СОДЕРЖАНИЕ

Семинар № 9 Правовые средства защиты государственной, служебной и коммерческой тайны

План

1. Понятие государственной тайны и методы ее защиты.

2. Сведения, относимые к государственной тайне.

3. Допуск к государственной тайне.

4. Понятие служебной и коммерческой тайны.

5. Понятие информации. Засекречивание информации.

Практические задания

I. Тесты

1. Перечень сведений отнесенных к государственной тайне утверждается

1. Президентом РФ
2. Председателем Правительства РФ
3. Директором Федеральной службы безопасности
4. руководителем организации

2. Перечень сведений, составляющих коммерческую тайну, утверждается

1. Президентом РФ
2. Председателем Правительства РФ
3. Директором Федеральной службы безопасности
4. руководителем организации

3. Закон "Об авторском праве и смежных правах" защищает права

1. исполнителей (актеров, певцов и т.д.)
2. производителей фонограмм
3. организации эфирного и кабельного вещания
4. всех лиц, перечисленных в остальных пунктах

4. Какой законодательный акт содержит сведения по защите коммерческой тайны?

1. Закон "Об авторском праве и смежных правах"
2. Закон "О коммерческой тайне"
3. Патентный закон
4. Закон "О правовой охране программ для ЭВМ и баз данных"

5. К информации ограниченного доступа не относится

1. государственная тайна
2. размер золотого запаса страны
3. персональные данные
4. коммерческая тайна

II. Задачи

В одной из газет появилось сообщение о том, что популярный телеведущий получил ссуду в размере 1 млн 200 тыс. рублей на строительство. Он открыл депозитный счет в одном из отделений коммерческого банка. После публикации данного материала в районный суд поступило исковое заявление от телеведущего к коммерческому банку о возмещении морального вреда и о разглашении коммерческой тайны.

Проанализируйте ситуацию с позиции нарушений законодательства.

Разберите ситуацию. Подлежат ли ответственности банк и газета?

Был ли нарушен редакцией газеты закон «О средствах массовой информации», а банком ГК РФ – закон «О банках и банковской деятельности»?

ГК РФ 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](https://www.consultant.ru/document/cons_doc_LAW_359091/d4984b968b67d38939333aa51c71bcb189047fbb/#dst100124). Государственным органам и их должностным лицам, а также иным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены [законом](https://www.consultant.ru/document/cons_doc_LAW_372893/5583e2cafb06542e33c725aa32666e8ab89b1cdc/#dst100524).

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

Согласно этой статье банк нарушил закон и выдал газете данные о размере банковского вклада. Банк разгласил эти сведения и клиент вправе потребовать возмещения причиненных убытков от банка

Согласно [закону РФ "О средствах массовой информации"](https://www.consultant.ru/document/cons_doc_LAW_1511/) в статье 49 Обязанности журналиста сказано, что журналист обязан:  получать согласие (за исключением случаев, когда это необходимо для защиты общественных интересов) на распространение в средстве массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей;

В статье 24 Конституции РФ закреплено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Согласно Федеральному закону «О персональных данных» обработка персональных данных, в том числе и сведений о частной жизни лица, включая их сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, может осуществляться только с согласия субъекта персональных данных.

Таким образом не получив согласие от популярного телеведущего на распространение данных газета нарушает вышеприведенные статьи.

III. Темы докладов

1. Юридическая ответственность за разглашение охраняемой законом информации.

Согласно ФЗ «Об информации, информационных технологиях и защите информации» понятие «конфиденциальная информация» характеризируется, как сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их правообладателя.

За разглашение конфиденциальной информации, утрату носителей конфиденциальной информации и нанесение вследствие этих действий ущерба предприятию (работодателю) виновные лица привлекаются к дисциплинарной, материальной, административной или уголовной ответственности.

Перечень сведений, составляющих государственную тайну указан в ст. 5 Закона РФ «О государственной тайне». В основном к ним относятся определенные сведения из военной области, области экономики, науки и техники, внешней политики и экономики, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Работник за разглашение конфиденциальной информации (при отсутствии в действиях такого работника состава преступления) несет дисциплинарную ответственность. Кроме того, в соответствии со ст.238 ТК РФ с сотрудника может быть взыскан прямой действительный ущерб, например стоимость носителя информации. Трудовой кодекс помимо включения в трудовой договор условия о неразглашении охраняемой законом тайны предусматривает возможность увольнения работника за разглашение государственной, коммерческой, служебной или иной тайны. Кроме того, ст. 243 ТК РФ устанавливает полную материальную ответственность работника за разглашение сведений, составляющих служебную, коммерческую или иную охраняемую законом тайну в случаях, предусмотренных федеральным законом. Доказать величину убытков достаточно сложно. И стоимость самой утраченной конфиденциальной информации, и размер упущенной выгоды являются величиной достаточно условной. Кроме того, рассматривая претензии организаций к работникам, суды часто встают на сторону персонала. Возможно и уголовное преследование лиц, разгласивших конфиденциальную информацию. Однако взысканные штрафы будут направлены в бюджет, а пострадавшая организация может рассчитывать только на моральное удовлетворение.

