На правах рукописи

Егошин Николай Сергеевич

МОДЕЛИ УГРОЗ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ В КИБЕРПРОСТРАНСТВЕ

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Томск 2021

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Научный руководитель – Шелупанов Александр Александрович, доктор технических наук, профессор

Официальные оппоненты: Ложников Павел Сергеевич, доктор технических наук, профессор, заведующий кафедрой комплексной защиты информации Омского государственного технического университета

Золотарев Вячеслав Владимирович, кандидат технических наук, заведующий кафедрой безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева, г. Красноярск

Ведущая организация – Национальный исследовательский ядерный университет «МИФИ», г. Москва

Защита состоится «28» декабря 2021 г. в 14:00 часов на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г. Томск, пр. Ленина 40, ауд. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУР по адресу: 634045, г. Томск, ул. Красноармейская 146, а также на сайте ТУСУР: https://postgraduate.tusur.ru/urls/wgihl0qc

Автореферат разослан «___» ноября 2021 г.

Ученый секретарь диссертационного совета  Костюченко Евгений Юрьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. 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.

Повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей. Преимущества данного подхода очевидны: снижение затрат на обработку и хранение документов, быстрый поиск. В эпоху «информационного бума» данный подход является единственным выходом из затруднительного положения, связанного с ростом объемов обрабатываемой информации.

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 современном 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. Очевидно, что 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 зависит 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. Rannenberg, B. Schneier, G. Stoneburmner, 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 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. Комплексное применение моделей угроз конфиденциальности и целостности/доступности информации позволило 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) 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 10 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 таблиц и 29 рисунков.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулирована цель, определены задачи, научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе рассматриваются подходы к формированию политик разграничения доступа к информации, обрабатываемой в системе, а также непосредственно подходы к описанию и идентификации угроз и построению моделей угроз информации.

В результате проведенного анализа можно заключить, что в российской законодательной базе нет унифицированного стандарта, содержащего методику формирования политики разграничения доступа. Существующие решения носят частный характер. Рассмотренные методики также не учитывают модель информационных потоков в системе, а руководствуются только регламентированным перечнем прав доступа, что не позволяет осуществлять полный контроль над разграничением доступа из-за вероятности появления новых неучтенных ранее информационных потоков. Также рассматриваемые методики не учитывают модель угроз информации, хотя именно модель угроз позволяет определить возможность появления несанкционированных информационных потоков.

Для того, чтобы разработать методику формирования политики разграничения доступа необходимо, чтобы модель элементарных информационных потоков:

1) учитывала все возможные типы каналов взаимодействия в информационной системе;
2) учитывала все возможные типы носителей информации в информационной системе.

Для обеспечения контроля управления доступом, необходимо учитывать и модель угроз безопасности информации. В ходе анализа подходов к построению моделей угроз безопасности информации были выявлены следующие недостатки:

1) в некоторых моделях угроз модель нарушителя оказывает непосредственное влияние на формирование перечня угроз;
2) отсутствие системности – в рамках одной модели описываются как обобщенные угрозы, так и частные случаи;
3) отсутствует разделение на угрозы, направленные на систему и информацию;
4) построение перечней угроз основывается на субъективном мнении эксперта.

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.

Во второй главе предлагается модель информационных потоков в системе, описывается процесс ее формирования и пример применения.

Модель информационных потоков позволяет построить полную схему информационных потоков в системе, которую в свою очередь можно применить при обеспечении некоторых вопросов информационной безопасности. Например, контроль управления доступом к информационным ресурсам и определение перечня угроз информации, обрабатываемой в системе.

Любую схему обмена информацией можно представить, как совокупность элементарных информационных потоков. Элементарный информационный поток включает в себя три элемента: источник, канал передачи информации, приемник.

Данное понятие можно наглядно продемонстрировать, если применить теорию графов. Введем следующие обозначения: V – множество носителей информации (множество вершин графа), E – множество каналов передачи информации (множество ребер графа). Сопоставив любые два элемента из V и один из E, мы получим элементарный информационный поток в виде неориентированного графа с двумя вершинами (рис. 1).

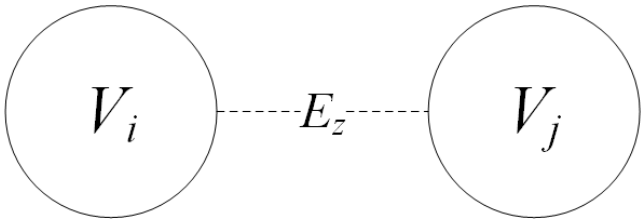

Рисунок 1 – Элементарный информационный поток.

