МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ «ЭКОНОМИКИ И ПРЕДПРИНИМАТЕЛЬСТВА»

###### Кафедра «Информационной безопасности»

КУРСОВАЯ РАБОТА

По курсу: Теория информационной безопасности и методология защиты информации (ТИБиМЗИ)

Тема: «ТЕОРИЯ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ В АДВОКАТСКОЙ КОНТОРЕ»

Работу выполнил:

студентка гр. ЭиП-284

Баликаева Ю.А.

Работу проверил:

Астахова Л.В.

Челябинск

2008

Содержание

[1. Введение](#_Toc196040864)

[1.1. Краткая характеристика (паспорт) предприятия](#_Toc196040865)

[1.2. Обоснование актуальности проблемы защиты информации в адвокатской фирме](#_Toc196040866)

[1.3. Цели](#_Toc196040867)

[1.4. Задачи](#_Toc196040868)

[2. Заключение](#_Toc196040869)

[2.1. Концепция защиты информации в адвокатской фирме «Юстина»](#_Toc196040870)

[2.2. Оценка степени важности полученной информации](#_Toc196040872)

[3. Рекомендации](#_Toc196040873)

[4. Информационно-аналитический обзор](#_Toc196040874)

[4.1. Цели и задачи защиты информации в адвокатской конторе](#_Toc196040876)

[4.2. Объекты и предметы защиты в адвокатской конторе](#_Toc196040877)

[4.3. Факторы, влияющие на защиту информации в адвокатской конторе](#_Toc196040878)

[4.4. Угрозы защищаемой информации в адвокатской конторе](#_Toc196040879)

[4.5. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию](#_Toc196040880)

[4.6. Причины дестабилизирующего воздействия на защищаемую информацию в адвокатской конторе](#_Toc196040881)

[4.7. Каналы и методы несанкционированного доступа к защищаемой информации в адвокатской конторе](#_Toc196040882)

[4.8. Основные направления, методы и средства защиты информации в адвокатской конторе](#_Toc196040883)

[4.9. Организация комплексной системы защиты информации в адвокатской конторе](#_Toc196040884)

[5. Источники информации и оценка их надежности](#_Toc196040885)

[5.1. Список выявленной литературы](#_Toc196040886)

[5.1.1. Консультант–Плюс](#_Toc196040887)

[5.1.2. Текущие библиографические указатели и реферативные журналы](#_Toc196040888)

[5.1.3. Электронный каталог](#_Toc196040889)

[5.1.4. Информационно–поисковые системы Интернет](#_Toc196040890)

[5.1.5. Сплошной просмотр периодических изданий](#_Toc196040891)

[5.2. Список использованной литературы](#_Toc196040892)

[5.2.1. Вторичные источники](#_Toc196040893)

[5.2.2. Первичные источники](#_Toc196040894)

[5.2.3. Оценка надежности использованных источников](#_Toc196040895)

[6. Недостающая информация](#_Toc196040896)

[7. Основная и альтернативная гипотезы](#_Toc196040897)

1. Введение

1.1. Краткая характеристика (паспорт) предприятия

1. Адвокатская фирма "Юстина" (конецформыначалоформыРоссия, 119019, г.Москва, Лебяжий переулок, д. 8/4, стр.1. Teл./факс: (495) 202-45-02, 202-35-25; 203-71-49, 203-43-53; 637-59-56, 637-26-51. E-mail: law@yustina.ru)

2. Фирма основана 25 марта 1992 года в городе Москве в форме товарищества юристов для оказания высококвалифицированных юридических услуг бизнесу.

3. Основной целью создания и деятельности фирмы было и остается предоставление юридических услуг российским и иностранным юридическим и физическим лицам в сфере бизнеса. Оказываемые услуги:

**Защита интересов в суде**

Фирма осуществляет представление и защиту интересов Клиента по любой категории дел во всех видах судопроизводства (арбитражных судах, судах общей юрисдикции, третейских судах, Конституционном Суде РФ, в Европейском Суде по правам человека) и на любых его стадиях.

**Практика в области собственности**

Специалисты Адвокатской фирмы «Юстина» по заданию Клиента осуществляют проведение юридических проверок (due diligence) предприятий, а также правовое сопровождение сделок с землей и другим недвижимым имуществом (изучение правоустанавливающих документов и «правовой истории» объекта недвижимости, выработка правовой концепции его приобретения, отчуждения, оптимизация налогообложения сделки, подготовка проекта договора, привлечение при необходимости нотариуса, оценщика, страховой организации).

**Корпоративное право**

Консультирование по любым вопросам корпоративных отношений. Подготовка правовой документации и организация проведения общих собраний акционеров крупных предприятий. Приобретение предприятий. Выработка рекомендаций по сохранению и защите собственности, организация учета и хранения прав собственника. Защита собственников предприятий от недружественных поглощений. Реструктуризация бизнеса. Сопровождение процесса приватизации государственных предприятий, акционерных обществ, созданных в порядке приватизации.

**Налогообложение**

Обжалование решений налоговых органов, действий должностных лиц в вышестоящих налоговых органах и судах. Обжалование нормативных правовых актов о налогах и сборах в судах. Защита интересов налогоплательщика путем обращения в Конституционный Суд РФ, в Европейский Суд по правам человека. Составление и подача заявлений, жалоб, других документов правового характера, представление интересов налогоплательщика в этих судах. Помощь руководству организаций и физическим лицам в принятии бизнес-решений, связанных с налогообложением. Правовой анализ документов, подготовка заключений, правовых позиций, выработка концепции защиты по сложным ситуациям и спорам (судебным делам) с налоговыми органами. Консультирование по вопросам налогообложения и ведения предпринимательской деятельности.

**Медиация**

Адвокаты Фирмы имеют опыт проведения согласительных процедур и участвуют в работе Объединенной службы медиации (посредничества) при РСПП.

**Финансовое право, ценные бумаги**

Оказание юридической поддержки компаниям, осуществляющим выпуск своих ценных бумаг, подготовка необходимых юридических документов. Рекомендации в области банковского права, в том числе при осуществлении международных финансовых операций. Правовое обслуживание банков и иных финансовых учреждений.

**Антикризисные (банкротные) процедуры**

Выработка рекомендаций по наиболее оптимальной процедуре банкротства предприятия-должника (внешнее управление, конкурсное производство), разработка концепции и сценария выбранной процедуры банкротства и ее правовое сопровождение.

**Страхование**

Выработка рекомендаций при подготовке сделок с участием страховых организаций. Оказание помощи в выборе типа страхования любого объекта – от сделки до недвижимого имущества. Представительство в арбитражных судах, судах общей юрисдикции при разрешении споров, связанных со страховыми отношениями.

**Международное право**

Правовая помощь при заключении контрактов и иных сделок с участием иностранных партнеров. Оказание услуг по разрешению вопросов, связанных с международным частным правом. Подготовка и правовая поддержка инвестиционных проектов.

**Защита интеллектуальной собственности**

Консультирование по вопросам владения, пользования, применения и распоряжения результатами интеллектуальной деятельности и другими, приравненными к ним объектами. Оказание правовой помощи в области авторского, патентного права, права на товарный знак и других средств индивидуализации участников гражданского оборота. Защита интеллектуальной собственности в суде.

**Защита нематериальных благ (честь, достоинство, деловая репутация, доброе имя)**

Правовая экспертиза перспективы защиты нематериальных благ. Представление интересов заказчика в суде.

**Экологическое право**

Консультирование по вопросам ответственности за экологические преступления. Участие в разработке проектов строительства промышленных объектов. Представительство в судебных инстанциях по вопросам применения экологического права.

**Уголовное и административное право**

Участие на предварительном следствии и в суде по уголовным делам в качестве защитника, представителя потерпевших, гражданских истцов и ответчиков. Защита интересов при производстве дел об административных правонарушениях, нарушениях таможенного и налогового законодательства. Представление прав и законных интересов руководителей компаний и граждан во всех правоохранительных и иных государственных органах в экстренных случаях с выездом на место конфликтной ситуации 24 часа в сутки. конецформыначалоформыконецформыначалоформыКроме этого, адвокатская фирма «Юстина» активно участвует в обучении юристов, менеджеров и других специалистов коммерческих организаций, частных предпринимателей основам гражданского права.

4. Организационная структура:

**Президент фирмы**

**Управляющие партнёры**

**Старшие партнёры**

**Партнёры**

**Юристы**

* Президент фирмы Буробин Виктор Николаевич
* Управляющие партнеры: конецформыначалоформыБуробин Виктор Николаевич, Бородин Сергей Вячеславович, Злобин Вадим Альбертович, Плетнев Владимир Юрьевич, Старовойтов Сергей Вальтерович, Степин Сергей Владимирович.
* Старшие партнеры:конецформыначалоформы Туктамишев Сергей Борисович, Федоров Ефим Петрович, Шаманский Олег Александрович
* Партнеры: Быковский Александр Васильевич, Вакула Владимир Васильевич, Гвоздяр Владимир Иванович, Гереев Артур Юсупович, Киселев Андрей Валентинович, Кривочкин Михаил Анатольевич, Малюгин Дмитрий Семенович, Неробеев Андрей Владимирович, Петров Сергей Борисович, Тарасенко Владимир Алексеевич, Поздняков Алексей Николаевич, Покусаев Илья Борисович, Скловский Константин Ильич, Сокол Павел Яковлевич, Томашевский Юрий Анатольевич, Чеблаков Дмитрий Сергеевич, Шубин Дмитрий Александрович
* Юристы: Буробина Екатерина Викторовна, Гренова Мария Геннадьевна, Казарез Павел Александрович, Каратеев Андрей Юрьевич, Кибенко Дмитрий Валерьевич, Леонькова Виктория Анатольевна, Луковников Константин Валерьевич

5. В составе фирмы сейчас 33 адвоката, 2 секретаря, 2 бухгалтера, 1 системный администратор, 2 охранника. «Юстина» состоит из дипломированных специалистов, среди которых доктора и кандидаты юридических наук, а также адвокаты со значительным опытом работы, профессиональный уровень которых подтвержден результатами практики. Партнеры фирмы являются членами Международного союза (Содружества) адвокатов и Федерального союза адвокатов России.

6. Средний доход предприятия за последние три года составляет примерно $ 245 тыс. Но при этом следует учитывать, что юридическая фирма уплачивает налоги в размере около 40% от чистой прибыли (доходы минус расходы). Кроме того, за счет получаемого вознаграждения адвокаты отчисляют средства на общие нужды адвокатской палаты; содержание соответствующего адвокатского образования; страхование профессиональной ответственности и иные расходы, связанные с осуществлением адвокатской деятельности.

7. Характеристика информационной системы предприятия.

Программно-аппаратные средства: система правового обеспечения LIGA; пакет Microsoft Office; 1С:Предприятие, Интернет-шлюз Advanced, биометрический турникет ТБИ 1.3, уличный комплект UPC-26-220(24), система видеонаблюдения внутри помещений, антижучки Профи (Antibug Profi): детекторы жучков и видеокамер, система сигнализации.

В офисе установлено 35 персональных компьютеров (у каждого адвоката свой, т.к. каждый занимается определенной отраслью права, + компьютер секретаря + компьютер системного администратора), 5 принтеров, 2 ксерокса, 2 сканера.

1С: Предприятие – это специализированная объектно-ориентированная система управления базами данных, предназначенная для автоматизации деятельности предприятия. В "Юстине" 1С-предприятие автоматизирует учетные задачи: кадровый учет, расчет зарплаты, бухгалтерский учет.

Для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз Advanced на платформе Windows (от ИТ Энигма). В состав программного обеспечения входят прокси-сервер, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам, система построения VPN, система биллинга, система квотирования трафика.

Так как фирма хранит данные, не подлежащие разглашению (т.е. доступ к которым разрешен не всем), в фирме установлен биометрический турникет ТБИ 1.3. Человек, проходящий через турникет, автоматически сравнивается с базой данных людей, которым разрешен вход. Доступ разрешен только в случае совпадения лица человека с его трехмерной фотографией в базе данных. Изображения лиц, которым отказано в доступе, записываются для выявления попыток нарушения. Для защиты помещений – антижучки Профи (Antibug Profi): детекторы жучков и видеокамер и система видеонаблюдения внутри помещений.