1. Проблемы правового регулирования Интернета.

Отсутствие нормативных правовых актов, регулирующих непосредственно отношения в сети Интернет, как и возможность их эффективного применения, уже сейчас оказывает негативное влияние на развитие общественных отношений (например, в области авторских прав, персональных данных, интернет-торговли, информационной безопасности и др.).

Основными проблемами в сети Интернет, нуждающимися в скорейшем нормативно-правовом урегулировании, являются:

1. Распространение экстремистских материалов в сети Интернет.

2. Проблемы, связанные с защитой прав интеллектуальной собственности в сети Интернет.

3. Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

4. Защита персональных данных.

5. Правовое регулирование электронной торговли в сети Интернет.

6. Пропаганда, незаконная реклама наркотических средств и психотропных веществ.

7. Незаконное распространение порнографических материалов в сети Интернет.

8. Клевета в сети Интернет.

9. Мошенничество в сети Интернет

Распространение экстремистских материалов в сети Интернет.

Сеть Интернет предоставляет членам экстремистских движений и групп возможность отстаивать и пропагандировать свою идеологию в информационных ресурсах интернета, где сосредоточено огромное количество пользователей. Особенно легко воздействию данной проблемы подвергаются подростки. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» устанавливает недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности (ст. 12), ответственность за распространение экстремистских материалов (ст. 13). Для решения данной проблемы необходимо усовершенствовать нормативно-правовую базу, разграничить компетенции правоохранительных органов в сфере борьбы с терроризмом и экстремизмом в сети Интернет, ужесточить меры наказания за совершение преступлений данного характера.

Проблемы, связанные с защитой прав интеллектуальной.

Нелегальное распространение фильмов, телепередач и иных видеороликов, а также музыкальных произведений, книг и программных продуктов в сети Интернет достигает гигантских масштабов, так как сеть Интернет предоставляет достаточно возможностей для фактически бесконтрольного воспроизведения и распространения таких объектов.  За нарушение авторских и смежных прав, а также изобретательских и патентных прав предусматривается гражданско-правовая, административная и уголовная ответственность. Согласно Гражданскому кодексу РФ защита исключительных прав осуществляется в соответствии со ст. 1252, в ст. 1253.1 говорится, что «информационный посредник несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных настоящим Кодексом, при наличии вины с учетом особенностей, установленных пунктами 2 и 3 настоящей статьи». В Уголовном кодексе — ст. 146, 147. Данному вопросу посвящена также ст. 15.2 Федерального закона «Об информации, информационных технологиях и о защите информации», где рассматривается порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав.

Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

Вопросы, связанные с правовым регулированием исключительных прав на сетевой адрес, приобретают всё более широкие границы. На данный момент судебные споры, касающиеся доменных имен, являются наиболее частыми в судебной практике, особенно в странах Запада. Возможность свободного выбора доменного имени породило противоправное явление - кибер-сквоттинг, означающее регистрацию доменных имен, совпадающих или сходных со средствами индивидуализации, с их последующим недобросовестным использованием как для собственных коммерческих целей, так и с целью предложения к продаже самим правообладателям средств индивидуализации. Далеко не всегда в этом случае владельцы товарных знаков добивались защиты своих прав и устранения нарушений. Суд отказывал правообладателю в защите прав со ссылкой на отсутствие законодательного регулирования отношений, связанных с наименованием доменов в сети Интернет, а также на то, что доменное имя не является ни товаром, ни услугой, поэтому не подпадает под действие Закона «О товарных знаках».

Защита персональных данных в сети Интернет.

Недостаточное обеспечение защиты персональных данных субъектов РФ является одной из распространенных проблем в виртуальной среде российского сегмента сети Интернет. Федеральный закон «О персональных данных» не решает большинства юридических проблем, даже дополнение Федерального закона «Об информации, информационных технологиях и о защите информации» [8] статьей 15.5, в которой указывается порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, оставляет данный вопрос открытым и актуальным.

Правовое регулирование электронной торговли в сети Интернет.

