

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ЛЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ительная техника"

Кафедра ИнОУП

Факультет "Вычисл

говки

46.04.02 "Документоведение и

Направление подго

архивоведение"

"Документационное обеспечение
управления электронного
правительства"

Магистерская программа

ЕРСКАЯ ДИССЕРТАЦИЯ
на тему

МАГИСТ

топотоками на основе анализа моделей
оборота

Управление конфиденциальными докумен
документо

20.06.2019

П.В. Пронькин

Автор работы

(инициалы, фамилия)

(подпись, дата)

А.В. Печерский

Научный руководитель

(инициалы, фамилия)

(подпись, дата)

Ю.Г. Кирюхин

Нормоконтролёр

Зам.зав.каф. ИнОУП,
доцент

(должность, место работы)

20.06.2019

(подпись, дата)

20.06.2019

Рецензент

научный руководитель

(должность, место работы)

20.06.2019

(подпись, дата)

анию, профилю
Государственной

Магистерская диссертация по содержанию и объему соответствует зад:
направления подготовки и может быть допущена к защите на заседании I
аттестационной комиссии "28" июня 2019 г.

Проверяющий преподаватель

20.06.2019

(подпись, дата)

А.В. Печерский
(инициалы, фамилия)

Работа допущена к защите (протокол заседания кафедры от 20.06.2019 № 10)

Заведующий кафедрой

20.06.2019

(подпись)

Л.Р. Фионова
(инициалы, фамилия)

Диссертация защищена с оценкой хорошо (протокол заседания ГЭК от 28.06.19 № 4)

етарь ГЭК

20.06.2019

(подпись)

Ю.Ю. Фионова
(инициалы, фамилия)

Секр

Реферат

Пояснительная записка содержит 74 листа, 18 рисунков, 14 источников.

КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ, СЛУЖБА КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА, СИСТЕМНЫЙ АНАЛИЗ, МОДЕЛИ ДОКУМЕНТООБОРОТА

Целью является оптимизация службы конфиденциального делопроизводства (КД) на основе анализа критериев и моделей управления в системе документооборота.

Задачами являются анализ процедуры оптимизации системы конфиденциального документооборота и анализ специфики системы конфиденциального документооборота организации с целью построения ее морфологической, иерархической и информационной моделей.

Объектом является документационное обеспечение организации при наличии защищаемой информации.

Предметом является технология обработки защищаемой документированной информации в системе ДООУ организации.

Проблема заключается в том, что эффективное управление документопотоками системы конфиденциального документооборота организации предполагает оперативный учет вероятных факторов внешних и внутренних информационных угроз, а также применение технологий конфиденциального делопроизводства; однако, выработка управляющего решения в такой системе возможна при моделировании и системном анализе документооборота с учетом специфики объекта управления.

Для достижения поставленных целей в работе применяются методы моделирования при системном подходе в проблеме управления.

В первом разделе рассмотрены критерии оптимизации документооборота, структура и модели службы конфиденциального документооборота.

Во втором разделе рассмотрены средства сохранения конфиденциальности защищаемых документов.

В третьем разделе рассмотрены действия, предшествующие созданию службы конфиденциального документооборота.

В четвертом разделе рассмотрены действия организации, желающей установить режим конфиденциальности документов.

Материалы диссертации апробированы на XIX Всероссийской научно-практической конференции «Современные технологии документооборота в бизнесе, производстве и управлении».

Отдельные результаты работы отражены в публикации Пронькина П.В. и Печерского А.В. «Управление конфиденциальным документооборотом на основе анализа моделей».

Содержание

Введение.....	6
1 Конфиденциальный документооборот	7
1.1 Структура службы конфиденциального делопроизводства	10
2 Система защиты информации.....	18
3 Работа эксперта	Ошибка! Закладка не определена.
3.1 Постановка задачи	43
3.2 Определение и классификация потенциальных угроз информации.	48
3.3 Оценка уязвимости информации.....	52
3.4 Постановка требований к защите информации	58
3.5 Моделирование и проектирование систем защиты информации.	61
4 Действия организации по установлению режима конфиденциальности документооборота	70
Заключение	72
Список использованных источников и литературы	73

Введение

Информация, особенно конфиденциальная, в настоящее время является важным объектом.

Задача сохранения конфиденциальности защищаемых документов является актуальной [9]. Создание службы конфиденциального документооборота и поддержка ее деятельности предполагает применение научных методов управления конфиденциальными документопотоками на основе системного анализа всех влияющих факторов на возможные риски реализации информационных угроз.

В настоящее время специалистами в сфере конфиденциального документооборота накоплен значительный опыт управления, однако дополнительные резервы в совершенствовании такого управления связаны с применением методологии системного анализа и моделирования конфиденциального документооборота с целью получения большего количества данных и их обработки.

В связи с этим предметом магистерской диссертации является рассмотрение процесса создания и поддержки деятельности службы конфиденциального документооборота с применением анализа различных моделей документооборота.

1 Конфиденциальный документооборот

Служба конфиденциального документооборота может рассматриваться как комплекс двух подсистем: службы документооборота и системы защиты информации.

Необходимо отметить, что из-за специфики обрабатываемой информации к конфиденциальному документообороту предъявляются особые требования, которые влияют на деятельность. Например, требование централизации и разделения открытых документов от закрытых (создание специального подразделения) способствует концентрации всех проводимых мероприятий, средств по установлению и поддержанию режима конфиденциальности. Также важной особенностью является необходимость тщательного и постоянного учета каждого из конфиденциальных документов.

Особо стоит вопрос оптимизации службы конфиденциального документооборота. Уровень оптимизации может быть оценен по экономическим показателям [7]. Подход к оценке представлен на рисунке 1.

К вложениям в безопасность относятся: установление и поддержание режима конфиденциальности, что подразумевает под собой проведение организационных мероприятий, создание и эксплуатацию системы защиты (оборудование (камеры, охранно-пропускная система и т.д.), служба безопасности), обучение персонала.

К потенциальным потерям относятся различные экономические, репутационные и т.д. убытки, возможные при компрометации защищаемой информации.

Эффективность системы КД можно оценивать по соотношениям риска от возможной реализации информационных угроз и затрат на защиту информации. На рисунке приведены возможные расходы на увеличение защищенности КД от информационных угроз во времени существования объекта защиты (восходящая

кривая) и кривая возможного значения риска (нисходящая кривая). Очевидно, что суммарные потери организации, вызванные проблемой защиты КД, являются суммой риска и затрат на обеспечение защиты.

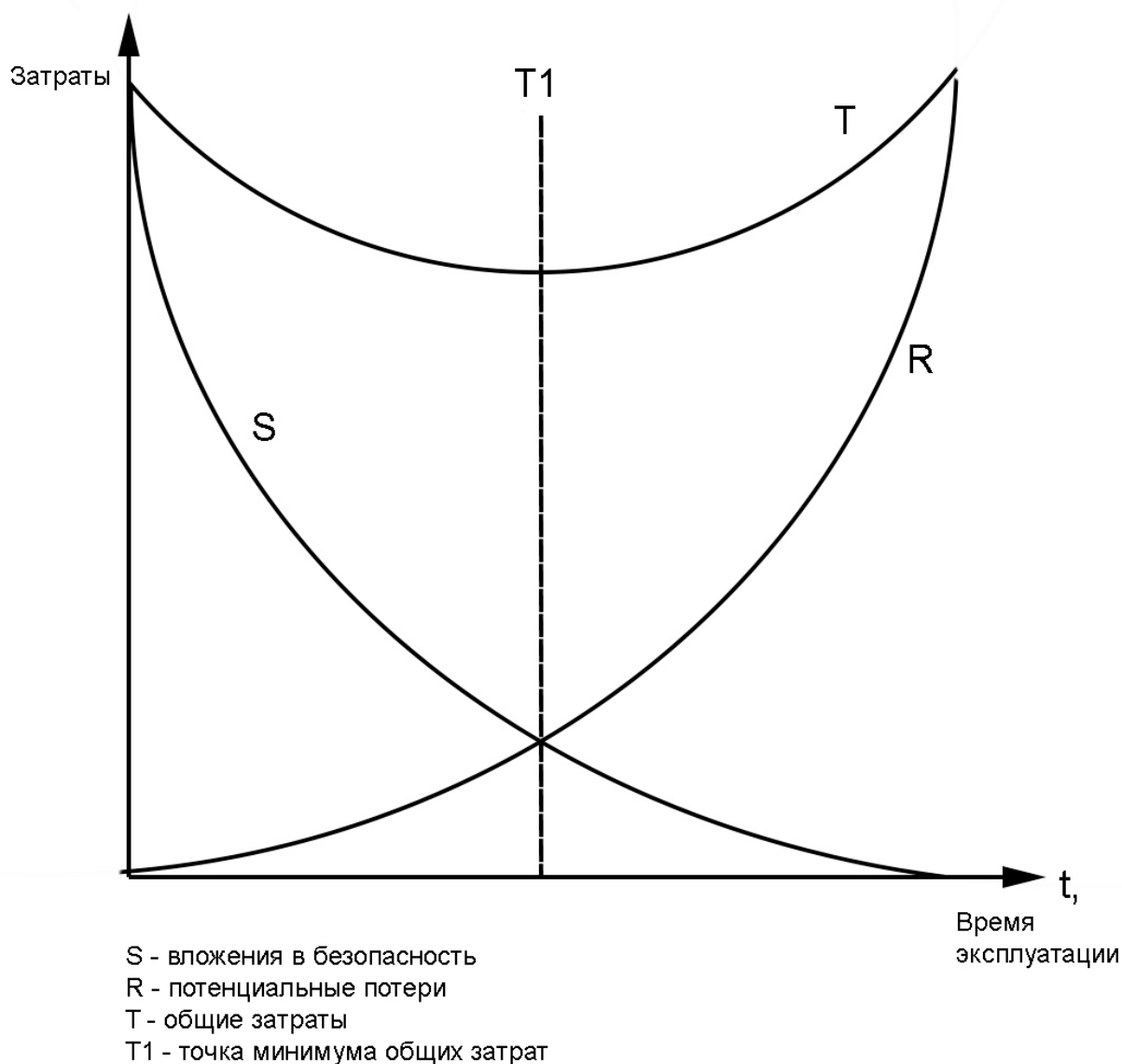


Рисунок 1 - Показатель степени оптимизации службы конфиденциального документооборота

Точка T1 является точкой, где общие затраты являются минимальными. Точки до нее являются точками, где возможные потери превышают затраты на безопасность, что означает недостаточную защиту. Точки после нее являются точками, где уже произведенные затраты превышают возможные при компрометации защищаемой информации, что показывает нецелесообразность таких затрат. Желательной является точка T1. Такая модель наглядно

демонстрирует тот факт, что существует значение оптимума затрат в некоторой точке на временной оси (параболическая кривая), соответствующее пересечению кривых риска и затрат на защиту [10].

Также существуют критерии эффективности самого документооборота. Можно выделить 8 таких критериев: объем, скорость прохождения, количество участников, степень конфиденциальности — относятся как к открытому, так и закрытому документообороту, конфиденциальность, целостность, достоверность, доступность — относятся только к закрытому документообороту. Желательные тенденции этих критериев представлены в таблице 1.

Таблица 1 - Желательные тенденции критериев эффективности документооборота

Относятся к открытому и закрытому документообороту	
Объем	Меньше - лучше
Скорость прохождения	Больше - лучше
Количество участников	Меньше - лучше
Степень конфиденциальности	Меньше - лучше
Относятся к закрытому документообороту	
Конфиденциальность	Больше - лучше
Целостность	Больше - лучше
Доступность	Больше - лучше
Достоверность	Больше - лучше

Критерий степени конфиденциальности влияет в том числе и на оптимизацию системы конфиденциального документооборота. Конфиденциальными должны признаваться документы в минимальном количестве, содержание которых действительно важно и неизвестно окружающим, следовательно, при неоптимальном составе конфиденциальных документов также неоптимальными являются затраты.

Критерии, которые относятся к закрытому документообороту, при отрицательных значениях свидетельствуют о компрометации защищаемой информации.

1.1 Структура службы конфиденциального делопроизводства

Уровень оптимизации системы КД не может быть определен точно; его оценивает эксперт (группа экспертов). На экспертное мнение влияют следующие факторы: безопасность помещения (на основе паспорта помещения, выдаваемого Бюро технической инспекции), криминогенная обстановка (определяется уполномоченными органами), сама система КД. При оценке системы КД может использоваться метод системного анализа. Для этого создаются модели системы КД: иерархическая, морфологическая, информационная.

Морфологическая модель службы конфиденциального делопроизводства.

Морфологическая модель описывает, что входит в системы, как эти элементы связаны, как система взаимодействует с внешней средой.

Сначала представляется отношение системы с внешней средой – с чем она связана, ее входы и выходы, поэтому система считается неделимой, т.к. здесь ее состав неважен. Только потом отрабатывается внутренний состав системы и связи ее элементов. Иными словами, здесь представляются модель «черного ящика» и модель состава системы соответственно.

Модель черного ящика. Служба конфиденциального делопроизводства является структурным подразделением, она связывается с руководством, в случаях работы с государственной тайны с Федеральной службой безопасности, с подразделениями, которые предоставляют информацию, с организациями, которым передаются документы и/или информация, с подразделением информационных технологий, с подразделениями (организациями), которые осуществляют передачу документов, с кадровой службой, с административно-хозяйственной службой.

Входами службы конфиденциального делопроизводства являются: руководящие действия, входящие документы, входящая информация, персонал, предметы снабжения.

Выходами службы конфиденциального делопроизводства являются: ответные реакции на руководящие действия, созданные документы, информация для руководства, информация для связанных структурных подразделений.

Модель черного ящика приведена на рисунке 2.

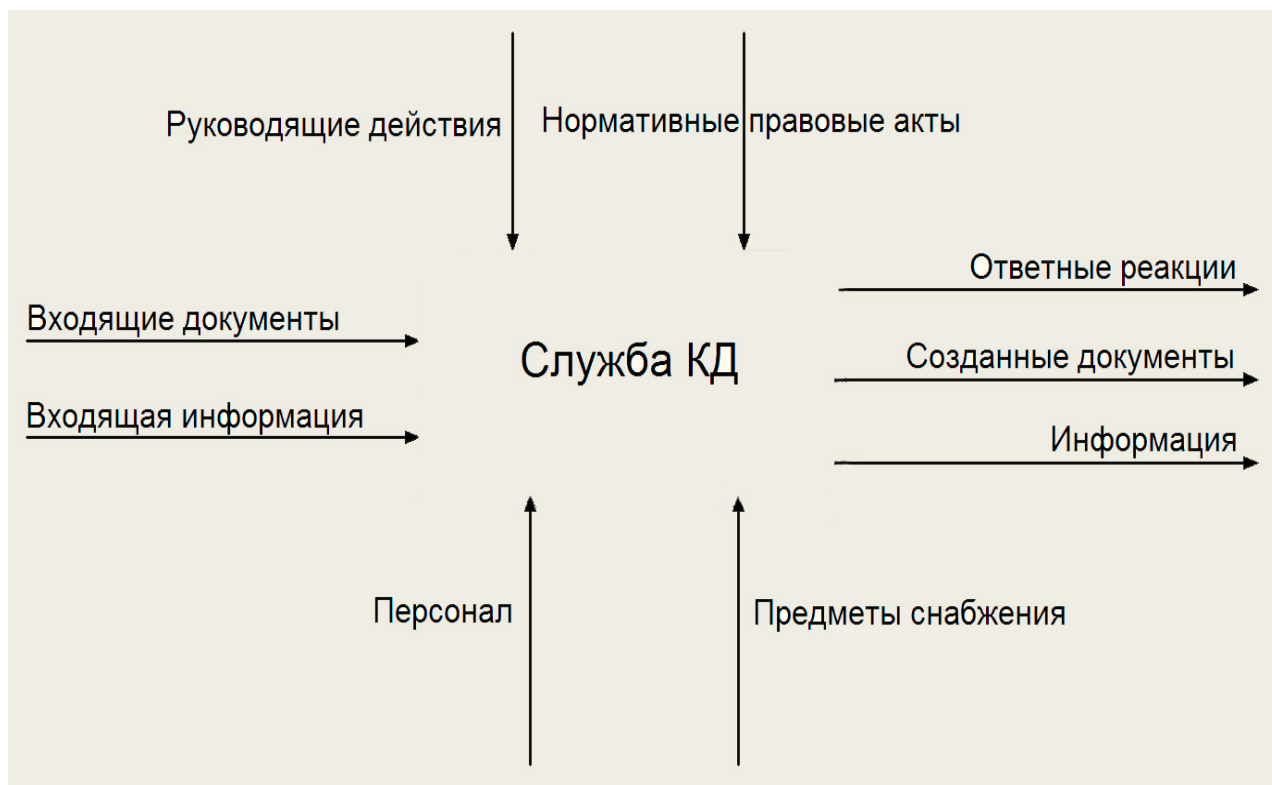


Рисунок 2 - Модель черного ящика

Модель состава системы. Служба конфиденциального делопроизводства является обычным структурным подразделением, но со своими особенностями, вызванными спецификой деятельности.

