$k_2$	Удаленная передача санкционированным процессом информации н/с процессу	Скрытое перенаправление информации на н/с адрес	$g_6k_2$
$k_3$	Передача информации по удаленному н/с каналу в виртуальной среде	Использование н/с драйвера сетевой карты и/или протокола	$g_6k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Анализ сетевого трафика – перехват сетевых пакетов	$g_6k_4$

Таблица 3.16 – Типовые угрозы для потока  $g_7 = (V_2, e_1, V_3)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Запись санкционированным процессом информации на н/с носитель информации	Н/с копирование файла	$g_7k_1$
$k_2$	Считывание н/с процессом информации из санкционированного носителя информации	Запись информации в файл, к которому не разграничен доступ (н/с файл)	$g_7k_2$
$k_3$	Передача информации по н/с каналу в электромагнитной среде	Использование н/с или скомпрометированного драйвера контроллера жесткого диска	$g_7k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Съем информации по ПЭМИН элементов аппаратных интерфейсов подключения и работы устройств ввода/вывода; установка аппаратных закладок	$g_7k_4$

Таблица 3.17 – Типовые угрозы для потока  $g_8 = (V_2, e_2, V_3)$ 

	Описание угрозы	Пример реализации угрозы	Наименование
$k_1$	Запись санкционированным процессом информации на н/с носитель информации	Запись защищаемой информации в н/с (незащищенный) файл	$g_8k_1$
$k_2$	Считывание н/с процессом информации из санкционированного носителя информации	Н/с считывание защищаемого файла	$g_8k_2$
$k_3$	Передача информации по н/с каналу в виртуальной среде	Передача информации с использованием н/с и скомпрометированного драйвера	$g_8k_3$
$k_4$	Получение информации из-за пределов санкционированной зоны	Считывание остаточной информации из виртуальной памяти	$g_8k_4$

Таким образом, был составлен перечень из 32-х типовых угроз конфиденциальности информации, обрабатываемой в компьютерной системе.

### **3.4 Комплексированная модель угроз и сравнение с аналогами**

Несмотря на то, что описанные двух в предыдущих пунктах модели угроз имеют разное обоснование полноты, в их основе всё же лежит одинаковый математический аппарат. Благодаря этому результирующие угрозы могут объединены в общее множество угроз. Итоговая мощность множества типовых угроз будет равняться сумме мощностей двух множеств, а значит общее количество типовых угроз по всем трём аспектам будет равняться 104.

Учитывая тот факт, что технологии развиваются нарастающими темпами, мы не можем с точностью предсказать какие устройства ввода/вывода, хранения или передачи в принципе будут существовать через несколько лет, что уж говорить об определении полного перечня угроз информации, которая будет обрабатываться с помощью ныне несуществующих приборов.

При всём при этом можно с уверенностью сказать, что множество типовых угроз останется неизменным, так как используемый в основе модели угроз аппарат имеет высокую степень абстракции и строится на теории графов, а не на объектах реального мира. В рамках модели любое устройство представляется как канал передачи информации независимо от своей реализации. От специалиста потребуется только обеспечить добавление этого канала (устройства) на этапе описания всей системы. Внедренная абстракция позволяет описать систему вплоть до минимального уровня взаимодействия элементов [114]. Глубину детального описания системы специалист определяет самостоятельно в зависимости от целесообразности и предъявляемых требований [115]. Однако, на данном этапе не идет речи об автоматизации процесса формирования полного перечня угроз, т.к. перечень актуальных угроз бесконечно дополняется, и такая задача является попросту

невыполнимой [116]. Данное исследование предполагает определение только типовых угроз [117, 118].

Из проведенного в [100] анализа моделей угроз [52], [54], [55] и [56] следует, что перечень угроз из [52] перекрывает все угрозы, обозначенные в [54], [55] и [56]. Следовательно, дальнейшее сравнение результатов настоящего исследования будет производиться именно с [52].

По результатам того же анализа из [100] была составлена таблица классификации угроз безопасности из [52] по объекту воздействия (таблица 3.9).

С тех пор как работа [100] была опубликована в [52] добавлено ещё четыре угрозы.

210: Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения

211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем

212: Угроза перехвата управления информационной системой

213: Угроза обхода многофакторной аутентификации

Данные угрозы были так же учтены и добавлены в таблицу 3.18.

Таблица 3.18 – 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, 210, 211, 212, 213	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

Учитывая специфику исследования, а именно обеспечение безопасности информации, обрабатываемой в системе, проведем сопоставление выделенных из [52] угроз информации с типовыми угрозами, представленными в авторской модели.

Таблица 3.19 – Сопоставление угроз из авторской модели с угрозами из банка угроз ФСТЭК

БДУ	Авторская модель	БДУ	Авторская модель
<b>Угрозы конфиденциальности</b>			
67, 68, 88, 115, 117, 135	$g_{1k_1}$	67, 80, 88, 117, 135	$g_{5k_1}$
67, 88, 117, 135, 175	$g_{1k_2}$	67, 88, 117, 135	$g_{5k_2}$
67, 88	$g_{1k_3}$	67, 88	$g_{5k_3}$
67, 88, 117, 135, 175	$g_{1k_4}$	67, 88, 116, 135	$g_{5k_4}$
17, 21, 44, 63, 67, 68, 81, 82, 85, 87, 88, 93, 115, 117, 118, 119, 120, 122, 135, 147, 148, 149, 152, 163, 175, 192, 201	$g_{2k_1}$	17, 21, 44, 63, 67, 80, 81, 82, 85, 87, 88, 93, 117, 118, 119, 120, 122, 130, 135, 147, 148, 149, 152, 163, 192, 199, 200	$g_{6k_1}$
63, 67, 88, 93, 117, 118, 119, 120, 122, 135, 147, 148, 149, 152, 163, 192	$g_{2k_2}$	63, 67, 88, 93, 117, 118, 119, 120, 122, 130, 135, 147, 148, 149, 152, 163, 192, 199, 200	$g_{6k_2}$
15, 16, 67, 88	$g_{2k_3}$	15, 16, 75, 67, 88	$g_{6k_3}$
17, 21, 34, 67, 88, 117, 135, 175	$g_{2k_4}$	17, 34, 75, 67, 88, 116, 117, 130, 135	$g_{6k_4}$
67, 88, 117, 135	$g_{3k_1}$	67, 84, 67, 88, 97, 101, 117, 135, 156, 203	$g_{7k_1}$
67, 88, 117, 135	$g_{3k_2}$	67, 88, 117, 135	$g_{7k_2}$
67, 88	$g_{3k_3}$	67, 88	$g_{7k_3}$
67, 88, 117, 135	$g_{3k_4}$	67, 88, 117, 135	$g_{7k_4}$
17, 44, 63, 67, 81, 82, 85, 87, 88, 93, 117, 118, 119, 120, 122, 130, 135, 147, 148, 149, 152, 163, 192, 199, 200	$g_{4k_1}$	21, 35, 57, 67, 82, 84, 85, 87, 88, 97, 101, 117, 118, 119, 120, 122, 147, 148, 149, 152, 156, 163, 192, 203, 209	$g_{8k_1}$
63, 67, 88, 93, 117, 118, 119, 120, 122, 130, 135, 147, 148, 149, 152, 163, 192, 199, 200	$g_{4k_2}$	35, 57, 67, 88, 117, 118, 119, 120, 122, 147, 148, 149, 152, 163, 192	$g_{8k_2}$
15, 16, 67, 88	$g_{4k_3}$	15, 16, 67, 88	$g_{8k_3}$

Таблица 3.19 (Продолжение)

17, 34, 67, 88, 117, 130, 135	<i>g<sub>4k4</sub></i>	34, 67, 88, 117	<i>g<sub>8k4</sub></i>
Угрозы целостности			
135	<i>g<sub>1c1</sub></i>	135	<i>g<sub>5c1</sub></i>
68, 135	<i>g<sub>1c2</sub></i>	80, 135	<i>g<sub>5c2</sub></i>
63, 68, 122	<i>g<sub>1c3</sub></i>	63, 68, 122, 135	<i>g<sub>5c3</sub></i>
	<i>g<sub>1c4</sub></i>	63, 68, 122	<i>g<sub>5c4</sub></i>
	<i>g<sub>1c5</sub></i>	135	<i>g<sub>5c5</sub></i>
	<i>g<sub>1c6</sub></i>		<i>g<sub>5c6</sub></i>
117	<i>g<sub>1c7</sub></i>		<i>g<sub>5c7</sub></i>
35, 44, 87, 149	<i>g<sub>2c1</sub></i>	35, 44, 77, 81, 87, 118, 119, 149, 163, 209	<i>g<sub>6c1</sub></i>
	<i>g<sub>2c2</sub></i>	35, 44, 77, 81, 87, 118, 119, 120, 149, 163, 209	<i>g<sub>6c2</sub></i>
13, 35, 39, 44, 51, 63, 68, 87, 113, 122, 192	<i>g<sub>2c3</sub></i>	13, 35, 39, 44, 51, 63, 68, 77, 81, 82, 87, 93, 113, 118, 119, 120, 121, 122, 135, 163, 192, 209	<i>g<sub>6c3</sub></i>
13, 35, 51	<i>g<sub>2c4</sub></i>	13, 35, 39, 44, 51, 77, 81, 82, 87, 93, 113, 118, 119, 120, 121, 122, 163, 192, 209	<i>g<sub>6c4</sub></i>
13, 35, 44, 87	<i>g<sub>2c5</sub></i>	13, 35, 44, 77, 81, 87, 93, 118, 119, 120, 135, 149, 163, 209	<i>g<sub>6c5</sub></i>
13, 35, 44	<i>g<sub>2c6</sub></i>	13, 35, 44, 77, 81, 87, 93, 118, 119, 120, 149, 163, 209	<i>g<sub>6c6</sub></i>
117	<i>g<sub>2c7</sub></i>	117, 130	<i>g<sub>6c7</sub></i>
	<i>g<sub>3c1</sub></i>	80, 101, 147	<i>g<sub>7c1</sub></i>
	<i>g<sub>3c2</sub></i>	136	<i>g<sub>7c2</sub></i>
63, 68, 122	<i>g<sub>3c3</sub></i>	63, 68, 80, 84, 101, 124, 143, 147, 152, 179	<i>g<sub>7c3</sub></i>
63, 68, 122	<i>g<sub>3c4</sub></i>	63, 68, 122	<i>g<sub>7c4</sub></i>
	<i>g<sub>3c5</sub></i>	80, 101, 124, 147, 152, 179	<i>g<sub>7c5</sub></i>
	<i>g<sub>3c6</sub></i>		<i>g<sub>7c6</sub></i>
	<i>g<sub>3c7</sub></i>		<i>g<sub>7c7</sub></i>