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

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

где V_i, V_j– множества носителей информации;

E_z – множество каналов передачи информации.

Множество носителей информации было разделено на три подмножества:

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

где V_1 – множество пользователей, V_2 – множество процессов, V_3 – множество устройств хранения информации (цифровой носитель, база данных и т. д.).

Множество каналов взаимодействия имеет 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.

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. 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.

Итоговое множество всех элементарных потоков имеет следующий вид:

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

где $g_1 = \{V_1, E_1, V_2\}$; $g_2 = \{V_1, E_2, V_2\}$; $g_3 = \{V_2, E_1, V_2\}$; $g_4 = \{V_2, E_2, V_2\}$; $g_5 = \{V_2, E_3, V_2\}$; $g_6 = \{V_2, E_4, V_2\}$; $g_7 = \{V_2, E_1, V_3\}$; $g_8 = \{V_2, E_2, V_3\}$.

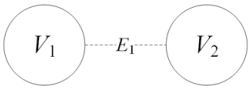

Рисунок 2 – Поток $g_1 = \{V_1, E_1, V_2\}$

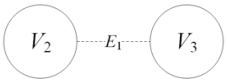

Рисунок 3 – Поток $g_2 = \{V_1, E_2, V_2\}$

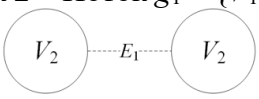

Рисунок 4 – Поток $g_3 = \{V_2, E_1, V_2\}$

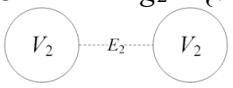

Рисунок 5 – Поток $g_4 = \{V_2, E_2, V_2\}$

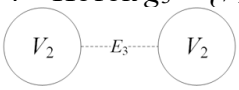

Рисунок 6 – Поток $g_5 = \{V_2, E_3, V_2\}$

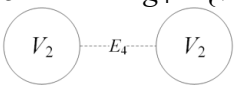

Рисунок 7 – Поток $g_6 = \{V_2, E_4, V_2\}$

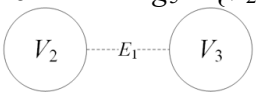

Рисунок 8 – Поток $g_7 = \{V_2, E_1, V_3\}$

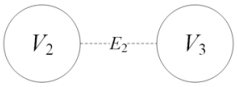

Рисунок 9 – Поток $g_8 = \{V_2, E_2, V_3\}$

Результатом объединения всех указанных на рисунках 2–9 графов будет являться ненаправленный мультипликативный граф (рис. 10), который и будет представлять из себя модель элементарных информационных потоков при осуществлении взаимодействия в киберпространстве.

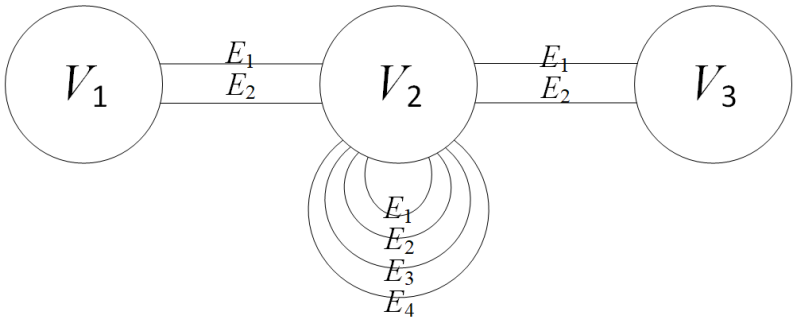

Рисунок 10 – Ненаправленный мультипликативный граф

Разработанная модель позволяет построить схему информационных потоков в организации, используя конечное множество G. Продемонстрируем применение модели информационных потоков на примере процесса обмена электронной почтой.

В рассматриваемом примере переписка осуществляется между двумя пользователями с их мобильных устройств, которые подключены к сети Интернет беспроводным соединением (общая схема описываемого процесса представлена на рисунке 11).