В случае малого количества конфиденциальных документов в организации всем конфиденциальным документооборотом может заниматься один специально назначенный работник.

В случае достаточно большого количества конфиденциальных документов в организации создается отдельное структурное подразделение, занимающееся работой с ними. В таком случае подразделение включает в себя, как и везде, начальника и подчиненных ему специалистов.

Отличительной особенностью службы конфиденциального делопроизводства является то, что все ее работники должны иметь допуск к защищаемой информации (в случае коммерческой тайны – допуск, выданный самой организацией; в случае государственной тайны – допуск, выданный Федеральной службой безопасности). Также необходимо выделить средства хранения и защиты конфиденциальной информации, средства разграничения доступа (сейфы, средства криптографии, пропускные системы, системы учетных записей и т.д.).

Модель состава системы приведена на рисунке 3.

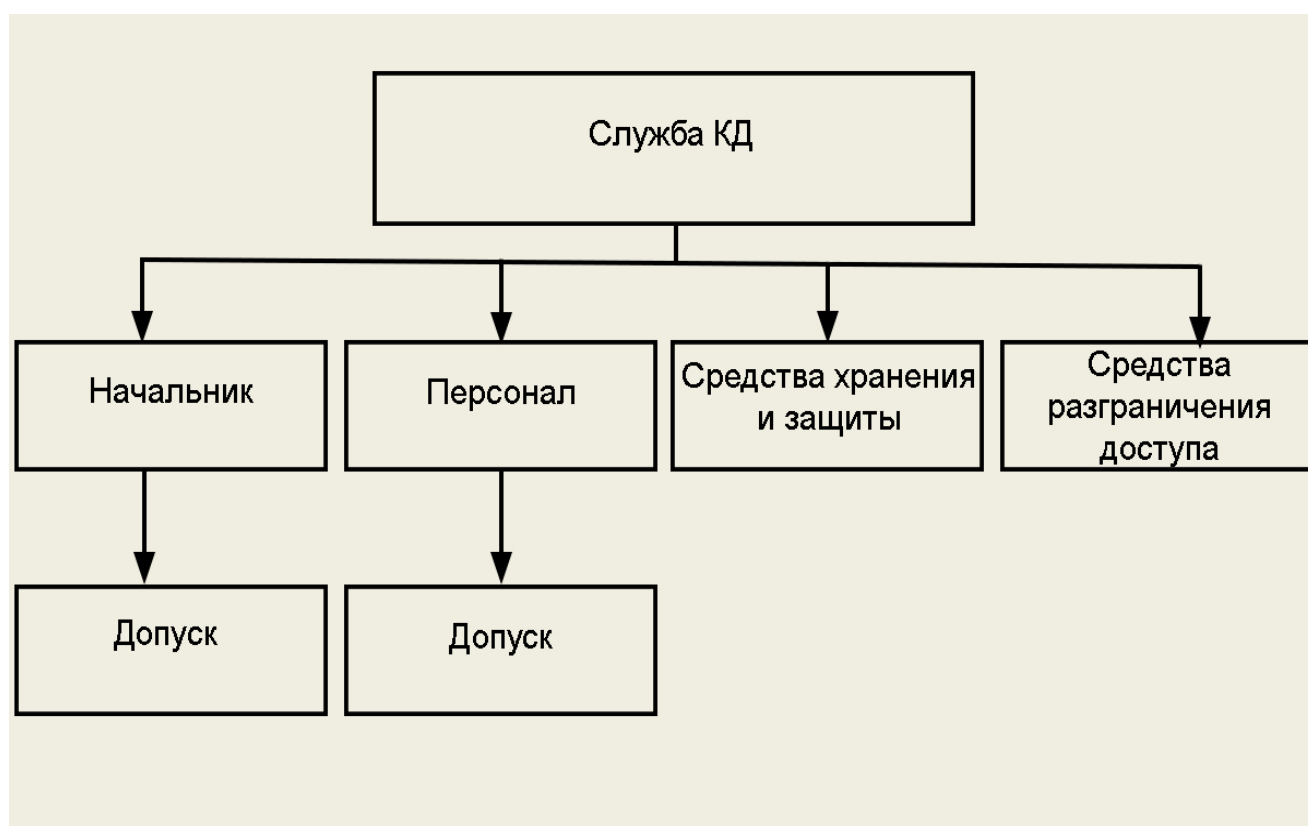


Рисунок 3 – Модель состава системы

Информационная модель службы конфиденциального делопроизводства.

Информационная модель — модель объекта, представленная в виде информации, описывающей существенные для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта и позволяющая путём подачи на модель информации об изменениях входных величин моделировать возможные состояния объекта.

Информационная модель приведена на рисунке 4.

Конфиденциальная информация подразделяется на 2 части – государственную тайну и коммерческую тайну.

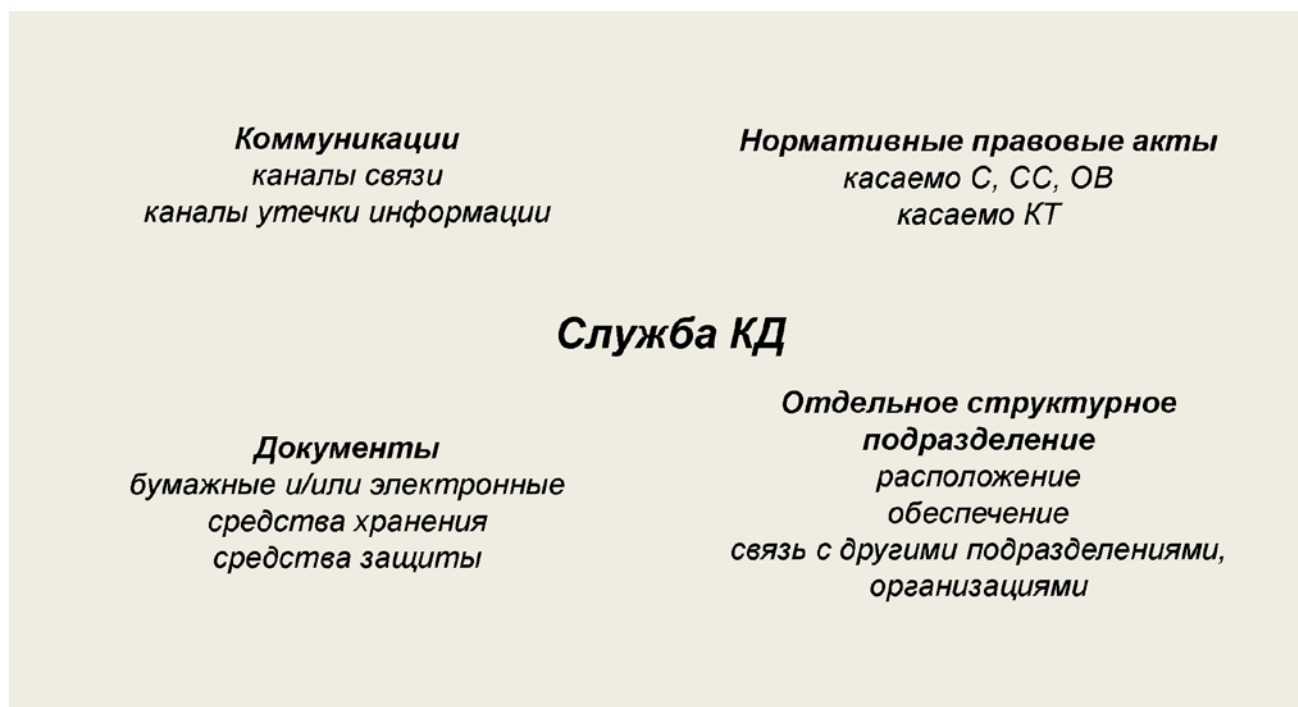


Рисунок 4 – Информационная модель

Основные нормативные правовые акты, регулирующие работу с государственной тайной: Закон РФ "О государственной тайне"¹, Указ Президента РФ "Об утверждении Перечня сведений, отнесенных к государственной тайне"², Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"³ (с последующими изменениями).

¹ Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (в ред. Федерального закона от 29.07.2018 N 256-ФЗ)

² Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне" (в ред. Указов Президента РФ от 14.01.2019 N 6).

³ Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" (в ред. Постановления Правительства РФ от 19.04.2019 N 468).

Основные нормативные правовые акты, регулирующие работу с коммерческой тайной: Федеральный закон "О коммерческой тайне"¹, Постановление Правительства РСФСР "О перечне сведений, которые не могут составлять коммерческую тайну"².

Служба конфиденциального делопроизводства – структурное подразделение, занимающееся работой с документами, отнесенными организацией к конфиденциальным. Оно оснащено особыми техническими средствами и сотрудничает с другими структурными подразделениями в целях обеспечения своей деятельности.

Служба может вести бумажный и/или электронный документооборот. В обоих случаях служба должна располагаться в отдельном помещении, имеет средства хранения и защиты информации (но в каждом случае они разные), может иметь на входе пропускную систему. Она связывается с руководством, с подразделениями, которые предоставляют информацию, с организациями, которым передаются документы и/или информация, с кадровой службой, с административно-хозяйственной службой.

Рассмотрим случай, когда служба работает с бумажными документами. В таком случае служба конфиденциального делопроизводства дополнительно взаимодействует с подразделениями (организациями), которые осуществляют передачу документов. К средствам хранения и защиты информации относятся закрытые шкафы, сейфы. Ведутся и защищаются учетные формы документов. К каналам связи относятся курьерская, почтовая и личная передача документов. К каналам утечки относятся физическая потеря документа, умышленный несанкционированный доступ к документу (подсматривание, фотографирование и т.д.), неумышленная выдача информации конфиденциального документа

¹ Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (в ред. Федерального закона от 18.04.2018 N 86-ФЗ).

² Постановление Правительства РСФСР от 05.12.1991 N 35 "О перечне сведений, которые не могут составлять коммерческую тайну" (в ред. Постановления Правительства РФ от 03.10.2002 N 731).

(неосторожное обсуждение при посторонних, случайная выдача сведений в частных беседах и т.д.).

Рассмотрим случай, когда служба работает с электронными документами. В таком случае служба конфиденциального делопроизводства дополнительно взаимодействует с подразделением информационных технологий. Причиной такого взаимодействия является использование системы электронного документооборота (СЭД) с особой шифровальной надстройкой, которая является средством работы с документами, средством их учета, хранения и защиты. Взаимодействие заключается в установке, обслуживании, совершенствовании самой СЭД и средств шифрования; в случае передачи документов еще должна быть обеспечена безопасность самой передачи и возможность работы с документом принимающей стороной. Шифрование может производиться с помощью симметричного (с использованием одного ключа), асимметричного (с использованием пары ключей: закрытого и открытого) алгоритмов, с помощью программ, защищенных паролем. Каналы связи различны: зашифрованные документы могут открыто передаваться через интернет, может использоваться закрытая сеть передачи данных, может использоваться курьерская, почтовая и личная передача электронного носителя документов. К каналам утечки относятся физическая потеря электронного носителя документа, умышленный несанкционированный доступ к документу (подсматривание, фотографирование и т.д.), неумышленная выдача информации конфиденциального документа (неосторожное обсуждение при посторонних, случайная выдача сведений в частных беседах и т.д.), компрометация ключей шифрования, пароля и перехват передаваемого документа, взлом компьютеров-рабочих станций, считывание сигналов и т.д..

Иерархическая модель службы конфиденциального делопроизводства.

Иерархическая модель представляет систему в виде структуры, состоящей из объектов различных уровней.

Объекты связаны, каждый объект может включать в себя несколько объектов более низкого уровня. Такие объекты находятся в отношении

начальствующего (вышестоящий объект) к подчиненному (нижестоящий объект).

Иерархическая модель позволяет быстро понять место подразделения в структуре, выяснить источники управляющих воздействий. В любом предприятии должна быть организационная структура – документ, являющий собой иерархическую модель.

При рассмотрении службы конфиденциального делопроизводства необходимо смоделировать две ситуации: когда работа ведется со сведениями, составляющими коммерческую тайну, и когда работа ведется со сведениями, составляющими государственную тайну. Работа с персональными данными не учитывается – они находятся в ведении службы открытого делопроизводства.

В первом случае все достаточно просто. Служба конфиденциального делопроизводства подчиняется руководству организации. У руководителя, возглавляющего саму службу, в подчинении находятся несколько работников. Иерархические модели организации и службы приведены на рисунке 5 и рисунке 6 соответственно.

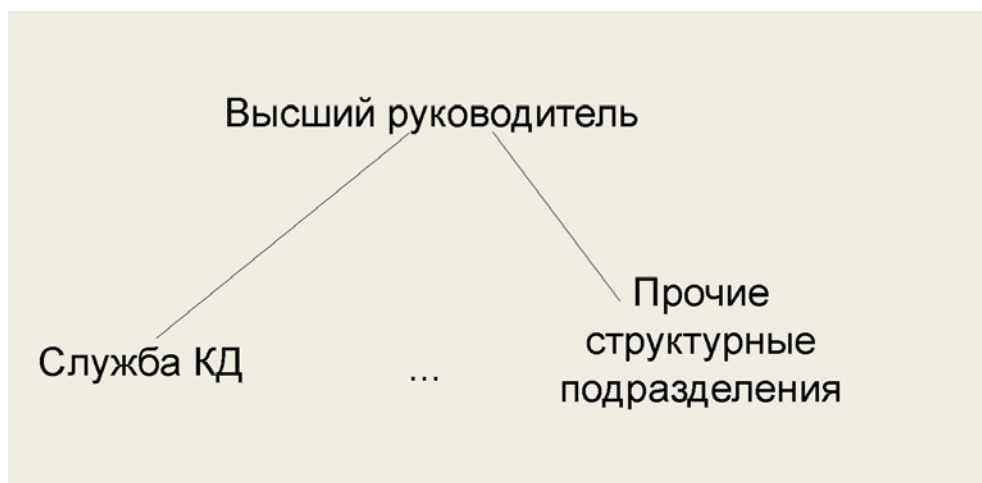


Рисунок 5 – Иерархическая модель организации

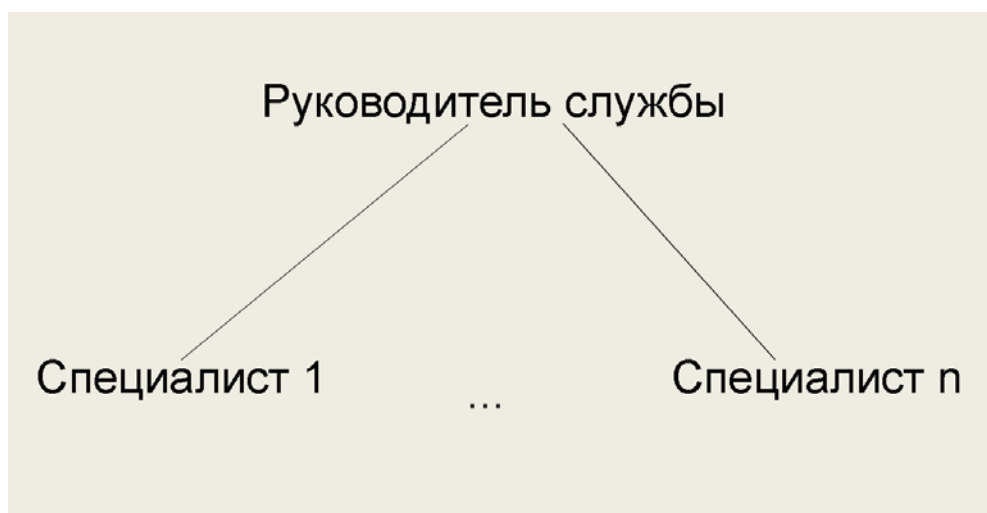


Рисунок 6 - Иерархическая модель службы конфиденциального документооборота

На основе анализа структуры службы конфиденциального документооборота рассмотрены показатели эффективности документооборота, показатель уровня оптимизации службы конфиденциального документооборота, построены модели конфиденциального документооборота.

2 Система защиты информации

Система защиты информации — комплекс мероприятий, средств, работ, направленный на противодействие получения несанкционированного доступа к защищаемой информации и направленный на повышение степени конфиденциальности такой информации. Из определения явно следует, что все ресурсы, задействованные в целях защиты информации, должны представлять собой единую систему.

Функциональным представлением системы защиты информации является комплекс защитных функций, обеспечиваемых системой. Организационным представлением системы защиты информации является комплекс средств и методов поддержания конфиденциальности информации, средств и методов управления системой защиты и принципов определения и организации работы системы с учетом специфики объекта защиты.

