**Этап 3)** Изучить и описать какие используются нормативные акты и законы в данной сфере деятельности.

В Российской Федерации сложилась трехступенчатая система регулирования страхового рынка.

**- Первая ступень**: Гражданский кодекс страны, некоторые законы и правовые акты, имеющие статус кодекса.

**- Вторая ступень**: Специальные законы по страховому делу.

**- Третья ступень**: Нормативные акты министерств и ведомств по страховому делу.

На сегодняшний день правовой фундамент, регулирующий страхование и страховую деятельность, состоит из следующих составных частей.

**1)** **Конституция Российской Федерации** – правовой документ, имеющий наивысшую юридическую силу (принята всенародным голосованием 12 декабря 1993 г.) (ред. от 14.10.2005 г.). Конституция декларирует основные стратегические направления развития страны, порядок формирования органов государственной власти и местного самоуправления; определяет полномочия законодательной, исполнительной и судебной властей, правовой статус Президента РФ, органов федерального, регионального и местного самоуправления.

**2)** **Гражданский Кодекс Российской Федерации, Часть II, глава 48 «Страхование» (N 14 – ФЗ от 26.01.1996) (ред. от 02.02.2006).** В ГК РФ сформулированы общие положения о формах страхования, договорах страхования, правах и обязанностях субъектов правовых отношений; об интересах, страхование которых не допускается; о последствиях наступления страхового случая; об основаниях по освобождению страховщика от выплаты страхового обеспечения и страхового возмещения; о перестраховании, взаимном государственном страховании и др.

**3)** **Федеральный закон «Об организации страхового дела в Российской Федерации» N 4015-1от 27 ноября 1992 г. г. (ред. от 21 июля 2005 г.);**

**4)** **федеральные законы**:

* Федеральный закон от 24 ноября 1996 г. N 132-ФЗ «Об основах туристской деятельности в Российской Федерации» (ред. от 22.08.2004);
* Федеральный закон от 28 июня 1991 г. N 1499-1 «О медицинском страховании граждан в Российской Федерации» (ред. от 23.12.2003);
* Федеральный закон от 23.12.2003 N 177-ФЗ (ред. от 20.10.2005) «О страховании вкладов физических лиц в банках Российской Федерации»;
* Федеральный закон от 25.04.2002 N 40-ФЗ (ред. от 21.07.2005) «Об обязательном страховании гражданской ответственности владельцев транспортных средств»;
* Федеральный закон от 15.12.2001 N 167-ФЗ (ред. от 02.02.2006) «Об обязательном пенсионном страховании в Российской Федерации»;
* Федеральный закон от 16.07.1999 N 165-ФЗ (ред. от 05.03.2004) «Об основах обязательного социального страхования»;
* Федеральный закон от 24.07.1998 N 125-ФЗ (ред. от 22.12.2005) «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;
* Федеральный закон от 28.03.1998 N 52-ФЗ (ред. от 02.02.2006) «Об обязательном государственном страховании жизни и здоровья военнослужащих, граждан, призванных на военные сборы, лиц рядового и начальствующего состава органов внутренних дел Российской Федерации, государственной противопожарной службы, органов по контролю за оборотом наркотических средств и психотропных веществ, сотрудников учреждений и органов уголовно-исполнительной системы и сотрудников федеральных органов налоговой полиции»;

**5) Указы президента РФ.**

* Указ Президента РФ от 07.07.1992 N 750 (ред. от 22.07.1998) «Об обязательном личном страховании пассажиров»;

**6) Законодательные и нормативные правовые акты, постановления Правительства РФ и положения:**

* Постановление Правительства РФ от 08.12.2005 N 739 «Об утверждении страховых тарифов по обязательному страхованию гражданской ответственности владельцев транспортных средств, их структуры и порядка применения страховщиками при определении страховой премии»;
* Постановление Правительства РФ от 24.08.2004 N 434 «О предоставлении государственной гарантии Российской Федерации при страховании гражданской ответственности российских авиаперевозчиков»;
* Постановление Правительства РФ от 30.06.2004 N 330 «Об утверждении положения о федеральной службе страхового надзора»;
* Постановление Правительства РФ от 06.02.2004 N 60 (ред. от 03.07.2006) «Об утверждении форм типового договора об обязательном пенсионном страховании между негосударственным пенсионным фондом и застрахованным лицом, форм заявлений застрахованного лица о переходе в негосударственный пенсионный фонд и о переходе в Пенсионный Фонд Российской Федерации»;
* Постановление Правительства РФ от 07.05.2003 N 263 «Об утверждении правил обязательного страхования гражданской ответственности владельцев транспортных средств»;
* Постановление Правительства РФ от 29.03.1994 N 251 (ред. от 14.10.2005) «Об утверждении правил лицензирования деятельности страховых медицинских организаций, осуществляющих обязательное медицинское страхование»;

**Этап 4) изучить и описать какие существуют требования к ИБ в данной сфере деятельности**.

Страховые компании оказывают услуги в сфере страховой защиты имущественных интересов юридических и физических лиц. В процессе деятельности они становятся обладателями большого объема информации, носящей характер коммерческой тайны или же персональных данных. И то и другое защищено законом. Распространение этих сведений среди широкого круга лиц может привести к финансовому ущербу для компании и ее клиентов. При этом страховая информация является активом, имеющим самостоятельную ценность. Поэтому специалисты службы безопасности страховых компаний обязаны прилагать значительные усилия в области защиты информации.

**Правовое регулирование защиты информации в сфере страховой деятельности.**

Статус информации как объекта правовой защиты регулируется несколькими федеральными законами. Среди них закон **«Об информации, информационных технологиях и защите информации»,** **Гражданский кодекс**, закон **«О защите персональных данных»** и другие.