Таблица 3.19 (Продолжение)

77, 87, 118, 119, 120, 149, 163, 209	<i>g4c1</i>	50, 80, 101, 105, 147	<i>g8c1</i>
77, 87, 118, 119, 120, 149, 163, 209	<i>g4c2</i>	136, 149	<i>g8c2</i>
13, 35, 39, 44, 63, 68, 77, 82, 87, 93, 113, 118, 119, 120, 121, 122, 163, 192, 209	<i>g4c3</i>	13, 35, 39, 44, 50, 60, 80, 84, 101, 124, 143, 147, 152, 179	<i>g8c3</i>
13, 35, 39, 44, 63, 68, 77, 82, 87, 93, 113, 118, 119, 120, 121, 122, 163, 192, 209	<i>g4c4</i>	13, 35, 39, 44, 63, 68, 122, 192	<i>g8c4</i>
13, 35, 44, 77, 93, 118, 119, 120, 149, 163, 209	<i>g4c5</i>	13, 35, 44, 50, 80, 101, 124, 130, 147, 152, 179	<i>g8c5</i>
13, 35, 44, 77, 87, 93, 118, 119, 120, 149, 163, 209	<i>g4c6</i>	13, 35, 44, 149	<i>g8c6</i>
117	<i>g4c7</i>	117	<i>g8c7</i>
<b>Угрозы доступности</b>			
47, 68, 113, 117, 118, 119, 120, 135, 140, 142, 149, 152, 155, 161, 163, 166, 205	<i>g1d1</i>	47, 80, 110, 113, 117, 118, 119, 120, 135, 140, 142, 153, 155, 161, 163, 166, 205	<i>g5d1</i>
47, 117, 118, 119, 120, 140, 142, 143, 155, 163, 205	<i>g1d2</i>	47, 64, 80, 110, 117, 118, 119, 120, 140, 142, 143, 153, 155, 163, 205	<i>g5d2</i>
43, 47, 51, 59, 68, 81, 87, 93, 113, 117, 118, 119, 120, 122, 135, 136, 140, 142, 149, 152, 155, 161, 163, 166, 192, 205	<i>g2d1</i>	43, 47, 59, 77, 81, 87, 93, 110, 113, 117, 118, 119, 120, 121, 122, 135, 136, 140, 142, 149, 152, 163, 153, 155, 161, 166, 192, 199, 205	<i>g6d1</i>
14, 17, 22, 29, 44, 47, 51, 59, 63, 81, 87, 117, 118, 119, 120, 140, 142, 143, 155, 163, 192, 205	<i>g2d2</i>	14, 17, 22, 29, 44, 47, 59, 63, 77, 81, 87, 110, 117, 118, 119, 120, 121, 140, 142, 143, 153, 155, 163, 192, 205	<i>g6d2</i>
47, 110, 113, 117, 118, 119, 120, 135, 140, 142, 149, 152, 155, 161, 163, 166, 205	<i>g3d1</i>	47, 84, 91, 97, 101, 105, 106, 113, 117, 118, 119, 120, 135, 140, 142, 149, 152, 155, 156, 161, 163, 166, 205	<i>g7d1</i>

Таблица 3.19 (Окончание)

47, 110, 117, 118, 119, 120, 140, 142, 143, 155, 163	$g_3d_2$	47, 84, 101, 106, 117, 118, 119, 120, 140, 142, 143, 155, 163	$g_7d_2$
43, 51, 59, 77, 81, 87, 93, 110, 113, 117, 118, 119, 120, 121, 122, 135, 136, 140, 142, 149, 152, 155, 161, 163, 166, 192, 199, 205	$g_4d_1$	35, 38, 43, 51, 60, 77, 84, 91, 93, 97, 101, 1053 106, 113, 117, 118, 119, 120, 121, 122, 135, 136, 140, 142, 149, 152, 155, 156, 161, 163, 166, 192, 205, 209	$g_8d_1$
14, 17, 22, 29, 44, 51, 59, 63, 77, 81, 87, 110, 117, 118, 119, 120, 121, 140, 142, 143, 155, 163, 192, 205	$g_4d_2$	14, 22, 29, 38, 51, 63, 77, 84, 101, 106, 117, 118, 119, 120, 121, 140, 142, 143, 155, 163, 192, 205, 209	$g_8d_2$

Таким образом, всем угрозам из [52] удалось определить соответствующие угрозы из авторской модели. Не трудно заметить, что соотношение не однозначно – одной угрозе из [52] могут соответствовать несколько угроз из авторской модели и наоборот. Связано это с тем, что модель угроз [52] не учитывает конкретный элемент информационного потока, к которому может быть применена угроза, а называет её в общем виде.

Можно сказать, что типовые угрозы из авторской модели являются классами угроз, которые представляются частными примерами из модели ФСТЭК.

И всё же составить полное соотношение не удалось: не для каждой типовой угрозы из авторской модели нашлись угрозы из [52]. В [52] нет примеров для следующих типовых угроз:

- $g_{1c4}$ – Уничтожение информации, обрабатываемой пользователем;
- $g_{1c5}$ – Подмена информации, обрабатываемой процессом;
- $g_{1c6}$ – Подмена информации, обрабатываемой пользователем;
- $g_{2c2}$ – Передача н/с процессом информации санкционированному пользователю;



- $g_{3c1}$  – Передача н/с процессом информации санкционированному процессу;
- $g_{3c2}$  – Передача н/с процессом информации санкционированному процессу;
- $g_{3c5}$  – Подмена информации, обрабатываемой процессом;
- $g_{3c6}$  – Подмена информации, обрабатываемой процессом;
- $g_{3c7}$  – Воздействие на информацию при ее передаче по каналу в электромагнитной среде;
- $g_{5c6}$  – Подмена информации, обрабатываемой процессом;
- $g_{5c7}$  – Воздействие на информацию при ее передаче по каналу в электромагнитной среде;
- $g_{7c6}$  – Подмена информации, хранящейся на носителе информации;
- $g_{7c7}$  – Воздействие на информацию при ее передаче по каналу в электромагнитной среде.

Можно заметить, что все обнаруженные пробелы относятся к угрозам целостности, а также то, что большая их часть относятся к потокам  $g_1$ ,  $g_3$ ,  $g_5$  и  $g_7$ , в которых передачи информации осуществляется по электромагнитному каналу. В модели угроз ФСТЭК были угрозы, которые могли бы подойти указанным типовым угрозам, однако они были отвергнуты в виду того, что в их описании было явно указано, что угроза вызвана программно и/или направлена на объект в виртуальной среде. К тому же модель ФСТЭК не учитывает деление канала передачи информации на виртуальный и электромагнитный, но делит на такие классы носители информации. Ещё одной проблемой является то, что модель ФСТЭК не учитывает направленность угрозы, что вызывает большое количество дублирований при сопоставлении моделей.

### 3.5 Выводы по главе

В данной главе предложена авторская модель угроз безопасности информации, которая учитывает модель элементарных информационных потоков и позволяет классифицировать угрозы по направленности на каждую из трёх составляющих элементарного информационного потока.

Сравнение разработанной модели с наиболее полной базой угроз [52] позволило выделить ещё 13 типовых угроз.

Разработанная модель угроз была внедрена в деятельность ООО «НПФ «ИСБ». Применение модели угроз, позволило получить полный перечень типовых угроз безопасности информации, обрабатываемой в ИСПДн. Полученный список был учтен при определении перечня актуальных угроз, что показало необходимость внедрения в систему дополнительных механизмов защиты. Результатом внедрения работы в деятельность ООО «НПФ «ИСБ» стал перечень из 43 угроз безопасности информации в ИСПДн, что на 14 % больше, чем количество угроз, выявленных экспертами ранее.

Внедрение модели угроз в учебный процесс кафедры КИБЭВС ТУСУР в рамках курса «Управление информационной безопасностью», позволяет студентам ознакомиться с процессом применения моделей угроз безопасности информации, обрабатываемой в информационной системе.

#### 4 Модель нарушителя информационной безопасности

Как показал мировой и отечественный опыт, атаки являются наиболее опасными угрозами. Атаки готовятся и проводятся нарушителем, причем возможности проведения атак обусловлены возможностями нарушителя. Иными словами, конкретные возможности нарушителя определяют конкретные атаки, которые может провести нарушитель. Но тогда с учетом определения понятия "модель нарушителя" все возможные атаки определяются моделью нарушителя. Модель нарушителя тесно связана с моделью угроз. В модели угроз содержится максимально полное описание угроз безопасности объекта. Модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак [119].