На улице установлен уличный комплект UPC-26-220(24) для осуществления видеонаблюдения возле офиса. В комплект входит видеокамера, система термостабилизации, источник питания, коммутационная коробка. Расстояние передаваемого сигнала через видеолинию до 1500 м, температура окружающей среды от -40С до +50С.

1.2. Обоснование актуальности проблемы защиты информации в адвокатской фирме

|  |
| --- |
| "Чтобы получать от адвокатов необходимую помощь, люди должны доверять им такую информацию, которую они никому и ни при каких условиях не доверили бы..." |
|  |
| **"Теория адвокатуры", с.296.** |
|  |

Эффективность современного предприятия (фирмы, организации и т.п.) сегодня всё больше определяется степенью использования информационных технологий в процессе его функционирования. Происходит непрерывное увеличение как объема информации, обрабатываемой в электронном виде, так и количества различных информационных систем. В связи с этим на передний план в задаче обеспечения безопасности предприятия выходит защита информации на предприятии.

Обеспечение защиты информации в адвокатской конторе предусматривает необходимость защиты нескольких видов тайн: адвокатской, коммерческой и персональных данных. Наиболее важной представляется защита адвокатской тайны, т.к. адвокат не может оказывать результативную профессиональную помощь доверителю без полного взаимопонимания. Доверитель должен чувствовать абсолютную уверенность в том, что вопросы, обсуждаемые с адвокатом, и предоставленная им адвокату информация останутся конфиденциальными, без каких-либо требований или условий. Это одно из условий необходимости защиты информации в адвокатской конторе. Но кроме этого в адвокатской конторе, как и в любой другой фирме, существует необходимость защиты и некоторых других видов конфиденциальной информации, а именно персональных данных и коммерческой тайны. В связи с этим система обеспечения информационной безопасности в адвокатской конторе является крайне важной.

1.3. Цели

Поэтому целью руководителя адвокатской конторы является обеспечение надежной защиты информации на предприятии для его нормального функционирования. Следовательно, моя цель, как аналитика, заключается в разработке концепции защиты информации в адвокатской фирме «Юстина», которая могла бы стать основой для формирования комплексной системы защиты информации на этом предприятии, при этом соответствовала требованиям к системе безопасности адвокатской конторы и помогала избежать неоправданных расходов и возрастания вероятности угроз.

1.4. Задачи

Для достижения поставленной передо мной цели мне необходимо решить следующие задачи:

1. Определить цели и задачи защиты информации в адвокатской конторе.
2. Определить основные объекты защиты на предприятии.
3. Определить предмет защиты на предприятии.
4. Определить и охарактеризовать факторы, влияющие на защиту информации на предприятии.
5. Выявить возможные угрозы защищаемой информации в адвокатской конторе и их структуру.
6. Выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию на предприятии
7. Выявить причины дестабилизирующего воздействия на защищаемую информацию на предприятии.
8. Выявить каналы и методы несанкционированного доступа к защищаемой информации на предприятии.
9. Определить основные направления, методы и средства защиты информации на предприятии.

2. Заключение

**2.1. Концепция защиты информации в адвокатской фирме «Юстина»**

Утверждено

постановлением

Президента фирмы «Юстина»

от \_\_\_\_\_\_\_ 200\_года № \_\_

Концепция защиты информации в адвокатской фирме «Юстина»

Концепция защиты информации в адвокатской фирме «Юстина» (далее - концепция) представляет собой систему взглядов на содержание проблемы защиты информации, а также на цели, задачи, принципы и основные направления формирования и развития системы защиты информации в адвокатской фирме «Юстина» (в дальнейшем – адвокатская фирма).

Цель разработки и внедрения Концепции – определение основных положений политики адвокатской фирмы в области защиты информации и создание единой системы правовых, организационных, технических и иных мер, надежно обеспечивающих защищенность адвокатской фирмы в информационной сфере.

Концепция служит основой для разработки целевых программ по обеспечению защиты информации адвокатской фирмы и подготовки предложений по их совершенствованию.

**I. Общие положения**

Отправной точкой при разработке политики адвокатской фирмы в области защиты информации является ясное понимание роли и места системы защиты информации в деятельности адвокатской фирмы и в сфере обеспечения его безопасности в целом. Защита информации является одним из элементов общей политики адвокатской фирмы в области безопасности, которая охватывает более широкий круг вопросов, начиная от охраны материальных ценностей адвокатской фирмы и защиты его персонала до использования криптографических средств защиты информации и предотвращения возможной утечки информации за счет побочных электромагнитных излучений. Элементы общей системы безопасности адвокатской фирмы должны быть взаимосвязаны и согласованы.

Защита информации в адвокатской фирме основывается на ряде основополагающих принципов:

* законности – соблюдение законодательства Российской Федерации по защите информации и законных интересов всех участников информационного обмена;
* приоритетности - предварительное категорирование (ранжирование) информационных ресурсов адвокатской фирмы по степени важности в виде перечней сведений, подлежащих защите, и оценка реальных угроз информационной безопасности;
* комплексного подхода – согласование мероприятий, проводимых в области защиты информации адвокатской фирмы, со всем комплексом мероприятий по физической и технической безопасности адвокатской фирмы, а также противодействие всем возможным угрозам информационной безопасности адвокатской фирмы; оптимальное сочетание проводимых мероприятий;
* единой политики - координация деятельности различных подразделений адвокатской фирмы по созданию и поддержанию необходимого уровня защиты информации в адвокатской фирме, определение обязанностей и ответственности подразделений (их руководителей);
* целесообразности - затраты на обеспечение защиты информации не должны превышать потери, которые может понести адвокатская фирма при реализации угроз.

Политика в области защиты информации в адвокатской фирме включает следующие основные этапы:

* определение информации, подлежащей защите (объекты защиты);
* определение возможных негативных воздействий на защищаемую информацию (угрозы) и способов реализации этих угроз;
* определение ценности защищаемой информации (риски) и ее ранжирование;
* разработка комплекса мер по поддержанию необходимого уровня защиты информации;
* распределение полномочий и ответственности за обеспечение установленного режима безопасности.

Законодательной основой настоящей Концепции являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы Федеральной службы по техническому и экспортному контролю (ФСТЭК), а также нормативно-методические материалы и организационно-распорядительные документы организации, отражающие вопросы обеспечения информационной безопасности предприятия.

**II. Цели и задачи защиты информации в адвокатской конторе**

Целями защиты информации в адвокатской фирме являются:

* предотвращение утечки, хищения, утраты, искажения, подделки конфиденциальной информации (коммерческой и адвокатской тайны);
* предотвращение угроз безопасности личности и адвокатской конторы;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации в адвокатской фирме относятся:

1. Обеспечение деятельности адвокатской фирмы режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необхо­димой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать адвокатской конторе преимущества перед конкурентами и оправдывать затраты средств на защиту информации.
2. Гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации.
3. Отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности адвокатской фирмы.
4. Документирование процесса защиты информации с тем, чтобы в слу­чае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что адвокатская фирма принимала необходимые меры к защите этих сведений.
5. Организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

**III. Основные объекты защиты**

Основными объектами защиты в адвокатской фирме являются:

1. Информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством к адвокатской тайне, коммерческой тайне и иной конфиденциальной информации (в дальнейшем - защищаемой информации);
2. Средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
3. Программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы адвокатской фирмы, с помощью которых производится обработка защищаемой информации;
4. Помещения, предназначенные для ведения закрытых переговоров и совещаний;
5. Помещения, в которых расположены средства обработки защищаемой информации;
6. Технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может находиться в адвокатской фирме:

* + на бумажных носителях;
  + в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
  + передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
  + присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
  + записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны и др.).

**IV. Угрозы защищаемой информации и возможные источники их возникновения**

Под угрозами защищаемой информации понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

1. Утрата сведений, составляющих адвокатскую тайну, коммерческую тайну адвокатской фирмы и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;
2. Утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;
3. Недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств.

Источниками (каналами) возникновения угроз могут являться:

* + стихийные бедствия (пожары, наводнения и т.п.);
  + технические аварии (внезапное отключение электропитания, протечки и т.п.);
  + несанкционированное получение идентификаторов пользователей и их паролей, паролей доступа к общим ресурсам;
  + несанкционированная передача защищаемой информации из внутренней (локальной) сети в глобальную сеть Internet;
  + умышленное или неумышленное разглашение защищаемой информации;
  + хищение носителей информации или несанкционированное копирование информации;
  + посылка в ЛВС пакетов, нарушающих нормальную работу сети;
  + внедрение программ-троянов, резидентных программ, обеспечивающих получение полного контроля над компьютером;
  + внедрение деструктивных программ – вирусов, сетевых червей и пр.;
  + проникновение зловредных программ через Internet, электронную почту, гибкие диски, CD-диски;
  + получение информации о топологии сети, принципах ее функционирования, характеристической информации сети или участка сети;
  + хищение, физический вывод из строя технических средств;
  + прослушивание сетевого трафика (с целью получения информации о сетевых ресурсах, хешированных паролях, идентификаторах пользователей и пр.) с использованием легальных рабочих станций;
  + прослушивание сетевого трафика с использованием нелегальных компьютеров, подключенных к ЛВС физически (локально) или удаленно;
  + внедрение технических и программных средств скрытного съема информации с рабочих станций, средств связи, из помещений адвокатской фирмы, в которых обрабатывается защищаемая информация;
  + использование специальных методов и технических средств (побочные излучения, наводки по цепям питания, электронные закладки, дистанционное скрытое видеонаблюдение или фотографирование, применение подслушивающих устройств, перехват электромагнитных излучений и наводок и т.п.);
  + использование для доступа к информации так называемых "люков", "дыр" и "лазеек" и других возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения (операционных систем, систем управления базами данных и др.) и неоднозначностями языков программирования, применяемых в автоматизированных системах обработки данных;
  + незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (перехват модемной и факсимильной связи);
  + умышленное изменение используемого программного обеспечения для несанкционированного сбора защищаемой информации.

**V. Меры по обеспечению защиты информации в адвокатской конторе**

Основными мерами по обеспечению защиты информации в адвокатской фирме являются:

* административно-правовые и организационные;
* технические, основанные на использовании аппаратно-программных и специальных средств;
* режимные.

1. Административно-правовые и организационные меры:

1.1. Определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и коммуникационных систем, установление их ответственности за соблюдение нормативных правовых актов адвокатской фирмы в этой сфере;

1.2. Разработка перечня возможных нарушений информационной безопасности и локальных нормативных актов, определяющих порядок защиты интересов адвокатской фирмы в сфере защиты информации;

1.3. Оценка эффективности действующих в адвокатской фирме локальных нормативных актов по обеспечению защиты информации;

1.4. Включение в должностные инструкции сотрудников обязанностей и ответственности в области обеспечения защиты информации;

1.5. Совершенствование системы обучения сотрудников адвокатской фирмы по вопросам защиты информации в адвокатской фирме;

1.6. Подготовка и повышение квалификации специалистов в области защиты информации;

1.7. Аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих адвокатскую тайну и коммерческую тайну адвокатской фирмы;

1.8. Разработка правил (регламентов, порядков) эксплуатации технических и программных средств с указанием действий в случаях нарушения режима безопасности (подозрений на нарушение);

1.9. Оперативное реагирование (внедрение) на появление новых разработок в области информационных технологий;

1.10. Совершенствование нормативно-правовой базы, регламентирующей порядок обращения и работы в адвокатской фирме с конфиденциальной информацией и сведениями, составляющими адвокатскую тайну и коммерческую тайну адвокатской фирмы;

1.11. Совершенствование нормативно-правовой базы, регламентирующие порядок обмена конфиденциальной информацией между адвокатской фирмой и сторонними организациями;

1.12. Обеспечение принципа разграничения доступа: информация должна быть доступна только тем, кому она предназначена и разрешена;

1.13. Предоставление сотрудникам минимально достаточных прав по доступу к информации, необходимых для выполнения ими своих функциональных обязанностей;

1.14. Использование E-mail только в служебных целях;

1.15. Пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации.