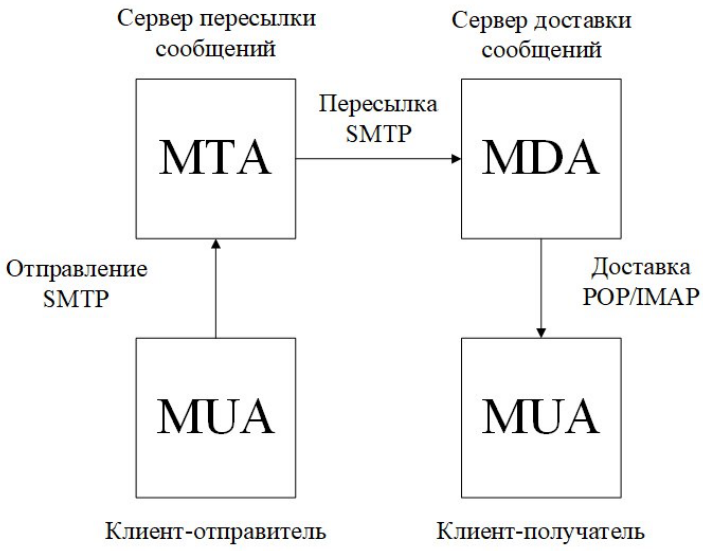

Рисунок 11 – Общая схема процесса передачи электронной почты

Из обозначенной схемы вытекает 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.

Теперь построим из этого перечня информационных потоков уже полный перечень элементарных информационных потоков, учитывая, что MDA и MTA – это разные устройства. И все же будем считать, что со стороны MDA за процессы получения, записи в хранилище, считывания из него и пересылки на MUA отвечает один и тот же программный продукт. Каждый поток разбивается на два элементарных, так как модель подразумевает разделение канала взаимодействия на электромагнитный и виртуальный. Дополнительно введем обозначения всех участников процесса согласно модели информационных потоков.

Множество пользователей:

$$V_1 = \{ v_1^1, v_1^2 \},$$

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

Множество ПО:

$$V_2 = \{v_2^1, v_2^2, v_2^3, v_2^4\},$$

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

Множество хранилищ информации:

$$V_3 = \{v_3^1\},$$

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:

$$S = \{ s_i \mid s \in S\},\ i = \overline{1,\ 14}$$

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

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 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 еще 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 ее элементов вместо бессистемного определения вероятных угроз.

А теперь, чтобы поставить смысловую точку в изучении примера, отметим следующее: можно заметить, что в рассматриваемом примере присутствует четырнадцать информационных потоков, в то время как в модели информационных потоков их только восемь. Дело в том, что модель по определению носит абстрактный характер, а каждый ее 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:

— $g_1 \sim s_1, s_{13}$;
— $g_2 \sim s_2, s_{14}$;
— $g_5 \sim s_3, s_5, s_6, s_{11}$;
— $g_6 \sim s_4, s_{12}$;
— $g_7 \sim s_7, s_9$;
— $g_8 \sim s_8, s_{10}$.

Таким образом, можно сделать вывод, что любой процесс передачи информации в системе можно не просто описать набором элементарных информационных потоков, но свести к конечному множеству, мощность которого равна восьми.

В **третьей главе** предлагается модель угроз информации, обрабатываемой в системе, которая отличается полнотой учета всех типовых угроз и каналов передачи информации как отдельных элементов системы. Описан процесс формирования модели угроз, представлен полный включенных в модель перечень типовых угроз информации, произведено сравнение авторской модели с наиболее полной моделью угроз – банком данных угроз безопасности информации ФСТЭК.

Для формирования собственной модели угроз была применена описанная ранее модель информационных потоков. Канал передачи информации – это не какой-то абстрактный объект, а вполне реальный элемент системы, который обладает некоторыми физическими и/или виртуальными свойствами. Это означает, что на него возможно такое же воздействие, как и на два других элемента потока.

Само определение несанкционированного воздействия подразумевает появление в системе нового элемента, который будет оказывать это самое воздействие.

Используя обозначенную ранее нотацию, данную ситуацию можно изобразить следующим образом (рис. 12).

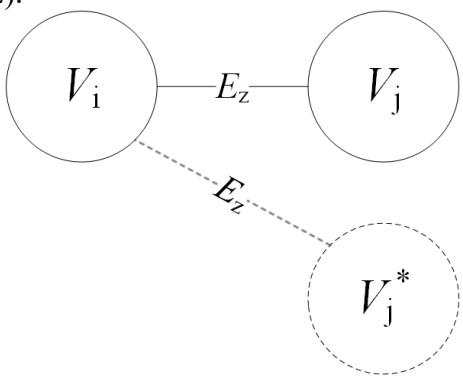

Рисунок 12 – Возникновение несанкционированного элемента V_j*, который оказывает воздействие на информацию в элементе V_i

Существует два способа взаимодействия с информацией:

1) Чтение;
2) Непосредственное воздействие (изменение, уничтожение, подмена)

Н/с действия первого вида приводят к нарушению конфиденциальности информации, а н/с действия второго приводят к нарушению целостности или доступности.