##### 4.1 Формирование модели нарушителя

С учетом недостатков описанных в обзоре аналогов моделей, был составлен перечень основных параметров нарушителя информационной безопасности, на основе которых будет строиться новая модель описания нарушителя (табл. 4.1) [120].

Таблица 4.1 – Параметры нарушителя информационной безопасности

Параметр	Значение
M(otivation) – преднамеренность совершения нарушения	0-случайное, 1-преднамеренное
P(lace) – положение относительно организации, работающей с информацией	0-внешний, 1-внутренний
T(ype) – тип нарушителя	4 типа на основе M и P (00, 01, 10, 11)
I(nformation) – знание рубежа защиты и уязвимости в нём	Отсутствие (0)/наличие (1)
E(xtra) – возможность использования несанкционированного средства обработки информации	Отсутствие (0)/наличие (1)

Таблица 4.1 (Окончание)

O(ff) – возможность отключения рубежа защиты	Отсутствие (0)/наличие (1)
D(isruption) – возможность нарушения работы рубежа защиты	Отсутствие (0)/наличие (1)
A(ttack) – возможность преодоления рубежа защиты	Отсутствие (0)/наличие (1)
Q(uality) – уровень нарушителя	От 0 до 7 согласно схеме (рис.1)
Th(reat) – привязка к определенной угрозе	Отсутствие (0) /наличие (1)
N(umber) – количество рубежей защиты, которые осталось преодолеть	0 – санкционированный пользователь, (число большее нуля) – несанкционированный

Условно параметры можно разделить на 2 части: а) параметры, описывающие тип (M, P и T) и качества нарушителя (I, E, O, D, A, Q); б) параметры, характеризующие систему защиты (Th и N).

Из схемы (рис. 4.1) видно, что в формируемой модели нарушителя произведено разделение:

- тип/качество нарушителя;
- поиск и использование уязвимости;
- произведено условное отделение санкционированных и несанкционированных действий и средств.

Для удобства пользователей данной модели нарушителя введена условная бальная система. По мере возрастания опасности от каждого нарушителя относительно каждого возможного действия поставлен определенный балл. Превосходство санкционированных средств над несанкционированными вызвано тем, что нарушитель, использующий санкционированные, то есть разрешенные самой системой, действия является гораздо более опасным, чем нарушитель, которому не хватает навыков и/или которому приходится использовать сторонние средства для достижения своей цели.

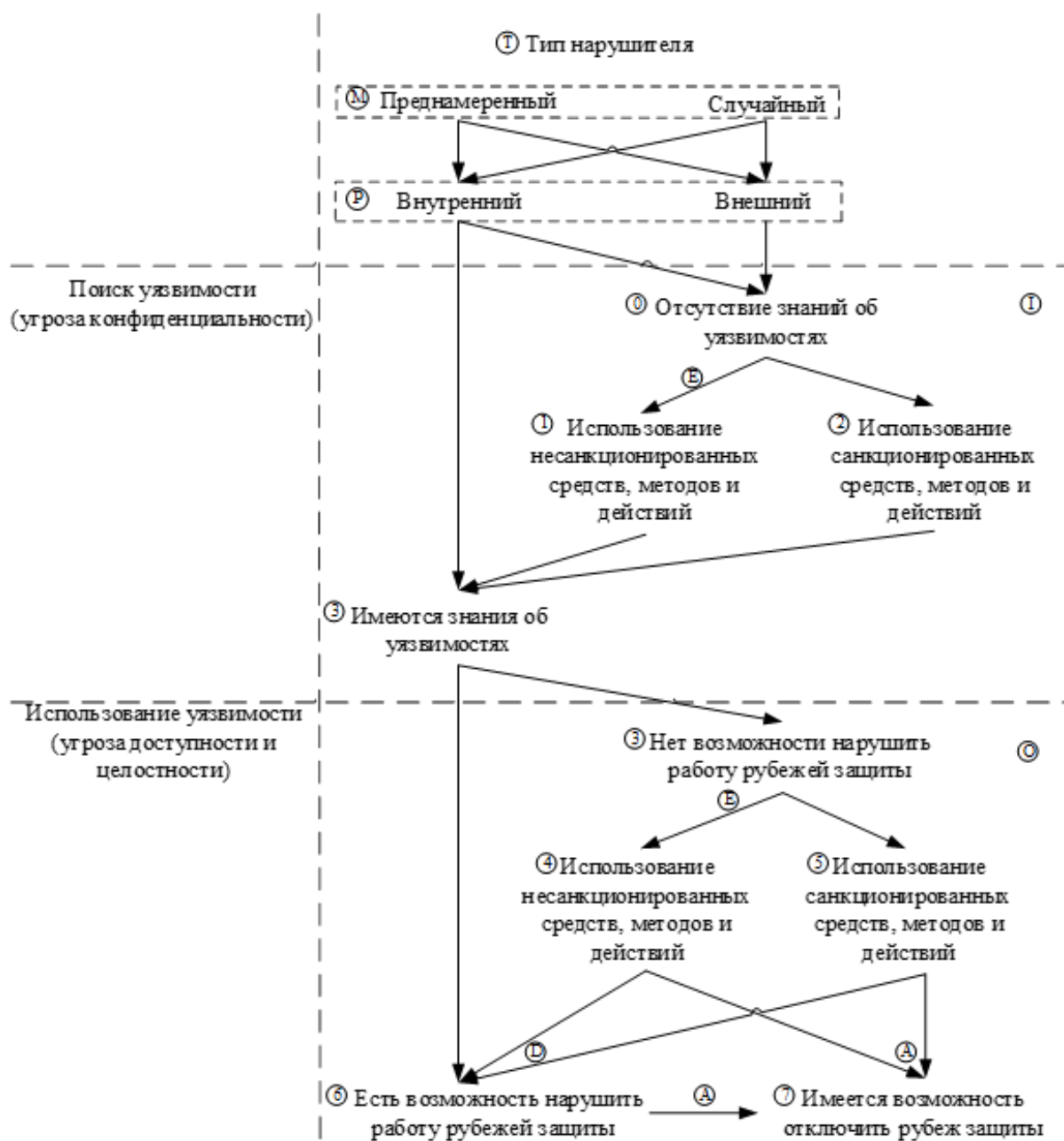


Рисунок 4.1 – Схема отображения параметров нарушителя

Разделение же уровней нарушителя на поиск и использование уязвимостей вызвано тем, что действия нарушителя носят двойственный характер по отношению к информации о рубежах и к системе, в которой хранится конфиденциальная информация. Владея информацией об уязвимостях в рубежах, нарушитель может лишь рассказать эту информацию кому-либо, что само по себе представляет угрозу конфиденциальности. Имея же информацию об уязвимостях и в попытке ее использовать, нарушитель осуществляет угрозу доступности компонентов рубежа, целостности рубежа и всей системы в целом.

Разделение так же вызвано тем, что при каждом из этих действий нарушитель будет использовать разные средства: в первом случае нарушитель будет искать уязвимости, что больше носит пассивный характер, а во втором уже использовать, что носит уже гораздо более активный характер.

Исходя из этой схемы (рис. 4.1), можно сделать предположения о том, кем может являться нарушитель для каждого уровня, который на ней изображен:

0 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, (например, уборщица), у которых нет мотивации;

1 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, которые для выявления угроз используют несанкционированные средства для получения информации об уязвимостях в рубежах защиты. Например, следят за тем, что происходит в окнах здания из неконтролируемой территории;

2 уровень – нарушитель, который использует своё положение чтобы собирать информацию об уязвимостях в рубежах защиты, используя санкционированные методы. Например, ходить по зданию и высматривать положение камер наблюдения;

3 уровень – нарушитель, обладающий информацией об уязвимостях, может быть, как сотрудником, имеющим отношение к конструированию данного рубежа защиты, так и одним из нарушителей, ранее имевших 1 или 2 балла, при условии, что их действия не были замечены и пресечены сотрудниками охраны;

4 уровень – изначально внутренний нарушитель, имеющий достаточно информации про уязвимости в рубеже, но не имеющий возможности нарушить или преодолеть защиту рубежа, используя свой уровень допуска и использующий для этого несанкционированные средства. Примером может быть сотрудник, работающий на другом этаже здания с другим видом информации, но знающий общую схему здания, расположение и уязвимости в рубежах защиты. Этот сотрудник мог принести плоскогубцы и с их помощью

вывести из строя камеры наблюдения. Перенося эту ситуацию в виртуальную среду, можно сделать предположение, что потенциальным нарушителем может являться пользователь внутренней компьютерной сети здания, имеющий пароль для входа в операционную систему, но не имеющий доступа к определенной информации и использующий для этого программы-переборщики паролей;

5 уровень – изначально внутренний нарушитель, который для достижения своих целей использует санкционированные методы. Например, пользователь, имеющий пароль к необходимой информации может пересылать конфиденциальные данные другому санкционированному пользователю, работающему за территорией этого здания, например, в филиале, используя заведомо ненадежный канал передачи данных;

6 уровень – изначально внутренний нарушитель с высоким уровнем доступа, имеющий возможность нарушить работу рубежей защиты, пользуясь своим служебным положением. Таким сотрудником может быть администратор информационной безопасности;

7 уровень – изначально внутренний нарушитель с очень высоким уровнем доступа, имеющий возможность отключить рубеж защиты, используя своё служебное положение.

