

Практическое занятие № 2

Тема «Правовые режимы информации с ограниченным доступом»



МОСКОВСКИЙ
ПОЛИТЕХ

Д.А. Сингилевич
Профессор кафедры
«Государственное управление и право»

Вопросы занятия

1. Персональные данные.
2. Государственная тайна.
3. Режим коммерческой тайны.

Персональные данные



Персональные данные

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.



Правовое регулирование



Правоотношения в сфере персональных данных регулируются федеральным законодательством РФ (Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»), Трудовым кодексом РФ (глава 14), а так же Гражданским кодексом РФ.

Защита персональных данных

- *Защита персональных данных* – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранению и передачи персональных данных граждан.



Комплекс мероприятий по обеспечению защиты персональных данных

Организационные меры по защите персональных данных включают в себя:

- Разработку организационно-распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
- Определение перечня мероприятий по защите персональных данных.



Комплекс мероприятий по обеспечению защиты персональных данных

Технические меры по защите персональных данных предполагают использование программно - аппаратных средств защиты информации. При обработке ПД с использованием средств автоматизации, применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из класса системы персональных данных.



Оператор персональных данных

Оператор персональных данных - государственный орган, муниципальный орган, юр. или физ. лицо, организующие и (или) осуществляющие обработку ПД, а также определяющие цели и содержание обработки ПД.

Закон «О персональных данных» обязывает оператора принимать необходимые организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.



Операторы, обрабатывающие ПД в информационных системах, обязаны обеспечить:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;
- б) своевременное обнаружение фактов несанкционированного доступа к ПД;
- в) недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;
- г) возможность незамедлительного восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- д) постоянный контроль за обеспечением уровня защищенности ПД.

Основные положения Закона «О персональных данных»

- Субъект ПД имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, обжаловав действия или бездействие оператора в уполномоченный орган по защите прав субъектов ПД или в судебном порядке;
- Нарушение требований Закона влечет гражданскую, уголовную, административную, дисциплинарную ответственность физических и должностных лиц.



Требования к информационным системам персональных данных

Требования к обеспечению безопасности персональных данных установлены Постановлением Правительства № 781 от 17.11.2007 г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных». Положение определяет требования по обеспечению безопасности персональных данных при их обработке в информационных системах в соответствии с их классом.

Контроль за выполнением возложен на следующие органы:

- Роскомнадзор – основной надзорный орган в области персональных данных;
- ФСБ – основной надзорный орган в части использования средств шифрования;
- ФСТЭК – надзорный орган в части использования технических средств защиты информации.



На кого распространяется Закон?

В любой компании, вне зависимости от её организационно-правовой формы, есть информация о сотрудниках, работающих в организации, а иногда и её контрагентах. Таким образом такая компания является оператором персональных данных, действия ФЗ-152 распространяются и на неё.



Ответственность

За нарушения законодательных актов РФ, регулирующих правоотношения в сфере ПД предусмотрены следующие санкции:

1. Привлечение к административной и гражданской ответственности
2. Направление в органы прокуратуры материалов о возбуждении уголовных дел
3. Прекращение обработки персональных данных
4. Приостановление деятельности оператора в случае осуществления ее без лицензии
5. Конфискация несертифицированных средств обеспечения безопасности и шифровальных средств

Государственная тайна



Государственная тайна

- Охраняется государством, и составляющие ее сведения относятся к жизненно важным сферам государственной деятельности;
- распространение сведений, образующих государственную тайну может повлечь за собой ущерб безопасности государства;
- распространение указанных сведений недопустимо.

Государственная тайна - это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб внешней безопасности Российской Федерации



Государственная тайна

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Перечень сведений, составляющих государственную тайну, – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.



