**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*ИНСТИТУТ* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*КАФЕДРА* ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

СПЕЦИАЛЬНОСТЬ ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***Информационная безопасность и защита информации***

**Курсовая работа**

На тему:

Юридические аспекты политики конфиденциальности компании

*Студент группы \_\_\_\_\_\_\_* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Руководитель работы*  \_\_\_\_\_\_\_\_\_\_

Москва 2010

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ……………………………………………………………………...3

ОСНОВНАЯ ЧАСТЬ……………………..………………………...……………..5

Информация и право……………………………………………………………5

Основные положения федерального закона «Об информации, информационных технологиях и защите информации……..........................7

Политика конфиденциальности………………………………………………10

Правовые аспекты защиты информации……………………………………..17

Ответственность за нарушение законодательства о защите информации…21

Гражданско-правовая ответственность……………………………………….21

Административная ответственность…………………………………………..23

Уголовная ответственность……………………………………………………..30

ЗАКЛЮЧЕНИЕ………………………………………………………………….34

ОСНОВНАЯ ЛИТЕРАТУРА……….…………………………………………...35

Приложение №1

**ВВЕДЕНИЕ**

Настоящая работа посвящена правовым вопросам защиты информации, основополагающие принципы которых заложены в политике конфиденциальности коммерческой компании.

Защита информации – одна из важнейших задач, стоящая перед руководством любой крупной компании, ведь те информационные ресурсы, которые формируют активы компании требуют их сохранения и нераспространения за пределами компании, а также ограниченного доступа к ним внутри неё.

Сегодня сформирован значительный массив источников информационного права – федеральных законов, актов Президента Российской Федерации, Правительства Российской федерации, актов других федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Однако, нередко качество этих актов невысокое, не хватает теоретических проработок для эффективного регулирования отношений в информационной сфере нормами этих актов.

**Цель работы:** проанализировать действующее законодательство в области защиты информации на предметналичия правовых норм, содержащих предписания, в соответствии с которыми необходимо осуществлять действия, направленные на защиту информации внутри компании и во вне.

**Задачи:**

1. Выявить правовые нормы, регламентирующие порядок защиты информации и ответственность за его нарушение.
2. Структурировать полученные данные по различным отраслям права.
3. Сформировать теоретические выводы.

**Структура курсовой работы:** настоящая работа состоит из введения, основной части, заключения, списка использованной литературы. В основной части рассматриваются вопросы правовой регламентации в российском законодательстве защиты информации, приводятся конкретные статьи нормативно-правовых актов в отношении ответственности за нарушение законодательства (административная, уголовная ответственность). Заключение содержит основные выводы работы.

**ОСНОВНАЯ ЧАСТЬ**

**Информация и право**

Информация определяется как основной объект, по поводу которого или в связи с которым возникают общественные отношения, регулируемые правом.

Информационные процессы – это процессы, в результате исполнения которых осуществляются информационные права и свободы, выполняются обязанности соответствующими структурами производить и вводить в обращение информацию, затрагивающую права и интересы граждан, а также решаются вопросы защиты личности, общества, государства от ложной информации и дезинформации, защиты информации и информационных ресурсов ограниченного доступа от несанкционированного доступа.

Информационные отношения – это те общественные отношения, которые возникают в информационных процессах. Информационные отношения составляют основной предмет информационного права, предмет его правового регулирования.

Важно отметить, что почти все обсуждаемые выше термины уже определены законодателем. Законодатель определил также и понятие «Информационная сфера» как сфера производства и обращения информации.

В целом, информационное право рассматривается как комплексная отрасль права, имеющая свой особый предмет правового регулирования – информационные отношения; свои принципы правового регулирования информационных отношений, базирующиеся на особенностях и юридических свойствах информации; и использующая весь спектр традиционных методов правового регулирования публичного и частного права.

Информационное право имеет свои собственные институты (институт массовой информации, институт документированной информации, институты информации ограниченного доступа) и использует хорошо известные институты права (например, институты интеллектуальной собственности).