Таким сотрудником может являться администратор системы защиты либо работник охраны. Так же под это описание подходят форс-мажорные обстоятельства (например, природные катастрофы, так как природе перед стихийными бедствиями не нужно получать информацию о рубежах защиты и отключать их).

Следует также отметить, что привязка нарушителя осуществляется к угрозе, которая влияет непосредственно на информацию, остальные же пункты закреплены за охраняющими эту информацию рубежами защиты, так как при устранении всех рубежей информация автоматически становится доступной и тот, кто нарушил целостность рубежей получает ее в свое распоряжение.

## 4.2 Соотнесение модели нарушителя и модели угроз

Как было указано в пунктах 1.2 и 1.3 данной работы, многие модели угроз основываются на моделях нарушителя и наоборот. Данный подход не является корректным, т. к. полнота итоговой модели напрямую зависит от полноты исходной.

По мнению автора, корректным подходом является параллельное применение двух независимых моделей, которые будут учитывать слабые места друг друга в случае обнаружения недостаточной полноты и заполнять эти пробелы.

Проведем сопоставление типовых угроз информационным потокам с четырьмя типами нарушителя без учета его уровня (таблица 4.2).

Таблица 4.2 - Сопоставление типов нарушителя с типовыми угрозами

Тип нарушителя	Типовые угрозы информационному потоку
Внутренний-преднамеренный	k <sub>1</sub> k <sub>2</sub> k <sub>3</sub> k <sub>4</sub> c <sub>1</sub> c <sub>2</sub> c <sub>3</sub> c <sub>4</sub> c <sub>5</sub> c <sub>6</sub> c <sub>7</sub> d <sub>1</sub> d <sub>2</sub>
Внутренний-случайный	k <sub>1</sub> k <sub>2</sub> k <sub>3</sub> k <sub>4</sub> c <sub>1</sub> c <sub>2</sub> c <sub>3</sub> c <sub>4</sub> c <sub>5</sub> c <sub>6</sub> c <sub>7</sub> d <sub>1</sub> d <sub>2</sub>
Внешний-преднамеренный	k <sub>3</sub> k <sub>4</sub> c <sub>7</sub> d <sub>1</sub> d <sub>2</sub>
Внешний-случайный	k <sub>3</sub> k <sub>4</sub> c <sub>7</sub> d <sub>1</sub> d <sub>2</sub>

Как видно из таблицы 4.2 каждому типу нарушителя соответствует определенный набор типовых угроз из авторской модели. Данные множества можно расширить, применив каждую типовую угрозу к каждому информационному потоку, как это сделано в авторской модели угроз. Можно заметить, что набор угроз не зависит от характера действия нарушителя (умышленный он или случайный). Набор угроз зависит исключительно от местонахождения нарушителя: внутри контролируемой зоны или нет. Случайный нарушитель может реализовать те же угрозы, что и преднамеренный, разница лишь в том, что преднамеренный нарушитель в большинстве случаев имеет более высокую квалификацию, и/или более полную информацию о системе и её средствах защиты, и/или обладает



подходящим техническим обеспечением. В большинстве случаев достаточный уровень защиты от случайных нарушителей обеспечивается организационными мерами.

### **4.3 Выводы по главе**

Разработанная модель нарушителя, позволяет проследить причинно-следственные связи между элементами модели и цепочками предполагаемых последствий. Основываясь на этом, а также на описании состояния окружающей среды, рубежей защиты и всех зон, окружающих конфиденциальную информацию, были описаны и ранжированы возможные виды предполагаемых нарушителей. Как следствие, модель позволяет построить полное и универсальное по отношению к различным системам описание вероятного нарушителя информационной безопасности.

## 5 Методика формирования политики разграничения доступа

### 5.1 Общее описание методики

Далее предлагается методика формирования политики разграничения доступа, основанная на модели элементарных информационных потоков. Разработанная методика отличается возможностью определения прав доступа с учетом типа канала связи, а также учетом всех возможных в системе информационных потоков.

Методика формирования политики разграничения доступа состоит из трёх функциональных блоков:

1. построение схемы информационных потоков;
2. определение прав доступа;
3. составление нормативного документа.

На рисунке 5.1 представлена функциональная схема методики в графической нотации IDEF0.

Входными данными методики являются:

1. список сотрудников ( $V_1$ );
2. список документов ( $V_3$ );
3. список программных средств ( $V_2$ );
4. список используемых протоколов ( $E_2, E_4$ );
5. список используемых драйверов ( $E_1, E_2$ );
6. список прав доступа ( $AP$ );
7. специалист по защите информации ( $T$ ).

На выходе методики получаем нормативный документ ( $N$ ), содержащий политику разграничения доступа, которая включает в себя следующие элементы:

1. схема информационных потоков;
2. список программного обеспечения;
3. список рабочих станций;
4. список используемых протоколов;
5. список используемых драйверов;

6. список помещений;
7. матрица доступа  $MD$ ;

Управляющее воздействие оказывается разработанной ранее моделью информационных потоков, а также должностными инструкциями для персонала.



Рисунок 5.1 – Методика формирования политики разграничения доступа

Согласно функциональной схеме методики для формирования политики разграничения доступа необходимо выполнить следующие шаги:

1. Определить перечень должностей.
2. Определить список всех информационных ресурсов.
3. Определить перечень программ, с помощью которых можно работать с информацией.
4. Составить список всех рабочих станций.
5. Составить список используемых драйверов и протоколов.
6. Определить перечень помещений.

7. Сопоставить рабочие станции с помещениями, т. е. указать их местоположение.
8. Сопоставить программы и информационные ресурсы.
9. Определить перечень протоколов и драйверов для осуществления взаимодействия ПО с информационными ресурсами.
10. На основании должностных инструкций определить наличие прав доступа к информационным ресурсам для каждой должности.
11. На основании должностных инструкций определить наличие прав доступа к рабочим станциям для каждой должности.
12. На основании прав доступа сотрудников к информационным ресурсам и сопоставлении программного обеспечения с информационными ресурсами определить наличие прав доступа к программному обеспечению для каждой должности.
13. На основании прав доступа сотрудников к программному обеспечению и сопоставлении программного обеспечения с протоколами и драйверами определить наличие прав доступа к драйверам и протоколам для каждой должности.
14. Определить у пользователей наличие прав доступа в помещения.
15. Сформировать итоговую матрицу доступа, объединив таблицы сопоставления из пунктов 7–14.

## **5.2 Пример применения методики**

Далее приводится пример реализации методики формирования политики разграничения доступа для абстрактного предприятия.

1. Определить перечень должностей.

$V_1$  – множество должностей.

$$V_1 = \{v_1, v_2, v_3\}, \text{ где}$$

$v_1^1$  – директор;

$v_{12}$  – бухгалтер;

$v_{13}$  – охранник.

2. Определить список всех информационных ресурсов.

$V_3$  – множество информационных ресурсов.

$$V_3 = \{v_{31}, v_{32}, v_{33}\}, \text{ где}$$

$v_{31}$  – сайт «firma.ru»;

$v_{32}$  – база данных «Работа-1»;

$v_{33}$  – файл «Работа.doc».

3. Определить перечень программ, с помощью которых можно работать с информацией.

$V_2$  – множество программного обеспечения.

$$V_2 = \{v_2^1, v_{22}, v_{23}, v_{24}\}, \text{ где}$$

$v_2^1$  – программа MS Word.

$v_{22}$  – программа Google Chrome.

$v_{23}$  – программа Mozilla Firefox.

$v_{24}$  – СУБД MySQL.

4. Составить список всех рабочих станций.

$A$  – множество рабочих станций.

$$A = \{a_1, a_2, a_3, a_4, a_5\}, \text{ где}$$

$a_1$  – рабочая станция директора.

$a_2$  – рабочая станция охранника.

$a_3$  – рабочая станция бухгалтера.

$a_4$  – рабочая станция бухгалтера.

$a_5$  – рабочая станция бухгалтера.

5. Составить список используемых драйверов и протоколов

$E$  – множество протоколов, драйверов.

$$E = E_1 \cup E_2 \cup E_3 \cup E_4,$$

где  $E_1$  – множество виртуальных каналов;

$E_2$  – множество электромагнитных каналов;

$E_3$  – множество удаленных виртуальных каналов;

$E_4$  – множество электромагнитных каналов.

$$E_2 = \{e_{21}, e_{22}, e_{23}\}, \text{ где}$$

$e_{21}$  – NTFS;

$e_{22}$  – FAT32;

$e_{23}$  – WPD.

$E_3 = \{e_{41}, e_{42}, e_{43}, e_{44}, e_{45}\}$ , где

$e_{41}$  - протокол http.

$e_{42}$  – протокол https.

$e_{43}$  – протокол ftp.

$e_{44}$  – протокол ftps.

$e_{45}$  – драйвер ODBC.

6. Определить перечень помещений

$P$  – множество помещений

$P = \{p_1, p_2, p_3\}$ , где

$p_1$  – кабинет директора.

$p_2$  – пост охраны.

$p_3$  – бухгалтерия.

7. Сопоставить рабочие станции с помещениями, т. е. указать их местоположение, результат представлен в таблице 5.1.