Режим государственной тайны, определяет и устанавливает:

- информацию, которая относится к государственной тайне, и информацию, которая не может быть отнесена к государственной тайне;
- порядок отнесения информации к государственной тайне (порядок засекречивания сведений, составляющих государственную тайну);
- порядок рассекречивания государственной тайны;
- особый порядок допуска (или доступа) к государственной тайне;
- порядок передачи сведений, составляющих государственную тайну;
- порядок обеспечения защиты государственной тайны;
- ответственность за нарушения режима государственной

Перечень сведений, составляющих государственную тайну

Государственную тайну составляют:

- 1) сведения в военной области;
- 2) сведения в области экономики, науки и техники;
- 3) сведения в области внешней политики и экономики;
- 4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности;



Органы защиты государственной тайны

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Федеральное агентство правительственной связи и информации при Президенте РФ);
- Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.



Допуск должностных лиц и граждан к государственной тайне

1. Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством РФ.

Допуск должностных лиц и граждан к государственной тайне предусматривает их согласие на ограничение их прав, проведение в отношении них проверочных мероприятий, а также предоставление льгот.



Допуск должностных лиц и граждан к государственной тайне

2. Устанавливается три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным.

В соответствии с законом по ряду оснований (ст. 22) должностному лицу или гражданину может быть отказано в допуске к государственной тайне.



Степени секретности сведений

Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности утверждены постановлением Правительства РФ от 4 сентября 1995 г. № 870.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности Российской Федерации и ее территориальными органами во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.

Допуск граждан по третьей форме осуществляется руководителем организации без проведения проверочных мероприятий органами безопасности.



Объективную сторону состава государственной измены

составляют:

- 1) шпионаж;
- 2) выдача государственной тайны;
- 3) иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ.



Огласка сведений, составляющих государственную тайну выражается в:

- а) устном или письменном сообщении кому-либо этих сведений;
- б) демонстрации постороннему лицу документов, материалов или изданий, содержащих государственную тайну;
- в) передаче соответствующих документов, материалов или изданий для перепечатки, копирования, использования в научных целях и т. д.

Разглашение тайны совершается только умышленно, причем умысел может быть прямым или косвенным.

Разглашение может быть совершено как действием, так и бездействием

Разглашение окончено с момента, когда сведения, составляющие государственную тайну, стали известны постороннему лицу



Уголовная ответственность за нарушение режима сохранения государственной тайны

Раздел X. Преступления против государственной власти

Глава 29. Преступления против основ конституционного строя и безопасности государства

ст. 275. Государственная измена - наказывается лишением свободы на срок от 12 до 20 лет

ст. 276. Шпионаж - наказывается лишением свободы на срок от 10 до 12 лет



Уголовная ответственность за нарушение режима сохранения государственной тайны

ст. 283. Разглашение государственной тайны наказывается арестом на срок от 4 до 6 месяцев либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового

ст. 284. Утрата документов, содержащих государственную тайну наказывается ограничением свободы на срок до 3 лет, либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового

Режим коммерческой тайны



Коммерческая тайна

В РФ определение коммерческой тайны дает ст. 139 Гражданского кодекса РФ, и Закон РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004г.

Коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую

выгоду

Критерии охраноспособности коммерческой тайны

Информация составляет служебную или коммерческую тайну в случае:

1. Когда информация имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам;
2. К ней нет доступа на свободном основании;
3. В отношении которой обладателем такой информации введен режим коммерческой тайны .

Только при соблюдении этих трех условий у предпринимателя есть возможность защитить свои права в судебном порядке.

Срок охраны коммерческой тайны не ограничен.



Коммерческая тайна



Не относятся к коммерческой тайне

- разрешительные документы (свидетельство о регистрации, лицензии, сертификаты);
- сведения о численности работающих, заработной плате, условиях труда;
- о задолженности работодателя по заработной плате и иным выплатам;
- сведения о загрязнении окружающей среды, состояния противопожарной безопасности, эпидемиологической обстановке;
- нарушении законодательства РФ и фактах привлечения к ответственности;
- несоблюдении безопасных условий труда;
- сведения о реализации продукции, причиняющей вред здоровью населения и т.д.