В деятельности страховой компании образуются следующие объекты информации:

* коммерческая тайна самой страховой компании, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших страховых событиях;
* персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;
* медицинская тайна клиентов компании, пользующихся услугами добровольного медицинского страхования.

Все массивы информации содержатся как на бумажных, так и на электронных носителях. Эти данные могут стать объектом противоправного покушения, их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением, предусмотренным статьей 272 Уголовного кодекса.

**Виды угроз информационной безопасности**

Перечень угроз безопасности включает атаки как внешнего, так и внутреннего происхождения. Информационные базы данных, принадлежащие страховым компаниям, часто становятся объектами покушений хакеров. Частыми целями преступных посягательств являются клиентские базы данных, содержащие информацию о номерах телефонов, номерах автомобилей, медицинских историях. В ряде случаев мошенники, используя данные, похищенные у страховщиков, создавали сайты-клоны, применяемые для продажи недействительных полисов ОСАГО. В США в прошлом году преступниками была взломана система защиты одной из крупнейших страховых компаний, данные сотен тысяч клиентов оказались в открытом доступе.

Кроме того, не исключен риск заражения компьютерных систем компании различными вирусами, которые могут причинить существенный ущерб в виде:

* блокировки доступа к важным файлам;
* уничтожения файлов;
* передачи информации третьим лицам.

Не всегда установленный антивирус будет надежной защитой от спланированной атаки. Кроме внешней угрозы проникновения в компьютерные сети страховой компании существуют и внутренние. Отдельные сотрудники могут намеренно похищать коммерческую информацию с целью ее распространения или передачи конкурентам.

**Меры и средства защиты информации**

Стандарты защиты информации в России предусмотрены ГОСТами. Кроме того, информационная безопасность страховой компании должна обеспечиваться целым комплексом мер, среди которых:

* административные;
* организационные;
* технические.

Все они должны применяться совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

**Административные меры безопасности**

Эти способы защиты включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о системе действий, необходимых для обеспечения информационной безопасности. Такие документы хранятся в открытом доступе, в страховой компании должно быть организовано ознакомление с ними персонала.

Служба безопасности страховой компании разрабатывает и предлагает на утверждение руководства политику защиты конфиденциальной информации.

Этот локальный нормативный акт должен содержать:

* основные принципы защиты конфиденциальной информации в компании;
* обязанности каждого сотрудника в части защиты доверенных ему сведений;
* задачи руководства по обеспечению охраны информации;
* регламенты обращения с компьютерной техникой и средствами коммуникации;
* меры ответственности за нарушение положений документа.

Кроме того, приложением ко всем трудовым договорам должен стать перечень информации, носящей характер коммерческой, а в самих договорах должны быть предусмотрены меры ответственности за ее разглашение.

**Организационные меры безопасности**

В большей степени они направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

В числе организационных мер обеспечения информационной безопасности можно назвать следующие:

* установление различных степеней допуска сотрудников к сведениям, содержащим коммерческую тайну;
* ограничение круга лиц, имеющих допуск к конфиденциальной информации страховой компании;
* организация порядка использования материальных носителей, установление контроля над копированием и сканированием документов, ограничение доступа сотрудников к внешней электронной почте;
* проведение периодических проверок соблюдения регламентов;
* привлечение специалистов для проведения тренингов по защите информации;
* проведение мероприятий по созданию режима коммерческой тайны;
* внесение в договоры компании с клиентами норм, касающихся обязательств соблюдения последними режима коммерческой тайны в отношении переданной им информации;
* привлечение к ответственности лиц, виновных в разглашении информации.

Иногда система работы с безопасностью информации требует создания в компании специального подразделения, в чьи функции будет входить только эта деятельность.

Также следует учитывать, что при проектировании большинства информационных систем уровень защиты от внешнего проникновения был значительно ниже, чем необходим в настоящее время. Среди организационных мер может быть и их аудит, который установит соответствие современным стандартам.

Существуют дополнительные меры организационного характера, позволяющие снизить потери от утечек информации. Уже несколько лет сами страховщики реализуют такой продукт, как страхование от угроз информационной безопасности. Он достаточно популярен. Применение этого способа защиты поможет минимизировать ущерб в случае расспрос транения коммерческой тайны.

**Технические меры**

Эта группа мер рассчитана на использование действенных технических средств защиты. Для ее реализации используются аппаратные, программные и криптографические средства.

Первые предполагают установку систем резервного копирования и защиту от несанкционированного проникновения, вторые отвечают за работу антивирусов и иных защитных программ, третьи обеспечивают шифрование всей хранимой и передаваемой по каналам связи информации.

Наиболее часто для защиты информации применяются межсетевые экраны и системы обнаружения вторжений. Технические средства требуют постоянного обновления и модернизации, так как скорость устаревания программных продуктов очень высока.

Сегодня предлагаются программы, которые обеспечивают комплексные меры по защите информации, это DLP-системы и SIEM-системы. Первые предотвращают утечку данных при их передаче по каналам электронной почты, с использованием мессенжеров или при передаче на принтер. Если программа зафиксирует преобразование информации в момент ее передачи, что может означать ее перехват, она прекращает ее направление на внешние каналы. SIEM-системы представляют из себя комплексные средства управления безопасности, они определяют все уязвимые места системы и предоставляют информацию обо всех возможных угрозах, выявляя паттерны, отличные от стандартного поведения самой системы и ее пользователей.

С каждым днем мошенники разрабатывают новые средства преодоления защитных барьеров, и степень опасности утраты ценных сведений растет, а вместе с ней и риск возможных финансовых потерь. Минимизировать риски можно, пройдя аудит своих систем защиты и получив рекомендации по их модернизации.

Комплексное применение современных технических средств в работе службы безопасности страховой компании может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа. Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям российского законодательства.