Таблица 5.1 – Соотношение элементов множеств  $V_2$  и  $V_3$

	$v_2^1$ – программа MS Word	$v_{22}$ – программа Google Chrome	$v_{23}$ – программа Mozilla Firefox	$v_{24}$ – СУБД MySQL
$b_{4,1}$ – сайт «firma.ru»	-	+	+	-
$b_{5,1}$ – база данных «Работа-1»	-	-	-	+
$b_{5,2}$ – файл «Работа.doc»	+	-	-	-

8. Сопоставить программы и информационные ресурсы, результат представлен в таблице 5.2.

Таблица 5.2 – Соотношение элементов множеств  $V_2$  и  $V_3$ 

	$v_2^1$ – программа MS Word	$v_{22}$ – программа Google Chrome	$v_{23}$ – программа Mozilla Firefox	$v_{24}$ – СУБД MySQL
$b_{4,1}$ – сайт «firma.ru»	-	+	+	-
$b_{5,1}$ – база данных «Работа-1»	-	-	-	+
$b_{5,2}$ – файл «Работа.doc»	+	-	-	-

9. Определить перечень протоколов и драйверов для осуществления взаимодействия ПО с информационными ресурсами, результат представлен в таблице 5.3.

Таблица 5.3 – Определение перечней драйверов и протоколов

	$v_2^1$ – программа MS Word	$v_{22}$ – программа Google Chrome	$v_{23}$ – программа Mozilla Firefox	$v_{24}$ – СУБД MySQL
$b_{4,1}$ – сайт «firma.ru».	-	$e_{41}$ - протокол http. $e_{42}$ – протокол https $e_{43}$ – протокол ftp. $e_{44}$ – протокол ftps	$e_{41}$ - протокол http $e_{42}$ – протокол https $e_{43}$ – протокол ftp $e_{44}$ – протокол ftps	-
$b_{5,1}$ – база данных «Работа-1».	-	-	-	$e_{45}$ – драйвер ODBC
$b_{5,2}$ – файл «Работа.doc».	$e_{21}$ – NTFS	-	-	-

На данном этапе работы методики мы уже будем иметь полную схему информационных потоков в системе, для этого необходимо сопоставить каждому сотруднику все элементы множества программного обеспечения, т. е. составить таблицы аналогичные таблице 5.2 для каждого пользователя. Как

было обозначено ранее, пользователь взаимодействует с ПО средствами операционной системы, потому нет необходимости обозначать полный перечень протоколов и драйверов для этого потока. Далее необходимо определить какие из потоков являются разрешенными.

10. На основании должностных инструкций определить наличие прав доступа к информационным ресурсам для каждой должности, результат представлен в таблице 5.4.

Таблица 5.4 – Определение наличия прав доступа к информационным ресурсам

	$v_1^1$ – директор	$v_{12}$ – бухгалтер	$v_{13}$ – охранник
$b_{4,1}$ – сайт «firma.ru».	+	+	+
$b_{5,1}$ – база данных «Работа-1».	+	+	-
$b_{5,2}$ – файл «Работа.doc».	+	-	-

11. На основании должностных инструкций определить наличие прав доступа к рабочим станциям для каждой должности, результат представлен в таблице 5.5.

Таблица 5.6 – Определение наличия прав доступа к рабочим станциям

	$v_1^1$ – директор	$v_{12}$ – бухгалтер	$v_{13}$ – охранник
$f_1$ – рабочая станция директора	+	-	-
$f_2$ – рабочая станция охранника	+	-	+
$f_3$ – рабочая станция бухгалтера	+	+	-
$f_4$ – рабочая станция бухгалтера	+	+	-
$f_5$ – рабочая станция бухгалтера	+	+	-



12. На основании прав доступа сотрудников к информационным ресурсам и сопоставлении программного обеспечения с информационными ресурсами определить наличие прав доступа к программному обеспечению для каждой должности, результат представлен в таблице 5.6.

Таблица 5.6 – Определение наличия прав доступа к программному обеспечению

	$v_1^1$ – директор	$v_{12}$ – бухгалтер	$v_{13}$ – охранник
$v_2^1$ – программа MS Word	+	-	-
$v_{22}$ – программа Google Chrome	+	+	+
$v_{23}$ – программа Mozilla Firefox	+	+	+
$v_{24}$ – СУБД MySQL	+	+	

13. На основании прав доступа сотрудников к программному обеспечению и сопоставлении программного обеспечения с протоколами и драйверами определить наличие прав доступа к драйверам и протоколам для каждой должности, результат представлен в таблице 5.7.

Таблица 5.7 – Определение наличия прав доступа к драйверам и протоколам

	$v_1^1$ – директор	$v_{12}$ – бухгалтер	$v_{13}$ – охранник
$e_{21}$ – NTFS	+	-	-
$e_{22}$ – FAT32	-	-	-
$e_{23}$ – WPD	-	-	-
$e_{41}$ – протокол http	+	+	+
$e_{42}$ – протокол https	+	+	+
$e_{43}$ – протокол ftp	+	+	+
$e_{44}$ – протокол ftps	+	+	+
$e_{45}$ – драйвер ODBC.	+	+	-

14. Определить у пользователей наличие прав доступа в помещения, результат представлен в таблице 5.8.

Таблица 5.8 – Определение наличия прав доступа в помещения

	$v_1^1$ – директор	$v_{12}$ – бухгалтер	$v_{13}$ – охранник
p1 – кабинет директора	+	-	+
p2 – пост охраны.	+	-	+
p3 – бухгалтерия	+	+	+

Наложив все указанные выше матрицы друг на друга, можно получить некоторую многомерную матрицу, которая будет содержать в себе полный перечень разрешенных информационных потоков с учетом определения прав доступа к каналам передачи информации, рабочим станциям и помещениям. Примером такой матрицы является таблица 5.9

Таблица 5.9 – Матрица доступа к информационным ресурсам

	ЭР1		ЭР2		ЭР3	
Пользователь 1	-		ПО1	PC1	ПО1	PC1
				PC2		PC2
				PC3		PC3
			ПО2	PC1		
Пользователь 2	ПО3	PC1	-	-		
		PC2				
Пользователь 3	ПО3	PC1	-	-	ПО1	PC1
		PC2				PC2
						PC3

Необходимо добавить, что на пересечении строк матриц могут быть указаны более подробные права доступа, чем указал автор работы. Автор обозначал только наличие или отсутствие таких прав исключительно для удобства представления результатов.

### 5.3 Выводы по главе

Результатом работы, представленной в настоящей главе, является методика формирования политики разграничения доступа к информации.

Разработанная методика формирования политики разграничения доступа, использующая упомянутую ранее модель элементарных информационных потоков, позволяет разграничить доступ к каналам передачи данных как к самостоятельным структурным единицам системы.

Предложенная методика была внедрена в деятельность ООО «УЦ Сибири», результатом внедрения стало уменьшение времени, необходимого для формирования политики разграничения доступа на 19 % (в частном случае с 16 до 13 часов).

Внедрение методики в учебный процесс кафедры КИБЭВС ТУСУР в рамках курса «Разработка и эксплуатация защищенных автоматизированных систем» позволило студентам ознакомиться с процессом построения политики разграничения доступа к ресурсам системы.

## Заключение

В ходе диссертационного исследования в соответствующих главах были достигнуты следующие результаты.

Результатами работы по созданию модели элементарных информационных потоков являются следующие положения:

— предложена мультиграфовая модель потоков данных в информационной системе, отличающаяся учетом гетерогенности каналов передачи информации;

— модель элементарных информационных потоков позволяет описать гетерогенную компьютерную систему с помощью восьмизначного алфавита;

— схема информационных потоков включает в себя все возможные потоки, которые могут возникнуть в системе как санкционированные, так и нет.

В ходе разработки модели угроз безопасности информации была предложена авторская модель угроз, которая учитывает модель элементарных информационных потоков и позволяет классифицировать угрозы по направленности на каждую из трёх составляющих элементарного информационного потока.

Сравнение разработанной модели с наиболее полным аналогом позволило выделить ещё 13 типовых угроз. Разработанная модель угроз была внедрена в деятельность ООО «НПФ «ИСБ». Применение модели угроз, позволило получить полный перечень типовых угроз безопасности информации, обрабатываемой в ИСПДн. Полученный список был учтен при определении перечня актуальных угроз, что показало необходимость внедрения в систему дополнительных механизмов защиты. Результатом внедрения работы в деятельность ООО «НПФ «ИСБ» стал перечень из 43 угроз безопасности информации в ИСПДн, что на 14 % больше, чем количество угроз, выявленных экспертами ранее.

Внедрение модели угроз в учебный процесс кафедры КИБЭВС ТУСУР в рамках курса «Управление информационной безопасностью», позволяет студентам ознакомиться с процессом применения моделей угроз безопасности информации, обрабатываемой в информационной системе.

В разработанной модели нарушителя были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий. Основываясь на этом, а также на описании состояния окружающей среды, рубежей защиты и всех зон, окружающих конфиденциальную информацию, были описаны и ранжированы возможные виды предполагаемых нарушителей. Как следствие, модель позволяет построить полное и универсальное по отношению к различным системам описание вероятного нарушителя информационной безопасности.

Разработанная методика формирования политики разграничения доступа, использующая упомянутую ранее модель элементарных информационных потоков, позволила разграничить доступ к каналам передачи данных как к самостоятельным структурным единицам системы. Предложенная методика была внедрена в деятельность ООО «УЦ Сибири», результатом внедрения стало уменьшение времени, необходимого для формирования политики разграничения доступа на 19 % (в частном случае с 16 до 13 часов).