Если говорить исключительно о конфиденциальности информации, то по определению ее нарушение безопасности не подразумевает нарушения целостности или доступности, хотя и может к этому привести. Исходя из определения элементарного информационного потока, 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 расчет мощности множества:

$$N = p^i,$$

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 трех элементов. В итоге общее количество завязанных на компрометации элементов состояний элементарного информационного потока будет равняться восьми. Все возможные комбинации представлены в таблице 1. В ячейки таблицы занесена информация о статусе компрометации элемента, где «1» - элемент скомпрометирован, «0» - не скомпрометирован.

Таблица 1 – 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 приведет к высокому уровню дублирования различных угроз, потому достаточным будет рассмотрение только четырех 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 «прослушки» элемента, т. е. доступ к хранимой в нем информации из-за пределов контролируемой зоны. Однако, «прослушка» уже не будет применима ко всем трем элементам, т. к. слежение за вершиной подразумевает либо внедрение в уже существующий канал передачи информации, что тождественно прослушиванию канала, либо возникновение нового неразрешенного, что совпадает с подменой канала, и все 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:

$$K = \{k_1, k_2, k_3, k_4\}, \text{ где}$$

k_1 – подмена приемника V_i (получение защищаемой информации несанкционированным элементом V_i^*);

k_2 – подмена приемника V_j (получение защищаемой информации несанкционированным элементом V_j^*);

k_3 – наличие несанкционированного канала E_z (подмена канала на н/с);

k_4 – контроль канала E_z (получение информации несанкционированным лицом из-за пределов санкционированной зоны).

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

Для начала рассмотрим первый поток $s_1 = (v_1^1, e_1^1, v_2^1)$. Напомним: v_1^1, – это 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 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_1^1. 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.

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 ее превентивного характера.

Снова вернемся к множеству элементарных информационных потоков и множеству угроз целостности и доступности. Зная, что оба эти множества конечны, можно применить каждую из угроз к каждому потоку, т. е. сопоставить каждый элемент множеств K с каждым элементом множества G и получить новое множество, которое будет состоять из всех сочетаний угроз и потоков, т. е. являться их декартовым произведением.

$$G \times K = \{g_i k_j \mid g \in G, k \in K\}, i = \overline{1, 8}, j = \overline{1, 4}$$

$$|G \times K| = |G| * |K| = 8 * 4 = 32.$$

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.

Как было сказано ранее, на любой из элементов элементарного информационного потока, а значит и на информацию, может быть оказано любой из трех видов несанкционированного воздействия:

— уничтожение;
— искажение;
— подмена.

Снова обратимся к понятию элементарного информационного потока и разберем 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. 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

Таблица 2 – Соотнесение видов воздействия и нарушаемого аспекта

Вид воздействия	V_i	E_z	V_j
Изменение	Целостность	Целостность	Целостность
Подмена	Целостность	Доступность	Целостность
Уничтожение	Целостность	Доступность	Целостность

Множество угроз целостности:

$$C = \{c_i \mid c \in C\},\ i = \overline{1,\ 7}\ ,\ \text{где}$$

c_1 – подмена источника V_i (передача искаженной информации элементу V_j);
c_2 – подмена источника V_j (передача искаженной информации элементу V_i);
c_3 – подмена источника V_i (уничтожение информации в элементе V_j);
c_4 – подмена источника V_j (уничтожение информации в элементе V_i);
c_5 – подмена источника V_i (подмена информации в элементе V_j);
c_6 – подмена источника V_j (подмена информации в элементе V_i);
c_7 – воздействие на информацию при передаче по каналу E_z (искажение информации в канале).

Обозначим множество угроз доступности:

$D = \{d_1, d_2\}$, где

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

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

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

Для начала рассмотрим первый поток $s_1 = (v_1^1, e_1^1, v_2^1)$. Применим каждую из четырех угроз к данному потоку.