Роль информационного права в информационном обществе 21 века переоценить трудно. По сути дела, это право составляет его правовой фундамент. А поскольку, в информационном обществе практически отсутствуют географические и геополитические границы, и даже временные рамки и часовые пояса, а также, как правило, не действуют национальные законодательства, то информационное право, как правовое отображение такого общества, должно строиться, главным образом, на нормах международного права, регулирующих основные группы информационных отношений на межгосударственном уровне. Поскольку в трансграничной сети Интернет отсутствует не только российское право, но и международное, а ученые правоведы всего мира озабочены скорейшим разрешением правовых проблем в Интернет, Россия имеет возможность внести свой большой вклад в формирование международной политики становления информационного права в международном масштабе. Российские ученые имеют большой задел в этой области, который можно было бы предложить международному сообществу. Естественно, если мы, как всегда, не отстанем в этой области. А такое отставание вполне возможно, если учесть сегодняшнее отношение государства к этим вопросам (как известно, в России нет четко сформированной государственной политики перехода к информационному обществу и формирования информационного права; Миннауки России только что исключило информационное право из блока юридических наук номенклатуры научных специальностей, а Государственная Дума РФ 3-го созыва выделила вопросы связи из ведения Комитета по информационной политики и связи Государственной Думы 2-го созыва (новый комитет называется Комитет по информационной политике, а вопросы связи переведены в один из комитетов по промышленности). И это на фоне мощнейшей интеграции корпораций Интернет и СМИ в США.

**Основные положения федерального закона**

**«ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ**

**И О ЗАЩИТЕ ИНФОРМАЦИИ»**

В законе используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

**Политика конфиденциальности (на примере компании Internet Projects, информационный канал Subscribe)**

Политика конфиденциальности компании состоит из следующих мер:

* Сбор личных сведений
* Использование личных сведений
* Разглашение личных сведений и передача этих сведений третьим лицам
* Доступ к личным сведениям
* Обеспечение безопасности личных сведений
* Использование файлов «cookie»
* Изменения в заявлении о соблюдении конфиденциальности

**Политика конфиденциальности**

Компания «Интернет-проекты» уделяет большое внимание защите конфиденциальности личных данных пользователей. Посетители могут просматривать большинство страниц узла, не сообщая о себе никакой информации. Однако для предоставления некоторых услуг компании могут потребоваться личные сведения пользователей. Компания предлагает вниманию пользователей принципы соблюдения конфиденциальности, объясняющие, каким образом осуществляется сбор и использование данных, которые сообщаются посетителями веб-узла в этих случаях. Данное заявление о соблюдении конфиденциальности относится только к сервисам, предоставляемым компанией «Интернет-проекты» в рамках веб-узлов [Subscribe.ru](http://subscribe.ru), [CityCat.ru](http://www.citycat.ru) и [Voxru.Net](http://voxru.net) (далее "Сервисы").

**Сбор личных сведений**

Компания ставит пользователей своих сервисов в известность, если ей требуется получить информацию, которая позволяет установить их личность (личные сведения), или их контактные данные. Обычно эти данные запрашиваются при подписке на информационные бюллетени, рассылаемые по электронной почте, регистрации для участия в мероприятиях, конкурсах, получении доступа к специальным тематическим разделам веб-узла с ограниченным доступом, а также при заказе и регистрации платных сервисов компании. Как правило, личные сведения, которые пользователям Сервисов требуется сообщить о себе, ограничиваются лишь адресом электронной почты, однако в некоторых случаях для получения тех или иных услуг необходимо будет предоставить и дополнительную информацию.

Например, если посетитель веб-узла захочет приобрести некоторый продукт или услугу, ему будет предложено сообщить сведения, необходимые для оплаты и предоставления доступа к выбранной им услуге или продукту, а именно: свои фамилию, имя, отчество, адрес, номер телефона и другие данные, необходимые для выполнения заказа.

Когда пользователь регистрирует подписку на информационные бюллетени, ему может быть предложено заполнить электронную анкету с расширенным перечнем вопросов, таким как пол, возраст, сфера занятости, уровень дохода, географическое положение, интересы и прочее. При этом регистрационные данные добавляются в файл, содержащий любые другие сведения, предоставленные пользователем при предыдущих посещениях данного веб-узла.