Внедрение упомянутой ранее методики в учебный процесс кафедры КИБЭВС ТУСУР в рамках курса «Разработка и эксплуатация защищенных автоматизированных систем» позволило студентам ознакомиться с процессом построения политики разграничения доступа к ресурсам системы.

Поставленные задачи были выполнены, а заявленная цель диссертационного исследования была достигнута.

**Список использованной литературы**

1. Шелупанов А.А., Евсютин О.О., Конев А.А., Костюченко Е.Ю., Кручинин Д.В., Никифоров Д.С. Актуальные направления развития методов и средств защиты информации. // Доклады ТУСУРа. – 2017. – Т. 20 – № 3 – С. 11-24.
2. Novokhrestov A.K., Konev A.A., Shelupanov A.A., Buymov A.G. Computer network threat modelling // Journal of Physics: Conference Series – 2020. – DOI: 10.1088/1742-6596/1488/1/012002.
3. Novokhrestov A.K., Konev A.A., Shelupanov A.A., Buymov A.G. Model of Threats to Computer Network Software // Symmetry – 2019. – DOI: 10.3390/sym11121506
4. Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУРа. – 2013. – №2 (28). – С. 107-111.
5. Akella R., Tang H., McMillin B. M. Analysis of information flow security in cyber-physical systems // Int. J. Crit. Infrastructure – 2010. – DOI: 10.1016/j.ijcip.2010.09.001
6. Burmester M., Magkos E., Chrissikopoulos V. Modeling security in cyber-physical systems // Int. J. Crit. Infrastructure – [Электронный ресурс]. – Режим доступа: <https://api.semanticscholar.org/CorpusID:11664905>, свободный (дата обращения: 07.10.2021)
7. Pendergrass J.C., Heart K., Ranganathan C., Venkatakrisnan V.N. A Threat Table Based Approach to Telemedicine Security // Transactions of the International Conference on Health Information Technology Advancement – [Электронный ресурс]. – Режим доступа: <https://api.semanticscholar.org/CorpusID:3329736>, свободный (дата обращения: 07.10.2021)
8. Seifert D., Reza H. A Security Analysis of Cyber-Physical Systems Architecture for Healthcare // Computers – 2016 – DOI: 10.3390/computers5040027

9. Almulhem A. Threat Modeling for Electronic Health Record Systems // Journal of medical systems – 2011. – DOI: 10.1007/s10916-011-9770-6
10. Yeboah-Ofori A., Islam S. Cyber Security Threat Modeling for Supply Chain Organizational Environments // Future Internet – 2019. – DOI: 10.3390/fi11030063
11. Ruiz G., Heymann E., César E., Miller B. P. Automating Threat Modeling through the Software Development Life-Cycle. – [Электронный ресурс]. – Режим доступа: <https://api.semanticscholar.org/CorpusID:14252675>, свободный (дата обращения: 07.10.2021)
12. Pan J., Zhuang Y. PMCAP: A Threat Model of Process “Memory Data on the Windows Operating System” // Security and Communication Networks – 2017. – DOI: 10.1155/2017/4621587
13. Li X., He K., Feng Z., Xu G. Unified threat model for analyzing and evaluating software threats // Security and Communication Networks – 2014. – DOI: 10.1002/sec.599
14. Yan B., Li X., Du Z. A Threat Model-Driven Security Testing Approach for Web Application // Contemporary Research on E-business Technology and Strategy – 2012. – DOI: 10.1007/978-3-642-34447-3\_14
15. Immanuvel Arokia J.K., Prabakaran R. Threat Modeling Framework for Electrical Distribution SCADA Networks // MEJSR – 2015. – DOI: 10.5829/idosi.mejsr.2015.23.09.96184
16. Cárdenas A.A., Roosta T., Sastry S. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems // Ad Hoc Networks – 2009. – DOI: 10.1016/j.adhoc.2009.04.012
17. Shelupanov A.A., Konev A.A., Kosachenko T.S., Dudkin D.G. Threat Model for IoT Systems on the Example of OpenUNB Protocol // IJATCSE – 2019 – DOI: 10.30534/ijeter/2019/11792019
18. Ingalsbe J.A., Shoemaker D., Mead N.R. Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise - an overview of considerations // AMCIS – 2011. – [Электронный ресурс]. – Режим

- доступа: [https://aisel.aisnet.org/amcis2011\\_submissions/359](https://aisel.aisnet.org/amcis2011_submissions/359), свободный (дата обращения: 07.10.2021)
19. Baquero A.O., Kornecki A., Zalewski J. Threat modeling for aviation computer security // *CrossTalk* – 2015. – [Электронный ресурс]. – Режим доступа: <https://www.researchgate.net/publication/298822749>, свободный (дата обращения: 07.10.2021)
  20. Olayemi O., Väänänen A., Haataja K., Toivanen P. Security issues in smart homes and mobile health system: threat analysis, possible countermeasures and lessons learned // *International Journal on Information Technologies and Security* – 2017. – [Электронный ресурс]. – Режим доступа: <https://erepo.uef.fi/handle/123456789/5124>, свободный (дата обращения: 07.10.2021)
  21. Kamatchi R., Ambekar K. Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models // *Indian Journal of Science and Technology* – 2016. – DOI: 10.17485/ijst/2016/v9i21/95282.
  22. Xiong W., Krantz F., Lagerström R. Threat Modeling and Attack Simulations of Connected Vehicles: A Research Outlook // *ICISSP* – 2019. – DOI: 10.5220/0007412104790486
  23. Deng M., Wuys K., Scandariato R., Preneel B., Joosen W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements // *Requirements Engineering* – 2011. – DOI: 10.1007/s00766-010-0115-7
  24. Tactical threat modeling // *Safecode* – 2019. – [Электронный ресурс]. – Режим доступа: <https://safecode.org/tactical-threat-modeling>, свободный (дата обращения: 07.10.2021)
  25. Torr P. Demystifying the Threat-Modeling Process. *Security & Privacy* // *IEEE* – DOI: 10.1109/MSP.2005.119
  26. Xu D., Pauli J. Threat-driven design and analysis of secure software architectures // *Journal of Information Assurance and Security* – 2006. – [Электронный ресурс]. – Режим доступа:



- <https://api.semanticscholar.org/CorpusID:17006191>, свободный (дата обращения: 07.10.2021)
27. Chen X., Liu Y., Yi J. A security evaluation framework based on STRIDE model for software in networks // *International Journal of Advancements in Computing Technology* – 2012. – [Электронный ресурс]. – Режим доступа: <https://api.semanticscholar.org/CorpusID:14340680>, свободный (дата обращения: 07.10.2021)
  28. Jouini M., Latifa Ben Arfa R., Aissa A. Classification of security threats in information systems // *International Conference on Ambient Systems, Networks and Technologies* – 2014. – DOI: 10.1016/j.procs.2014.05.452
  29. Lavrova D., Pechenkin A. Adaptive reflexivity threat protection // *Automatic Control and Computer Sciences* – 2015. – DOI: 10.3103/S0146411615080106
  30. Kammüller F. Modeling and Verification of Insider Threats Using Logical Analysis // *IEEE Systems Journal* – 2017. – DOI 10.1109/JSYST.2015.2453215
  31. Suleiman H., Alqassem I., Diabat A., Arnautovic E., Svetinovic D. Integrated smart grid systems security threat model // *Information Systems* – 2014. – DOI: 10.1016/j.is.2014.12.002
  32. Falah B., Akour M., Oukemeni S. An Alternative Threat Model-based Approach for Security Testing // *International Journal of Secure Software Engineering* – 2015. – DOI: 10.4018/IJSSE.2015070103
  33. Sharma A., Gandhi R., Zhu Q., Mahoney W., Sousan W. A social dimensional cyber threat model with formal concept analysis and fact-proposition inference // *International Journal of Information and Computer Security* – 2013. – DOI: 10.1504/IJICS.2013.058213
  34. Li X., Liu R., Feng Z., He K. Threat modeling-oriented attack path evaluating algorithm // *Transactions of Tianjin University* – 2009. – DOI: 10.1007/s12209-009-0029-y

35. Granström K., Willett P., Bar-Shalom Y. Asymmetric Threat Modeling Using HMMs: Bernoulli Filtering and Detectability Analysis // IEEE Transactions on Signal Processing – 2016. – DOI: 10.1109/TSP.2016.2529584
36. Zegzhda P., Zegzhda D., Kalinin M., Konoplev A. Security Modeling of Grid Systems Using Petri Nets // MMM-ACNS – 2012. – DOI: 10.1007/978-3-642-33704-8\_25
37. Xu D., Nygard K.E. Threat-driven modeling and verification of secure software using aspect-oriented Petri nets // IEEE Transactions on Software Engineering – 2006. – DOI: 10.1109/TSE.2006.40
38. Samson G.L., Usman M. Securing an Information Systems from Threats: A Critical Review // International Journal of Computer Applications Technology and Research – 2015. – vol. 4. – pp. 425-434
39. Андреев Н.О. Формирование и развитие угроз в информационных системах / Н.О. Андреев. – Москва: Московский финансово-промышленный университет «Синергия», 2006. – С. 87-100
40. 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
41. Чулков Д.Н. Модель угроз информационно-технических воздействий на информационные объекты – как основа создания комплексной системы обеспечения безопасности / Д.Н. Чулков. – Санкт – Петербург: Научно-технологические технологии, 2016. – С. 82-86
42. 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
43. 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
44. Нестерук Ф.Г., Нестерук Л.Г. Разработка модели пограничных угроз информационной безопасности // Инновации в науке. – 2017. – № 15(76). – С. 17–21.
45. 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
46. 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
47. 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
48. 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
49. 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