Организации – владельцы информации самостоятельно определяют, какую информацию отнести к защищенной (за исключением некоторых случаев согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»¹). На этом этапе возникают две задачи: какую информацию действительно стоит признать конфиденциальной (отнесение лишней повысит нагрузку на систему защиты и приведет к повышенному расходу средств) и как эту информацию защитить. Чем больше объем и чем ценней информация, тем выше требования к надежности системы защиты.

В целях построения надежной системы защиты информации организация должна обеспечить выполнение нескольких условий. К ним относятся: определение ответственных за установление режима конфиденциальности,

¹ Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в ред. Федерального закона от 18.03.2019 N 31-ФЗ)

определение перечня защищаемых документов и данных, определение и разграничение допущенных и недопущенных к конфиденциальным сведениям, создание отдела (назначение работника), который будет заниматься нормативно-методической и практической работой по защите информации.

Как сказано выше, система защиты информации должна быть комплексной, один совершенный элемент не сможет закрыть недочеты других [12]. Должна быть защищена сама организация (ее территория, здания, помещения и т.д.), электронные системы организации, бумажный документооборот, должны быть обучены сотрудники. Выбор и построение элементов зависят от документооборота организации и вероятных угроз. При этом малейшая недоработка, халатность или ошибка работника, ответственного за проектирование, построение, настройку системы, работника, непосредственно взаимодействующего с защищаемыми документами, может привести к компрометации всей системы безопасности и конфиденциальной информации. Устранению и профилактике компрометирующих ситуаций, связанных с т.н. человеческим фактором, необходимо уделить много внимания. К ошибкам и недоработкам, которые способны привести к нарушению конфиденциальности информации, можно отнести следующее:

- умышленное и неумышленное непроставление метки ограничения доступа (гриф «Коммерческая тайна»);
- незнание основ информационной безопасности;
- незнание правил работы с конфиденциальными документами (если такой документ существует в организации);
- отступление от правил работы с конфиденциальными документами (если такой документ существует в организации);
- потеря, некачественное уничтожение конфиденциального документа;
- неаккуратное обсуждение закрытой информации при посторонних;
- неумышленное раскрытие конфиденциальной информации.

Элементы системы защиты информации можно классифицировать по следующей схеме [9]:

- правовой;
- организационный;
- инженерно-технический;
- программно-аппаратный;
- криптографический.

Правовой элемент системы защиты информации зависит от законодательства в области информационного права. Этот элемент определяет:

- возможно, и законно ли отнесение конкретных сведений к неразглашаемым, какое положение они могут приобрести. Согласно Федеральному закону "О коммерческой тайне"¹, организация вправе выбирать, какую именно информацию считать конфиденциальной, однако есть некоторые ограничения;

- характер работы персонала с конфиденциальной информацией. Определяется правовое положение защищаемой информации в организации. Определяется, возложены ли на работника обязательства по неразглашению, поддержанию конфиденциальности определенной информации, возможная ответственность за разглашение и нарушение конфиденциальности;

- возможность и порядок оформления передачи конфиденциальной информации партнеру контрагенту. Передача должна производиться только при необходимости и оформляться документально. Организация, получившая конфиденциальную информацию, должна также принять на себя обязательства по неразглашению и защите.

Организационный элемент системы защиты информации определяет управленческий, методический, режимный подходы к работе с конфиденциальной информацией. Названные подходы влияют на определение,

¹ Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (в ред. Федерального закона от 18.04.2018 N 86-ФЗ).

формулирование и построение системы защиты информации и ее объекта на уровне решений руководителей. Здесь устанавливается и формируется сам режим конфиденциальности. Этот этап регламентирует следующие работы:

- принятие и оформление решения о создании системы защиты информации, решения о выборе, приобретении, вводу в эксплуатацию, эксплуатации, обновлении или замены различных средств защиты информации;
- создание отдела (найм работника), который будет заниматься работой по защите информации, и обеспечение его деятельности;
- создание отдела, предназначением которого является физическая охрана организации, кадровое, правовое (например, получение разрешительных документов, лицензий персоналом), техническое (приобретение средств видеонаблюдения, средств обороны и т.д.) обеспечение его деятельности;
- создание комплекса документов (правил, положений), определяющих правовое положение конфиденциальной информации в организации, их своевременное обновление и приведение в соответствие с действующими нормами законодательства. К таким документам относятся: условно называемые положение о защите информации, перечень конфиденциальных документов, обязательство о не разглашении, журнал конфиденциальных документов;
- анализ сложившейся системы документооборота, материально-технической базы и возможных угроз в целях определения слабых мест в системе защиты информации, определения возможных направлений попыток нарушения конфиденциальности. При создании системы защиты и при ее использовании продолжающаяся работа по оценке степени эффективности ее работы, при необходимости определение мест, требующих изменения, обновления, доработки;
- определение и формирование системы разграничения доступа к информации, последующее определение уровня доступа различных категорий работников (при необходимости, конкретного работника);
- кадровая работа, включающая в себя формирование отдела по защите информации, определение его качественного и количественного состава,

возможность назначения работника на должность, связанную с конфиденциальной информацией (определение степени лояльности), оформление обязательств о неразглашении;

- информационно-обучающая работа со всем персоналом по информационной безопасности, работе с конфиденциальной информацией;
- разработка технологии работы (создания, использования, хранения, защиты) с конфиденциальными документами;
- отработка действий персонала при внештатных ситуациях;
- работа по разграничению открытого документооборота с закрытым;
- работа, связанная с администрированием системы защиты информации.

Организационный элемент системы защиты информации является важнейшим в составе комплекса, любые недоработки здесь неизбежно окажут влияние на другие элементы. В то же время, даже совершенные другие элементы не смогут «прикрыть» возможные бреши организационного элемента. С этого элемента и начинается построение всей системы, т.к. решение о причислении некоторой информации к защищаемой и последующей ее защите принимается на этом этапе. К организационному элементу относится принятие решения о выборе, приобретении, вводе в эксплуатацию, эксплуатации, обновлении или замены различных средств защиты информации. Именно здесь начинается и ведется работа с персоналом, который будет работать над построением системы защиты информации и с конфиденциальной информацией. Хорошо обученные и лояльные работники смогут сформировать качественную систему защиты и грамотно ее использовать, смогут своевременно обнаружить возможные недоработки и пути улучшения защиты. Также на этом этапе разрабатываются документы, влияющие на систему защиты информации: перечень конфиденциальных документов и правила работы с ними.

Инженерно-технический элемент системы защиты информации представляет собой подсистемы материально-технических средств, направленных на противодействие физическим способам несанкционированного

проникновения и нарушения конфиденциальности защищаемой информации. Является наиболее явным элементом защиты.

На этом этапе система защиты информации обеспечивается следующим:

- средства физической защиты от несанкционированного проникновения на территорию организации (заборы, замки различных принципов действия, двери и т.д.). Является самым явным средством, достаточно простым, при этом весьма важным. Качественные средства физической защиты заставят искать другие, более сложные способы приобретения защищаемой информации;

- средства физической защиты конфиденциальной информации на материальных носителях (закрывающиеся шкафы, сейфы и т.д.). Их суть и предназначение такие же, как у средств физической защиты от несанкционированного проникновения;

- средства подсистемы разграничения доступа, пропускного режима, которая может применяться как по всей территории, так и только в наиболее важных зонах;

- средства безопасности территории, сооружений (системы видеонаблюдения, сигнализации, датчики и т.д.);

- оборудование специально предназначенных для работы с защищаемой информацией помещений (могут обособляться средствами пропускного режима, должны обладать необходимым оборудованием (шкафы, сейфы), не должны быть легкопросматриваемыми);

- оборудование специально предназначенных для конфиденциальных переговоров, совещаний помещений, которые должны быть экранированы от возможных попыток подслушивания, подсматривания и т.д. В такое помещение не должны впускаться посторонние;

- средства экранирования технических каналов возможной утечки сведений, которые могут возникнуть, например, при использовании компьютеров;

- техническое обеспечение создания внутренней, локальной сети компьютеров, предназначенных для работы с защищаемой информацией. Задействованные компьютеры не должны быть связаны с другими сетями, в том числе сетью Интернет. При необходимости отправки конфиденциального документа через сеть Интернет, этот документ должен быть перенесен на компьютер вне выделенной сети, для минимизации вероятности компрометации локальной сети;

- устройства поиска средств технической разведки, которые могут появиться на территории организации (приборы подслушивания и передачи, приборы перехвата сигналов, передающихся как проводным, так и беспроводным способами и т.д.);

- контролирующие устройства, препятствующие выносу работниками предметов с нанесенными специальными метками.

Программно-аппаратный элемент системы защиты информации представляет собой комплекс программ и методов, препятствующих попаданию и внедрению вредоносных программ на компьютеры организации, особенно используемые при работе с конфиденциальной информацией. Применяется, если в организации существует электронный документооборот и/или применяются компьютеры при работе с документами; при работе с документами только на бумаге этот элемент системы защиты не имеет смысла. Препятствует несанкционированному доступу к защищаемой информации, скрытому «подслушиванию» каналов связи, устройств ввода-вывода (проведение интернет-трафика через компьютеры злоумышленников, снятие сигналов с клавиатуры и т.д.).

К этому элементу системы защиты информации относятся такие программы и методы, как [13]:

- программы фильтрации интернет-трафика (firewall);
- программы активного противодействия вредоносным программам (антивирусы);

- программы сканирования компьютеров на наличие вредоносных программ;
- методы подтверждения подлинности веб-сайта, с которым устанавливается соединение (шифрование и проверка сертификатов, используемых при использовании протокола прикладного уровня HTTPS сетевой модели OSI).

Необходимо отметить, что вышеперечисленные средства и методы могут являться самостоятельными средствами защиты и использоваться на любых компьютерах любыми пользователями.

Также к этому элементу относятся следующие программы и методы:

- программы, которые управляют средствами безопасности территории и сооружений;
- средства, ограничивающие или блокирующие доступ к компьютерам;
- программы, при экстренной ситуации стирающие указанные данные/форматирующие носители информации;
- средства, контролирующие подключение внешних устройств, носителей информации к компьютерам;
- программы и методы, обеспечивающие защищенные каналы связи (в связке с криптографическим элементом системы защиты информации).

Комплексное развертывание и качественная настройка этого элемента системы защиты информации позволяют успешно противодействовать большинству угроз, потенциально возникающих при работе с конфиденциальными документами с использованием компьютеров. Более того, качественная настройка в комбинации с небольшим курсом обучения и/или подробными настройками для конечных пользователей позволит свести к практическому минимуму вероятность неумышленного действия, которое могло бы привести к возможности угрозы конфиденциальности информации. Также качественная настройка этого элемента системы защиты информации может предотвратить или снизить вероятность умышленных действий работника по

нарушению конфиденциальности конфиденциального документа (например, копирование файла на носитель информации, отправка через Интернет).

Криптографический элемент системы защиты информации представляет собой средство защиты конфиденциальной информации с помощью шифрования.

На этом этапе проводятся следующие работы:

- выбор и определение правил использования методов и протоколов шифрования информации, циркулирующей по компьютерам и различным сетям;
- принятие решения о возможности передачи защищаемой информации по незащищенным каналам связи различных видов. В случае принятия решения о невозможности передачи необходимо определить иные пути и способы передачи защищаемой информации, в случае принятия решения о возможности такой передачи необходимо определить порядок передачи: какие каналы предпочтительны, как и какими методами защищать конфиденциальную информацию;
- принятие решения о возможности проведения переговоров посредством незащищенных каналов связи. В случае принятия решения о невозможности проведения таких переговоров необходимо определить иные пути и способы проведения переговоров, в случае принятия решения о возможности проведения таких переговоров необходимо определить порядок защиты голосовых сообщений;
- необходимо выбрать и регламентировать использование программ и методов, обеспечивающих защищенные каналы связи (в связке с программно-аппаратным элементом системы защиты информации);
- необходимо выбрать и регламентировать использование программ и протоколов шифрования защищаемой информации. Затем требуется внедрение выбранных средств, их настройка. Также требуется определение правил использования работниками средств шифрования.

Все выбранные способы, методы, программы, протоколы шифрования должны пройти проверку на соответствие требованиям надежности. Также

необходимо не забывать о возможных уязвимостях «нулевого дня» - ситуациях, когда брешь в шифровании известна только обнаружившему ее злоумышленнику и, следовательно, еще не существует способ исправления этой бреши. Более того, даже самые надежные из существующих протоколов шифрования являются условно невзламываемыми — современные компьютеры могут их вычислить, но на это потребуется огромное количество времени, вплоть до сотен лет. В целом, текущее состояние индустрии криптографии позволило сделать шифрование информации достаточно надежным [14].

В целом, система защиты информации состоит из подсистем защиты информации — компонентов системы, распределенных по организационно-структурным подразделениям, - и компонента, управляющего работой всех подсистем и объединяющий их в единую систему. Этот управляющий компонент принято называть ядром системы защиты информации. К функциям ядра системы защиты должны относиться:

- организация и обеспечение ограниченного согласно уровням допуска доступа к защищаемой информации;
- обеспечение своевременной обработки подсистемами взаимодействий с конфиденциальными данными;
- организация работы всей системы защиты при ее взаимодействии с защищаемой информацией;
- организация и выполнение мероприятий по контролю правильности деятельности системы защиты;
- обработка сигналов подсистем защиты информации и обеспечение ответной реакции;
- ведение журналов системы защиты информации.

Вместе с этим, к системе защиты информации можно отнести следующие объекты:

- системные программисты (взаимодействующие с программно-аппаратным и криптографическими элементами);
- работники, обслуживающие систему защиты информации;

- администраторы информационных баз;
- работники, управляющие работой системы защиты;
- работники, непосредственно работающие со средствами защиты;
- работники, взаимодействующие с защищаемой информацией.

Сами системы защиты информации можно разделить на несколько групп по разным классификациям.

По уровню предоставляемой защиты системы защиты информации можно разделить на:

- системы слабой защиты — подходящие для работы с информацией, обладающей невысокой ценностью и не требующей высокой степени конфиденциальности;
- системы средней защиты — подходящие для работы с информацией, требующей высокой степени конфиденциальности, но объем этой информации не является большим, и взаимодействие с ней происходит достаточно редко;
- системы сильной защиты — подходящие для работы с информацией, требующей высокой степени конфиденциальности, при этом объем этой информации достаточно велик;
- системы особой защиты — подходящие для работы с информацией, требующей очень высокой степени конфиденциальности, при этом ее объем достаточно велик и взаимодействие с ней происходит регулярно.

По активности реагирования на обнаруженные действия, направленные на нарушение конфиденциальности защищаемой информации, системы защиты информации можно разделить на:

- системы пассивного действия, которые не обладают ни возможностью сигнализации о действиях, направленных на нарушение конфиденциальности защищаемой информации, ни возможностью противодействия попыткам нарушения конфиденциальности защищаемой информации;
- системы полуактивного действия, которые обладают возможностью сигнализации о действиях, направленных на нарушение конфиденциальности

защищаемой информации, но не обладают возможностью противодействия попыткам нарушения конфиденциальности защищаемой информации;

- системы активного действия, которые обладают возможностью сигнализации о действиях, направленных на нарушение конфиденциальности защищаемой информации, и возможностью противодействия попыткам нарушения конфиденциальности защищаемой информации.

Теоретически представленные классификации позволяют разбить системы защиты информации на 12 групп, системы разных уровней защиты и разной активности, однако на практике это невозможно из-за вопроса целесообразности. Системе слабой защиты нецелесообразно быть активной, при этом вполне допустимо быть пассивной или полуактивной. В то же время, система особой защиты из-за очень высоких требований не может быть пассивной или полуактивной, она должна быть активной. Системы средней и защиты не могут быть пассивными, такие системы предполагают полуактивное и активное реагирование.

При этом следует принимать во внимание тип объекта, на котором должна быть развернута система защиты информации. Компьютер, не имеющий подключения к распределенным сетям, предъявляет не столь высокие требования к предоставляемой защите, как сильнораспределенные сети. Следовательно, целесообразность применения той или иной системы защиты должна рассчитываться, исходя из требований защиты, соответствующей активности реагирования и типа объекта. В целях проведения такого расчета объекты можно разбить на:

- персональный компьютер;
- компьютер, обслуживающий несколько пользователей;
- локальная сеть;
- распределенная сеть;
- глобальная сеть.

Как было сказано выше, система защиты должна быть комплексной, развитие элементов системы должно быть сбалансированным, преимущества

одного из них не сможет закрыть недостатки другого, эффективность действия всей системы защиты информации достигается только при условии связанной работы всех подсистем защиты. Также важнейшим требованием, предъявляемым к системам защиты информации, является ее способность подстраиваться к различным факторам и условиям, т.к., во-первых, эти факторы и условия могут постоянно меняться и существенно влиять на саму систему защиты и возможные угрозы, во-вторых, невозможно точно структурировать процессы защиты информации.