2. Технические меры:

2.1. Использование лицензионного программного обеспечения;

2.2. Использование сертифицированных средств защиты информации для обработки, хранения и передачи конфиденциальной информации;

2.3. Соблюдение положений информационно-технологической политики адвокатской фирмы;

2.4. Обеспечение безотказной работы аппаратных средств;

2.5. Проведение комплексной антивирусной защиты;

2.6. Проведение аудита (контроль за деятельностью пользователей – успешный или неуспешный доступ к сетевым ресурсам, вход-выход в систему и пр.);

2.7. Проведение контроля трафика сети на отдельных ее участках (сегментах);

2.8. Проведение контроля состояния программного и информационного обеспечения компьютеров (состава и целостности программного обеспечения, корректности настроек и т.д.) и маршрутизаторов (маршрутных таблиц, фильтров, паролей);

2.9. Проведение эффективной парольной защиты;

2.10. Обеспечение резервного копирования;

2.11. Проведение контроля за несанкционированными физическими подключениями к автоматизированным системам;

2.12. Внедрение в ЛВС современной системы обнаружения вторжений;

2.13. Использование для подключения к почтовому серверу защищенного соединения с целью шифрования паролей;

2.14. Запрет несанкционированного доступа к ЛВС через удаленное соединение.

3. Режимные меры:

3.1. Хранение информации ограниченного распространения, составляющей адвокатскую тайну и коммерческую тайну адвокатской фирмы, разрешено только на специально подготовленной вычислительной технике, расположенной в специальных (выделенных) помещениях с ограниченным доступом;

3.2. Круг лиц из числа сотрудников адвокатской фирмы, имеющих право работы со сведениями, составляющими адвокатскую тайну и коммерческую тайну адвокатской фирмы, должен быть ограничен;

3.3. Установление специальных режимных мер, применяемых в целях защиты информации в адвокатской фирме (ведение специального делопроизводства, выделение специально оборудованных помещений, поддержание необходимого уровня пропускного и внутриобъектового режима, подбор кадров, проведение комплексных защитно-поисковых мероприятий и т.п.);

3.4. Аттестация объектов информатизации на соответствие требованиям обеспечения защиты информации при проведении работ, связанных с использованием конфиденциальных сведений, составляющих коммерческую тайну адвокатской фирмы;

3.5. Совершенствование пропускного и внутриобъектового режима в адвокатской фирме и повышение ответственности сотрудников за выполнение требований установленных режимов;

3.6. Разграничение доступа и контроль за доступом в выделенные помещения;

3.7. Создание эффективной системы контроля за выполнением сотрудниками адвокатской фирмы требований локальных нормативных актов по обеспечению защиты информации адвокатской фирмы;

3.8. Совершенствование нормативно-правовой базы, регламентирующей порядок обращения и работы в адвокатской фирме с конфиденциальной информацией и сведениями, составляющими адвокатскую тайну и коммерческую тайну адвокатской фирмы.

**VI. Организация системы обеспечения защиты информации в адвокатской конторе**

Система обеспечения информационной безопасности адвокатской фирмы строится на основе разграничения полномочий управленческих и функциональных подразделений адвокатской фирмы в данной сфере.

Основными элементами организационной системы обеспечения информационной безопасности адвокатской фирмы являются: Президент адвокатской фирмы, управляющие партнеры и служба защиты информации.

Президент адвокатской фирмы определяет приоритетные направления деятельности в области обеспечения защиты информации в адвокатской фирме и меры по реализации Концепции защиты информации, утверждает списки сведений, подлежащих защите.

Управляющие партнеры с учетом определенных Президентом адвокатской фирмы приоритетных направлений в области обеспечения защиты информации предусматривают выделение средств, необходимых для реализации программ и координируют деятельность подразделений с учетом требований защиты информации в адвокатской конторе.

Служба защиты информации во взаимодействии с другими структурными подразделениями адвокатской фирмы обеспечивает выполнение административно-правовых, организационных и режимных мер по обеспечению защиты информации, координирует деятельность подразделений адвокатской фирмы в области информационной безопасности, проводит работу по выявлению и оценке угроз, разрабатывает предложения по их предотвращению, контролирует деятельность подразделений по обеспечению информационной безопасности.

Руководители структурных подразделений адвокатской фирмы обеспечивают выполнение всеми подчиненными сотрудниками установленных требований в области обеспечения защиты информации.

Обеспечение защиты информации в адвокатской фирме непосредственно на рабочих местах возлагается на сотрудников адвокатской фирмы.

**VII. Ответственность за нарушение требований защиты информации в адвокатской фирме**

По степени опасности нарушения, связанные с несоблюдением локальных нормативных актов по обеспечению защиты информации в адвокатской фирме делятся на две группы:

1. Нарушения, повлекшие за собой наступление указанных выше нежелательных для адвокатской фирмы последствий (утечку или уничтожение информации);

2. Нарушения, в результате которых созданы предпосылки, способные привести к нежелательным для адвокатской фирмы последствиям (угроза уничтожения или утраты информации).

Нарушение требований локальных нормативных актов адвокатской фирмы по обеспечению защиты информации в адвокатской фирме является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами и договорами, заключенными между адвокатской фирмой и сотрудниками.

Степень ответственности за нарушение требований локальных нормативных актов в области защиты информации в адвокатской фирме определяется исходя из размера ущерба, причиненного адвокатской фирме.

Руководители структурных подразделений адвокатской фирмы несут персональную ответственность за обеспечение защиты информации в возглавляемых ими подразделениях.

**VIII. Ожидаемые результаты реализации концепции защиты информации в адвокатской фирме**

Реализация настоящей Концепции позволит:

* улучшить организационную структуру системы защиты информации в адвокатской фирме, ее кадровое обеспечение;
* повысить оснащенность адвокатской фирмы высокоэффективными средствами защиты информации, а также средствами контроля ее эффективности;
* улучшить обеспеченность адвокатской фирмы документами в области защиты информации;

В результате будет создана система, соответствующая задачам обеспечения защиты информации в адвокатской конторе, и адекватно реагирующая на угрозы защищаемой информации в процессе деятельности адвокатской конторы.

**2.2. Оценка степени важности полученной информации**

Так как система организации защиты конфиденциальной информации включает в себя комплекс **заранее** разработанных на определенный срок мер, охватывающих совокупность всех видов деятельности, направленных на совершенствование обеспечения сохранности информации с учетом изменений внешних и внутренних условий и предписывающих конкретным лицам или подразделений определенный порядок действий, то **крайне важным** представляется ознакомление с полученной информацией.

Например, знание объекта и предмета защиты в адвокатской конторе позволит определиться с целями и задачами разрабатываемой системы защиты информации на предприятии, знание возможностей методов и средств защи­ты информации позволит активно и комплексно применить их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты конфиденци­альной информации. Аналитические исследования, моделирование вероятных угроз позволят наметить при необходимости дополнительные меры защиты. При этом характеристика предприятия поможет оценить вероятность выполнения мер защиты, наличие методического материала, материального обеспечения, готовность службы защиты информации и персонала выполнить все необходимые меры. Знание недостатков в обеспечении сохранности конфиденциальной информации поможет спланировать дальнейшие мероприятия по обеспечению защиты информации.

Таким образом, я могу сделать вывод, что полученная информация не только поможет определиться с целями и задачами создания службы защиты информации, но и усовершенствовать уже имеющуюся службу защиты информации и спланировать дальнейшие мероприятия по защите конфиденциальной и общедоступной информации в адвокатской конторе «Юстина».

3. Рекомендации

I. Для обеспечения работоспособности разработанной системы защиты информации необходимо создать специальный отдел в составе организации, занимающийся данными вопросами – Службу защиты информации (СлЗИ).

1. Руководитель предприятия своим приказом должен назначить начальника службы защиты информации во главе группы компетентных сотрудников, которые высказывают свои предложения по объему, уровню и способам обеспечения сохранности конфиденциальной информации.

2. Руководитель группы, обладая соответствующей квалификацией в этой области, с привлечением отдельных специалистов должен сформировать предварительный список сведений, которые в дальнейшем войдут в «Перечень сведений, составляющих конфиденциальную информацию предприятия».

3. Руководитель группы на основе этого списка должен определить и представить на согласование необходимые к защите объекты (оборудование для обработки и обращения информации, программное обеспечение, коммуникации для передачи конфиденциальных данных, носители информации, персонал, допущенный к работе с использованием различных тайн).

4. Необходимы анализ существующих мер защиты соответствующих объектов, определение степени их недостаточности, неэффективности, физического и морального износа.

5. Необходимо изучение зафиксированных случаев попыток несанкционированного доступа к охраняемым информационным ресурсам и разглашения информации.

6. На основе опыта предприятия, а также используя метод моделирования ситуаций, группа специалистов должна выявить возможные пути несанкционированных действий по уничтожению информации, ее копированию, модификации, искажению, использованию и т. п. Угрозы ранжируются по степени значимости и классифицируются по видам воздействия.

7. На основе собранных данных необходимо оценить возможный ущерб предприятия от каждого вида угроз, который становится определяющим фактором для категорирования сведений в «Перечне» по степени важности, например — для служебного пользования, конфиденциально, строго конфиденциально.

8. Необходимо определить сферы обращения каждого вида конфиденциальной информации: по носителям, по территории распространения, по допущенным пользователям. Для решения этой задачи группа привлекает руководителей структурных подразделений и изучает их пожелания.

9. Группе необходимо подготовить введение указанных мер защиты.

Начальник СлЗИ является новой штатной единицей. На эту должность необходимо взять профессионала и специалиста в области защиты информации, а также хорошо знающего юридическую сторону этой проблемы, имеющего опыт руководства и координации работы подобных служб. Требования – высшее профессиональное образование и стаж работы в области защиты информации не менее 5 лет, хорошее знание законодательных актов в этой области, принципов планирования защиты.

В адвокатской фирме «Юстина» целесообразно организовать Службу защиты информации в следующем составе:

* + Руководитель СлЗИ;
  + сотрудник, занимающийся программно-аппаратной защитой;
  + сотрудник, занимающийся инженерно-технической защитой.

Функции конфиденциального делопроизводства возложить на уже имеющихся сотрудников, занимающихся в данное время созданием и обработкой документов, содержащих конфиденциальную информацию (секретаря).

Для работы СлЗИ необходимо подготовить ряд нормативных документов:

* + - Положение о СлЗИ;
    - Инструкцию по безопасности конфиденциальной информации.
    - Перечень сведений, составляющих конфиденциальную информацию.
    - Инструкцию по работе с конфиденциальной информацией.
    - Должностные инструкции сотрудников СлЗИ.
    - Инструкцию по обеспечению пропускного режима в компании.
    - Памятку работнику (служащему) о сохранении конфиденциальной информации.

II. Внести дополнения в Устав предприятия для документационного обеспечения защиты: «Предприятие имеет право самостоятельно устанавливать объем сведений, составляющих коммерческую и иную охраняемую законом тайну и порядок ее защиты. Фирма имеет право в целях защиты экономического суверенитета требовать от персонала, партнеров, контрагентов и иных физических и юридических лиц, учреждений и организаций обеспечения сохранности конфиденциальных сведений предприятия на основании договоров, контрактов и других документов». А также необходимо проставить грифы конфиденциальности:

* Самый низкий гриф конфиденциальности «ДСП» проставить на телефонные справочники, в которых указываются отдельные данные о кадровом составе или партнерах; журналы регистрации, документы, регламентирующие деятельность, служебную переписку (заявления, распоряжения, приказы, докладные и т.д.).
* Гриф “КОНФИДЕНЦИАЛЬНО” проставить на информации об отдельных аспектах деловых сделок за короткий промежуток времени; развернутые сведения о персонале компании (персональные данные работников); текущие документы, отражающие финансовую деятельность (коммерческая тайна); документы, содержащие данные о клиентах, не предоставляемые третьим лицам (сведения, составляющие адвокатскую тайну).
* Гриф “СТРОГО КОНФИДЕНЦИАЛЬНО” присвоить документам, содержащим данные о деловых сделках с партнерами или клиентами фирмы, об итогах деятельности за продолжительный период времени; документам, содержащим важнейшие аспекты коммерческой деятельности компании, стратегии деятельности, документам, содержащим детальную информацию о финансовом положении.