50. 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
51. 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
52. Банк данных угроз безопасности информации. ФСТЭК России [Электронный ресурс]. – Режим доступа: <http://bdu.fstec.ru>, свободный (дата обращения: 07.10.2021)
53. Методика определения угроз безопасности в информационных системах. ФСТЭК России [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/812>, свободный (дата обращения: 07.10.2021)
54. 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: 07.10.2021)
55. Рекомендации в области стандартизации ЦБР РС БР ИББС-2.4-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/902224877>, свободный (дата обращения: 07.10.2021)
56. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных учреждений здравоохранения,

- социальной сферы, труда и занятости. [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/902301906>, свободный (дата обращения: 07.10.2021)
57. ГОСТ Р ИСО/МЭК 27005 – 2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/1200084141>, свободный (дата обращения: 07.10.2021)
58. A. Shostack, Threat Modeling: Designing for Security // John Wiley & Sons Incorporation.
59. SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [Электронный ресурс]. – Режим доступа: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>, свободный (дата обращения: 07.10.2021)
60. Лукинова О.В. Компьютерные модели и алгоритмы управления безопасностью информационных систем // Автореферат диссертации на соискание ученой степени доктора технических наук. [Электронный ресурс]. – Режим доступа: <https://www.dissercat.com/content/kompyuternye-modeli-i-algoritmy-upravleniya-bezopasnostyu-informatsionnykh-sistem>, свободный (дата обращения: 07.10.2021)
61. Дунин В.С. Моделирование интеллектуальных систем управления защитой информации в инфокоммуникационных системах ОВД // Автореферат диссертации на соискание ученой степени кандидата технических наук. [Электронный ресурс]. – Режим доступа: <https://www.dissercat.com/content/modelirovanie-intellektualnykh-sistem-upravleniya-zashchitoy-informatsii-v-infokommunikatsionnykh-sistemah-ovd>, свободный (дата обращения: 07.10.2021)

62. Ерохин С.С. Методика аудита информационной безопасности объектов электронной коммерции // Автореферат диссертации на соискание ученой степени кандидата технических наук. [Электронный ресурс]. – Режим доступа: <https://www.dissercat.com/content/metodika-audita-informatsionnoi-bezopasnosti-obektov-elektronnoi-kommertsii>, свободный (дата обращения: 07.10.2021)
63. Герасименко В. А. Основы защиты информации в автоматизированных системах: В 2 кн. – Кн. 2. – М.: Энергоатомиздат, 1994. – 176 с.
64. Методические рекомендации ФСБ по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/420220524>, свободный (дата обращения: 07.10.2021)
65. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/901817218>, свободный (дата обращения: 07.10.2021)
66. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/902330983>, свободный (дата обращения: 07.10.2021)
67. Модель угроз типовой медицинской информационной системы (МИС) типового лечебного профилактического учреждения (ЛПУ) [Электронный ресурс]. – Режим доступа: [https://static-2.rosminzdrav.ru/system/attachments/attaches/000/017/251/original/Model\\_u\\_ugroz\\_MIS\\_LPU\\_2009\\_all.pdf?1389769143](https://static-2.rosminzdrav.ru/system/attachments/attaches/000/017/251/original/Model_u_ugroz_MIS_LPU_2009_all.pdf?1389769143), свободный (дата обращения: 07.10.2021)

68. Diasamidze S.V., Kuzmenkova E. Yu., Kuzntesov D.A., Sarkisyan A.R. Implementation of the role based access control in application for mobile device on the Android OS platform // Интеллектуальные технологии на транспорте. – 2016. – № 1(5). – С. 21-26
69. Королев И.Д., Поддубный М.И. Представление политики мандатного разграничения доступа через модель Харрисона-Руззо-Ульмана // Политический сетевой электронный журнал Кубанского Государственного Аграрного Университета. – 2015. – № 107. – С. 1715-1731.
70. Белим С.В., Богаченко Н.Ф. Использование решетки формальных понятий для построения ролевой политики разграничения доступа // Информатика и системы управления – 2018. – № 1(55). – С. 16-28.
71. Богаченко Н.Ф. Локальная оптимизация политики ролевого разграничения доступа // Статья в сборнике трудов конференции. Омск: Data, Modeling And Security: DMS 2017. [Электронный ресурс]. – Режим доступа: <http://ceur-ws.org/Vol-1965/paper14.pdf>, свободный (дата обращения: 07.10.2021)
72. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Аппроксимация функции безопасности дискреционной политики разграничения доступа // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции. – Омск. – 2016. – С. 9-11.
73. Бяшев А.Г., Калимолдаев М.Н., Рог О.А. Разработка методов многокритериального атрибутивного разграничения доступа к защищаемой информации // Знание. – 2016. – № 1-1(30). – С. 70-74.
74. Кучин И.Ю., Иксанов Ш.Ш., Белов С.В., Нургалиев М.М. Усовершенствование дискреционной модели доступа мобильных приложений к сервисам операционной системы Android // Вестник астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2016. – № 1. –

- С. 17-25.
75. Сизоненко А.Б. Арифметико-логическое представление матрицы доступа в дискреционной модели разграничения доступа // Вестник воронежского института МВД России – №3 – 2012. – С. 201-206
76. Кубышкин А.С. Разграничение прав доступа в системах защиты информации в АСТУ // Материалы XLVIII Международной научной студенческой конференции «Студент и научно-технический прогресс»: Информационные технологии / Новосиб. гос. ун-т. Новосибирск, 2010. С. 73
77. Иванов М.Е. Аспекты реализации моделей разграничения доступа и недостатки существующих подходов к документированию матрицы разграничения доступа // материалы Международной (заочной) научно-практической конференции “Теория и практика современной науки” – 2019. – С. 20-24
78. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с.
79. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с.
80. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/902301906>, свободный (дата обращения: 07.10.2021)
81. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования». [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/1200004675>, свободный (дата обращения: 07.10.2021)
82. СТО БР ИББС-1.0-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие



- положения. [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/902223529>, свободный (дата обращения: 07.10.2021)
83. Payment Card Industry Data Security Standard (PCI DSS) v2.0. [Электронный ресурс] – Режим доступа: [https://www.pcisecuritystandards.org/documents/pci\\_ds\\_s\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_ds_s_v2.pdf), свободный (дата обращения: 07.10.2021)
84. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. Приложение 10. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости. [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/902301906/titles/4ASLFF>, свободный (дата обращения: 07.10.2021)
85. Чекулаева Е.Н., Скворцова Н.О. Защита информационных потоков на предприятии // Ученый XXI века. – 2015. – №12(13) – С. 36-40
86. Макаров О.Ю., Хвостов В.А., Хвостова Н.В. Метод построения формальных моделей реализации угроз информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. – 2010 – Т. 6 – № 11 – С. 22-24.
87. Скрыль С.В., Джоган В.К., Киселев В.В., Демченков А.В. Особенности реализации математических моделей для оценки характеристик угроз безопасности использования информационных технологий // Информация и безопасность. – 2012. – Т. 15 – № 1 – С. 89-92.
88. Шапорин В.О., Плачинда О.Е. Разработка моделей угроз информационной безопасности для оценки вреда активам //

Технологический аудит и резервы производства. – 2015. – Т. 4 – №2(24) – С.10-15.

89. Карабанов Ю.С., Привалов А.А., Чимирзаев П.Э. Модуль анализа потенциальных моделей угроз телекоммуникационных объектов ОАО «РЖД» // Сборник трудов конференции «Юбилейная 70-я всероссийская научно-техническая конференция, посвященная дню радио» – 2015. – С. 310-311.
90. Новохрестов А.К. Модель угроз безопасности информации и её носителей / Новохрестов А.К., Конев А.А., Шелупанов А.А., Егошин Н.С. // Вестник Иркутского государственного технического университета. – 2017. – Т. 21. – № 10.
91. Французова Г.А., Гунько А.В., Басыня Е.А. Обеспечение информационной безопасности внутренних информационных потоков корпоративной сети // Материалы всероссийской научной конференции молодых ученых «Наука. Технологии. Инновации». – Новосибирск, 2013. – С. 41-43
92. Десницкий В.А., Котенко И.В., Чечулин А.А. Верификация информационных потоков для проектирования защищенных информационных систем со встроенными устройствами // Системы высокой доступности. – 2013. – Т. 9. - № 3. – С. 112-117
93. Киреенко А.Е. Разработка метода и алгоритма контроля информационных потоков в операционных системах с дискретным разграничением доступа к объектам // Безопасность информационных технологий. – 2013. – № 2. – С. 47-53.
94. Левченков А.Н., Хаджи Р.Х. Модель угроз безопасности информационного потока // Сборник материалов III Международной научно-практической конференции «Научное и образовательное пространство: перспективы развития». – 2016. – С. 19-24.
95. 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: <https://www.researchgate.net/publication/307107552>, свободный  
(дата обращения: 07.10.2021)

96. Alhabeeb M., Almuhaideb A., Le P., Srinivasan B. Information security threats classification pyramid // 24th IEEE International Conference on Advanced Information Networking and Applications Workshops. – 2010. – DOI: 10.1109/WAINA.2010.39
97. 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
98. Egoshin N.S., Konev A.A., Shelupanov A.A. Functional scheme of the process of access control: Methodology for the formation of normative documents on the access control // 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), DOI: 10.1109/RPC.2018.8482179
99. 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
100. 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.
101. Берж К. Теория графов и её применения. Пер. с фр. – М.: Иностранная литература, 1962. – 319 с