На веб-узлах компании осуществляется также сбор некоторых сведений об используемом компьютерном оборудовании и программном обеспечении. Информация такого рода может включать в себя IP-адрес пользователя, имя домена, сведения об операционной системе, типе обозревателя, количестве предыдущих посещений и веб-узле, с которого пользователь осуществил переход на данный веб-узел. Данная информация используется при реализации процесса предоставления соответствующих услуг в целях повышения их качества, а также для подготовки обобщенных статистических данных, характеризующих использование веб-узлов компании «Интернет-проекты».

На веб-узлах компании осуществляется также сбор сведений о том, какие именно страницы данного узла посещаются пользователями Сервисов. Эти сведения определяются только по уникальному ID-коду и никогда не связываются c личными данными пользователя, если на то нет его согласия.

**Использование личных сведений**

Личные сведения посетителей веб-узла помогают компании в решении следующих задач:

- обеспечение наиболее полного удовлетворения потребностей посетителей;

- предоставление широкого спектра услуг, таких как подписка на информационные бюллетени, рассылка сообщений о событиях, интерактивное обучение, заказ товаров и услуг пользователями;

- подготовка и публикация наиболее интересных для посетителей веб-узла материалов;

- оперативное оповещение об обновлениях продуктов, специальных предложениях, обновлении информации и других новых услугах, предоставляемых компанией "Интернет-проекты" по запросу пользователей;

- предоставление доступа к сервисам, к которым допуск пользователей ограничен;

- сведения, полученные от посетителей веб-узла, будут объединяться с анонимной демографической информацией. На этой основе могут проводиться исследования, обобщенные результаты которых позволят более точно подбирать материалы, размещаемые на веб-узле. В некоторых разделах веб-узлов Сервисов, доступ к которым ограничен, информация, полученная от посетителей этих разделов, будет с согласия последних объединяться с их личными сведениями, что позволит предоставлять в распоряжение посетителей веб-узла материалы с учетом их личных предпочтений. Если посетитель не согласится с этим предложением, его личные сведения не будут объединяться с данными о посещении веб-узла, и предоставляемые ему услуги не будут носить индивидуальный характер.

Время от времени компания привлекает другие компании для предоставления отдельных услуг (упаковка, рассылка и доставка покупок, консультирование заказчиков о продуктах и услугах, рассылка почтовых сообщений, обработка регистрируемых событий и т.д.) от имени компании "Интернет-проекты". Компания предоставляет этим компаниям только ту информацию, которая необходима для выполнения возложенных на них задач, и запрещает использовать личные сведения клиентов в каких-либо иных целях.

**Разглашение личных сведений и передача этих сведений третьим лицам**

Личные сведения пользователей могут быть разглашены компанией «Интернет-проекты» только в том случае, если этого требует закон или если есть твердая уверенность в том, что это необходимо для:

(а) обеспечения соответствия предписаниям закона или требованиям судебного процесса в отношении компании «Интернет-проекты» или ее Сервисов;

(б) защиты прав или собственности компании «Интернет-проекты» или ее Сервисов;

(в) принятия срочных мер по обеспечению личной безопасности сотрудников компании «Интернет-проекты», пользователей ее Сервисов или потребителей предоставляемых ею услуг, а также обеспечению общественной безопасности.

Личные сведения, полученные в распоряжение компании «Интернет-проекты» при регистрации или каким-либо иным образом, не будут без разрешения пользователей передаваться третьим организациям и лицам, за исключением тех немногих случаев, перечень которых уже приводился. Эти сведения не будут использоваться в каких-либо иных целях, кроме перечисленных выше.

[Регистрация](http://subscribe.ru/member/join?) также предоставляет пользователю возможность определить, каким образом он будет пользоваться Сервисами (или же отказаться от этой возможности). После регистрации пользователь посещает [Центр подписки](http://subscribe.ru/member/) и указывает свои предпочтения в анкете. Здесь он может определить, какую информацию хотел бы получать, и указать способ ее получения. Пользователь также может отказаться поддерживать в будущем какие-либо контакты с компанией «Интернет-проекты», для чего следует снять флажки с соответствующих параметров, определяющих порядок связи с компанией.