Рассмотрим возможные сценарии попыток нарушения конфиденциальности информации и работы системы защиты информации.

Сначала должно быть принято управленческое решение о создании и развертывании системы защиты. Далее должен быть создан отдел, который будет заниматься всеми вопросами информационной безопасности. Далее должен быть проведен анализ сложившейся системы документооборота в организации, возможных угроз конфиденциальности (с привлечением эксперта в соответствующей области). После этого трудоемкого и затратного этапа, который в любом случае не даст точных результатов (только оценочные), можно получить представление о будущей системе. Придет понимание того, что должно входить в состав системы, какими должны быть средства защиты (зависит от оценки возможных угроз), каких работников необходимо дополнительно нанять, сколько времени и ресурсов придется потратить. Затем должны быть разработаны документы, регламентирующие правовое положение защищаемой информации, соответствующие выдвинутым требованиям безопасности и действующего законодательства. Должен быть регламентирован порядок работы персонала с конфиденциальными документами. Должны быть определены возможность и порядок передачи защищаемой информации партнерам, контрагентам. Параллельно с этим необходимо приступить к построению системы защиты информации. После окончания работ по созданию системы необходимо ее настроить и проверить путем имитации попыток нарушения конфиденциальности защищаемой информации. В случае успешного

прохождения тестирования необходимо разработать достаточно подробные инструкции по использованию средств защиты и информационной безопасности для персонала, провести курс обучения. Далее потребуются постоянное обслуживание системы защиты и, при необходимости, ее обновление.

Технологии и устройства постоянно совершенствуются, и можно с уверенностью сказать, что системе защиты потребуется обновление. Со временем она может становиться все сложнее и сложнее. При этом простые средства безопасности и защиты информации могут предотвратить большинство проблем. Тщательное формирование перечня защищаемых документов и их маркирование (проставление грифа «Коммерческая тайна») поможет предотвратить случайное, «из любопытства», нарушение конфиденциальности информации. Заборы, надежные замки и служба безопасности не допустят нахождения на территории организации посторонних людей. Оборудование специального помещения, предназначенного для работы с конфиденциальными документами, позволит снизить вероятность случайного смешивания открытых и закрытых документов. Вместе с этим, попытки получения действительно ценной и нужной информации могут быть очень хитрыми и настойчивыми, что потребует создать и настроить сложную и продуманную систему защиты информации, оснащенную современными средствами защиты, которые используют новейшие технологии и могут противостоять свежеразработанным методам получения доступа к конфиденциальной информации.

Однако на практике не представляется возможным приобретение и развертывание самых качественных (дорогих, популярных и т.д.) средств информационной безопасности; проблема построения системы защиты гораздо более сложна. Необходимо учитывать вопрос экономической целесообразности — не получится ли так, что стоимость разрабатываемой системы защиты информации заметно превышает возможные оценочные потери от нарушения конфиденциальности защищаемой информации? Возможные потери и потенциальные угрозы невозможно точно рассчитать — эти показатели являются оценочными и приблизительными. Построение качественной и экономически

целесообразной системы защиты информации не может обойтись без экспертного мнения.

При этом, в любом случае возможна потеря информации в результате действий «изнутри» - может быть «завербован» нелояльный работник с достаточным для извлечения нужной информации уровнем доступа, в случае особо ценной и «долгоиграющей» информации злоумышленник может получить работу в организации и дослужиться до нужного уровня полномочий [11]. Также некоторая защищаемая информация (например, ноу-хау) может быть получена законными способами — путем скрупулезного изучения производимой продукции, анализа открытой документации.

Анализ систем защиты информации позволил классифицировать сами системы и средства защиты конфиденциальных документов, что способствует повышению эффективности управления в сфере выбора применяемых средств.

3 Построение службы конфиденциального документооборота

В сфере защиты информации большое количество расчетов и прогнозов зависит от степеней потенциальных угроз и рисков, которые не могут быть оценены точно. Из этого следует, что решение большинства задач (например, оценка состояния системы документооборота, оценка возможных угроз нарушения конфиденциальности защищаемой информации) строится на суждениях, опыте и интуиции эксперта. Следовательно, мнения разных экспертов об одном и том же объекте могут заметно отличаться. Разумеется, у каждого эксперта свой подход к работе, что приводит к необходимости самостоятельной систематизации и формализации знаний. Можно использовать следующий подход [8]. Сначала экспертом проводится анализ информации, которая уже имеется в распоряжении. Затем ставится задача, проводится построение базовых моделей, выбираются методы решения и анализа результатов, определяются допуски точности. Далее определяется форма расчетного эксперимента и проводится сам эксперимент (моделирование). Полученные результаты анализируются, в случае адекватности эксперимента, удовлетворенности эксперта результатами и отсутствии необходимости повторения эксперимента (проведения еще одного) полученные сведения вносятся в структурированную базу данных, иначе проводится доработка необходимого элемента. Схема подхода к систематизации знаний приведена на рисунке 7.

Необходимо принимать во внимание, что исходные данные могут быть неточными и неполными (не могут быть точными и полными). Они могут быть недостоверными, более того, все исходные данные могут быть восприняты экспертом субъективно, с некоторым предубеждением. Также нельзя исключать возможные попытки дезинформации в целях дальнейшего облегчения попыток

нарушения конфиденциальности информации, которая будет защищаться построенной системой защиты.

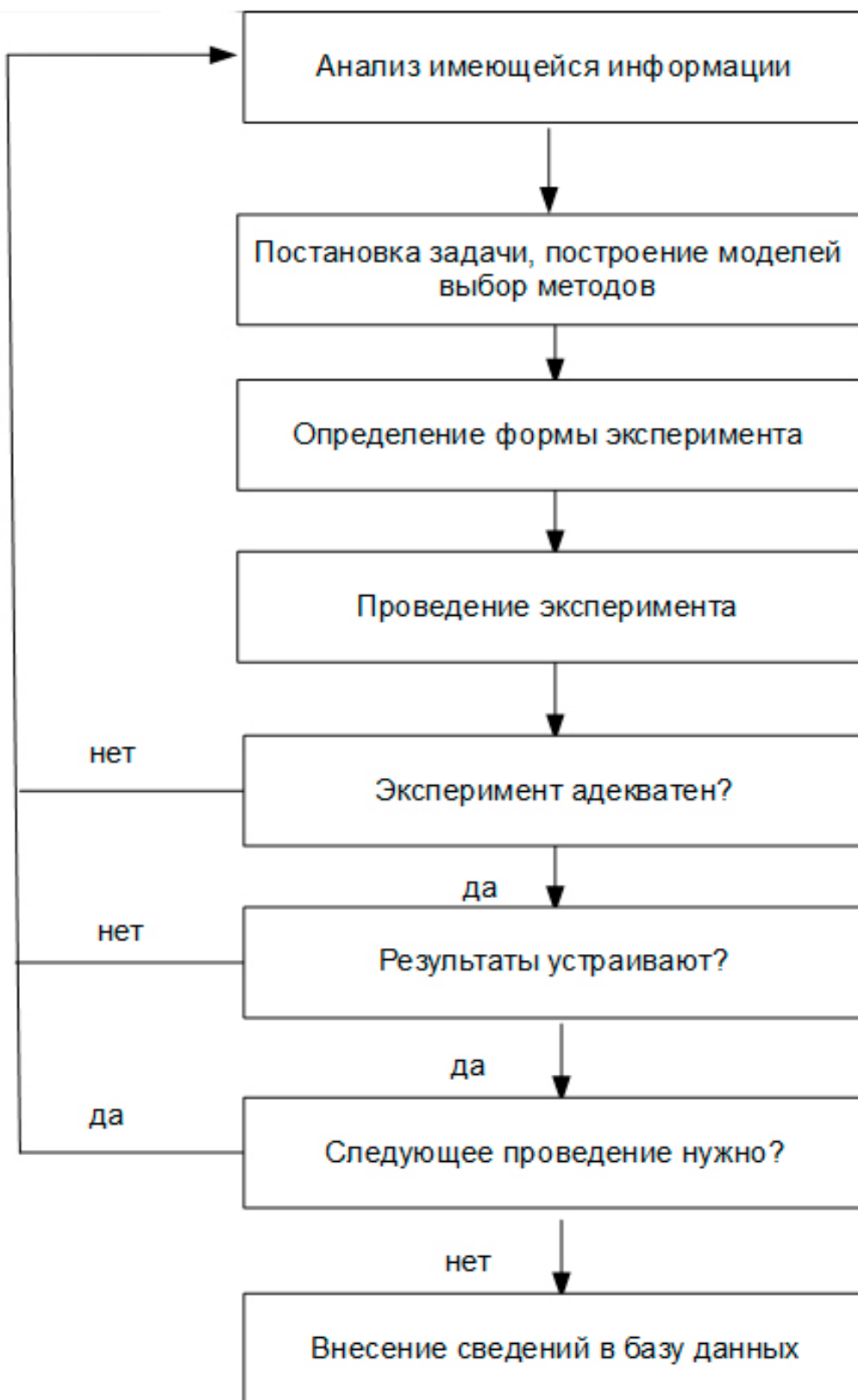


Рисунок 7 - Схема подхода к систематизации знаний

Возникает проблема разработки методов, которые помогали бы оценивать степень достоверности имеющейся информации с учетом вновь поступающих сведений.

Также существует проблема учета неполных и неточных сведений при моделировании. Существуют работы, предлагающие подходы, которые требуют предварительной работы с неопределенными данными и многозначной логикой. Однако, это подходы сложные, требующие проведения слишком большого количества предварительной работы, к тому же избавиться от неполных и неточных данных в любом случае не удастся.

Более того, перед экспертом всегда стоит задача поиска оптимального решения. Построение системы, предоставляющей максимально возможный уровень защиты, не всегда является целесообразным. Во-первых, уровень предоставляемой защиты должен соответствовать уровню предполагаемых угроз конфиденциальности информации и потерям, которые возможны при нарушении конфиденциальности. Во-вторых, важен экономический фактор, приобретение дорогостоящего средства защиты, противодействующего маловероятной (малоэффективной) потенциальной атаке, может быть нецелесообразным. Также расчет эффективности комплекса подсистем защиты или всей системы может быть затрудненным из-за сложности построения схемы всех связей, в то же время расчет эффективности отдельных подсистем (элементов) защиты, как правило, не является затрудненным.

Эксперт при исследовании проблем и процессов защиты, при поиске оптимального решения может использовать методы, которые в достаточной степени подходят для ситуаций с высокой степенью случайности и неопределенности [7]. К таким методам относятся:

- методы математического программирования;
- методы стохастического программирования;
- методы случайного поиска;
- методы моделирования;

- метод лингвистических переменных;
- метод нечетких множеств;
- метод формально-эвристического программирования;
- метод неформально-эвристического программирования;
- метод экспертных оценок;
- методы управления продуктивным мышлением.

Эти методы могут быть классифицированы по способу реализации и по степени формализации процедуры поиска.

По способу реализации методы подразделяются на следующие виды:

- аналитические. Такие методы предполагают построение модели в виде в виде комплекса аналитических и логических формул, при этом значения необходимых величин могут быть определены с помощью вычислений;
- статистические. Такие методы предполагают получение необходимых данных с помощью моделей, имитирующих деятельность системы и соответствующие «наблюдение и съем» данных;
- человеко-активные. Такие методы требуют активного участия человека, при этом человек сам создает информацию, необходимую для поиска решения.

По степени формализации процедуры поиска методы подразделяются на следующие виды:

- конечные. Предполагают нахождение оптимального решения за конечное число шагов строгого алгоритма;
- формально-эвристические. Предполагают использование формализованных эвристических процедур, подходящих для решения слабоструктурированных задач;
- неформально-эвристические. Предполагают, что человек должен вести процедуру поиска решения и управлять поиском.

Классификационная схема методов представлена на рисунке 8.

		Способ реализации		
		Аналитический	Статистический	Человеко-активный
Степень формализации процедуры поиска	Конечные	Методы математического программирования		
		Методы стохастического программирования		
		Методы случайного поиска		
			Методы моделирования	
	Формально-эвристические		Методы моделирования	
			Метод лингвистических переменных	
			Метод нечетких множеств	
			Метод формально-эвристического программирования	
	Неформально-эвристические			Метод неформально-эвристического программирования
				Метод экспертных оценок
				Методы управления мышлением

Рисунок 8 - Классификационная схема методов поиска оптимальных решений

Методы математического программирования. Математическое программирование является областью математики, к которой относится разработка теоретических положений, методов решения многомерных задач с ограничениями. Методы математического программирования являются методами, которые предполагают нахождение лучших из возможных путей решения задачи. К математическому программированию относятся следующие разделы: линейное, параметрическое, нелинейное, динамическое программирование. Методы математического программирования не подходят в случае, если в процедуре возможны случайные операции или существуют случайные величины.

Методы стохастического программирования. Стохастическое программирование является подразделом математического программирования, к которому относится разработка теоретических положений, методов решения условных экстремальных задач, когда не все параметры условий этой задачи известны. К стохастическому программированию относятся задачи, параметры условий которых неизвестны или имеют вероятностный характер. Также различаются подходы к задачам, при решении которых необходимо одно конечное действие и при решении которых требуются последующие, корректирующие действия. Методы стохастического программирования по сравнению с методами математического программирования более применимы в жизни, т.к. в сфере защиты информации очень редко возникают ситуации, когда известны все параметры и условия.

Методы случайного поиска. Идея, которая способствовала разработке этих методов, гласит, что оптимальное значение целевой функции может быть найдено посредством перебора случайных значений управляемого параметра. Простейшим подходом является перебор значений параметра с заданным шагом, однако такой подход является очень ресурсозатратным. В целом подход может быть эффективным, но неоптимальным с точки зрения выполненных операций.

Методы теории лингвистических переменных. Содержит комплекс приемов построения и эксплуатации моделей больших систем, которые

сформированы посредством тезисов эксперта, которые были выведены на основе опыта этого эксперта. Теория становится популярной из-за того, что множество систем не поддаются строгому моделированию в следствие высокой степени неопределенности этих систем (например, такие системы, к задачам которых относится удовлетворение человеческих потребностей). Теория лингвистических переменных основывается на трех положениях:

- вместо числовых переменных для оценки характеристик систем используются лингвистические переменные («высокий», «средний», «значительный» и т.д.);
- простые зависимости между переменными представляются в виде нечеткого высказывания структурой «из переменной 1 следует переменная 2»;
- сложные зависимости между переменными представляются в виде нечеткого алгоритма, который может быть представлен деревом вариантов, где с момента входа необходимо дать несколько ответов в речевой форме, что приведет к одному из возможных вариантов.

Применение теории может быть полезным в случаях, когда четкое моделирование систем, процессов, алгоритмов невозможно или нецелесообразно, например, при определении эффективности системы защиты конфиденциальной информации, при попытках построить общий, универсальный алгоритм построения системы защиты.

При этом стоит отметить, что применение и использование результатов этой теории требует грамотных действий персонала, знакомого с основами теории, иначе эффективность теории негарантирована, т.к. она позволяет систематизировать некоторые сведения, но не дает конкретных значений.

Неформальные методы поиска оптимальных решений. Эта группа методов подразделяется на 2 подгруппы: методы сведения задачи к формальной и методы непосредственного поиска решений. Первая подгруппа включает в себя следующие методы:

- теория нечетких множеств;
- формально-эвристическое программирование;

- эволюционное моделирование.

Вторая подгруппа включает в себя следующие методы:

- метод экспертных оценок;
- неформально-эвристическое программирование;
- методы управления продуктивным мышлением, к которым относятся

мозговой штурм и психо-интеллектуальная генерация.

Методы теории нечетких множеств. Применяются для описания систем, элементы которой с некоторой вероятностью принадлежат множествам — объединениям различных элементов, которые в контексте конкретной задачи могут (должны) считаться одним целым. Предусматривается числовая оценка вероятности принадлежности элемента к множеству и разработка строгого алгоритма решения поставленной задачи как результат.

Формально-эвристическое программирование. Так названы методы нахождения оптимального решения с использованием строгих алгоритмов, построенных на основе правил, знаний, закономерностей, «ноу-хау», которые были выявлены специалистом с опорой на опыт, интуицию и которые доказали свою способность быть полезными при решении определенных задач.

Важно знать, что метод предполагает получение решения, но не предполагает, что это решение будет оптимальным.

Существует два подхода к применению метода: лабиринтный и концептуальный.

Лабиринтный представляет собой дерево вариантов на пути от начала решения задачи к завершению, и предполагается, что в процессе прохождения дерева человек будет способен исключить неподходящие варианты и оставить только подходящие.