III. Необходимо дополнить технические средства защиты информации, а именно установить средства, защищающие от прослушивания телефонных переговоров, т.к. бывают случаи, когда клиенту нужна экстренная юридическая помощь или он находится в таком нервном состоянии, что может наговорить по телефону такие вещи, которые конкуренты могут использовать против него. К этому адвокатская фирма «Юстина» не готова. Поэтому некоторые юридические дела проигрываются из-за того, что противник имеет более современные средства перехвата необходимой информации для принятия соответствующих мер. Особенно это касается сложных и запутанных уголовных дел, а также связанных с собственностью большой стоимости.

IV. Периодически проводить тренинги с сотрудниками, на которых им объясняется важность защиты конфиденциальной информации в адвокатской фирме. А также ознакомить всех сотрудников с главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации».

V. Зафиксировать предложенные рекомендации, разработав пакет документов, включающий в себя:

* + - * Положение о конфиденциальной информации предприятия;
      * Инструкцию по защите конфиденциальной информации в информационной системе предприятия;
      * Предложения по внесению изменений в Устав предприятия;
      * Предложения по внесению изменений в трудовой договор, контракт с руководителем и коллективный договор;
      * Соглашение о неразглашении конфиденциальной информации предприятия с сотрудником;
      * Обязательство сотрудника о неразглашении конфиденциальной информации предприятия при увольнении;
      * Предложения о внесении изменений в Правила внутреннего распорядка предприятия (в части регламентации мер физической защиты информации и вопросов режима);
      * Предложения о внесении изменений в должностное (штатное) расписание предприятия (штат Службы защиты информации);
      * Предложения о внесении дополнений в должностные инструкции всему персоналу;
      * Ведомость ознакомления сотрудников предприятия с Положением о конфиденциальной информации и Инструкцией по защите конфиденциальной информации в ИС предприятия;
      * План проведения занятий с персоналом по сохранению и неразглашению конфиденциальной информации;
      * Предложения о внесении изменений в структуру интервью при приеме на работу (уточнение обязательств информационного характера с последних мест работы);
      * Предложения о внесении дополнений в стандартный договор с контрагентами.

4. Информационно-аналитический обзор

План

[4.1. Цели и задачи защиты информации в адвокатской конторе](#_Toc195975527)

[4.2. Объекты и предметы защиты в адвокатской конторе](#_Toc195975528)

[4.3. Факторы, влияющие на защиту информации в адвокатской конторе](#_Toc195975529)

[4.4. Угрозы защищаемой информации в адвокатской конторе](#_Toc195975530)

[4.5. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию](#_Toc195975531)

[4.6. Причины дестабилизирующего воздействия на защищаемую информацию в адвокатской конторе](#_Toc195975532)

[4.7. Каналы и методы несанкционированного доступа к защищаемой информации в адвокатской конторе](#_Toc195975533)

[4.8. Основные направления, методы и средства защиты информации в адвокатской конторе](#_Toc195975534)

[4.9. Организация комплексной системы защиты информации в адвокатской конторе](#_Toc195975535)

4.1. Цели и задачи защиты информации в адвокатской конторе

Целями защиты информации предприятия являются:

* предотвращение утечки, хищения, утраты, искажения, подделки конфиденциальной информации (коммерческой и адвокатской тайны);
* предотвращение угроз безопасности личности и предприятия;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение, конфиденциальности документированной информации в соответствии с законодательством [22].

К задачам защиты информации на предприятии относятся:

1. Обеспечение управленческой, фи­нансовой и маркетинговой деятельности предприятия режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необхо­димой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать предприятию преимущества перед конкурентами и оправдывать затраты средств на защиту информации.
2. Гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации.
3. Отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности компании.
4. Документирование процесса защиты информации, особенно сведений, составляющих коммерческую тайну, с тем, чтобы в слу­чае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предпри­ятие принимало необходимые меры к защите этих сведений.
5. Организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации [4, с.313].

4.2. Объекты и предметы защиты в адвокатской конторе

Основными объектами защиты в адвокатской конторе являются:

* + персонал (так как эти лица допущены к работе с охраняемой законом информацией (адвокатская и коммерческая тайны, персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается).
  + объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров с клиентами;
  + информация ограниченного доступа:
  + ***адвокатская тайна*** (факт обращения к адвокату, включая имена и названия доверителей; все персональные данные клиентов; все доказательства и документы, собранные адвокатом входе подготовки к делу; сведения, полученные адвокатом от доверителей; информация о доверителе, ставшая известной адвокату в процессе оказания юридической помощи; содержание правовых советов, данных непосредственно доверителю или ему предназначенных; все адвокатское производство по делу; условия соглашения об оказании юридической помощи, включая денежные расчеты между адвокатом и доверителем; любые другие сведения, связанные с оказанием адвокатом юридической помощи) [9, с. 30],
  + ***коммерческая тайна*** (сведения о применяемых оригинальных методах управления фирмой, сведения о подготовке, принятии и исполнении отдельных решений руководства фирмы по коммерческим, организационным и др. вопросам; сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации (управляющих партнеров); сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредитов организации (пассивы и активы); сведения о рыночной стратегии фирмы, об эффективности коммерческой деятельности фирмы; обобщенные сведения клиентах и других партнерах, состоящих в деловых отношениях с организацией; обобщенные сведения о внутренних и зарубежных фирм как потенциальных конкурентах, оценка качества деловых отношений с конкурирующими предприятиями; сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с клиентами; сведения о методах расчета, структуре, уровне реальных цен на услуги и размеры скидок; сведения о порядке и состоянии организации защиты коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме[19]),
  + ***персональные данные работников*** (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника[20]).
  + защищаемая от утраты общедоступная информация:
    - документированная информация, регламентирующая статус предприятия, права, обязанности и ответственность его работников (Устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников)
    - информация, которая может служить доказательным источником в случае возникновения конфликтных ситуаций (расписки)
  + материальные носители охраняемой законом информации (личные дела работников, личные дела клиентов, электронные базы данных работников и клиентов, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов, составляющих коммерческую тайну)
  + средства защиты информации (Интернет-шлюз Advanced, биометрический турникет ТБИ 1.3, уличный комплект UPC-26-220(24), система сигнализации, антижучки и др.)
  + технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (личные дела бывших клиентов)

**Предметом защиты информации** в адвокатской конторе являются носители информации, на которых зафиксированы, отображены защищаемые сведения [4, с.311]:

* Личные дела клиентов в бумажном и электронном (база данных клиентов) виде;
* Личные дела работников в бумажном и электронном (база данных работников) виде;
* Приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы, составляющие коммерческую тайну, в бумажном и электронном виде.

4.3. Факторы, влияющие на защиту информации в адвокатской конторе

Внешние факторы:

* деятельность конкурентных юридических фирм, направленная против интересов фирмы «Юстина»;
* деятельность правоохранительных органов власти, направленная на удовлетворение собственных интересов и не учитывающая при этом интересы адвокатской фирмы (обыски адвокатов без предварительного получения решения суда; изъятие в ходе обысков документов, содержащих конфиденциальную информацию; формальный подход судей при вынесении решений о проведении обыска у адвоката; обыск в помещениях занимаемых адвокатом в отсутствие адвоката; незаконный досмотр адвокатского производства адвокатов как один из способов незаконного доступа к адвокатской тайне) [8, 14];
* недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика (например, несостыковка пунктов Уголовно-процессуального кодекса Российской Федерации и закона «Об адвокатской деятельности и адвокатуре в Российской Федерации», закон **«О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», предписывающий адвокатам выполнять роль секретных сотрудников правоохранительных органов**) [8, 14, 21].

Внутренние факторы:

* недостаточное внимание к обеспечению защиты информации со стороны руководства (в адвокатской фирме нет отдельной службы защиты информации);
* довольно равнодушное отношение к обеспечению защиты информации со стороны сотрудников фирмы (записывание паролей на бумаге, использование одинаковых паролей и т.д.);
* недостаточное финансирование мероприятий по обеспечению информационной безопасности предприятия;
* недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности в адвокатской фирме (в данный момент в штате фирмы «Юстина» нет ни одного специалиста по защите информации).

4.4. Угрозы защищаемой информации в адвокатской конторе

Внешние угрозы:

* Конкуренты (адвокатские фирмы, являющиеся конкурентами «Юстине»);
* Административные органы (органы государственной власти);
* Преступники, хакеры.

Внутренние угрозы:

* Персонал;
* Администрация предприятия.

Классификация угроз:

1. По объектам:
   1. Персонал;
   2. Материальные ценности;
   3. Финансовые ценности.
2. По ущербу:
   1. Материальный;
   2. Моральный.
3. По величине ущерба:
   1. Предельный (полное разорение);
   2. Значительный (некоторая валового дохода);
   3. Незначительный (потеря прибыли).
4. По отношению к объекту:
   1. Внутренние;
   2. Внешние.
5. По вероятности возникновения:
   1. Весьма вероятные;
   2. Вероятные;
   3. Маловероятные.
6. По характеру воздействия:
   1. Активные;
   2. Пассивные.
7. По причине проявления:
   1. Стихийные;
   2. Преднамеренные.

4.5. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

К источникам дестабилизирующего воздей­ствия на информацию относятся [4, с.203]:

1. люди;
2. технические средства отображения (фикса­ции), хранения, обработки, воспроизведения, пе­редачи информации, средства связи и системы обеспечения их функционирования;
3. природные явления.

Самым распространенным, многообразным и опасным источником дестабилизирующего воздей­ствия на защищаемую информацию являются люди. К ним относятся:

* сотрудники данной адвокатской фирмы;
* лица, не работающие в фирме, но име­ющие доступ к защищаемой информации предпри­ятия в силу служебного положения (из контролирующих органов государственной и муниципальной власти и др.);
* сотрудники конкурирующих отечественных и зарубежных фирм;
* лица из криминальных структур, хакеры.

Эти категории людей подразделяются на две группы:

* имеющие доступ к носителям данной защища­емой информации, техническим средствам ее ото­бражения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функциони­рования и
* не имеющие такового.

Самым многообразным этот источник являет­ся потому, что ему, по сравнению с другими ис­точниками, присуще значительно большее количе­ство видов и способов дестабилизирующего воз­действия на информацию [4, с. 204].

Самым опасным этот источник является пото­му, что он самый массовый; воздействие с его стороны носит регулярный характер; его воздействие может быть не только непреднамеренным но и преднамеренным и ока­зываемое им воздействие может привести ко всем формам проявления уязвимости информации (со стороны остальных источников – к отдельным фор­мам).

К техническим средствам отображения, хране­ния, обработки, воспроизведения, передачи информации и средствам связи в адвокатской конторе относятся электронно-вычислительная техника (персональные компьютеры); копировально-множительная техника (ксероксы, принтеры, сканеры); средства видео- и звукозаписывающей и вос­производящей техники (видеокамеры, диктофоны) и средства телефонной, телеграфной, факси­мильной, громкоговорящей передачи информации.

Системы обеспечения функционирования технических средств отображения, хранения, обра­ботки, воспроизведения и передачи информации это системы электро­снабжения, водоснабжения, теплоснабжения, кон­диционирования и вспомогательные электрические и радиоэлектрон­ные средства (электрические часы, бытовые магнитофоны и др.).

Природные явления включа­ют стихийные бедствия и атмос­ферные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям[4, с. 207]**.**

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

1. Непосредственное воздействие на носители за­щищаемой информации.

2. Несанкционированное распространение конфиденциальной информации.

3. Вывод из строя технических средств отобра­жения, хранения, обработки, воспроизведения, пе­редачи информации и средств связи.

4. Нарушение режима работы перечисленных средств и технологии обработки информации.

5. Вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

* физическое разрушение носителя (поломка, разрыв и др.);
* создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т.д.);
* удаление информации с носителей (замазыва­ние, стирание, обесцвечивание и др.);
* создание искусственных магнитных полей для размагничивания носителей;
* внесение фальсифицированной информации в носители;
* непреднамеренное оставление их в нео­храняемой зоне, чаще всего в общественном транс­порте, магазине, на рынке, что приводит к потере носителей[4].