Иногда компания «Интернет-проекты» разрешает другим компаниям размещать сведения об их продуктах и услугах в бюллетенях, рассылаемым пользователям Сервисов. При этом рассылка может осуществляться только по каналам электронной почты. Если пользователь не хочет получать данную информацию, он снимите соответствующие флажки в анкете [Центра подписки](http://subscribe.ru/member/).

От компании «Интернет-проекты» могут периодически присылаться сообщения электронной почты с информацией о проблемах безопасности или технической поддержки, связанных с продуктом или службой, интересующей пользователя. Данные сообщения могут также содержать подтверждение принятия сделанного пользователем заказа на тот или иной продукт или услугу. Возможность отказа от подписки на эти почтовые сообщения не предусмотрена, поскольку они рассматриваются в качестве важной части предоставляемой пользователю услуги.

**Доступ к личным сведениям**

Посетителям веб-узлов компании предоставляются средства, которые позволяют им проверять точность указанных личных сведений и производить их обновление в случае необходимости.

Пользователи, зарегистрированные на веб-узле Subscribe.ru или подписавшиеся на информационные бюллетени, могут просматривать и редактировать свои личные сведения в Центре подписки. При этом предварительно, прежде чем они смогут получить доступ к личным сведениям, им будет предложено ввести свой адрес электронной почты и пароль.   
  
В Центре подписки пользователь может:

- просмотреть и отредактировать личные сведения, уже представленные ранее при посещении веб-узла Subscribe.ru;

- сообщить, желает ли он, чтобы с веб-узла Subscribe.ru ему присылалась рекламная и маркетинговая информация;

- указать, желает ли он, чтобы другие компании могли присылать ему по почте свои предложения. оформить или отменить подписку на бюллетени с информацией о продуктах и услугах компании «Интернет-проекты» и ее партнеров.

Некоторые Сервисы могут осуществлять сбор информации, доступ к которой не может быть получен через Центр подписки. Однако в таких случаях пользователь все же может получить доступ к своим личным сведениям, обратившись для этого на веб-узел Subscribe.ru, как описывается в нижней части настоящего заявления, или же воспользовавшись альтернативными средствами доступа, предоставляемыми данной службой.

**Обеспечение безопасности личных сведений**

Компания «Интернет-проекты» уделяется большое внимание обеспечению безопасности личных данных пользователей. Здесь применяются самые разнообразные технологии и процедуры, помогающие защитить личные сведения от несанкционированного доступа, использования и разглашения. Так, например, хранение предоставленных пользователями личных данных осуществляется на серверах с ограниченным доступом, расположенных в охраняемых помещениях. При передаче секретной информации (например, номера кредитной карты) через Интернет она защищается посредством специальных методов шифрования, например, с помощью протокола SSL (Secure Socket Layer).

**Использование файлов «cookie»**

Когда пользователь посещает веб-узел, на его компьютер записывается файл «cookie» (если пользователь разрешает прием таких файлов). Если же пользователь уже посещал данный веб-узел, файл «cookie» считывается с компьютера. Одно из направлений использования файлов «cookie» связано с тем, что с их помощью облегчается сбор статистики посещения, о которой говорилось выше.

Файлы «cookie» могут использоваться также для сбора сведений о том, какие ссылки в информационных бюллетенях выбираются посетителями. Эти сведения помогают определять, какая информация, отправляемая заказчикам, может представлять для них наибольший интерес. Сбор этих данных осуществляется в обобщенном виде и никогда не соотносится с личными сведениями пользователей.

Отключив в обозревателе прием файлов «cookie»с узлов компании «Интернет-проекты», пользователь сможет просматривать текст на веб-страницах, однако возможности индивидуальной настройки и подписки на Службы веб-узла будут ему недоступны.