При реализации угрозы c_1 осуществляется подмена пользователя v_1^1 несанкционированным пользователем $v_1{}_1^{1*}$, 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_{11} 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_{21}. 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_{21} 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_{11} 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_{21} несанкционированным софтом $v_2^{1\,*}$, в результате чего санкционированный пользователь v_{11} 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 все к тому же примеру с экраном, примером реализации

угрозы может являться частичная неработоспособность устройства вывода в результате действия закладок.

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.

$$G \times (C \cup D) = \{g_i c_j, g_i d_k \mid g \in G, c \in C, d \in D\}, i = \overline{1, 8}, j = \overline{1, 7}, k = \overline{1, 2}$$

$$|G| * (|C| + |D|) = 8 * (7+2) = 72.$$

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

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

По итогу сравнения авторской модели с аналогом – «Банком данных угроз ИБ ФСТЭК», всем угрозам из аналога удалось определить соответствующие угрозы из авторской модели, однако, составить полное взаимное соотношение не удалось: не для каждой типовой угрозы из авторской модели нашлись угрозы из аналога. В «Банке данных угроз ИБ ФСТЭК» нет примеров для следующих типовых угроз:

1. g_1c_4 – Уничтожение информации, обрабатываемой пользователем, при взаимодействии по электромагнитному каналу;
2. g_1c_5 – Подмена информации, обрабатываемой процессом, при взаимодействии по электромагнитному каналу;
3. g_1c_6 – Подмена информации, обрабатываемой пользователем, при взаимодействии по электромагнитному каналу;
4. g_2c_2 – Передача н/с процессом информации санкционированному пользователю по виртуальному каналу;
5. g_3c_1 – Передача н/с процессом информации санкционированному процессу V_j по электромагнитному каналу;
6. g_3c_2 – Передача н/с процессом информации санкционированному процессу V_i по электромагнитному каналу;
7. g_3c_5 – Подмена информации, обрабатываемой процессом V_j, при передаче по электромагнитному каналу;
8. g_3c_6 – Подмена информации, обрабатываемой процессом V_i, при передаче по электромагнитному каналу;
9. g_3c_7 – Воздействие на информацию при передаче по электромагнитному каналу между процессами;
10. g_5c_6 – Подмена информации, обрабатываемой процессом V_j, при взаимодействии по удаленному электромагнитному каналу;
11. g_5c_7 – Воздействие на информацию при ее передаче по удаленному электромагнитному каналу между процессами;
12. g_7c_6 – Подмена информации, хранимой на носителе информации, при взаимодействии по электромагнитному каналу;
13. g_7c_7 – Воздействие на информацию при ее передаче по электромагнитному каналу от процесса к носителю.

Четвертая глава посвящена апробации результатов диссертационного исследования, разработке методики формирования политики разграничения доступа и модели нарушителя.

Разработанная методика отличается возможностью определения прав доступа с учетом типа канала связи.

На вход методики поступают следующие элементы:

— список сотрудников (V_1);
— список документов (V_3);
— список программных средств (V_2);
— список рабочих станций (A);
— список используемых протоколов (E_2, E_4);
— список используемых драйверов (E_1, E_2);
— список правд доступа (AP).

Управляющее воздействие оказывается разработанными ранее моделями информационных потоков и угроз информации, а также должностными инструкциями для персонала.

Механизмом служат сотрудники службы безопасности непосредственно либо через предлагаемое программное средство.

Выходными данными методики является нормативный документ (N), который содержит в себе итоговую политику разграничения доступа.

На рисунке 13 представлена методика в графической нотации IDEF0. Как видно, она состоит из четырех функциональных блоков.

Рисунок 13 - Методика формирования политики разграничения доступа

На первом этапе применения методики строится схема информационных потоков в организации. Данная схема включает в себя полное множество всех возможных информационных потоков в системе.

Получившаяся схема поступает на вход блоков 2 и 3.

На втором этапе на основе полной схемы информационных потоков и согласно разработанной автором модели угроз информации определяется полный перечень типовых угроз информации.

На третьем этапе методики на основе перечня прав доступа определяется список разрешенных потоков, а на их основе строится матрица доступа к информационным ресурсам. Пример матрицы доступа представлен в таблице 19.