Концептуальный подход представляет собой процесс создания множества готовых путей решения задачи. Считается, что среди множества решений будут и те, которые наиболее подходят для решения задачи. Предполагается, что при построении путей решения задачи человек тщательно анализирует заданную

ситуацию и структурирует исходную и создаваемую информацию, что помогает построить достаточно качественные пути решения задачи.

Статистическое моделирование. Статистическим моделированием является метод изучения объектов на основе их статистических моделей. Здесь величины, которые необходимо получить, представляют характеристиками вероятности события, затем это событие моделируется, и на основе моделирования проводится статистическая обработка данных, полученных во время моделирования, которое заменяет собой процесс наблюдения.

Эволюционное моделирование. Этот метод представляет собой развитие статистического моделирования. При эволюционном моделировании алгоритм, посредством которого производится моделирование, сам изменяется (эволюционирует) с помощью статистических методов. При использовании метода эволюционного моделирования, можно сказать, имитируется не только действие системы, но и процессы ее жизненного цикла.

Применение метода включает в себя следующие этапы:

- построение начальной модели имитируемого процесса;
- построение алгоритма изменения (эволюционирования) модели имитируемого процесса;
- нахождение необходимых характеристик процесса на начальной модели;
- изменение (эволюционирование) начальной модели процесса;
- нахождение необходимых характеристик процесса на измененной модели;
- проведение сравнительного анализа начальной и измененной моделей имитируемого процесса;
- принятие решения о необходимости дальнейшего изменения моделей имитируемого процесса или окончании моделирования.

Метод экспертных оценок (относится к неформальным методам оценки). Применяется при решении задач, которые не поддаются формализации. Результатом применения метода является свод мнений (усредненная оценка), которые даны компетентными в определенной сфере специалистами.

Опрос экспертов может проходить в нескольких формах. К ним относятся: выражение мнения в свободной форме по поставленному вопросу, интервью, анкетирование.

Очень важной является проблема подбора экспертов и определение их необходимого количества. Во-первых, эксперты должны быть достаточно компетентны. Во-вторых, они должны обладать некоторыми качествами, такими, как способность решать нетривиальные задачи, способность не поддаваться авторитетным мнениям, способность работать в коллективе, способность давать практически значимые и применимые решения, самокритичность. Количество экспертов также не должно быть слишком маленьким или, наоборот, большим. Слишком малое число специалистов может не предоставить достаточной выборки мнений. Слишком большое число может создать множество сложностей при организации работы, может затратить слишком много ресурсов, также это серьезно осложняет сведение экспертных оценок к итоговой, которая являлась бы результатом применения метода.

Неформально-эвристическое программирование. Является разновидностью формально-эвристического программирования - метода нахождения оптимального решения с использованием строгих алгоритмов, построенных на основе правил, знаний, закономерностей, «ноу-хау», которые были выявлены специалистом с опорой на опыт, интуицию и которые доказали свою способность быть полезными при решении определенных задач. Разница в том, что здесь человек не только составляет модели поиска решений, но также проводит подготовку к решению задач в конкретных условиях и непосредственно участвует в процессе решения задачи.

К этому методу также относится (можно выделить) метод неформальных аналогов — когда специалист находит прецеденты и использует найденные там решения.

Метод «мозгового штурма» является методом нахождения решений в процессе коллективного обсуждения несколькими экспертами проблемы и творческого подхода к ее решению.

Существует два подхода к применению метода. При первом возникшие идеи сразу обсуждаются и оцениваются. При втором задействуется две группы специалистов: одна занята процессом нахождения и создания решений, вторая — их оценкой.

Метод психо-интеллектуальной генерации представляет собой процесс беседы, которая включает в себя ведущего и решающего и контролируется и целенаправленно управляется ведущим. Ведущий ответственен за постановку задач, решающий — за нахождение решений поставленных задач. Предполагается, что в процессе такой беседы возникнет дискуссия касательно предлагаемых решений, что должно привести к комплексному и подробному изучению проблемы. Также в беседе возможно участие оппонента и эксперта. Оппонент ответственен за нахождение неточностей, потенциальных ошибок в предлагаемых решающим идеях, формирование примечаний, требование уточнений и пояснений. Эксперты отвечают за оценку предлагаемых решений и помогают в дальнейшем формировании беседы с учетом вновь возникших идей.

Итого, первым этапом построения системы защиты конфиденциальной информации должна стать постановка задачи. Здесь определяется, какую систему необходимо построить, какие требования она должна удовлетворять, какую информацию она должна защищать.

3.1 Постановка задачи

Согласно Федеральному закону "Об информации, информационных технологиях и о защите информации"¹, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

— обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

¹ Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в ред. Федерального закона от 18.03.2019 N 31-ФЗ).

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Исходя из определения, можно сделать вывод, что проблема защиты информации базируется на трех положениях:

- система информации (в широком смысле) должна быть в состоянии противостоять вредоносному воздействию внутренних и внешних угроз, при этом оставляя в неизменности собственные структуру и степень эффективности осуществления деятельности;

- система информации должна быть в состоянии поддерживать стабильное состояние самой себя и своих подсистем вне зависимости от условий, создаваемых внешней и внутренней средами;

- система информации должна быть удобной, не должна создавать препятствий работы для своих пользователей, администраторов и обслуживающего персонала.

В общем можно сказать, что задачей является построение надежной, стабильной, неуязвимой системы защиты информации, которая способна обеспечить наиболее эффективную и рациональную работу с информацией.

В целях обеспечения построения такой системы и дальнейшего ее развития необходимо решать следующие задачи:

- длительный и постоянный контроль состояния действующих систем и сбор различных сведений об их функционировании. Это позволит наработать базу данных о работе различных систем, их компонентов, обобщить опыт, что поможет выявить наиболее, наименее эффективные и неэффективные способы и методы защиты информации;

- дальнейшая наработка и развитие научно-методической базы теории защиты информации. Это облегчит работу эксперта, которому в основном приходится основываться на своем опыте и интуиции.

К функциям защиты информации относятся:

– функция 1 — предупреждение проявления ситуаций, при которых могут возникнуть дестабилизирующие факторы. Данная функция подразумевает действие на упреждение. Предполагается, что система документооборота, система защиты конфиденциальной информации, сопутствующая инфраструктура спроектированы, построены и эксплуатируются и персонал, работающий с конфиденциальной информацией и обслуживающий системы документооборота и защиты информации, осуществляют свою деятельность таким образом, что возможность возникновения каких-либо дестабилизирующих факторов является маловероятной;

– функция 2 — обнаружение возникших и проявившихся, независимо от условий, дестабилизирующих факторов. Предполагается, что дестабилизирующие факторы (или условия, при которых вероятность их возникновения является очень высокой) должны быть обнаружены до того момента, когда они могут повлиять на состояние конфиденциальной информации. Иначе, предполагаются мероприятия по постоянной проверке систем документооборота, защиты информации и их сред на возможность проявления дестабилизирующих факторов;

– функция 3 — предупреждение влияния дестабилизирующих факторов на конфиденциальную информацию. Предполагается, что должны производиться такие действия, которые смогут противодействовать влиянию дестабилизирующих факторов в случае их возникновения и проявления. Стоит отметить, что возникшие и проявившиеся дестабилизирующие факторы могут остаться необнаруженными, поэтому предполагается, что надежная система защиты конфиденциальной информации должна быть способна предупредить влияние даже необнаруженных дестабилизирующих факторов на конфиденциальную информацию;

– функция 4 — обнаружение влияния дестабилизирующих факторов на конфиденциальную информацию. Предполагается, что, в случаях, когда не удалось предупредить влияние дестабилизирующих факторов на конфиденциальную информацию, такое влияние должно быть хотя бы обнаружено. Осуществление функции считается успешным, если влияние дестабилизирующих факторов обнаружено на момент возможности локализации влияния на защищаемую информацию;

– функция 5 — локализация влияния дестабилизирующих факторов на конфиденциальную информацию. Предполагается, что, в случае результативного проявления дестабилизирующих факторов, их влияние должно быть сведено к минимуму — должны быть перекрыты возможные пути дальнейшего проникновения к защищаемой информации сквозь систему защиты информации;

– функция 6 — ликвидация последствий проявления и влияния дестабилизирующих факторов на конфиденциальную информацию. Предполагаются действия, при которых устраняются последствия локализованного влияния дестабилизирующих факторов и система документооборота, система защиты конфиденциальной информации и сопутствующая инфраструктура приводятся в состояние, соответствующее состоянию до момента проявления дестабилизирующих факторов.

Очевидно, что осуществление функций на практике является последовательным — в случае осуществления системой защиты конфиденциальной информации первой функции качественно и без сбоев, осуществление последующих функций не будет необходимым, однако при проектировании должны быть учтены все из них.

Также необходимо предусмотреть всеобъемлющее покрытие имущества организации (как материального, так и нематериального, которое влияет на степень конфиденциальности защищаемой информации) системой защиты.

Раньше, различные средства коммуникации не были развиты, следовательно, необходимо было защищать сами носители информации и прилегающую территорию. Затем, при развитии средств коммуникации (например, телефон), появилась возможность перехватывать данные с каналов связи и последующая необходимость эти каналы защищать. Далее, с появлением и повсеместным распространением компьютеров, стали использоваться различные средства и системы электронного документооборота, что сделало возможными новые виды атаки на защищаемую информацию. Система защиты информации должна быть комплексной, и именно сейчас они становятся наиболее сложными и многосоставными. Необходимо распространять действие системы защиты на территорию организации-владельца конфиденциальной информации, ее здания и помещения, персонал, компоненты самой системы защиты информации, непосредственно конфиденциальную информацию. Весь этот комплекс должны покрывать несколько подсистем защиты информации, которые и представляют собой систему.

Эксперту необходимо собрать и систематизировать большое количество информации, чтобы построить надежную, стабильную, комплексную систему защиты информации. Чтобы собрать эту информацию, необходимо пройти несколько этапов:

- определение и классификация потенциальных угроз;
- оценка уязвимости информации;
- оценка уязвимости защищаемой информации и оценка возможного ущерба в случае нарушения степени конфиденциальности;
- постановка требований к защите информации;
- моделирование процессов защиты информации и управление ими.

Затем возможен переход к построению системы защиты информации и ее дальнейшему управлению.

3.2 Определение и классификация потенциальных угроз информации.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ 50922).

Угрозы безопасности информации могут быть поделены на 3 группы: угрозы конфиденциальности информации, угрозы целостности информации, угрозы доступности информации.

К причинам возникновения угроз безопасности информации относятся следующие условия:

- сбои, отказы, ошибки в работе оборудования;
- катаклизмы, стихийные бедствия;
- непреднамеренные действия персонала;
- непреднамеренные действия посторонних;
- нехватка качества и/или количества элементов системы защиты информации;
- целенаправленные действия злоумышленников;
- технические и программные средства нарушения работы системы защиты информации, ее преодоления;
- факторы внешней среды (состояние атмосферы, наводки различной природы).

К причинам возникновения угроз целостности информации относятся следующие условия:

- сбои, отказы, ошибки в работе оборудования;
- катаклизмы, стихийные бедствия;
- непреднамеренные действия персонала;
- целенаправленные действия злоумышленников;
- факторы внешней среды (состояние атмосферы, наводки различной природы).

К причинам возникновения угроз доступности информации относятся следующие условия:

- сбои, отказы, ошибки в работе оборудования;
- катаклизмы, стихийные бедствия;
- непреднамеренные действия персонала;
- факторы внешней среды (состояние атмосферы, наводки различной природы).

К причинам возникновения угроз конфиденциальности информации относятся следующие условия:

- сбои, отказы, ошибки в работе оборудования;
- непреднамеренные действия персонала;
- непреднамеренные действия посторонних;
- нехватка качества и/или количества элементов системы защиты информации;
- целенаправленные действия злоумышленников;
- технические и программные средства нарушения работы системы защиты информации, ее преодоления.

Для построения качественной системы защиты информации необходимо особенно тщательно рассмотреть потенциальные угрозы конфиденциальности информации.

Реализация угрозы конфиденциальности информации предполагает создание канала несанкционированного получения защищаемой информации. Как правило, их возникновение связано с преднамеренными действиями злоумышленников, что значительно осложняет задачу классификации каналов, т.к. получение защищаемой информации является во многом «творческим» процессом. Классифицировать каналы можно следующим образом: критериями выбираются показатели «состояние защищаемой информации» и «степень проникновения через систему защиты». По первому критерию возможны два значения: активное (конкретная защищаемая информация находится в работе) и пассивное. По второму критерию возможны три значения: без проникновения и с

проникновением, что разбивается на с изменением системы защиты и без изменения. В итоге возникает 6 классов каналов несанкционированного получения защищаемой информации (представлены на рисунке 9) [8].

Критерии			Состояние информации	
			Пассивное	Активное
Степень проникновения через систему защиты	Без проникновения		1 класс	2 класс
	С проникновением	Без изменения системы защиты	3 класс	4 класс
		С изменением системы защиты	5 класс	6 класс

Рисунок 9 - Классификация каналов несанкционированного получения защищаемой информации

Первый класс — пассивное состояние и без проникновения. К таким каналам можно отнести: кражу носителей информации, подслушивание неаккуратных обсуждений, случайная выдача конфиденциальной информации, случайная утеря носителей информации.

Второй класс — активное состояние и без проникновения. К таким каналам можно отнести: электромагнитное излучение каналов связи, электромагнитное излучение аппаратуры, наводки в электрике, наводки в каналах связи.

Третий класс — пассивное состояние, с проникновением, но без изменения системы защиты. К таким каналам можно отнести: копирование материальных и нематериальных носителей информации, фотографирование материальных носителей информации.

Четвертый класс — активное состояние, с проникновением, но без изменения системы защиты. К таким каналам можно отнести: фотографирование отображения нематериальных носителей информации, компрометация учетных записей авторизованных пользователей, использование «лазеек» программного обеспечения, использование специального шпионящего программного обеспечения.

Пятый класс — пассивное состояние, с проникновением и с изменением системы защиты. К таким каналам можно отнести: подмена носителей информации, хищение носителей информации, включение в программное обеспечение шпионящих элементов, снятие сигналов из оперативной памяти компьютеров.

Шестой класс - активное состояние, с проникновением и с изменением системы защиты. К таким каналам можно отнести: включение шпионящей аппаратуры в каналы связи, включение шпионящей аппаратуры в оборудование, снятие сигналов с каналов связи, снятие сигналов с оборудования.

Определение и оценка угроз безопасности информации являются важными этапами при построении системы защиты информации. Это оказывает существенное влияние на модели и необходимые элементы системы защиты.

Необходимо учитывать, что должны быть найдены и определены все потенциальные угрозы безопасности информации. Любой упущенный фактор может привести к практической неэффективности системы защиты информации. При этом проблемы выявления потенциальных угроз информации является неформализованной, т.к. в нынешних реалиях на функционирование систем документооборота, систем защиты информации оказывает влияние (иногда случайное) большое количество факторов. Эта проблема может быть разрешена посредством моделирования и проведения эксперимента над системой, что, однако, является дорогим и затратным. Также возможно применение метода экспертных оценок.

3.3 Оценка уязвимости информации

Под уязвимостью информации понимается ситуация, когда система защиты информации неспособна противостоять несанкционированным действиям в отношении защищаемой информации и/или дестабилизирующим факторам. Рисунок 10 содержит модель уязвимости в общем виде.