102. Уровни эталонной модели OSI. [Электронный ресурс] – Режим доступа: <http://just-networks.ru/osnovy-setej-peredachi-dannykh/model-osi>, свободный (дата обращения: 07.10.2021)
103. Кручинин С.В. О Некоторых обобщениях графов: мультиграфы, гиперграфы, метаграфы, потоковые и портовые графы, протографы, архиграфы // Вопросы науки. – 2017. - №3. – С. 48-67
104. BugTraq.Ru: Модели механизмов реализации типовых угроз безопасности PBC [Электронный ресурс]. – Режим доступа: <https://bugtraq.ru/library/books/attack/chapter03/02.html?k=9>, свободный (дата обращения: 07.10.2021)
105. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие // Ю. Н. Загинайлов. – М. Берлин: Директ-Медиа, 2015. – 253с.
106. 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.
107. Тарасенко А.И. Критерии оценки эффективности обеспечения информационной безопасности при управлении информационными потоками на основе динамических приоритетов // Science Time. – 2016. – № 4 – С. 816-825.
108. Способ защиты информационных потоков в многооператорных информационно-телекоммуникационных сетях / Верешник А.В., Федоров В.Г., Попова А.В. // Материалы IV Всероссийской научно-практической конференции “Современные информационные технологии. Теория и практика.”. – 2018 – С.154-158
109. Реализация средств верификации сетевых информационных потоков с использованием метода “Проверка на модели” / Десницкий В.А. // Материалы 9-й конференции по проблемам управления “Информационные технологии в управлении” – 2016. – С. 680-683

110. Jouini M., Latifa Ben Arfa Threat classification: State of art // Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber – 2016. – [Электронный ресурс]. – Режим доступа: [https://www.researchgate.net/publication/313241139\\_Threat\\_classification\\_State\\_of\\_art](https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art), свободный (дата обращения: 07.10.2021)
111. Ruf L., Thorn A., Christen T., Gruber B., 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.issss.ch/fileadmin/publ/agss/ISSS-AG-Security-Architecture\\_\\_Threat-Modeling\\_Lukas-Ruf.pdf](https://www.issss.ch/fileadmin/publ/agss/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf), свободный (дата обращения: 07.10.2021)
112. Geric S., Hutinski Z. Information system security threats classifications. // Journal of Information and Organizational Sciences. – 2007. – [Электронный ресурс]. – Режим доступа: <https://jios.foi.hr/index.php/jios/article/view/29>, свободный (дата обращения: 07.10.2021)
113. Ануфриенко С.А. Введение в теорию множеств и комбинаторику: учебное пособие/ С.А. Ануфриенко – Екб., 1998. – 62 с
114. Егошин Н.С. Модель угроз безопасности информации, передаваемой через Интернет / Егошин Н.С., Конев А.А., Шелупанов А.А. // Информация и безопасность. – 2018. – Т. 21 – № 4 – С. 530-533.
115. Модель угроз целостности информации / Штыренко С.И., Егошин Н.С. // Сборник избранных статей Научной Сессии ТУСУР – Т.1 – №1 – 2018. – С. 178-181
116. Приезжая А.Н. Автоматизированное формирование модели угроз безопасности // Вестник РГТУ. Серия: документоведение и архивоведение. Информатика. Защита информации и информационная безопасность – № 14(94) – 2012. – С. 240-257

117. Егошин Н.С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков. // Доклады ТУСУРа. – 2021. (направлено для публикации)
118. Egoshin N.S., Konev A.A., Shelupanov A.A. A Model of Threats to the Confidentiality of Information Processed in Cyberspace Based on the Information Flows Model // Symmetry. – 2020. – Volume 12. – Issue 11. – 1840. – pp. 1-18
119. Петренко В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко, И.В. Мандрица // Северо-Кавказский федеральный университет, 2018. – 118 с.
120. Егошин Н.С. Формирование модели нарушителя / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Безопасность информационных технологий. – 2017. – Т. 24. – №4. – С. 19–26. – DOI: 10.26583/bit.2017.4.02

## Приложение А – Акты внедрения



Общество с ограниченной ответственностью  
«Научно производственная фирма «Информационные Системы Безопасности»  
(ООО «НПФ «ИСБ»)

### АКТ

«08» 08 2021 г.

г. Томск

№ 1

#### Внедрения результатов диссертационной работы Егошина Николая Сергеевича

Комиссия в составе:

**Председатель комиссии:**

Смолянинов В.В. – Генеральный директор.

**Члены комиссии:**

Давыденко А.В. – Заместитель генерального директора;

Анфиногенов Д.С. – Заместитель директора департамента – начальник отдела ПНР;

Турунтаев М.А. – Ведущий специалист по защите информации ОПНР.

Составили настоящий акт о том, что результаты диссертационной работы Егошина Н.С. «Модели угроз нарушения безопасности информационных потоков в киберпространстве», представленной на соискание ученой степени кандидата технических наук, внедрены в деятельность ООО «НПФ «ИСБ» при оказании услуг проведения аудита информационной безопасности ИСПДи.

При проведении аудита информационной безопасности, который включает в себя определение актуальных угроз, была использована разработанная Егошиным Н.С. модель угроз безопасности информации. Ее использование позволило расширить перечень актуальных угроз информации за счет выделения типовых угроз с последующей конкретизацией.

Применение модели модели угроз, разработанной Егошиным Н.С., позволило получить полный перечень типовых угроз безопасности информации, обрабатываемой в ИСПДи. Полученный список был учтен при определении перечня актуальных угроз, что показало необходимость внедрения в систему дополнительных механизмов защиты.

Результатом внедрения работы Егошина Н.С. в деятельность ООО «НПФ «ИСБ» стал перечень из 43 угроз безопасности информации в ИСПДи, что на 14 % больше, чем количество угроз, выявленных экспертами ранее.

Председатель комиссии:

Смолянинов В.В.

Члены комиссии:

Давыденко А.В.

Анфиногенов Д.С.

Турунтаев М.А.






Удостоверяющий  
центр Сибири

Общество с ограниченной  
ответственностью  
«Удостоверяющий центр  
Сибири»

634009, г. Томск, пр-т Ленина, 110  
ИНН/КПП/ОГРН 7017311494/701701001/1127017020767

тел: (3822) 900-111  
факс: (3822) 900-111  
e-mail: office@uacs.ru  
http:// www.uacs.ru

УТВЕРЖДАЮ  
Директор  
ООО «УЦ Сибири»  
  
Перфильев А.В.  
2021 г.

АКТ  
внедрения результатов диссертационной работы  
Егошина Николая Сергеевича

Комиссия в составе:

**Председатель комиссии:**  
Перфильев А.В. – директор.

**Члены комиссии:**  
Михайлов Н.С. – руководитель отдела по защите информации;

Составили настоящий акт о том, что результаты диссертационной работы Егошина Н.С. «Модели угроз нарушения безопасности информационных потоков в киберпространстве», представленной на соискание ученой степени кандидата технических наук, внедрены в деятельность ООО «УЦ Сибири» при оказании услуг по разработке организационно-распорядительных документов.

При формировании политики разграничения доступа к информации в информационной системе была использована разработанная Егошиным Н.С. методика формирования политики разграничения доступа. Ее использование позволило разграничить доступ к каналам информационного взаимодействия как самостоятельным структурным элементам системы.

Применение методики формирования политики разграничения доступа, разработанной Егошиным Н.С. позволило расширить содержание указанной политики и сократить время, затрачиваемое на её разработку.

Результатом внедрения работы Егошина Н.С. в деятельность ООО «УЦ Сибири» стало уменьшение времени, необходимого для формирования политики разграничения доступа на 19 % (в частном случае с 16 до 13 часов).

Председатель комиссии

  
Перфильев А.В.

Члены комиссии

  
Михайлов Н.С.





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

**УТВЕРЖДАЮ**

Проректор по учебной работе ТУСУР

П.В. Сенченко

2021 г.

«10» 09

**АКТ**

о внедрении результатов диссертационной работы  
Егошина Николая Сергеевича в учебный процесс

Комиссия в составе:

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

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

Костюченко Е.Ю., к.т.н., доцент кафедры КИБЭВС ТУСУР;

Новохрестов А.К., к.т.н., доцент кафедры КИБЭВС ТУСУР

составила настоящий акт о нижеследующем.

Результаты диссертационной работы Егошина Н.С., используются в учебном процессе на факультете безопасности ТУСУР при чтении курса лекций и проведении практических занятий по «Управление информационной безопасностью» и «Разработка и эксплуатация защищенных автоматизированных систем» для подготовки специалистов по защите информации, обучающихся по специальностям «10.05.02 – Информационная безопасность телекоммуникационных систем», «10.05.03 – Информационная безопасность автоматизированных систем» и «10.05.04 – Информационно-аналитические системы безопасности».

В курсе «Управление информационной безопасностью» используются результаты работы Егошина Н.С. по разработке моделей угроз безопасности информации, позволяющие студентам ознакомиться с процессом применения моделей угроз безопасности информации, обрабатываемой в информационной системе.

В курсе «Разработка и эксплуатация защищенных автоматизированных систем» используется предложенная Егошиным Н.С. методика формирования политики разграничения доступа в информационной системе, позволяющая студентам ознакомиться с процессом построения последней. 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 формированию политики разграничения доступа.

Председатель комиссии:

 Давыдова Е.М.

Члены комиссии:

 Копев А.А.

 Костюченко Е.Ю.

 Новохрестов А.К.