Возможные каналы утечки информации

- -публикации в отечественных и международных изданиях;
- -любые формы международного сотрудничества;
- - экспонирование на отечественных и международных выставках, любые формы международного сотрудничества;
- -передача документации и образцов представителям других фирм (в том числе при заключении контракта, если в контракте не оговорены положения о сохранении коммерческой тайны);



Возможные каналы утечки информации

- -участие в конференциях, конгрессах и семинарах;
- -пребывание в лабораториях специалистов других фирм, в том числе стажеров, практикантов и студентов;
- -разглашение коммерческой тайны не информированным сотрудником.
- Если разглашение коммерческой тайны произошло по одному из вышеперечисленных каналов, то защитить свои права предпринимателю будет практически невозможно.



Введение режима охраны коммерческой тайны

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации (установления порядка обращений с этой информацией и контроля за соблюдением порядка);
- 3) учет лиц, получивших доступ к информации;
- 4) регулирование отношений по использованию информации работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители (документы) грифа «Коммерческая тайна» с указанием обладателя этой информации.



Введение режима охраны коммерческой тайны

Обладателем коммерческой тайны является работодатель. Для сохранения режима коммерческой тайны работодатель обязан урегулировать данный аспект отношений с работником.

Для этого необходимо:

- 1) ознакомить под расписку работника с перечнем информации, составляющей коммерческую тайну.
- 2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;



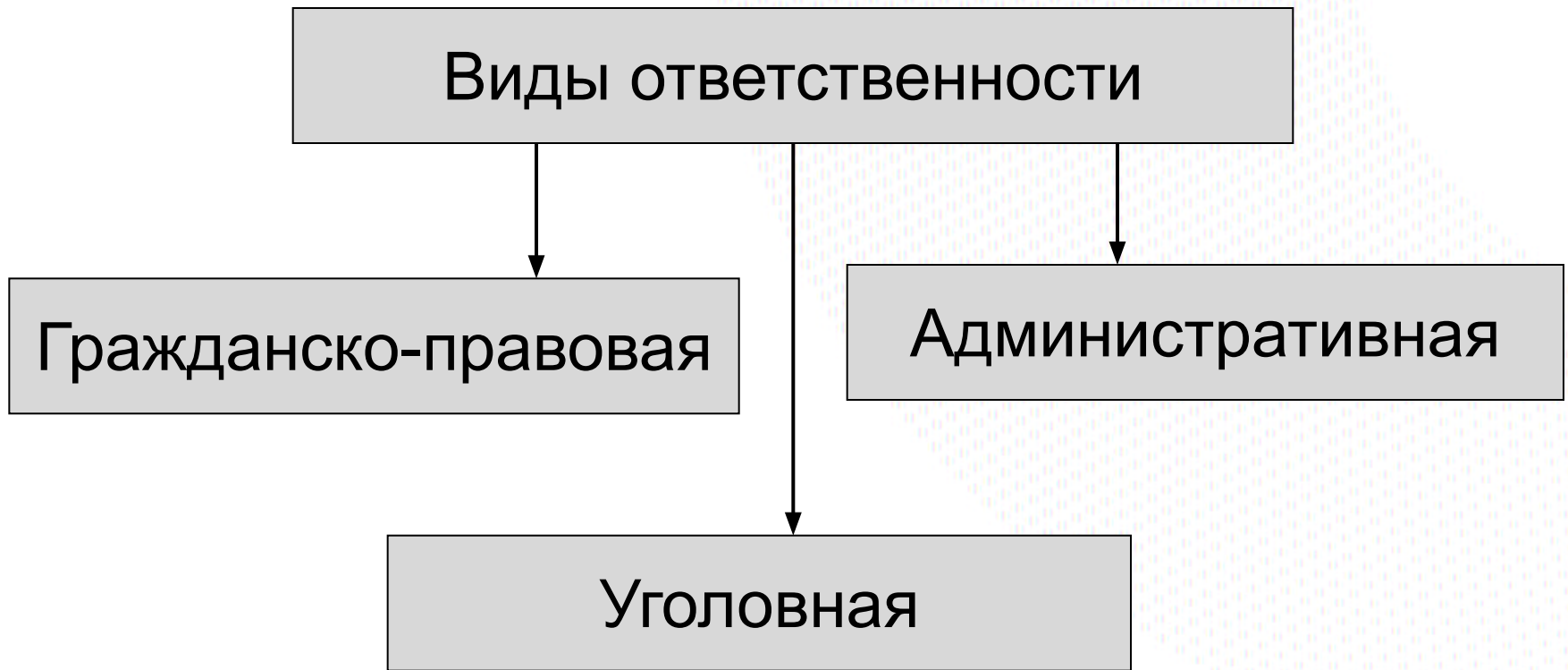
Введение режима охраны коммерческой тайны