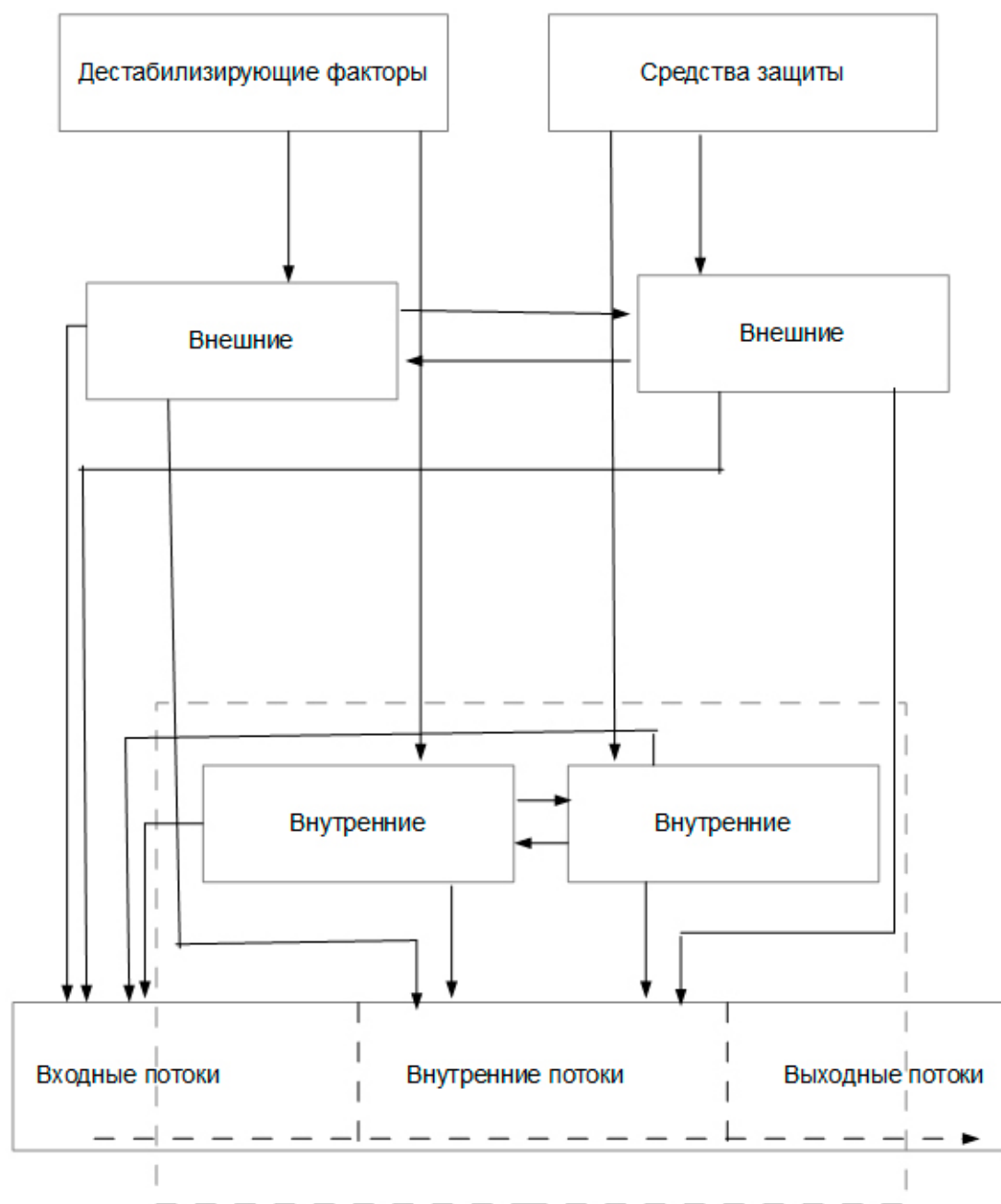


Рисунок 10 – Общая модель уязвимости информации

В случае рассмотрения частной ситуации (нарушение целостности информации, несанкционированное получение) общая модель уязвимости детализируется.

При рассмотрении ситуации нарушения целостности информации необходимо учитывать, что целостность информации зависит не только от процессов работы с ней, но и от ее состояния на входе в систему документооборота. Наиболее вероятным является возникновение случайных дестабилизирующих факторов (отказы, сбои, ошибки), которые могут проявиться в любой момент, независимо от иных обстоятельств, что позволяет считать такие факторы регулярными. Остальные факторы нарушения целостности относятся к возможным. Из стихийных бедствий наиболее вероятными являются пожары, побочные явления могут быть практически исключены путем грамотного подбора и размещения компонентов системы документооборота, злоумышленные действия зависят от ценности защищаемой информации, уровня конкуренции. Модель уязвимости целостности информации представлена на рисунке 11.

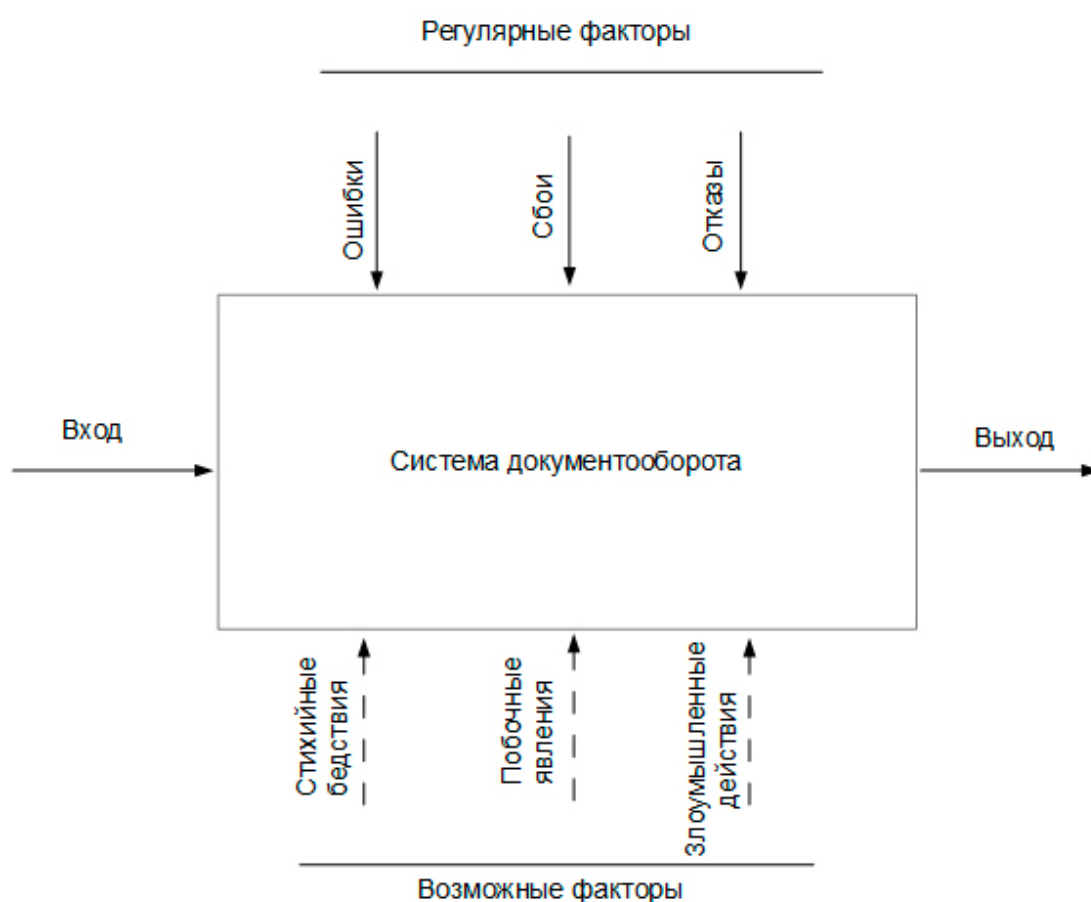


Рисунок 11 - Модель уязвимости целостности информации

В современных условиях существует множество возможных путей несанкционированного получения информации. При этом необходимо учитывать, что для этого требуются целенаправленные злоумышленные действия со стороны людей; возникновение случайных факторов непосредственно не ведет к компрометации защищаемой информации, но создает предпосылки к этому (создает возможные каналы несанкционированного получения информации). Для несанкционированного получения информации требуется проникновение злоумышленника тем или иным путем к тому или иному элементу системы документооборота. Вместе с этим, в зоне проникновения в то же время должен проявиться один из каналов несанкционированного получения информации, который может привести к нужной информации и которым злоумышленник способен воспользоваться. Модель проникновения в службу конфиденциального документооборота представлена на рисунке 12.

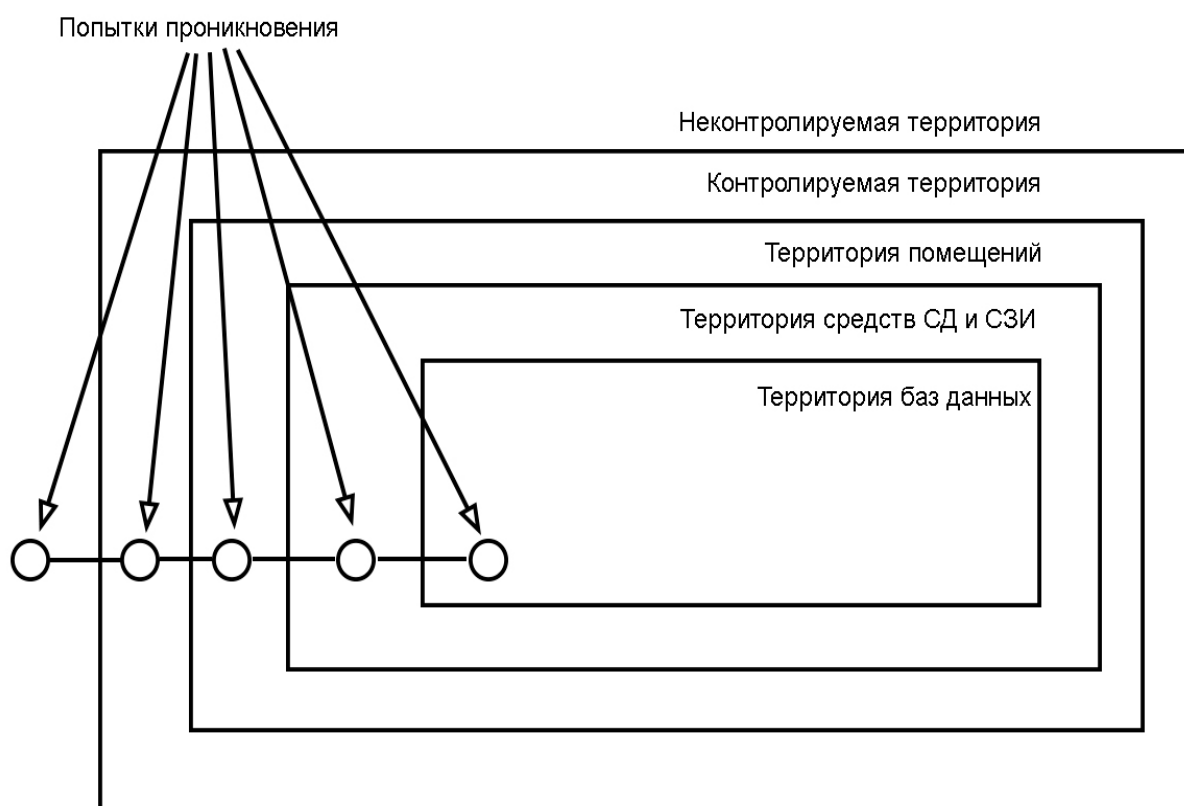


Рисунок 12 - Модель проникновения в службу конфиденциального документооборота

На рисунке 12 обозначены пять зон. К неконтролируемой территории относится территория вне пределов организации, следовательно, на которую не распространяется действие элементов системы защиты информации и состоянием которой организация управлять не может. К контролируемой территории относится территория, принадлежащая организации, на которой расположены здания и имущество организации; на эту территорию распространяется действие элементов системы защиты информации и ее состоянием организация может управлять. К территории помещений относятся все помещения во всех зданиях организации, на эту территорию распространяется действие элементов системы защиты информации и ее состоянием организация может управлять. К территории средств системы документооборота и системы защиты информации относятся все помещения, в которых размещены какие-либо элементы систем документооборота и защиты информации и/или в которых проводятся работы с документами или по информационной безопасности организации; на эту территорию распространяется действие элементов системы защиты информации и ее состоянием организация может управлять. К территории баз данных относятся те помещения, в которых можно получить непосредственный доступ к защищаемой информации (к компьютерам, на которых хранится такая информация, к различным носителям информации); на эту территорию распространяется действие элементов системы защиты информации и ее состоянием организация может управлять.

В каждой из этих зон возможно проведение целенаправленных злоумышленных действий с целью несанкционированного получения информации. Неконтролируемая территория не может быть включена в зону действия системы защиты информации, но вместе с этим она предоставляет наименьшее количество путей несанкционированного получения информации. Другие зоны предоставляют большее количество возможностей для действий по несанкционированному получению информации, которые, однако, могут и

должны пресекаться системой защиты информации. Модель несанкционированного получения информации представлена на рисунке 13.

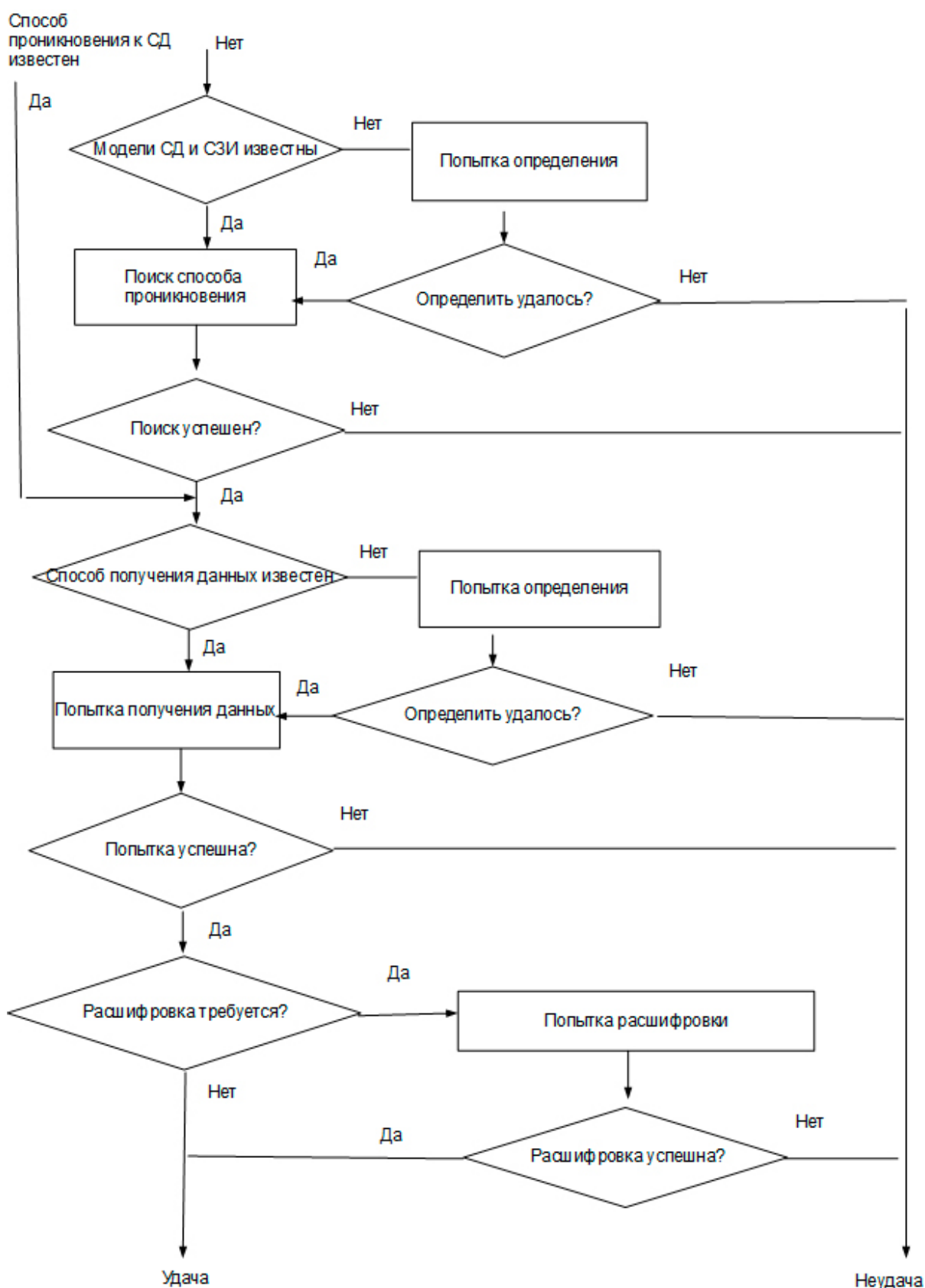


Рисунок 13 – Алгоритм несанкционированного получения информации

Показатели уязвимости информации могут быть оценены с помощью применения моделирования работы системы документооборота, системы защиты информации и возникновения дестабилизирующих факторов различной природы [8]. Моделирование процесса определения уязвимости информации представлена на рисунке 14.