**Изменения в заявлении о соблюдении конфиденциальности**

Заявление о соблюдении конфиденциальности на веб-узле Subscribe.ru предполагается периодически обновлять. При этом будет изменяться дата предыдущего обновления, указанная в начале документа. Сообщения об изменениях в данном заявлении будут размещаться на видном месте данного веб-узла.

**Правовые аспекты защиты информации**

Защита информации в правовом смысле означает комплекс мер законодательного и правоприменительного характера, связанных со следующими действиями:

- отражение положений, в соответствии с которыми осуществляется защита информации во внутренней документации организации (локальные нормативные акты, такие как: должностные инструкции, положение о защите персональных данных сотрудников, положение о коммерческой тайне и проч.);

- отражение в документации с контрагентами предприятия положений, в соответствии с которыми осуществляется определенная совокупность мер, направленных на защиту информации (разделы в договорах с контрагентами - «гарантии», «ответственность»);

- защита информации на уровне отношений со штатными сотрудниками организации - (трудовой договор, коллективный договор);

- на законодательном уровне: конкретные правовые нормы, обеспечивающие сохранение определенных групп информации в каком-либо режиме.

**Внутрикорпоративная документация** – как правило, положения о защите информации содержатся в должностных инструкциях сотрудников со следующими оговорками:

- «обязуется соблюдать требования организации в отношении защиты персональных данных работников»;

- «обязуется предпринимать меры по неразглашению конфиденциальной информации и информации, составляющей коммерческую тайну компании»;

Указанные оговорки сопровождаются отсылкой на соответствующие положения, утвержденные в компании.

Положения о защите информации также могут содержаться в положении о защите персональных данных работников (Приложение №1 к настоящей работе).

**Положения о защите информации, содержащиеся в договорах с контрагентами.**

Формулировки могут быть следующими:

«Условия настоящего Договора, касающиеся пределов права использования Фильма, Элементов Фильма и Рабочих материалов Фильма, переданного Продюсером Телекомпании по настоящему Договору, размера и порядка оплаты вознаграждения, а также иная информация и документы, предоставляемые Сторонами друг другу в ходе исполнения Договора, являются конфиденциальной информацией и подлежат разглашению Продюсером третьим лицам в течение периода производства Фильма и в течение 3 (Трех) лет с даты сдачи Телекомпании Комплекта поставки Фильма по настоящему Договору только после получения предварительного письменного согласия Телекомпании, а также в случаях, прямо предусмотренных действующим законодательством Российской Федерации».

«1.1. Условия Договора, касающиеся объема и перечня прав на Фильм, Синопсиса Фильма, Литературного и Режиссерского сценариев, Постановочного проекта, порядка выплаты вознаграждения, а также любая информация, касающаяся Элементов Фильма, Ноу-хау, Рабочих материалов Фильма, и не являющаяся общеизвестными сведениями («Общеизвестные сведения»), является конфиденциальной информацией («Конфиденциальная информация») и не подлежит разглашению Исполнителем в течение срока действия Договора и в течение 10 (Десяти) лет после его окончания, а в отношении Ноу-хау в течение всего срока охраны соответствующих объектов.

1.2. Под Общеизвестными сведениями понимаются сведения известные широкой общественности и/или сведения, ставшие известными широкой общественности в результате действий Заказчика.

1.3. Исполнитель вправе раскрывать Конфиденциальную информацию третьим лицам только:

1.3.1. при получении предварительного письменного согласия Заказчика;

1.3.2. в случаях, прямо предусмотренных законодательством РФ, с обязательным незамедлительным письменным уведомлением Заказчика о раскрытии Конфиденциальной информации и причинах ее раскрытия с приложением копий соответствующих документов (запросы полномочных органов государственной власти);

1.3.3. работникам Исполнителя, в т.ч. по гражданско-правовым договорам, правообладателям охраняемых результатов интеллектуальной деятельности и средств индивидуализации, чьи объекты использованы в Фильме, и/или привлеченным третьим лицам для производства Фильма в оправданном объеме и при условии заключения с ними соглашений о не разглашении Конфиденциальной информации, при этом Исполнитель несет ответственность перед Заказчиком за соблюдение вышеназванными лицами требований к Конфиденциальной информации;

1.4. Исполнитель обязан по письменному требованию Заказчика передать Заказчику и/или уничтожить все документы и материалы, содержащие Конфиденциальную информацию (и предоставить акт об уничтожении – в последнем случае).»