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

В свою очередь работник обязан: выполнять режим коммерческой тайны, не разглашать коммерческую тайну, а в случае разглашения возместить причиненный работодателю ущерб.



Ответственность в информационных отношениях



Основания наступления ответственности

- Отказ в доступе к открытой информации;
- Предоставление недостоверной информации;
- Разглашение информации, составляющей коммерческую тайну;
- Распространение ложных и порочащих сведений о конкурентах;
- Необоснованное отнесение информации к категории ограниченного доступа;
- Неисполнение обязанностей по предоставлению информации для формирования государственных информационных фондов



Административный порядок защиты коммерческой тайны

Предусматривает возможность обращения с заявлением в федеральный антимонопольный орган либо его территориальные представительства.

Разглашение коммерческой тайны квалифицируется как **«недобросовестная конкуренция»**.

Согласно Закона РФ «О защите конкуренции» антимонопольный орган имеет возможность вынести обязательное для исполнения предписание об устранении нарушения и применять к нарушителю установленные законом санкции.



Административный порядок защиты коммерческой тайны

Что бы квалифицировать действия как акт недобросовестной конкуренции, необходимо и вполне достаточно квалификации 3 признаков:

1. Действия должны быть направлены на приобретение преимуществ в предпринимательской деятельности.

2. Действия должны противоречить требованиям действующего законодательства, обычаям делового оборота требованиям добропорядочности, разумности и справедливости.

3. Действия должны причинить или быть способными причинить убытки другим хозяйствующим субъектам либо нанести ущерб их деловой репутации.



Судебный порядок защиты коммерческой тайны

Подразумевает обращение с иском о защите нарушенных прав в суд.

Вопрос о коммерческой тайне непосредственно связан с предпринимательской деятельностью, поэтому иски относятся к подведомственности арбитражных судов.

В тех случаях, когда в качестве ответчика выступает работник - дело рассматривается в суде общей юрисдикции.



Судебный порядок защиты коммерческой тайны

Ст. 139 ГК РФ указывает лишь один из них — возмещение причиненных убытков, но допускает применение и других способов. Если нарушение права на коммерческую тайну причиняет ее обладателю убытки, то виновное лицо должно эти убытки возместить.

Убытки должны быть возмещены в полном объеме: компенсации подлежит как реальный ущерб, так и упущенная выгода.



Вопросы для самопроверки

1. Какая область отношений регулируется информационным правом?
2. Почему необходимо правовое регулирование отношений, связанных с информацией?
3. Что является предметом отношений в информационной сфере?
4. Как можно определить понятие информационных ресурсов?
5. Что является объектом правового регулирования в информационном праве?

Рекомендуемая литература

1. Законодательные и нормативные правовые акты

Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». http://www.consultant.ru/document/cons_doc_LAW_82839/

2. Основная

Дорский А.Ю. Правовое регулирование рекламной деятельности и связей с общественностью. Учебник/ А.Ю.Дорский. – Санкт-Петербургский государственный университет, 2019. – 280 с

Шарков, Ф.И. Правовые основы коммуникации: в рекламе, связях с общественностью, журналистике. Учебник/ Ф.И. Шарков, В.И. Захарова. – Москва : Проспект, 2016. – 224 с

3. Дополнительная

Шарков, Ф.И. Коммуникология: коммуникационный консалтинг. Учебное пособие / Ф.И. Шарков. – 2-е изд., стер. – Москва: Дашков и К°, 2020. – 488 с.

**Спасибо
за внимание!**



**МОСКОВСКИЙ
ПОЛИТЕХ**

Д.А. Сингилевич
Профессор кафедры
«Государственное управление и право»