Несанкционированное распространение конфиденциальной информации может осуществ­ляться путем*:*

* словесной передачи (сообщения) информа­ции;
* передачи копий (снимков) носителей инфор­мации;
* показа носителей информации;
* ввода информации в вычислительные сети;
* опубликования информации в открытой пе­чати;
* использования информации в открытых пуб­личных выступлениях, в т.ч. по радио, телевидению;
* потеря носителей информации.

К способам вывода из строя технических средств отображения, хранения, обработки, вос­произведения, передачи информации и средств связи и систем обеспечения их функционирования, при­водящим к уничтожению, искажению и блокированию, можно отнести:

* неправильный монтаж средств;
* поломку (разрушение) средств, в т.ч. разрыв (повреждение) кабельных линий связей;
* создание аварийных ситуаций для техничес­ких средств (поджог, искусственное затопление, взрыв и др.);
* отключение средств от сетей питания;
* вывод из строя или нарушение режима рабо­ты систем обеспечения функционирования средств;
* вмонтирование в ЭВМ разрушающих радио- и программных закладок;
* нарушение правил эксплуатации систем.

Способами нарушения режима работы тех­нических средств отображения, хранения, обра­ботки, воспроизведения, передача информации, средств связи и технологии обработки информа­ции, приводящими к уничтожению, искажению и бло­кированию информации, могут быть:

* повреждение отдельных элементов средств;
* нарушение правил эксплуатации средств;
* внесение изменений в порядок обработки ин­формации;

- заражение программ обработки информации вредоносными программами;

* выдача неправильных программных команд;
* превышение расчетного числа запросов;
* создание помех в радио эфире с помощью до­полнительного звукового или шумового фона, из­менения (наложения) частот передачи информа­ции;

- передача ложных сигналов – подключение подавляющих фильтров в инфор­мационные цепи, цепи питания и заземления;

* нарушение (изменение) режима работы сис­тем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизве­дения, передачи информации и средств связи и систем обеспечения их функционирования относятся выход средств из строя; сбои в работе средств и создание электромагнитных излучений. Это приводит к уничтожению, искаже­нию, блокированию, разглашению (соединение с номером телефона не того або­нента, который набирается, или слышимость раз­говора других лиц из-за неисправности в цепях ком­мутации телефонной станции). Электромагнитные излучения, в том числе побочные, образующиеся в процессе эксплуатации средств, приводят к хищению информации.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясение, навод­нение, ураган (смерч) и шторм. К атмосферным явлениям (видам воздействия) относят грозу, дождь, снег, перепады температуры и влажности воздуха, магнитные бури. Они приводят к потере, унич­тожению, искажению, блокированию и хищению.

Способами воздействия со стороны и стихий­ных бедствий и атмосферных явлений могут быть:

- разрушение (поломка);

- затопление;

- сожжение но­сителей информации, средств отображения, хра­нения, обработки, воспроизведения, передачи ин­формации и кабельных средств связи, систем обес­печения функционирования этих средств;

- наруше­ние режима работы средств и систем, а также тех­нологии обработки информации.

4.6. Причины дестабилизирующего воздействия на защищаемую информацию в адвокатской конторе

К причинам, вызывающим преднамеренное дес­табилизирующее воздействие, следует отнести [4, с. 213]:

* стремление получить материальную выгоду (подзаработать);
* стремление нанести вред (отомстить) руковод­ству или коллеге по работе;
* стремление оказать бескорыстную услугу при­ятелю из конкурирующей фирмы;
* стремление продвинуться по службе;
* стремление обезопасить себя, родных и близ­ких от угроз, шантажа, насилия;
* физическое воздействие (побои, пытки) со сто­роны злоумышленника;
* стремление показать свою значимость.

Причинами непреднамеренного дестабилизиру­ющего воздействия на информацию со стороны людей могут быть:

* неквалифицированное выполнение операций;
* халатность, безответственность, недисциплини­рованность, недобросовестное отношение к выпол­няемой работе;
* небрежность, неосторожность, неаккуратность;

- физическое недомогание (болезни, переутом­ление, стресс, апатия).

Причинами дестабилизирующего воздействия на информацию со стороны технических средств отображения, хранения, обработки воспроизведения, передачи информации и средствсвязи и систем обеспечения их функционирования могут быть:

- недостаток или плохое качество средств;

* низкое качество режима функционирования средств;
* перезагруженность средств;
* низкое качество технологии выполнения работ.

В основе дестабилизирующего воздействия на информацию со стороны природных явлений ле­жат внутренние причины и обстоятельства, непод­контрольные людям, а, следовательно, и не поддаю­щиеся нейтрализации или устранению.

4.7. Каналы и методы несанкционированного доступа к защищаемой информации в адвокатской конторе

К числу наиболее вероятных каналов утечки информации можно отнести [15]:

* совместную с другими фирмами деятельность, участие в переговорах;
* фиктивные запросы со стороны о возможности работать в фирме на различных должностях;
* посещения фирмы;
* общения представителей фирмы о характеристиках предоставляемых услуг;
* чрезмерную рекламу;
* консультации специалистов со стороны, которые в результате этого получают доступ к установкам и документам фирмы;
* публикации в печати и выступления;
* совещания, конференции и т.п.;
* разговоры в нерабочих помещениях;
* обиженных сотрудников фирм;
* технические каналы;
* материальные потоки (транспортировка спецпочты).

При организации защиты информации в адвокатской конторе необходимо учитывать следующие возможные методы и способы сбора информации:

* опрос сотрудников изучаемой фирмы при личной встрече;
* навязывание дискуссий по интересующим проблемам;
* рассылка в адреса предприятий и отдельных сотрудников вопросников и анкет;
* ведение частной переписки научных центров и ученых со специалистами.

Для сбора сведений в ряде случае представители конкурентов могут использовать переговоры по определению перспектив сотрудничества, созданию совместных предприятий. Наличие такой формы сотрудничества, как выполнение совместных программ, предусматривающих непосредственное участие представителей других организаций в работе с документами, посещение рабочих мест, расширяет возможности для снятия копий с документов, сбора различных образцов материалов, проб и т.д. При этом с учетом практики развитых стран экономические соперники могут прибегнуть в том числе и к противоправным действиям, промышленному шпионажу.

Наиболее вероятно использование следующих способов добывания информации [15]:

* визуальное наблюдение;
* подслушивание;
* техническое наблюдение;
* прямой опрос, выведывание;
* ознакомление с материалами, документами, изделиями и т.д.;
* сбор открытых документов и других источников информации;
* хищение документов и других источников информации;
* изучение множества источников информации, содержащих по частям необходимые сведения.

4.8. Основные направления, методы и средства защиты информации в адвокатской конторе

**Направления защиты информации**

***Правовая защита*** – специальные правовые правила, процедуры и мероприятия, создаваемые в целях обеспечения информационной безопасности предприятия.

Правовые меры, регулирую­щие вопросы защиты конфиденциальной информа­ции, можно разделить на две основные группы. К первой группе относятся законодательные акты государства, регла­ментирующие деятельность предприятий в области защиты различных видов тайн, определяющие объем их прав и обязанностей в области защиты. К этой группе можно отнести такие законы, принятые в Российской Федерации, как: «О коммерческой тайне» от 29 июля 2004 года; «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31.05.2002; «О персональных данных» от 27.07.2006; «О предприятиях и предпринимательской деятельности» от 25 декабря 1990 г.; «О частной детективной и охранной деятель­ности в РФ» от 11 марта 1992 г.; «О конкуренции и ограничении монополистической деятельности на товарных рынках» от 22 марта 1991 г.; Гражданский кодекс; Кодекс профессиональной этики адвоката от 31.01.2003; Трудовой кодекс Российской Федерации от 30.12.2001 и др.

Ко второй группе относятся нормативно-правовые докумен­ты, регламентирующие организацию, порядок и правила защиты конфиденциальной информации на предприятии. К ним относятся:

1. Устав предприятия, в котором указываются цели его деятельности, права, в том числе право иметь тайну и осуществлять ее защиту.
2. Коллективный договор, в котором определяются права и  
   обязанности сторон, заключивших договор, в том числе по защите конфиденциальной информации, обеспечению необходимых условий и средств ее защиты.
3. Правила внутреннего трудового распорядка, в которые также могут быть включены статьи, обязывающие всех работников защищать интересы предприятия, его информацию, в том числе защищать и различные виды тайн.
4. Инструкция, определяющая организацию, порядок и правила защиты тайны на предприятии. Могут быть под­готовлены различные положения, регламентирующие права и де­ятельность различных подразделений этого предприятия, напри­мер, службы защиты информации предприятия.

5. Документы, типа перечня, реестра и т.п., определяющие ка­тегории сведений, которые отнесены к конфиденциальной ин­формации предприятия. В этих перечнях следует также указывать сроки засекречивания информации и уровень ее защиты.

Уголовно-правовые нормы по своему содержанию являются, с одной стороны, запрещающими, то есть они под страхом приме­нения мер уголовного наказания запрещают гражданам нарушать свои обязанности и совершать преступления, а с другой стороны, они обязывают соответствующие органы государства (ФСБ, МВД, прокуратуру) привлечь лиц, виновных в совершении преступле­ния, к уголовной ответственности.

Кроме того, нарушения режима секретности, правил сохране­ния тайны, не являющиеся пре­ступлением, могут повлечь ответственность материального, дис­циплинарного или административного характера в соответствии с действующими нормативными актами: отстранение от работы, связанной с секретами, или перевод на другую работу, менее оп­лачиваемую и тоже не связанную с засекреченной информацией.

***Организационная защита*** – регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, использующей нанесение ущерба. Организационную защиту обеспечивает:

* Организация режима охраны, работы с кадрами, документами;
* Использование технических средств безопасности;
* Использование информационно-аналитической работы по выявлению угроз.

Организационная служба защиты информации состоит из:

1. Подразделение режима и охраны предприятия;
2. Специальных подразделений обработки документов конфиденциального характера, а также инженерно-технических подразделений;
3. Информационно-аналитический подразделений.

Организационные меры по защите информации предусматривают, прежде всего, подбор и расстановку кадров, которые будут осу­ществлять мероприятия по защите информации, обучение сотруд­ников правилам защиты засекреченной информации, осуществле­ние на практике принципов и методов защиты информации.

***Инженерно-техническая защита*** – использование различных технических средств для обеспечения защиты конфиденциальной информации. Инженерно-техническая защита использует такие средства как:

* Физические – устройства, инженерные сооружения, организационные меры, исключающие или затрудняющие проникновение к источникам конфиденциальной информации (системы ограждения, системы контроля доступа, запирающие устройства и хранилища);
* Аппаратные – устройства, защищающие от утечки, разглашения и от технических средств промышленного шпионажа
* Программные средства.

Методы защиты информации

**Метод –** в самом общем значении это способ достижения цели, определенным образом упорядоченная деятельность [4, с. 270].

Основными методами, используемыми в защите информации в адвокатской конторе, являются следующие: скрытие, ранжирова­ние, морально-нравст­венные методы и учет.

**Скрытие** – как метод защиты информации является реализацией максимального огра­ничения числа лиц, допускаемых к секретам. Реализация этого метода достигается обычно путем засекречивания информации, то есть отнесение ее к секретной или конфиденциальной информации различной степени секрет­ности и ограничение в связи с этим доступа к этой информации в зависимости от ее важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности; устранения или ослабления технических демаскирующих при­знаков объектов защиты и технических каналов утечки сведений о них.

**Ранжирование** как метод защиты информации включает, во-первых, деление засекречиваемой информации по степени сек­ретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивиду­альных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных опера­ций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности инфор­мации и определяется матрицей доступа. Т.е. пользователь не допускается к ин­формации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

**Морально-нравственные методы защиты информации** предполагают, прежде всего, воспитание сотрудника, допущенного к секре­там, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (понимания важности и полезности за­щиты информации и для него лично), и обучение сотрудника, ос­ведомленного в сведениях, составляющих охраняемую тайну, пра­вилам и методам защиты информации, привитие ему навыков ра­боты с носителями секретной и конфиденциальной информации.