Таблица 19 – Матрица доступа к информационным ресурсам

<table>
<tr><td></td><td colspan="2">ЭР1</td><td colspan="2">ЭР2</td><td colspan="2">ЭР3</td></tr>
<tr><td rowspan="5">Пользователь 1</td><td colspan="2" rowspan="5">-</td><td rowspan="4">ПО1</td><td>РС1</td><td rowspan="4">ПО1</td><td>РС1</td></tr>
<tr><td>РС2</td><td rowspan="3">РС2</td></tr>
<tr><td>РС3</td></tr>
<tr><td>ПО2</td><td>РС1</td><td>РС3</td></tr>
<tr><td></td></tr>
<tr><td rowspan="2">Пользователь 2</td><td rowspan="2">ПО3</td><td>РС1</td><td colspan="2" rowspan="2">-</td><td colspan="2" rowspan="2">-</td></tr>
<tr><td>РС2</td></tr>
<tr><td rowspan="2">Пользователь 3</td><td rowspan="2">ПО3</td><td>РС1</td><td colspan="2" rowspan="2">-</td><td rowspan="2">ПО1</td><td>РС1</td></tr>
<tr><td>РС2</td><td>РС2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>РС3</td></tr>
</table>

В данной методике матрица доступа – это не дискреционная матрица в ее привычном понимании. Авторская матрица позволяет определить какому пользователю необходимы права доступа к какой рабочей станции и к каким программным средствам, чтоб он смог реализовать свое право доступа к защищаемой информации.

Итоговый нормативный документ содержит в себе следующие части:

— схема информационных потоков;
— список программного обеспечения, к которому имеют доступ сотрудники;
— список рабочих станций, к которым имеют доступ сотрудники;
— список используемых протоколов;
— список используемых драйверов;
— матрица доступа MD;
— список типовых угроз информации.

Процесс разграничения доступа неотделим от формирования модели нарушителя. Учитывая недостатки описанных в обзоре аналогов моделей, можно составить перечень основных параметров нарушителя информационной безопасности, на основе которых будет строиться новая модель описания нарушителя (табл. 3).

Таблица 3 – 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 нем	Отсутствие(0)/наличие (1)
E(xtra) – возможность использования несанкционированного средства обработки информации	Отсутствие(0)/наличие (1)
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. 14)
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. 14) 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.