К проблематичным вопросам в сфере электронной торговли в интернете относятся вопросы заключения контрактов посредством сети Интернет, вопросы недобросовестной рекламы, спама, проблема налогообложения предпринимательства в сети Интернет. Крайне важной в интернет-праве является в настоящее время проблема ответственности за качество информации, предоставляемой продавцом в рамках электронной торговли. Практика показывает, что приобретение товаров через сеть Интернет сопряжено со многими возможными конфликтными ситуациями, которые следует учитывать как продавцам, так и покупателям, т.е. всем субъектам (участникам) отношений в сети Интернет.

Есть проблемы, связанные с деятельностью коммерческих онлайновых компаний. Эти проблемы можно подразделить на следующие:

1) регулирование содержания (вредное и незаконное);

2) соблюдение авторских и смежных прав в условиях технически легкого копирования любой информации, представленной в цифровом виде;

3) вопросы формирования киберэкономики (электронные деньги, реклама, маркетинг, электронные публикации, электронные контракты, налог на передачу информации);

4) информационная безопасность, понимаемая в широком смысле как безопасность жизненно важных для общества систем управления: транспортом, войсками, хозяйством крупных городов и т.п.

Незаконное распространение порнографических материалов в сети Интернет.

Отметим, что эротическая и порнографическая продукция в большинстве стран мира не запрещена, а ограничена. Данные ограничения касаются:

1) времени публичного показа данной продукции;

2) места ее расположения;

3) вовлечения несовершеннолетних.

Основная цель введения этих ограничений — сделать эротические и порнографические материалы недоступными для несовершеннолетних, так как данный вид продукции оказывает травмирующее воздействие на психику подростков (ст. 5 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Клевета в сети Интернет.

В сети Интернет имеется возможность, которая позволяет распространять информацию, дискредитирующую граждан, субъекты отношений в сети Интернет, сохраняя при этом анонимность.

Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети Интернет, гражданин вправе требовать удаления соответствующей информации, а также опровержения указанных сведений способом, обеспечивающим доведение опровержения до пользователей сети Интернет (ч. 5 ст. 152 Гражданского кодекса РФ). По Уголовному кодексу РФ в соответствии с ч. 2 ст. 128.1 клевета наказывается штрафом.

Мошенничество в сети Интернет.

Мошенничество в соответствии со ст. 159 Уголовного кодекса РФ — «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». На данный момент существует огромное количество различных видов мошенничества в сети Интернет, следует учитывать и то, что с течением времени появляются все новые виды мошенничества. [3]

Выделим те из них, которым наиболее часто подвергаются пользователи Сети:

* Интернет-попрошайничество — один из наиболее известных видов мошенничества в Сети, которое выражается в просьбе пожертвовать некоторую сумму денежных средств под различными предлогами, например от имени благотворительных фондов;
* Сайты-подделки — внешне не отличаются от оригинальных сайтов. Однако сайты-подделки популярных социальных сетей создаются с целью выманивания денежных средств или взлома аккаунтов, с последующей рассылкой писем, содержащих ссылки на вредоносные программы - спама;
* Программы-блокеры — созданы для проникновения в систему и блокирования доступа к ней. Для разблокировки системы пользователю требуется, как пример, отправить платное sms-сообщение;
* Фишинг является также одним из наиболее распространенных видов мошенничества, его целью является получение доступа к конфиденциальным данным пользователей (логинам и паролям). Осуществляется данный вид интернет-мошенничества путем проведения массовых рассылок электронных писем от известных пользователю представителей.

Решение данных проблем, несомненно, требует правового государственного регулирования, а также межгосударственного сотрудничества в борьбе с сетевой преступностью, терроризмом и экстремизмом в сети Интернет. Но большее внимание следует уделить проблеме предупреждения преступлений в сети Интернет. При подключении к сети Интернет пользователь порой не получает никакой информации об устройстве Сети, о мерах защиты данного соединения и тем более о том, какие меры предосторожности стоит соблюдать. Необходимо разработать программы, программные продукты и обеспечение по защите от возможных опасностей, связанных с использованием сети Интернет. В особенности это важно и актуально для тех пользователей сети Интернет, которые только начинают ее осваивать, особое внимание необходимо уделить несовершеннолетним пользователям. Законодательство Российской Федерации отражает постепенное формирование правовой базы регулирования отношений в данной сфере деятельности, однако стремительное развитие информационно-телекоммуникационных технологий, в особенности сети Интернет, не позволяет своевременно обновлять законодательную базу, вносить изменения и дополнения.

1. Связь технических и правовых средств обеспечения информационной безопасности.