**Учет** обеспечивает возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и мес­тонахождении всех носителей засекреченной информации, а также данные обо всех пользователях этой информации.

Принципы учета засекреченной информации:

* обязательность регистрации всех носителей защищаемой информации;
* однократность регистрации конкретного носителя такой информации;
* указание в учетах адреса, где находится в данное время дан­ный носитель засекреченной информации (в СлЗИ, у исполнителя и т.д.);
* единоличная ответственность за сохранность каждого носи­теля защищаемой информации и отражение в учетах пользователя данной информации в настоящее время, а также всех предыдущих пользователей данной информации.

**Средства защиты информации**

**Средства защиты информации** – это совокупность инженер­но-технических, электрических, электронных, оптических и дру­гих устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения раз­личных задач по защите информации, в том числе предупрежде­ния утечки и обеспечения безопасности защищаемой информа­ции [4, с. 273].

В качестве основания классификации средств защиты инфор­мации используются основные группы задач, решаемые с помощью технических средств:

1. создание физических (механических) препятствий на путях проникновения злоумышленника к носителям информации (решетки, сейфы, замки и т.д.);
2. выявление попыток проникновения на объект охраны, к местам сосредоточения носителей защищаемой информации (электронные и электронно-оптические сигнализаторы);
3. предупреждение о возникновении чрезвычайных ситуаций (пожар, наводнение и т.п.) и ликвидация ЧП (средства пожаротушения и т.д.);
4. поддержание связи с различными подразделениями, помещениями и другими точками объекта охраны;
5. нейтрализация, поглощение или отражение излучения эксплуатируемых или испытываемых изделий (экраны, защитные фильтры, разделительные устройства в сетях электроснабжения и т.п.);
6. комплексная проверка технического средства обработки информации и выделенного помещения на соответствие требованиям безопасности обрабатываемой речевой информации установленным нормам;
7. комплексная защита информации в автоматизированных системах обработки данных с помощью фильтров, электронных замков и ключей в целях предотвращения несанкционированного доступа, копирования или искажения информации.

Знание возможностей методов и средств защи­ты информации позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты конфиденци­альной информации.

4.9. Организация комплексной системы защиты информации в адвокатской конторе

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

* обеспечить обращение сведений, содержащих различные виды тайн, в заданной сфере;
* предотвратить кражу и утечку секретов, любую порчу конфиденциальной информации;
* документировать процесс защиты тайны, чтобы в случае попы­ток незаконного завладения какой-либо тайной предприятия можно было защитить свои права юридически и наказать нару­шителя.

Для определения объема информации, нуждающейся в защи­те, следует привлекать работников предприятия. Во главе этой работы должен стоять опытный менеджер.

Программа будет отражать размер данного предприятия, тип технологии и деловой информации, которую необходимо защи­щать, финансовые возможности предприятия, прошлые случаи кражи подобной информации, реальный, имевший место в про­шлом, или потенциальный урон от таких краж и другие обстоя­тельства. В программе должны учитываться возможные источни­ки и каналы утечки информации.

Для построения системы защиты конфиденциальной информации на предприятии необходимо создание службы защиты информации (СлЗИ), которая будет являться структурной единицей предприятия, непосредственно участвующей в производственно-коммерческой деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями предприятия. Структура и штат СлЗИ в зависимости от объема работ и особенностей производственно-коммерческой деятельности определяются руководителем предприятия и, как правило, должны комплектоваться инженерно-техническими работниками - специалистами основного профиля работы данного предприятия (фирмы), а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника (зама) СлЗИ предприятия (фирмы), а также его освобождение производится только руководителем предприятия. Руководитель службы защиты информации регулярно, в установленные сроки отчитывается в своей работе перед директором предприятия.

Основны­ми функциями СлЗИ являются проблемы организации защиты све­дений, отнесенных к конфиденциальной информации. В частности, деятельность, которая включает обучение работ­ников предприятия умению хранить секреты своей фирмы; под­готовку различных методических документов, связанных с защи­той тайны, плакатов, разъясняющих правила защиты конфиден­циальной информации и др.

СлЗИ готовит руководству предприятия предложения по вопро­сам защиты конфиденциальной информации, порядка определения и пере­смотра перечня сведений, составляющих эту информацию, степени и сроков секретности такой информации; определение круга и по­рядка допуска лиц к сведениям, составляющим различные виды тайн. СлЗИ выполняет также своеобразные разведывательные функции, в частности добывание информации о состоянии рынка, конкурентах, финансовых возможностях партнеров по переговорам и др.

СлЗИ проводит контрольные и аналитические функции. Кон­троль за соблюдением работниками предприятия, связанными по службе с тайной, правил ее защиты. Анализ посту­пающей информации с целью выявления попыток конкурентов получить несанкционированный доступ к защищаемой предпри­ятием информации и т.д. Она должна находиться на высоком уровне в организационной структуре предприятия с тем, чтобы располагать необходимыми административными полномочиями, с извещением об этом всех сотрудников предприятия. СлЗИ должна принимать срочные меры по устранению выявленных недостат­ков в области защиты конфиденциальной информации. Сотрудники фирмы должны знать политику фирмы по защите этой информации и меры наказания за нарушение этих правил.

Периодический пересмотр Перечня сведений, составляющих конфиденциальную информацию предприятия, осуществляется специально созданной комиссией, возглавляемой одним из руководителей предприятия. Однако в этой работе активное участие принимает и СлЗИ. Цель пересмотра Перечня – исключение из него сведений, утративших свою актуальность, и включение новых, изменение при необходимости степени секретности и т.д. О результатах этой работы информируются все исполнители в той части, которая нужна каждому для его работы.

Система доступа к сведениям, составляющим какую-либо тайну, должна обеспечить безусловное ознакомление с такими материалами только тех лиц, которым они нужны по службе. Сис­тема доступа к конфиденциальной информации – есть комплекс административно-правовых норм, обеспечивающих получение необходимой для работы информации каждым исполнителем и руководителем секретных работ. Цель системы – обеспечить только санкционированное получение необходимого объема конфиденциальной информации. В структуру этой системы входят:

* разрешительная система доступа к документальной конфиденциальной информации;
* система пропусков и шифров, обеспечивающая только санкционированный доступ в поме­щения, где ведутся секретные работы.

Для обеспечения физической сохранности носителей засекре­ченной информации и предотвращения доступа посторонних лиц нужна система охраны, кото­рая включает в себя комплекс мероприятий, сил и средств, задействованных для преграждения доступа посторонних лиц к носите­лям защищаемой информации. Обеспечение физической целост­ности и сохранности конфиденциаль­ных документов, различных зданий, помещений, где производятся работы с носителями защищаемой информации, достигается ис­пользованием сейфов и металлических шкафов для хранения кон­фиденциальных документов, постановкой металлических решеток на окна хранилищ таких документов, введением специ­альных пропусков или магнитных карточек для доступа в помеще­ния, где ведутся работы с носителями конфиденциальной инфор­мации. Помещения, в которых ведутся такие работы с документа­ми, хранилища защищаемой информации должны иметь круглосуточную охрану с помощью технических средств.

Осуществление мер – это деятельность администрации и СлЗИ по защите конфиденциальной информации, направленная на реализацию за­ложенных в системе возможностей по защите конфиденциальной информации. Эти меры включают:

**- во-первых,** повседневный контроль со стороны руководства предприятия и СлЗИ за соблюдением всеми сотрудниками, связан­ными по работе с конфиденциальной информацией, правил ее защиты. Особое внимание при этом обращается на работников предприятия, имеющих постоянное общение с населением;

**- во-вторых,** обеспечение соблюдения всеми сотрудниками предприятия требований, предусмотренных правилами внутреннего распорядка, нормами правил пожарной безопасности, ин­струкцией по защите сведений, составляющих различные виды тайн, и другими нормативными документами, регламентирую­щими поведение работников на предприятии.

Все посещения предприятия посторонними лицами должны быть строго регламентированы. Вход – только через одну проходную по разовым пропускам или отметкам в жур­нале: данные о пришедшем, откуда, к кому, время входа и выхода. Продвижение по фирме только в сопровождении принимающего его сотрудника.

Не допускается ведение по открытым каналам связи (телефон, радиотелефон и т.п.) переговоров, содержащих конфиденциаль­ные сведения;

**- в-третьих,** выявление каналов и источников утечки защищае­мой информации и принятие мер по их перекрытию. Утечка за­щищаемой информации происходит чаще всего по вине сотруд­ников предприятия, связанных по работе с конфиденциальной информацией, и принятия недостаточных мер по защите информации в техни­ческих средствах (СВТ, средствах связи и т.д.).

Все сигналы о возможной утечке информации должны тщатель­но проверяться и в случае выявления виновных в этом лиц должны быть приняты меры, как к виновникам (перевод на работу, не свя­занную с тайной, возмещение ущерба, увольнение и др.), так и принятие мер по предотвращению подобных явлений в будущем;

**- в-четвертых,** защита конфиденциальной информации предполагает также принятие мер по предотвращению разглашения защищаемой ин­формации в открытых публикациях сотрудниками предприятия, особенно при подготовке и публи­кации научных работ (статей, брошюр и др.). Все эти документы и публикации должны предварительно согласовываться со специ­алистами и руководящими работниками предприятия;

**-** **в-пятых,** важным звеном защиты конфиденциальной информации пред­приятия является работа с клиентами, партнерами и др. При ведении таких переговоров важно убедиться, что другая сторона преследует в переговорах те же цели, что и вы, то есть заключить взаимовыгод­ное соглашение, а не получение конфиденциальной информации о вашей фирме.

Приступая к разработке системы мер по обеспечению защиты информации на предприятии, его руководитель (или начальник СлЗИ) должен получить ответы на следующие вопросы:

* что конкретно необходимо защищать (охранять), от кого и когда?
* кто организует и обеспечивает защиту (охрану)?
* как оценивать эффективность и достаточность защиты (охраны)?

Для грамотного построения и эксплуатации системы защиты необходимо соблюсти следующие принципы ее применения [15]:

* простота защиты;
* приемлемость защиты для пользователей;
* подконтрольность системы защиты;
* постоянный контроль за наиболее важной информацией;
* дробление конфиденциальной информации на составляющие элементы, доступ к которым имеют разные пользователи;
* минимизация привилегий по доступу к информации;
* установка ловушек для провоцирования несанкционированных действий;
* независимость системы управления для пользователей;
* устойчивость защиты во времени и при неблагоприятных обстоятельствах;
* глубина защиты, дублирование и перекрытие защиты;
* особая личная ответственность лиц, обеспечивающих безопасность информации;
* минимизация общих механизмов защиты.

Алгоритм создания системы защиты конфиденциальной информации таков [23]:

1. Определяется предмет защиты. Разрабатывается Перечень сведений, составляющих различные виды тайн, в котором выделяется наиболее ценная информация, нуждающаяся в особой охране, учитываются требования по защите других предприятий (фирм), участвующих в совместных работах.
2. Устанавливаются периоды существования конкретных сведений в качестве различных видов тайн.
3. Выделяются категории носителей ценной информации: персонал, документы, изделия и материалы; технические средства хранения, обработки и передачи информации; физические излучения. Для обеспечения восприятия разрабатываемой системы защиты можно составить схему, в которой указываются конкретные сотрудники, осведомленные о различных видах тайн, названия (категории) классифицированных документов и т.п.
4. Перечисляются стадии (этапы) работ, время материализации различных видов тайн в носителях информации применительно к пространственным зонам (местам работы с ними внутри и за пределами предприятия). Например, договоры, подписываемые за пределами предприятия; выступления участников отчетных совещаний в конкретных кабинетах; размножение классифицированных документов на множительном участке и т.п.
5. Составляется схема работ с конкретными сведениями, материализованными в носителях, в пределах предприятия (фирмы) и вне его и предполагаемого их перемещения. Рассматриваются возможные для предприятия несанкционированные перемещения, которые могут быть использованы конкурентами для овладения различными видами тайн.
6. Разрабатываются (или корректируются) в процессе анализа разрешительные подсистемы допуска и доступа к конкретным сведениям, составляющим различные виды тайн.
7. Определяется, кто реализует мероприятия и кто несет ответственность за защиту конкретной информации, процессов работ с классифицированными данными. Намечаются меры по координации, назначаются конкретные исполнители.
8. Планируются действия по активизации и стимулированию лиц, задействованных в защите.
9. Проверяется надежность принятых к реализации мер обеспечения защиты.