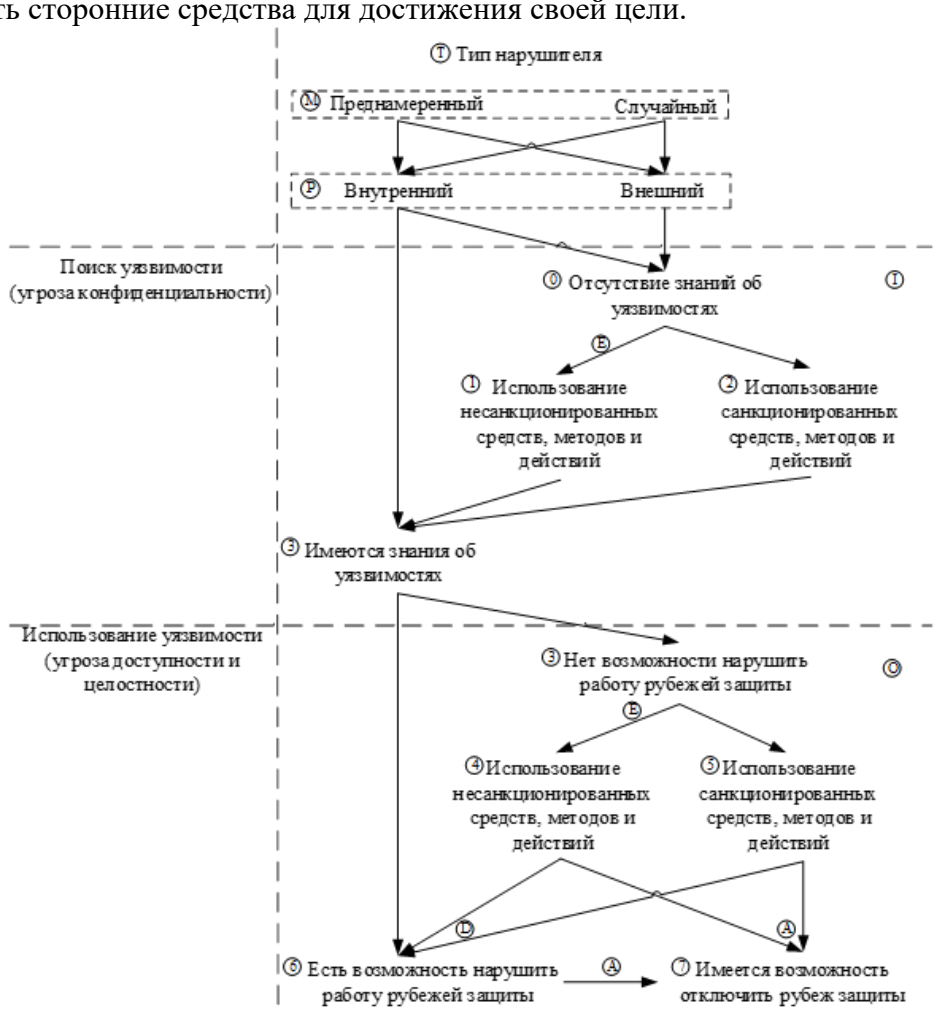

Рисунок 14 – Схема отображения параметров нарушителя

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 активный характер.

Исходя из этой схемы (рис. 4), 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;

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;

2 уровень – нарушитель, который использует свое положение чтобы собирать информацию об уязвимостях в рубежах защиты, используя санкционированные методы;

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;

5 уровень – изначально внутренний нарушитель, который для достижения своих целей использует санкционированные методы;

6 уровень – изначально внутренний нарушитель с высоким уровнем доступа, имеющий возможность нарушить работу рубежей защиты, пользуясь своим служебным положением;

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

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.

В заключении приведены основные результаты и выводы по проделанной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В результате выполненного исследования в области разработки методики формирования политики разграничения доступа была достигнута поставленная цель. Получены следующие основные результаты:

2. выполнен анализ текущего состояния предметной области: методик формирования политик разграничения доступа и моделей угроз информации, использующихся при идентификации угроз; были выделены недостатки требующие устранения;

3. на основе теории графов разработана модель элементарных информационных потоков, которая позволяет построить полную схему информационных потоков, которая учитывает все возможные случаи взаимодействия в киберпространстве и содержит описание всех элементов системы, участвующих в процессах информационного взаимодействия;

4. на основе модели элементарных информационных потоков разработана модель угроз безопасности информации, обрабатываемой в информационной системе, которая позволяет классифицировать типовые угрозы информации в зависимости от скомпрометированного элемента;

5. комплексное применение моделей угроз информации позволило выявить 13 дополнительных угроз в сравнении с аналогом – «Банк данных угроз безопасности информации ФСТЭК»;

6. с использованием созданных моделей разработана методика формирования политики разграничения доступа, отличающаяся от аналогов наличием возможности разграничить доступ к каналам взаимодействия, как к самостоятельным элементам системы;

7. методика была апробирована в ходе деятельности НПК «Информационные системы безопасности» и в рабочих процессах «УЦ Сибири», применение методики позволило модифицировать существующие политики разграничения доступа.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ РАБОТЫ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

1. Егошин Н.С. Модель угроз безопасности информации, передаваемой через интернет / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Информация и безопасность. – 2018. – Т. 21. – №4. – С. 530-533.

2. 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

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

4. Егошин Н.С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков. // Доклады ТУСУРа. – 2021. (направлено для публикации)

В изданиях WoS и Scopus:

5. 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

6. 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

В других изданиях, сборниках трудов и тезисов конференций:

7. Егошин Н.С., Конев А.А., Шелупанов А.А. Применение модели информационных потоков при разработке политики разграничения доступа и определении перечня угроз информации в системе // Микроэлектроника и информатика – 2019. 26-я Всероссийская межвузовская научно-техническая конференция студентов и аспирантов: тезисы докладов. – М.: МИЭТ, 2019. – С. 159.

8. Егошин Н.С. Модель информационных потоков в контексте обеспечения информационной безопасности // Сборник научных трудов XV Международной конференции студентов, аспирантов и молодых ученых. В 7-ми томах. Под редакцией И.А. Курзиной, Г.А. Вороновой. 2018 - С 75-77

9. Егошин Н.С., Конев А.А., Шелупанов А.А. Методика формирования политики разграничения доступа к информационной системе // Доклады VII Пленума СибРОУМО по образованию в области информационной безопасности и XVI конференции: Томск, 6–9 июня 2018 г. – Томск: В-Спектр, 2018. – С. 126-132.

10. Штыренко С.И., Егошин Н.С. Модель угроз целостности информации // Сборник избранных статей Научной Сессии ТУСУР - Т.1 - №1 - 2018 - с. 178-181