«В случае нарушения Исполнителем и/или лицами, указанными в п. 11.3.3. Договора, требований настоящего раздела Договора, Заказчик имеет право на пресечение соответствующих нарушений и/или применение мер ответственности к Исполнителю и/или лицу, указанному в п.1.3.3. Договора».

«Все условия настоящего Договора являются конфиденциальными.

Каждая из Сторон примет все необходимые меры для того, чтобы предотвратить ознакомление с настоящим Договором третьих лиц без согласия другой Стороны.

По требованию уполномоченных государственных органов (правоохранительные, налоговые органы и т.п.), а также акционеров, адвокатов, аудиторов, уполномоченных банков и иных уполномоченных Сторонами лиц, каждая из Сторон может их ознакомить с содержанием настоящего Договора без предварительного согласия другой Стороны, требуя при этом от таких лиц соблюдения конфиденциальности информации.

В случае нарушения одной из Сторон требований, предусмотренных настоящим пунктом, другая Сторона будет нести ответственность за причиненные другой Стороне убытки».

**Ответственность за нарушение законодательства о защите информации**

**Гражданско-правовая ответственность**

Статья 727. Конфиденциальность полученной сторонами информации

Если сторона благодаря исполнению своего обязательства по договору подряда получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, которые могут рассматриваться как коммерческая тайна (статья 139), сторона, получившая такую информацию, не вправе сообщать ее третьим лицам без согласия другой стороны.

Порядок и условия пользования такой информацией определяются соглашением сторон.

Статья 732. Предоставление заказчику информации о предлагаемой работе

1. Подрядчик обязан до заключения договора бытового подряда предоставить заказчику необходимую и достоверную информацию о предлагаемой работе, ее видах и об особенностях, о цене и форме оплаты, а также сообщить заказчику по его просьбе другие относящиеся к договору и соответствующей работе сведения. Если по характеру работы это имеет значение, подрядчик должен указать заказчику конкретное лицо, которое будет ее выполнять.

2. Если заказчику не предоставлена возможность незамедлительно получить в месте заключения договора бытового подряда информацию о работе, указанную в пункте 1 настоящей статьи, он вправе потребовать от подрядчика возмещения убытков, вызванных необоснованным уклонением от заключения договора (пункт 4 статьи 445).

Заказчик вправе требовать расторжения заключенного договора бытового подряда без оплаты выполненной работы, а также возмещения убытков в случаях, когда вследствие неполноты или недостоверности полученной от подрядчика информации был заключен договор на выполнение работы, не обладающей свойствами, которые имел в виду заказчик.

Подрядчик, не предоставивший заказчику информации о работе, указанной в пункте 1 настоящей статьи, несет ответственность и за те недостатки работы, которые возникли после ее передачи заказчику вследствие отсутствия у него такой информации.

Статья 771. Конфиденциальность сведений, составляющих предмет договора

1. Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре.

2. Каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.

Статья 946. Тайна страхования

Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса.

Статья 857. Банковская тайна

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

**Административная ответственность**

Статья 5.39. Отказ в предоставлении гражданину информации

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации -

влечет наложение административного штрафа на должностных лиц в размере от пятисот до одной тысячи рублей.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) -

влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -

влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), -

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, -

влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, -

влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц - от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -

влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от одной тысячи до одной тысячи пятисот рублей; на юридических лиц - от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

5. Осуществление лицензируемой деятельности с нарушением (в том числе с грубым нарушением) указанных лицензионных требований и условий влечет за собой ответственность, установленную законодательством Российской Федерации. При этом под грубым нарушением лицензионных требований и условий понимается невыполнение лицензиатом требований и условий, предусмотренных подпунктами "а", "в", "г" пункта 3 и подпунктами "б", "и", "к" пункта 4 настоящего Положения.

а) наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;

в) выполнение требований конструкторской, программной и технологической документации, единой системы измерений, системы разработки и запуска в производство средств защиты конфиденциальной информации, а также иных нормативных правовых актов Российской Федерации в области технической защиты информации;

г) соответствие помещений, производственного, испытательного и контрольно-измерительного оборудования, предназначенных для осуществления лицензируемой деятельности, техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации;

б) выполнение лицензиатом режима конфиденциальности при обращении со сведениями, которые ему доверены или стали известны в ходе служебной деятельности: обеспечение ограничения круга лиц, допущенных к конфиденциальной информации, установление порядка допуска лиц к работам, связанным с использованием конфиденциальной информации, организация обеспечения безопасности ее хранения, обработки и передачи по каналам связи и выполнение установленных обладателем конфиденциальной информации требований к обеспечению безопасности этой информации;

и) наличие у руководителя соискателя лицензии (лицензиата) и (или) уполномоченного им лица документа о высшем профессиональном образовании в области технической защиты информации либо документов о высшем или среднем профессиональном (техническом) образовании и о переподготовке или повышении квалификации по вопросам технической защиты информации, а также производственного стажа в области лицензируемой деятельности не менее 5 лет;

к) наличие у инженерно-технического персонала, осуществляющего работы в области лицензируемой деятельности, документа о высшем образовании или профессиональной подготовке со специализацией, соответствующей выполняемым работам.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), -

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии -

влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц - от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, -

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей.

Статья 23.46. Органы, осуществляющие государственный контроль в области обращения и защиты информации

1. Органы, осуществляющие государственный контроль в области обращения и защиты информации, рассматривают дела об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.5, статьей 13.6, частями 1 и 2 статьи 13.12, частью 1 статьи 13.13, статьями 13.17, 13.22, 20.23, 20.24 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1) утратил силу. - Федеральный закон от 30.06.2003 N 86-ФЗ;

2) руководитель федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители - об административных правонарушениях, предусмотренных статьей 13.6, частями 1 и 2 статьи 13.12, частью 1 статьи 13.13 настоящего Кодекса;

3) руководитель федерального органа исполнительной власти, уполномоченного в области безопасности Российской Федерации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители - об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.5, статьей 13.6, частями 1 и 2 статьи 13.12, частью 1 статьи 13.13, статьями 13.17, 20.23, 20.24 настоящего Кодекса;

4) руководитель федерального органа исполнительной власти, уполномоченного в области печати и средств массовой информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители - об административных правонарушениях, предусмотренных статьями 13.17, 13.22 настоящего Кодекса;

5) руководитель федерального органа исполнительной власти, уполномоченного в области телевидения и радиовещания, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители - об административных правонарушениях, предусмотренных статьями 13.17, 13.22 настоящего Кодекса.

**Уголовная ответственность**

Статья 140. Отказ в предоставлении гражданину информации

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, -

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом -

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -

наказываются лишением свободы на срок до десяти лет.

**Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок до четырех лет.

**ЗАКЛЮЧЕНИЕ**

Исследовав основополагающие нормы законодательства в области защиты информации, автор пришел к следующим выводам:

1. Защита информации – законодательно урегулированное понятие.
2. Меры по обеспечению защиты информации относятся к компетенции участников рыночных отношений – субъектов.
3. Защита информации – комплексный процесс, включающий в себя совокупность мер, изложенных, в том числе в политике конфиденциальности компании.
4. Оговорки в договорах между субъектами могут быть совершенно различны, в том числе стороны могут на законных условиях устанавливать ответственность для себя.

**ОСНОВНАЯ ЛИТЕРАТУРА**

1. Федеральный закон об информации, информационных технологиях и о защите информации.
2. Гражданский кодекс РФ.
3. Кодекс об административных правонарушениях.
4. Уголовный кодекс РФ.
5. Труды по интеллектуальной собственности. Т.2. Актуальные проблемы информационного права. 2008г.
6. Бюллетень "Труды по интеллектуальной собственности" // Кафедра ЮНЕСКО по авторскому праву и другим отраслям права интеллектуальной собственности, Федотов М.А., 2009г.