Аналитические исследования, моделирование вероятных угроз позволяют наметить при необходимости дополнительные меры защиты. При этом следует оценить вероятность их выполнения, наличие методического материала, материального обеспечения, готовность СлЗИ и персонала их выполнить. При планировании учитываются имевшие место на предприятии недостатки в обеспечении сохранности конфиденциальной информации [25].

Планируемые мероприятия должны [15]:

* способствовать достижению определенных задач, соответствовать общему замыслу;
* являться оптимальными.

Не должны [15]:

* противоречить законам, требованиям руководителя фирмы (интересам кооперирующихся фирм);
* дублировать другие действия.

Таким образом, система организации защиты конфиденциальной информации включает в себя комплекс заранее разработанных на определенный срок мер, охватывающих совокупность всех видов деятельности, направленных на совершенствование обеспечения сохранности информации с учетом изменений внешних и внутренних условий и предписывающих конкретным лицам или подразделений определенный порядок действий.

5. Источники информации и оценка их надежности

5.1. Список выявленной литературы

5.1.1. Консультант–Плюс

1. **Российская Федерация. Законы.** Гражданский кодекс Российской Федерации (часть первая): федер. закон: [от 30.11.1994 № 51-ФЗ; принят Гос.Думой 21.10.1994; в ред. от 03.06.2006].- КонсультантПлюс.- (http://www.consultant.ru).
2. **Российская Федерация. Законы.** Гражданский кодекс Российской Федерации (часть вторая): федер. закон: [от 26.01.1996 № 14-ФЗ; принят Гос.Думой 22.12.1995; в ред. от 02.02.2006].- КонсультантПлюс.- (http://www.consultant.ru).
3. **Российская Федерация. Законы.** Кодекс профессиональной этики адвоката: [принят Всероссийским съездом адвокатов 31.01.2003; в ред. от 08.04.2005].- КонсультантПлюс.- (http://www.consultant.ru).
4. **Российская Федерация. Законы.** Об адвокатской деятельности и адвокатуре в Российской Федерации: федер. закон: [от 31.05.2002 № 63-ФЗ; в ред. от 20.12.2004].- КонсультантПлюс.- (http://www.consultant.ru).
5. **Российская Федерация. Законы.** Об утверждении перечня сведений конфиденциального характера: указ Президента РФ: [от 06.03.1997 N 1300; в ред. от 10.01.2000].- КонсультантПлюс.- (http://www.consultant.ru).
6. **Российская Федерация. Законы.** О коммерческой тайне: федер. закон: [от 29.07.2004 № 98-ФЗ; принят Гос.Думой 09.07.2004; в ред. от 02.02.2006].- КонсультантПлюс.- (http://www.consultant.ru).
7. **Российская Федерация. Законы.** О персональных данных: федер. закон: [от 27.07.2006 № 152-ФЗ; принят Гос.Думой 08.07.2006].- КонсультантПлюс.- (http://www.consultant.ru).
8. **Российская Федерация. Законы.** О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон: [от 07.08.2001 № 115-ФЗ; принят Гос.Думой 13.07.2001; в ред. от 16.11.2005].- КонсультантПлюс.- (http://www.consultant.ru).
9. **Российская Федерация. Законы.** О федеральной службе безопасности: федер. закон: [принят Гос. Думой 22.02.1995; в ред. от 15.04.2006].- КонсультантПлюс.- (http://www.consultant.ru).
10. **Российская Федерация. Законы.** Трудовой кодекс Российской Федерации: федер. закон: [от 30.12.2001 № 197-ФЗ; принят Гос.Думой 21.12.2001; в ред. от 09.05.2005].- КонсультантПлюс.- (http://www.consultant.ru).

5.1.2. Текущие библиографические указатели и реферативные журналы

1. Беляев, Е.А. Исторические аспекты защиты информации в России/ Е.А.Беляев// Информационная безопасность = Inform.security.- М., 2004.- № 3.-С.58–59.
2. Домов, С. Информационная безопасность/ С.Домов// Вестн. Волжского ун–та.- Сер.Информат, 2005.- № 8.- С.53–55
3. Кальченко, Д. Безопасность в цифровую эпоху/ Д.Кальченко// Компьютер Пресс, 2005.- №4.- С.34, 36,38–41.
4. Колесников, К.А. Социальные факторы информационного управления и информационная безопасность в России/ К.А.Колесников// Интеллектуальная собственность: правовые, экономические и социальные проблемы: Сб. тр. аспирантов РГИИС: В 2 ч.- М., 2005.-Ч.2.-С.140–143.
5. Минакова, Н.Н. Особенности подготовки специалистов по информационной безопасности автоматизированных систем/ Н.Н.Минакова, В.В.Поляков// Вестн. Алтайск. науч. центра САН ВШ, 2005.- № 8.- С.125–128.
6. Мешкова, Т.А. Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности: автореф. дис….канд. наук/ Мешкова Т.А.; МГУ им.М.В.Ломоносова.– М., 2003.-26 с.

5.1.3. Электронный каталог

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций/ Л.В.Астахова.- Челябинск: Изд–во «ЗАО Челябинская межрайонная типография», 2006.- 361 с.
2. Буробин, В.Н. Адвокатская тайна/ В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин.- М.: Статут, 2006.- 253 с.
3. Иванов, А.В. Экономическая безопасность предприятий/ А.В.Иванов.- М.: Вираж-центр, 1995.- 39 с.
4. Курело, А.П. Обеспечение информационной безопасности бизнеса/ А.П.Курело, С.Г.Антимонов, В.В.Андрианов и др.- М.: БДЦ–пресс, 2005.- (t–Solutions).- 511 с.
5. Петрухин, И.Л. Личные тайны: человек и власть/ И.Л.Петрухин.- М.: ЦГПАН, 1998.- 230 с.
6. Поздняков, Е.Н. Защита объектов: Рекомендации для руководителей и сотрудников служб безопасности/ Е.Н.Поздняков.– М.: Концерн «Банковский деловой центр», 1997.- (Советы «профи»).- 222 с.
7. Соловьев, Э. Коммерческая тайна и её защита/ Э.Соловьев.- М.: Главбух, 1995.- 48 с.
8. Шафикова, Г.Х. К вопросу о защите персональных данных работника/ Г.Х.Шафикова// Региональная информационная экономика: проблемы формирования и развития: Сб. науч. тр. Междунар. науч-практ. конф. 25-26 октября 2002.- Челябинск: Изд-во ЮУрГУ, 2003.- С. 359-362.
9. Ярочкин, В.И. Коммерческая информация фирмы: утечка или разглашение конфиденциальной информации/ В.И.Ярочкин.- М.: Ось-89, 1997.- 160 с.

5.1.4. Информационно–поисковые системы Интернет

* 1. Адвокатская тайна/ Юридическая библиотека [Электронный ресурс]// Юридическая библиотека URKA.ru.- (http://www.urka.ru/library.php/chat/chat/library/arch/library.php?parent=419).
  2. Анализ угроз и построение системы информационной безопасности [Электронный ресурс]// МРЦБ. Консультационная фирма. IT-консалтинг.- (http://www.mrcb.ru/).
  3. Астахов, А. Разработка эффективных политик информационной безопасности/ А.Астахов [Электронный ресурс]// Директор ИС #01/2004.- (http://www.osp.ru/cio/2004/01/rub/1072641.html).
  4. Аудит информационной безопасности [Электронный ресурс]// Микротест. IT-услуги.- (http://www.microtest.ru/services/).
  5. Брединский, А. Защита коммерческой тайны. Теория и практика/ А.Брединский, А.Беручашвили [Электронный ресурс]// Информационно-справочный сайт «Безопасность для всех».- (http://www.sec4all.net/).
  6. Буробин, В.Н. Кто посягнул на адвокатскую тайну/ В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин [Электронный ресурс]// Дайджест правовой прессы в Санкт-Петербурге на информационно-правовом портале Кадис.- (http://www.kadis.ru/daily/).
  7. Буробин, В.Н. Нарушения адвокатской тайны в России / В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин [Электронный ресурс]// Адвокатская фирма «Юстина», Новости- (http://www.yustina.ru/).
  8. Васильевский, А. Защита коммерческой тайны: организационные и юридические аспекты / А.Васильевский [Электронный ресурс]// Valex Consult- (http://www.valex.net/).
  9. Демин, В. Правовое обеспечение системы защиты информации на предприятии/ В.Демин, В.Свалов [Электронный ресурс]// Компьютер-информ.- (http://www.ci.ru/inform11\_97/f1.htm).
  10. Касперский, Е. Защита коммерческой тайны/ Е.Касперский [Электронный ресурс]// Электронная версия журнала «Консультант».- (http://www.berator.ru/consultant/article/).
  11. Комплексные системы защиты информации [Электронный ресурс]// AM-SOFT. Деятельность компании. Защита информации.- (http://am-soft.ua/site/page4044.html).
  12. Корня, А. Защиту пробили. Адвокатская тайна может быть упразднена/ А.Корня [Электронный ресурс]// Новая газета.- (http://www.ng.ru/politics/).
  13. Кучерена, А. Адвокатская тайна/ А.Кучерена [Электронный ресурс]// reflexion.ru/Library.- (http://www.reflexion.ru/Library).
  14. Михеева, М.Р. Проблема правовой защиты персональных данных/ М.Р.Михеева [Электронный ресурс]// Владивостокский центр исследования организованной преступности.- (http://www.crime.vl.ru/).
  15. Определение Конституционного Суда Российской Федерации от 8 ноября 2005 г. N 439-О по жалобе граждан С.В. Бородина, В.Н. Буробина, А.В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс]// Российская газета.– (http://www.rg.ru/).
  16. Организация защиты коммерческой тайны на предприятии [Электронный ресурс]// Пензенский деловой портал.- (http://www.penza-job.ru/).
  17. Петренко, С. Разработка политики информационной безопасности предприятия/ С.Петренко, В.Курбатов [Электронный ресурс]// Сетевые решения A-Z.- (http://www.nestor.minsk.by/sr/help/2007/07/130100.html).
  18. Служба защиты информации на предприятии. Что она из себя представляет и как ее организовать [Электронный ресурс]// Спектр безопасности.- (http://www.spektrsec.ru/).
  19. Столяров, Н.В. Разработка системы защиты конфиденциальной информации/ Н.В.Столяров [Электронный ресурс]// 4Delo.ru Библиотека.- (http://www.4delo.ru/inform/articles/).
  20. Цыпкин, А.Л. Адвокатская тайна/ А.Л.Цыпкин [Электронный ресурс]// Russian-lawyers.ru..- (http://russian-lawyers.ru/files/cypkin.doc).
  21. Чен Энн. Юристы выдвигают аргументы в пользу eRoom/ Энн Чен [Электронный ресурс]// PC WEEK, RE, № 17/2007.- (http://www.pcweek.ru/?ID=629431).
  22. Шуличенко, А.А. Адвокатская тайна в показаниях обвиняемого/ А.А.Шуличенко [Электронный ресурс]// Бизнес mix.- (http://www.businessmix.ru/).
  23. Щеглов, А.Ю. Часть 12. Общие вопросы построения системы защиты информации/ А.Ю.Щеглов, К.А.Щеглов [Электронный ресурс]// Мост безопасности. Библиотека.- (http://articles.security-bridge.com/).