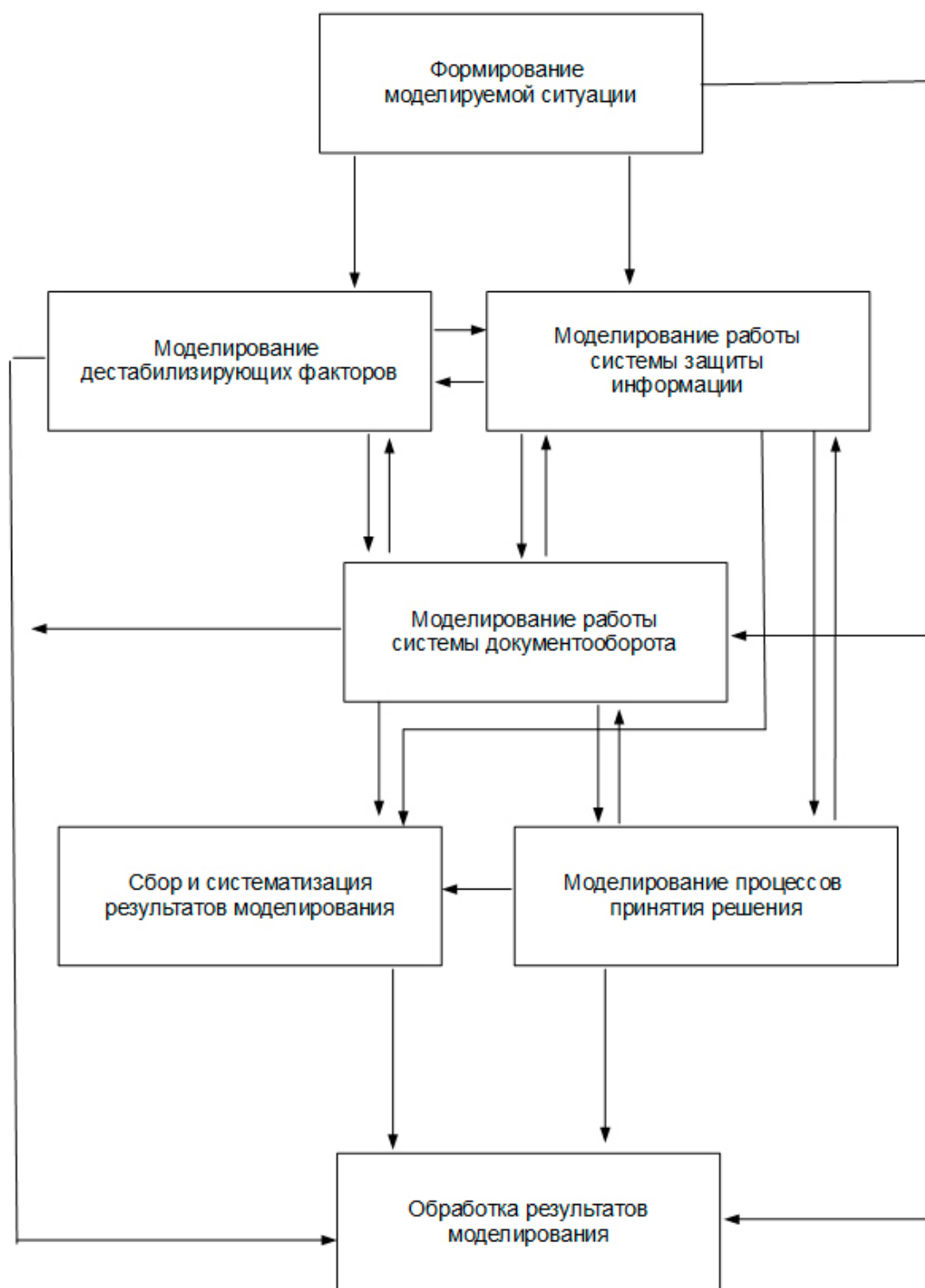


Рисунок 14 –Моделирование процесса определения уязвимости информации

3.4 Постановка требований к защите информации

Требованием к защите информации может быть необходимость противодействия угрозам информации, однако такой подход не учитывает то, что многие события и явления в сфере информационной безопасности не являются постоянными, не могут быть предварительно рассчитаны и носят случайный характер. С учетом этих факторов требование к защите информации можно выразить как превосходство вероятности защищенности информации над требуемым уровнем защиты.

Более детализированные требования зависят от многих факторов. К таким факторам можно отнести: характер информации, объем информации, структура системы документооборота и структура системы защиты информации, вид объекта, носители информации, степень обученности персонала, степень лояльности персонала.

Характер информации определяет необходимый уровень защиты информации: например, коммерческая тайна подлежит более тщательной защите, чем информация «для служебного пользования».

Объем информации определяет требования к размещению информации и документов. Особенные трудности может вызвать большое количество защищаемой информации, размещенной на бумажных носителях.

Структура системы документооборота и структура системы защиты информации определяют требования к выбору, размещению, применению средств, методов работы с документами и информацией и требования к выбору, размещению, применению средств, методов защиты информации, документов, сопутствующей инфраструктуры (например, линии связи).

Вид объекта определяет требования к обработке этого объекта, которые зависят от его природы и формы (информация, документ, текстовая форма, графическая форма и т.д.).

Носитель информации определяет требования к средствам, методам его обработки и требования к условиям его размещения (сейфы, шифрованные жесткие диски и т.д.).

Степень обученности персонала определяет требования к организационной работе в сфере информационной безопасности и требования к оснащенности системы защиты различными средствами, которые способны предотвратить неумышленное потенциально компрометирующее действие.

Степень лояльности персонала определяет требования к организационной работе в сфере информационной безопасности и требования к оснащенности системы защиты различными средствами, которые способны предотвратить потенциальное несанкционированное действие.

Также важно определить ценность самой защищаемой информации. Информация может быть рассмотрена как средство обеспечения решения задач и как объект деятельности. Для первого случая можно выделить следующие параметры: значимость (важность информации при осуществлении деятельности), полнота (является ли количество сведений достаточным для осуществления деятельности), адекватность (соответствие информации текущей обстановке), релевантность (степени наличия нужной и отсутствия «ненужной» информации), удобство восприятия (насколько сложно воспринимать информацию). Для второго случая можно выделить следующие параметры: форма представления, объем.

С точки зрения поддержания степени конфиденциальности защищаемой информации определяющими являются значимость и полнота, важными являются адекватность, релевантность, объем, удобство восприятия и форма представления являются второстепенными.

Также важным этапом является определение факторов, которые влияют на требуемый уровень защиты. Т.к. многие процессы в сфере информационной безопасности носят случайный характер и отсутствуют базы данных статистических данных по системам защиты информации, задача определения таких факторов является неформальной. При ее решении можно применить

метод психо-интеллектуальной генерации. Процедуру определения факторов можно разбить на три этапа: определение списка групп факторов, определение списка факторов по группам, определение значений факторов.

Можно сформировать следующий список факторов, которые влияют на требуемый уровень защиты [8]:

- зависящие от защищаемой информации;
 - степень конфиденциальности;
 - объем;
 - интенсивность работы с этой информацией;
- зависящие от строения системы документооборота и системы защиты информации;
 - физические размеры;
 - распределенность;
 - структуры систем;
- зависящие от условий работы системы документооборота и системы защиты информации;
 - внешнее расположение;
 - внутреннее расположение;
 - оснащенность систем элементами;
- зависящие от методов работы с информацией;
 - методы создания (получения) информации;
 - методы применения информации;
 - методы хранения информации;
 - методы уничтожения информации;
- зависящие от организации работы с защищаемой информацией;
 - общая организация работы с информацией и документами;
 - организация защиты информации и документов;
 - степень обученности персонала;
 - степень лояльности персонала.

3.5 Моделирование и проектирование систем защиты информации.

Моделирование — процесс проектирования и реализации образа (модель) изучаемого объекта и сбора необходимых данных с помощью этого образа. Модель должна соответствовать целям и задачам исследования — должны быть точно и детально переданы те параметры системы, которые могут повлиять на значение искомых данных, в то же время второстепенные, согласно целям и задачам исследования, параметры могут быть переданы схематично. Таким образом, моделирование является процессом, состоящим из трех этапов: проектирование модели, ее реализация и эксплуатация.

Необходимо провести классификацию моделей, которые могут быть использованы при работе в сфере информационной безопасности. Модели могут быть классифицированы по трем критериям: способ моделирования, характер исследуемого объекта, масштаб моделирования.

Способ моделирования, который использован при построении модели. Данный критерий имеет два возможных значения: модели могут быть аналитическими и статистическими. Аналитической моделью является совокупность зависимостей аналитической и/или логической природы, с помощью которых могут быть найдены искомые данные посредством выполнения расчетов по этим зависимостям. Статистической моделью является модель, построенная на основе совокупности зависимостей, которые определены на основе опыта эксплуатации реальной системы, подобной исследуемой и которые обрабатываются при исследовании.

Характер системы. Здесь определяется характер отношений между теми параметрами, которые должны быть найдены при использовании модели, и параметрами, принадлежащими системе, внешней среде, которые оказывают влияние на искомые параметры. Данный критерий имеет два возможных значения: модели могут быть детерминированными и стохастическими. При детерминированном характере исследуемого объекта все зависимости

определены однозначно и строго, при стохастическом же характере системы зависимости подвержены влиянию неопределенных, вероятных факторов.

Масштаб моделирования. Здесь определяется уровень характеристик, которые отражает проектируемая модель. Данный критерий имеет два возможных значения: модели могут быть общими и частными. При общем масштабе моделирования могут быть найдены значения общих характеристик системы, при частном уровне могут быть найдены местные характеристики, характеристики отдельных элементов системы.

Классификационная схема моделей представлена на рисунке 15.

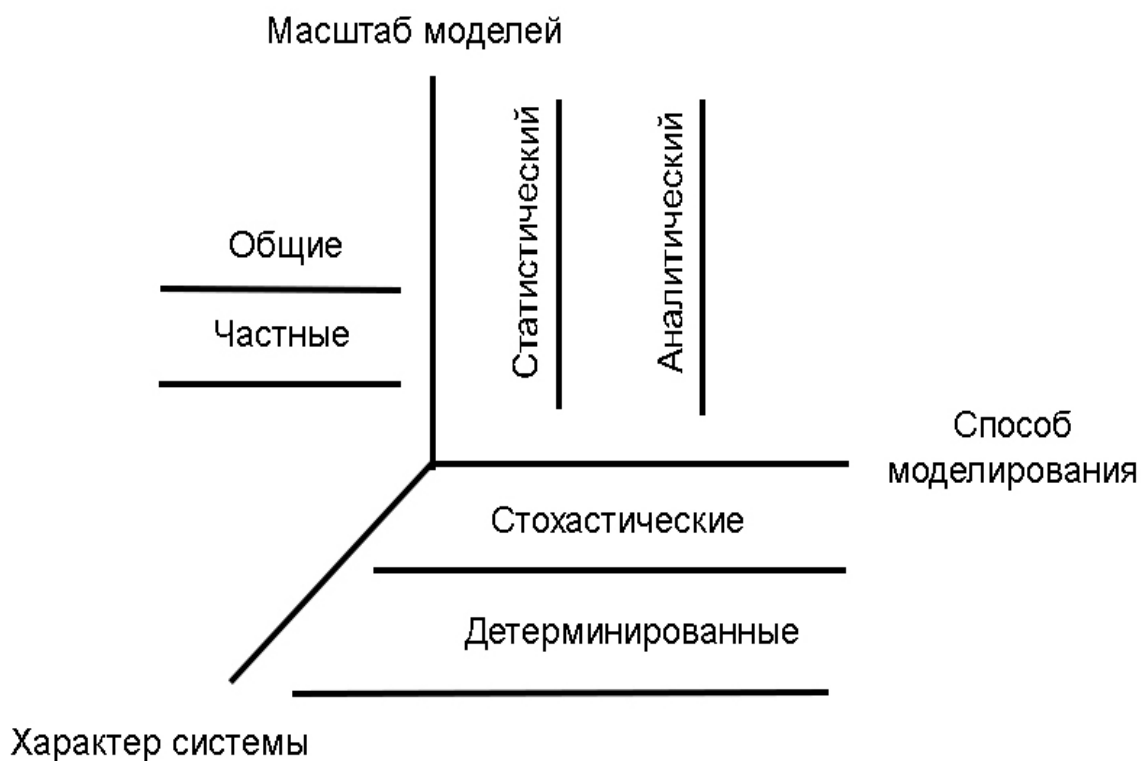


Рисунок 15 - Классификационная схема моделей

Как уже было сказано, различные процессы, относящиеся к сфере информационной безопасности, носят вероятностный, неопределенный характер, следовательно, в этой сфере модели детерминированного характера использоваться быть не могут. Это приводит к тому, что в сфере информационной

безопасности могут быть применены модели четырех разновидностей: статистические частные, статистические общие, аналитические частные, аналитические общие.

При применении аналитического способа моделирования структура исследуемой системы и процессы ее функционирования выражены посредством выражений, которые определяют взаимосвязь искомых параметров и параметров самой системы и внешней относительно нее среды. В аналитических моделях имитация процессов деятельности системы, по сути, не производится; вместо имитации и «смены времени» производится расчет параметров с использованием выражений, положенных в основу модели.

При применении статистического способа моделирования структура исследуемой модели четко и явно отражена в построенной модели, процессы функционирования системы и «смена времени» отыгрываются. При этом смоделированные структура системы и процессы должны в необходимой для конкретного исследования степени соответствовать соответственно структуре и процессам функционирования существующей системы.

Систему защиты конфиденциальной информации функционально можно рассматривать как организованную совокупность элементов, направленных на осуществление функций защиты. Общая функциональная модель системы защиты в таком аспекте представлена на рисунке 16 [8].

Механизмы обеспечения защиты информации состоят из переменных и постоянных механизмов. Постоянными механизмами представляют собой такие механизмы, которые являются неотъемлемыми элементами всей системы защиты информации, не являются самостоятельными, осуществляют свои функции постоянно в течение времени работы системы защиты. Переменными механизмами представляют собой такие механизмы, которые не являются встроенными в систему защиты, являются автономными и для осуществления своих функций в целях защиты информации требуют своего включения в систему защиты. Природа таких механизмов является общей: они могут быть техническими, программными, организационными.

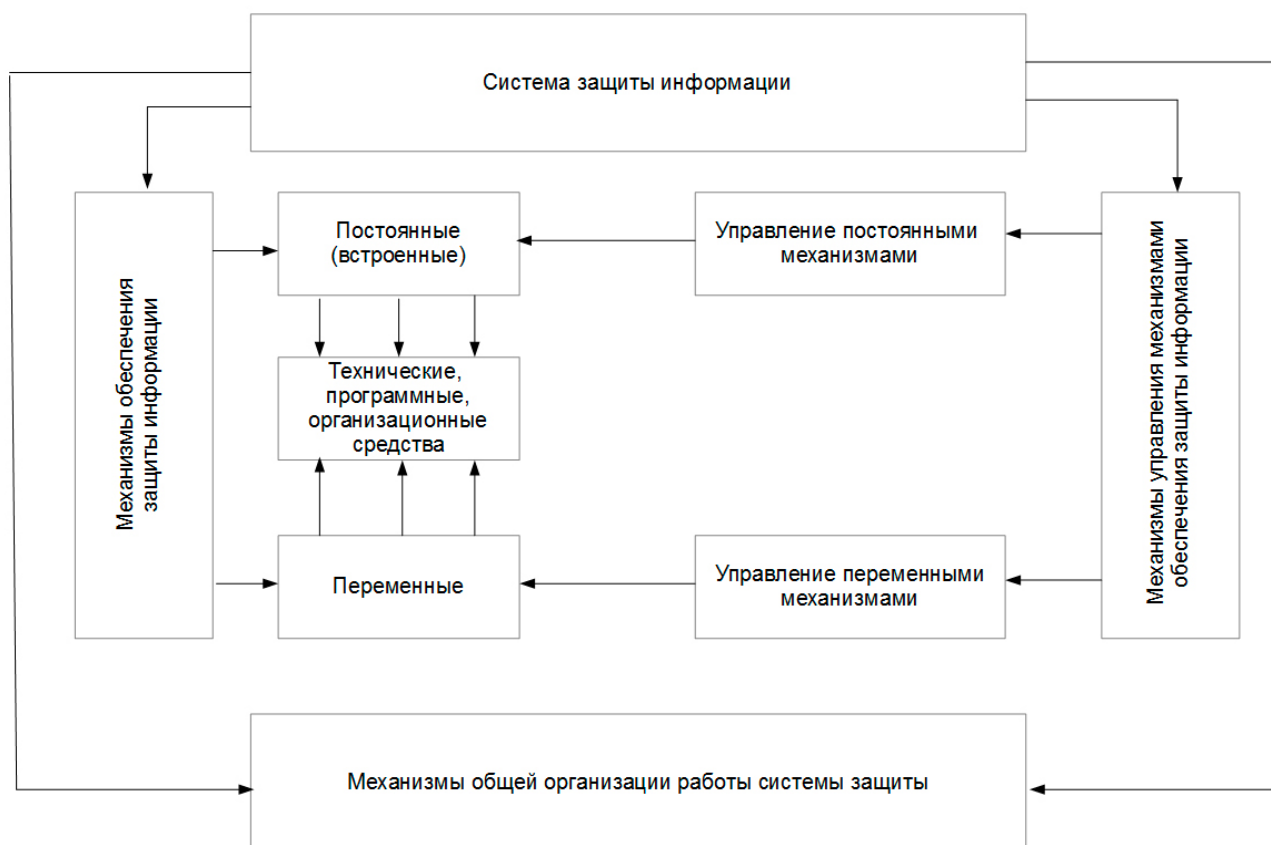


Рисунок 16 - Общая функциональная модель системы защиты

Механизмы управления должны повторять структуру и построение самих механизмов защиты.