5.1.5. Сплошной просмотр периодических изданий

1. Алексенцев, А.И. Понятие и назначение комплексной системы защиты информации/ А.И.Алексенцев// Вопросы защиты информации.- 1996.- № 2. - С. 2 - 3.
2. Алябушев, И.Б. Методики защиты баз данных от внутренних злоумышленников/ И.Б.Алябушев, В.В.Бабушкин// Информационно–методический журнал «Защита информации INSIDE».- 2006.- № 6 (12).- С.58.
3. Брединский, А.Г. Люди – источники конфиденциальной информации/ А.Г.Брединский// Информационно–методический журнал «Защита информации Конфидент».- 2004.- № 2 (56).- С.32.
4. Буробин, В.Н. Правовой режим адвокатской тайны/ В.Н.Буробин// «Бизнес-адвокат».- 2006.- № 3, 4.- С.28-33.
5. Журин, С.И. Вопросы оценки благонадежности персонала в подготовке администратора информационной безопасности/ С.И.Журин, М.Ю.Калинкина// Информационно–методический журнал «Защита информации Конфидент».- 2004.- № 3 (57).- С.28.
6. Казанцев, В.Г. Обучение руководителей служб безопасности/ В.Г.Казанцев// Информационно–методический журнал «Защита информации INSIDE».- 2005.- № 6 (06)– С.66.
7. Казанцев, В.Г. Профессиональное образование сотрудников подразделений экономической и информационной безопасности. В.Г.Казанцев// Информационно–методический журнал «Защита информации Конфидент».- 2004.- № 3 (57).- С.30.
8. Как найти и обезвредить сотрудника–саботажника// Информационно–методический журнал «Защита информации INSIDE».- 2005.- № 5 (05).- С.28.
9. Копейкин, В.Г. Экономическая безопасность предприятия: обучение персонала/ В.Г.Копейкин, Н.А.Лапина// Информационно–методический журнал «Защита информации Конфидент».- 2004.- № 3 (57).- С.44.
10. Кучерена А. Адвокатская тайна/ А.Кучерена // Законность.- 2003. – № 2. – С. 47 – 50.
11. Шатунов, В.М. Обучение персонала как составная часть проблемы обеспечения информационной безопасности энергосистемы/ В.М.Шатунов, И.Н.Бабков// Информационно–методический журнал «Защита информации Конфидент».- 2004.- № 3 (57).- С.53.
12. DeviceLock 5.72. - защита от локального администратора!// Information Security.- 2005.- № 4.- С.38.

**5.2. Список использованной литературы**

5.2.1. Вторичные источники

1. Адвокатская тайна/ Юридическая библиотека [Электронный ресурс]// Юридическая библиотека URKA.ru.- (http://www.urka.ru/library.php/chat/chat/library/arch/library.php?parent=419).
2. Алексенцев, А.И. Понятие и назначение комплексной системы защиты информации/ А.И.Алексенцев// Вопросы защиты информации.- 1996.- № 2. - С. 2 - 3.
3. Астахов, А. Разработка эффективных политик информационной безопасности/ А.Астахов [Электронный ресурс]// Директор ИС #01/2004.- (http://www.osp.ru/cio/2004/01/rub/1072641.html).
4. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций/ Л.В.Астахова.- Челябинск: Изд–во «ЗАО Челябинская межрайонная типография», 2006.- 361 с.
5. Брединский, А. Защита коммерческой тайны. Теория и практика/ А.Брединский, А.Беручашвили [Электронный ресурс]// Информационно-справочный сайт «Безопасность для всех».- (http://www.sec4all.net/).
6. Буробин, В.Н. Адвокатская тайна/ В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин.- М.: Статут, 2006.- 253 с.
7. Буробин, В.Н. Кто посягнул на адвокатскую тайну/ В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин [Электронный ресурс]// Дайджест правовой прессы в Санкт-Петербурге на информационно-правовом портале Кадис.- (http://www.kadis.ru/daily/).
8. Буробин, В.Н. Нарушения адвокатской тайны в России / В.Н.Буробин, В.Ю.Плетнев, Д.А.Шубин [Электронный ресурс]// Адвокатская фирма «Юстина», Новости- (http://www.yustina.ru/).
9. Буробин, В.Н. Правовой режим адвокатской тайны/ В.Н.Буробин// «Бизнес-адвокат».- 2006.- № 3, 4.- С.28-33.
10. Васильевский, А. Защита коммерческой тайны: организационные и юридические аспекты / А.Васильевский [Электронный ресурс]// Valex Consult- (http://www.valex.net/).
11. Демин, В. Правовое обеспечение системы защиты информации на предприятии/ В.Демин, В.Свалов [Электронный ресурс]// Компьютер-информ.- (http://www.ci.ru/inform11\_97/f1.htm).
12. Касперский, Е. Защита коммерческой тайны/ Е.Касперский [Электронный ресурс]// Электронная версия журнала «Консультант».- (http://www.berator.ru/consultant/article/).
13. Кучерена, А. Адвокатская тайна/ А.Кучерена [Электронный ресурс]// reflexion.ru/Library.- (http://www.reflexion.ru/Library).
14. Определение Конституционного Суда Российской Федерации от 8 ноября 2005 г. N 439-О по жалобе граждан С.В. Бородина, В.Н. Буробина, А.В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс]// Российская газета.– (http://www.rg.ru/).
15. Организация защиты коммерческой тайны на предприятии [Электронный ресурс]// Пензенский деловой портал.- (http://www.penza-job.ru/).
16. Петренко, С. Разработка политики информационной безопасности предприятия/ С.Петренко, В.Курбатов [Электронный ресурс]// Сетевые решения A-Z.- (http://www.nestor.minsk.by/sr/help/2007/07/130100.html).
17. **Российская Федерация. Законы.** Кодекс профессиональной этики адвоката: [принят Всероссийским съездом адвокатов 31.01.2003; в ред. от 08.04.2005].- КонсультантПлюс.- (http://www.consultant.ru).
18. **Российская Федерация. Законы.** Об адвокатской деятельности и адвокатуре в Российской Федерации: федер. закон: [от 31.05.2002 № 63-ФЗ; в ред. от 20.12.2004].- КонсультантПлюс.- (http://www.consultant.ru).
19. **Российская Федерация. Законы.** О коммерческой тайне: федер. закон: [от 29.07.2004 № 98-ФЗ; принят Гос.Думой 09.07.2004; в ред. от 02.02.2006].- КонсультантПлюс.- (http://www.consultant.ru).
20. **Российская Федерация. Законы.** О персональных данных: федер. закон: [от 27.07.2006 № 152-ФЗ; принят Гос.Думой 08.07.2006].- КонсультантПлюс.- (http://www.consultant.ru).
21. **Российская Федерация. Законы.** О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон: [от 07.08.2001 № 115-ФЗ; принят Гос.Думой 13.07.2001; в ред. от 16.11.2005].- КонсультантПлюс.- (http://www.consultant.ru).- КонсультантПлюс.- (http://www.consultant.ru).
22. **Российская Федерация. Законы.** Трудовой кодекс Российской Федерации: федер. закон: [от 30.12.2001 № 197-ФЗ; принят Гос.Думой 21.12.2001; в ред. от 09.05.2005].- КонсультантПлюс.- (http://www.consultant.ru).
23. Служба защиты информации на предприятии. Что она из себя представляет и как ее организовать [Электронный ресурс]// Спектр безопасности.- (http://www.spektrsec.ru/).
24. Столяров, Н.В. Разработка системы защиты конфиденциальной информации/ Н.В.Столяров [Электронный ресурс]// 4Delo.ru Библиотека.- (http://www.4delo.ru/inform/articles/).
25. Щеглов, А.Ю. Часть 12. Общие вопросы построения системы защиты информации/ А.Ю.Щеглов, К.А.Щеглов [Электронный ресурс]// Мост безопасности. Библиотека.- (http://articles.security-bridge.com/).

5.2.2. Первичные источники

1. Конференция-online ИА REGNUM «Кибертерроризм и безопасность бизнеса в России» 9 февраля 2007 с 13 до 14 часов по московскому времени. Отвечал Клепов Анатолий Викторович, президент ЗАО «Анкорт». Вопрос Ильи Седова, Санкт-Петербург.
2. Лекции по теории информационной безопасности и методологии защиты информации, прочитанные Рагозиным Андреем Николаевичом.

5.2.3. Оценка надежности использованных источников

1. Надежный источник (4, 6-9, 14, 17-22, первичные – 2) – 48%
2. Обычно надежный источник (2, 12) – 7%
3. Довольно надежный источник (1, 3, 5, 10-11, 15-16, 23-25, первичные – 1)– 41%
4. Не всегда надежный источник (13) – 4%
5. Ненадежный источник – 0%
6. Источник неустановленной надежности – 0%

6. Недостающая информация

Для подтверждения окончательной гипотезы и принятия правильного решения мне необходима была следующая информация: Положение о конфиденциальной информации предприятия; Инструкция по защите конфиденциальной информации в информационной системе предприятия; трудовой договор, соглашение о неразглашении конфиденциальной информации предприятия с сотрудником и обязательство сотрудника о неразглашении конфиденциальной информации предприятия при увольнении. На основе этих документов я смогла бы сделать вывод о степени защищенности конфиденциальной информации и избежать рекомендаций, которые уже сейчас выполняются в адвокатской фирме «Юстина» (а именно: я рекомендовала подготовить некоторые из этих документов, считая, что они отсутствуют в организации). Но эти документы, относящиеся к безопасности, являются коммерческой тайной организации, поэтому мне не удалось с ними ознакомиться.

Сведения о наличии пропускного режима мне удалось найти, но о порядке его проведения и состоянии организации охраны мне ничего не известно, т.к. это тоже коммерческая тайна организации. А между тем эта информация позволила бы мне сделать вывод о том, достаточно ли строги эти меры.

Таким образом, вся недостающая мне информация не была мною получена в связи с тем, что относится к информации ограниченного доступа.

7. Основная и альтернативная гипотезы

Не многие руководители предприятий осознают насущную необходимость в организации на предприятии системы защиты конфиденциальной информации для обеспечения его информационной безопасности. Из числа тех, кто осознает такую необходимость, есть те, которые не знают, что следует предпринять, чтобы сохранить те или иные сведения в тайне, с выгодой реализовать их, не понести убытки от их утечки или утраты. Многие идут только по пути оснащения предприятия техническими средствами защиты, полностью игнорируя организационно-правовые методы, в частности создание нормативно-правовой базы, принятие и строгое соблюдение которой позволит предприятию не только сохранить и использовать с выгодой свои секреты, а в случае утечки информации явится основанием для подачи искового заявления в суд.

Однако известно, что только «комплексная система может гарантировать достижение максимальной эффективности защиты информации, т.к. системность обеспечивает необходимые составляющие защиты и устанавливает между ними логическую и технологическую связь, а комплексность, требующая полноты этих составляющих, всеохватности защиты, обеспечивает ее надежность» [2].

Основываясь на этих фактах, в начале работы я сформулировала основную и альтернативную гипотезу. ***Моя основная гипотеза*** – в адвокатской фирме «Юстина» не уделяется должное внимание системе защиты конфиденциальной информации, т.е. используются только некоторые технические средства защиты информации (биометрические турникеты, система видеонаблюдения, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам, система построения VPN, система биллинга, система квотирования трафика и др.).

И ***альтернативная гипотеза:*** в адвокатской фирме «Юстина» создана идеальная система защиты информации, обеспечивающая комплексную безопасность информации фирмы.

Гипотезу об отсутствии системы защиты информации я рассматривать не стала, т.к. «Юстина» довольно крупная, известная и далеко не молодая фирма. Также сведения об информационной системе не дают возможности выдвинуть эту гипотезу.

В ходе подготовки информационно-аналитического обзора я поняла, что система защиты конфиденциальной информации далеко не идеальна, т.к. в такой фирме просто необходимо существование собственной службы защиты информации, а ее до сих пор нет. Однако мне не удалось ознакомиться с некоторыми документами, которые позволили бы сделать вывод об объективном состоянии защиты информации в «Юстине». Скорее всего, положение о конфиденциальной информации предприятия, инструкция по её защите, соглашение о неразглашении конфиденциальной информации предприятия с сотрудником и обязательство сотрудника о неразглашении конфиденциальной информации предприятия при увольнении в фирме есть. Однако это не все необходимые документы и, кроме того, как видно из характеристики информационной системы фирмы технических средств не достаточно для обеспечения должной информационной безопасности. Поэтому я склоняюсь к правильности моей основной гипотезы.