Механизмы общей организации работы осуществляют функцию связи и координации всех элементов системы защиты информации.

Структурная модель системы защиты конфиденциальной информации приведена на рисунке 17 [7].

К взаимодействующему персоналу относятся все работники организации, которые тем или иным образом взаимодействуют с защищаемой информацией, системой документооборота, системой защиты информации. Такими являются: сотрудники, непосредственно работающие с конфиденциальной информацией; руководители (в первую очередь высшее руководство организации, также руководители подразделений, которым может быть необходимо знать о защищаемой информации, например, главный бухгалтер); персонал, так или иначе обслуживающий системы документооборота и защиты информации.

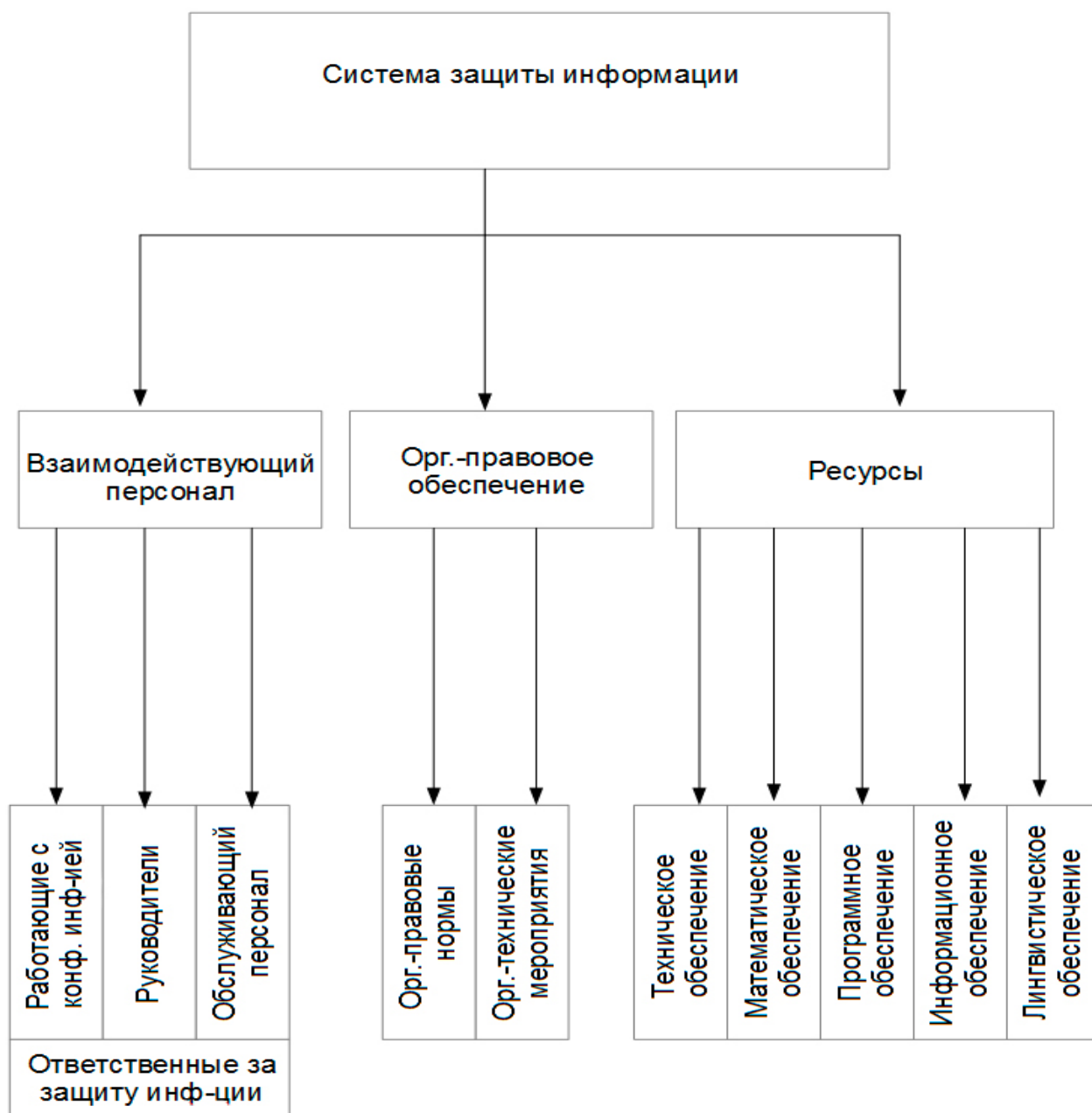


Рисунок 17 - Структурная модель системы защиты

Ответственные за защиту информации также относятся к взаимодействующему персоналу, но вынесены в отдельный ряд, т.к. именно они контролируют остальной персонал по вопросам, которые касаются информационной безопасности, и в целом отвечают за установление и поддержание режима конфиденциальности.

К организационно-правовому обеспечению относятся организационно-правовые нормы и организационно-технические мероприятия. Организационно-правовые нормы представляют собой документы, которые устанавливают правовой режим защиты информации, регулируют и регламентируют этот режим

защиты, работу системы защиты информации. Организационно-технические мероприятия представляют собой действия по осуществлению функций защиты информации и действия по соединению всех элементов системы защиты информации в единую комплексную систему.

К ресурсам относятся те средства, методы и данные, которые необходимы для проектирования, реализации и функционирования системы защиты информации.

Техническое обеспечение — комплекс технических средств, предназначением которых является техническая поддержка осуществления тех функций защиты, с учетом которых спроектирована и реализована система защиты.

Математическое обеспечение — комплекс математических методов, способов решения задач, с применением которых решаются задачи оценки стоимости защищаемой информации, потенциальных рисков нарушения конфиденциальности информации, степени защищенности информации и т.д..

Программное обеспечение — комплекс программ, которые относятся к той части системы защиты информации, которая реализована на основе компьютеров, работе которой компьютеры оказывают поддержку.

Информационное обеспечение — комплекс баз данных, моделей, систематизированной информации, документов, которые тем или иным образом относятся к системе защиты информации: документы, регламентирующие работу системы защиты, модели подсистем защиты информации и т.д..

Лингвистическое обеспечение — комплекс формализованных языковых средств, направленных на описание различных информации и алгоритмов. Позволяет осуществлять взаимодействие между различными частями информационной системы, между информационной системой и человеком.

Система защиты информации может быть спроектирована на основе типового или индивидуального проекта. Первый вариант предполагает меньшие денежные, трудовые и временные затраты, второй вариант позволяет построить систему защиты, обеспечивающую максимально возможную степень защиты.

Процесс проектирования состоит из десяти этапов [8]. Схема, отражающая процесс, приведена на рисунке 18.

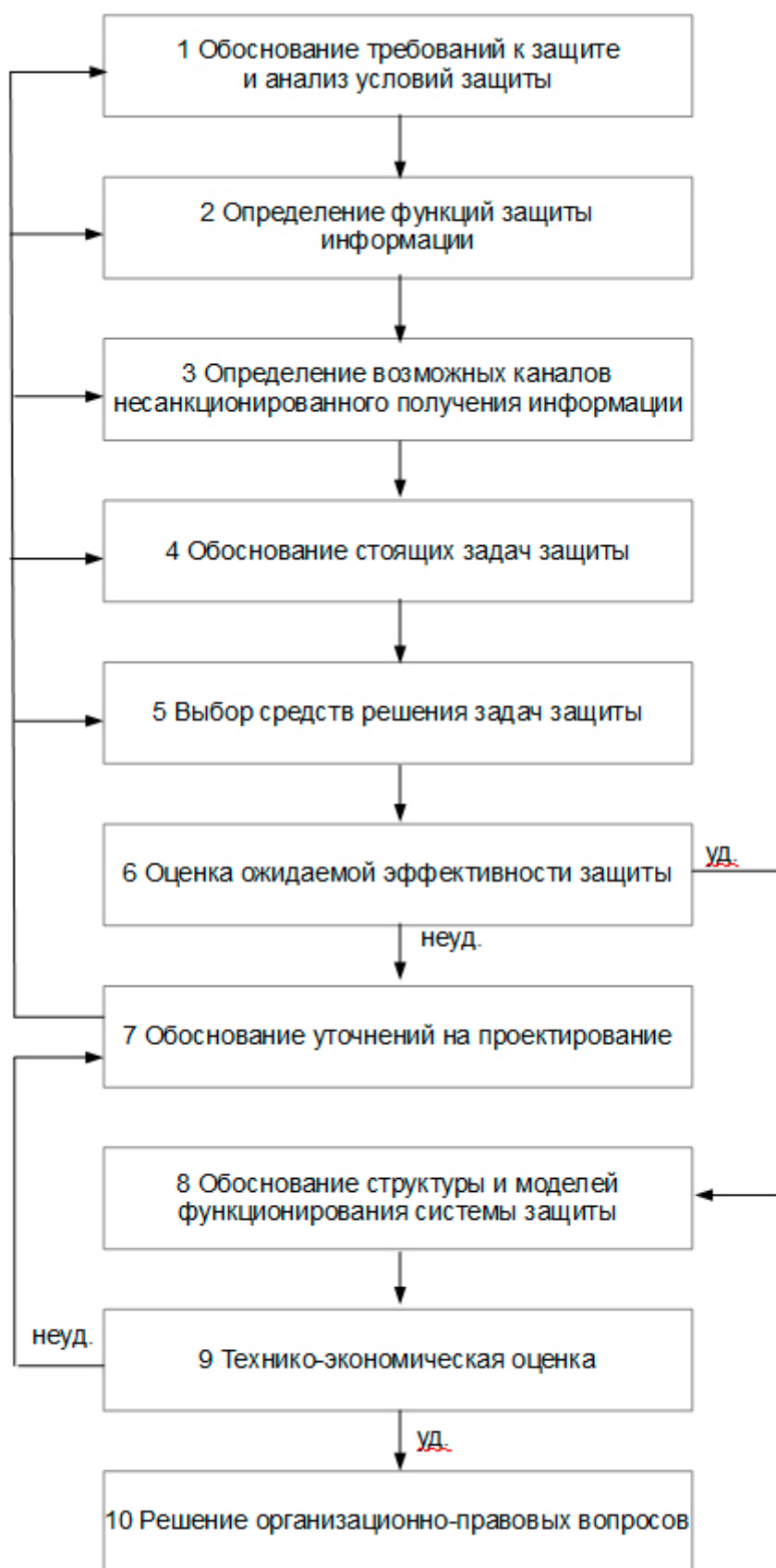


Рисунок 18 – Процесс проектирования системы защиты

Этап 1 — формирование списка условий, которые сказываются на защите информации, постановка и разъяснение выдвигаемых требований по защите информации, исследование факторов защиты информации.

Этап 2 — разработка списка функций защиты, которые должны быть осуществлены посредством проектирования и реализации системы защиты, и обоснование, почему и как именно эти функции поспособствуют сохранению необходимого уровня конфиденциальности информации.

Этап 3 — разработка списка потенциальных каналов несанкционированного получения информации, систематизация этих каналов и определение их параметров.

Этап 4 — разработка списка задач защиты, решение которых в рамках проектируемой системы защиты информации позволит не допустить проявления каналов несанкционированного получения информации, позволит достичь необходимого уровня эффективности защиты информации; систематизация этих задач.

Этап 5 — выбор используемого подхода к проектированию системы защиты (по типовому или индивидуальному проекту), подбор и обоснование средств, подходящих для решения поставленных задач защиты, в случае проектирования системы на основе типового проекта выбор такого проекта, определение и обоснование необходимых индивидуальных изменений в проекте.

Этап 6 — оценка проектируемой системы защиты по итогам выполнения предыдущих этапов (верно ли выбраны подлежащие решению задачи защиты и соответствующие им проекты и средства защиты) и эффективности ее работы, определение соответствия показанной эффективности защиты информации и требуемой.

Этап 7 — (опционально) выявление причин несоответствия показанной и требуемой эффективности защиты информации, определение способов доработки проектируемой системы защиты по итогам выполнения предыдущих этапов и определения эффективности системы и реализация доработки.

Этап 8 — обоснование структуры и моделей проектируемой системы защиты, выбор и обоснование состава системы защиты.

Этап 9 — оценка параметров надежности проектируемой системы защиты, устойчивости системы, бухгалтерская оценка проектирования и реализации системы защиты информации.

Этап 10 — разработка необходимых нормативных, правовых документов; обучение персонала, взаимодействующего с защищаемой информацией и системами документооборота и защиты, определение ответственных за защиту информации.

В процессе анализа процесса построения службы конфиденциального документооборота построены модели, отражающие различные аспекты документооборота, что позволит повысить эффективность управления конфиденциальным документооборотом и оптимизировать службу конфиденциального документооборота.

4 Действия организации по установлению режима конфиденциальности документооборота

Деятельность службы конфиденциального документооборота должна начинаться с управленческого решения и последующих организационных мероприятий. Решение должно приниматься высшим руководством и оформляться документально.

Последующим действием является определение состава документов, подлежащих отнесению к числу конфиденциальных.

Также на данном этапе необходимо создать подразделение, которое будет ответственно за действия по сохранению конфиденциальности информации (при малых объемах возможно возложение таких обязанностей на отдельного работника), и определить список допущенных к тем или иным конфиденциальным документам.

В силу стохастической природы различных факторов, влияющих на поддержание режима конфиденциальности защищаемой информации, оценка этих факторов, как правило, является задачей, которая может быть решена только с применением неформальных методов [8]. Следовательно, далее необходимо привлечение к работе специалиста, обладающего особыми знаниями и навыками (эксперта). Такой специалист способен грамотно и четко поставить задачу, определить возможные угрозы и каналы несанкционированного получения информации, оценить уязвимость документов, поставить требования к защите документов, смоделировать и построить систему защиты информации. Эксперт сможет составить и проанализировать модели, касающиеся различных факторов конфиденциального документооборота, что поспособствует более точной оценке степени эффективности и оптимизации службы конфиденциального документооборота.

После создания и начала деятельности службы конфиденциального документооборота необходимо вести постоянные поддержку и контроль этой деятельности. Также необходимой является периодическая переоценка степени эффективности работы службы конфиденциального документооборота и актуализация структуры, применяемых средств и методов работы с защищаемыми документами и их защиты.

Краткая сводка действий по построению службы конфиденциального документооборота позволит облегчить и ускорить процесс построения.

Заключение

Поставленная цель - оптимизация службы конфиденциального делопроизводства (КД) на основе анализа критериев и моделей управления в системе документооборота – достигнута.

В процессе исследования решены следующие задачи:

Произведен анализ специфики системы конфиденциального документооборота организации с целью построения ее морфологической, иерархической и информационной моделей. Итогом решения задачи являются построенные модели системы конфиденциального документооборота.

Произведен анализ процедуры оптимизации системы конфиденциального документооборота, что позволило определить подходы к управлению в системе конфиденциального документооборота.

Практическая ценность магистерской диссертации заключается в возможности применения рассмотренных моделей при управлении конфиденциальным документооборотом с учетом специфики режимной организации.

Список использованных источников и литературы

I. Источники

Федеральные законы Российской Федерации

1. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (в ред. Федерального закона от 18.04.2018 N 86-ФЗ).
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в ред. Федерального закона от 18.03.2019 N 31-ФЗ).

Законы Российской Федерации

3. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (в ред. Федерального закона от 29.07.2018 N 256-ФЗ).

Постановления Правительства Российской Федерации и РСФСР

4. Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" (в ред. Постановления Правительства РФ от 19.04.2019 N 468).
5. Постановление Правительства РСФСР от 05.12.1991 N 35 "О перечне сведений, которые не могут составлять коммерческую тайну" (в ред. Постановления Правительства РФ от 03.10.2002 N 731).

Указы Президента Российской Федерации

6. Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне" (в ред. Указа Президента РФ от 14.01.2019 N 6).

II. Литература

7. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М: Горячая линия-Телеком, 2004.

8. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник для вузов. – М: МИФИ, 1997.
9. Артемов А.В. Информационная безопасность. Курс лекций. - М.: Академия безопасности и выживания, 2014.
10. Пронькин П.В., Печерский А.В. Управление конфиденциальным документооборотом на основе анализа моделей.
11. Скабцов Н. Аудит безопасности информационных систем. – СПб: Питер, 2018.
12. Доценко С.М., Шпак В.Ф. Комплексная безопасность объекта: от теории к практике. – СПб: Издательство Полигон, 2000.
13. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – М: МГТУ им. Н. Э. Баумана, 2016.
14. Мельников Д.А. Информационная безопасность открытых систем. – М: Флинта, 2013.

В соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» приложения к выпускным квалификационным работам (ВКР) хранятся в архиве кафедры ИнОУП и не могут быть переведены в электронный вид.