**Организационно-правовое обеспечение Информационной Безопасности.**

# **Лекция 1. Информация – как объект правового регулирования.**

1. Понятие и виды информации
2. Информация категории ограниченного доступа

Статья 2 ФЗ «Об информации…» дает определение информации.

Информация – это сведения (сообщения, данные) независимо от формы их представления.

Существует классификация информации по разным критериям.

1. Виды информации по содержанию
   1. Правовая
   2. Научно-техническая
   3. Политическая
   4. Финансово-экономическая
   5. Статистическая
   6. Стандарты и регламенты
   7. Социальная
   8. Здравоохранение
   9. ЧС
   10. ПД
   11. Кадастры
   12. Лесное, имущественное и другое
2. Информационные ресурсы по способу доступа
   1. Общедоступная информация
   2. Информация ограниченного доступа
      1. Государственная тайна
      2. Коммерческая тайна
      3. Персональные данные
3. Информационные ресурсы по виду носителя
   1. На бумаге
   2. В памяти компьютера
   3. Канал связи
4. Информационные ресурсы по способу формирования и распространения
   1. Стационарные
   2. Передвижные
5. Информационные ресурсы по способу организации хранения и использования
   1. Традиционные формы
   2. Автоматизированные формы (интернет, банк данных)
6. Информация по форме собственности
   1. Общероссийское национальное достояние
   2. Государственная собственность
   3. Частная собственность
   4. Etc.

В соответствии с частью 3 ФЗ «Об информации…». В зависимости от порядка распространения и предоставления. Информация делится на 4 вида:

1. Свободно распространяемая информация
2. Информация, распространение которой в Российской Федерации ограничивается или запрещается
3. Информация, предоставляемая по соглашению лиц
4. Информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению

Статья 7 ФЗ «Об информации…» содержит определение и правовую регламентацию общедоступной информации.

Часть 3 статьи 7. Обладатель информации, ставшей общедоступной по её решению, в праве требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Статья 9 ФЗ «Об информации…» регламентирует ограничение доступа к информации.

Информация ограниченного доступа

1. Государственная тайна (статья 5 закона РФ «О государственной тайне»)
2. Коммерческая тайна (ФЗ «О коммерческой тайне»)
3. Персональные данные (ФЗ «О персональных данных»)
4. Врачебная тайна (статьи 13, 92 ФЗ 2011 года «Об основах охраны здоровья граждан в российской федерации», статья 9 закона РФ «О психиатрической помощи…»)
5. Тайна следствия (статья 61 УПК РФ)
6. Тайна судопроизводства (статья 194 ГПК РФ, статья 20 АПК, статьи 298, 341 УПК РФ)
7. Налоговая тайна (статьи 102, 313 налогового кодекса РФ)
8. Банковская тайна (статья 26 ФЗ «О банках и банковской деятельности»)
9. Аудиторская тайна (статья 9 ФЗ «Об аудиторской деятельности»)
10. Тайна усыновления (статья 139 семейного кодекса РФ)
11. Адвокатская тайна, тайна страхования, тайна связи, тайна завещания …

**Тема:** Информация ограниченного доступа.

Выбрать любой вид тайны. Правовое регулирование и судебная практика.

**Правовой режим информации и защита информации.**

Правовой режим информации – это объектный режим, позволяющий обеспечить комплексность воздействия посредством совокупности регулятивных, охранительных, процессуальных средств, характеризующих особое сочетание дозволений, запретов и обязываний.

Различают общие, специальные и смешанные режимы.

Все меры защиты информации делятся на 3 вида:

1. Правовые
2. Организационные
3. Техническое

Правовое обеспечение защиты информации – совокупность нормативно-правовых актов, которые регламентируют вопросы обеспечения защиты информации, организацию и функционирование защиты информации.

С правовой регламентацией информационной безопасности связаны следующие отрасли права:

1. Конституционная
2. Уголовная
3. Гражданская
4. Административная
5. Предпринимательская
6. Финансовая

К общедоступной информации согласно статье 7 149-ФЗ к общедоступной информации относятся общеизвестные сведения и другая информация, доступ к которой не ограничен.

Статья 8 149-ФЗ предусматривает ситуации, когда доступ к информации не может быть ограничен. К такой информации относятся:

1. Нормативно-правовые акты, затрагивающие права, свободы и обязанности личности
2. О состоянии окружающей среды
3. Информация о деятельности государственных органов и органов местного самоуправления, в том числе об использовании бюджетных средств (кроме государственная тайна)
4. Информация из открытых фондов, библиотек, музеев, а также в государственных и иных системах, созданных для обеспечения граждан информацией.

В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного предоставления, предоставления не достоверной информации, были причинены убытки, то такие убытки подлежат возмещению.

Статья 9 содержит основание и порядок, ограничения доступа к информации.

**Конституционные гарантии прав на информацию и механизм их реализации**

В России реализация права на получение достоверной информации является одной из мер по предупреждению коррупции. Такие гарантии являются основой антикоррупционного контроля за деятельностью органов власти и их служащих со стороны населения. Для реализации конституционных прав на информацию необходимы следующие гарантии:

1. Общие (едины для всех)
2. Специальные юридические:
   1. Выполнение государственными органами юридической обязанности по обеспечению реализации конституционного права на информацию
   2. Создание необходимых условий для реализации права на информацию
   3. Наблюдение и контроль за реализацией права
   4. Охрана прав и свобод граждан
   5. Применение санкций
3. Механизмы реализации
   1. Свобода СМИ
   2. Распространение информации в соответствии с законом
   3. Защита прав интеллектуальной собственности
   4. Развитие информационных технологий
   5. Создание государственных информационных систем
   6. Организация привлечения к уголовной, административной, гражданско-правовой ответственности в информационной сфере

Проблемы при реализации:

1. Высокий процент подзаконного регулирования, что подрывает реализацию прав граждан на информацию (перечень сведений государственной тайны определяется подзаконным актом)
2. Пробелы законодательного характера (мало норм, ограничивающих произвол государственных органов в указанной сфере)

Проблемы организационного характера, которые снижают эффективность реализации прав граждан. Часть вины лежит на самих гражданах, которые не используют средства защиты своих прав. ФЗ-149, предусматривает возможность не обосновывать необходимость получения запрашиваемой информации о деятельности государственных органов и органов местного самоуправления, доступ к которой не ограничен.

**Доктрина информационной безопасности РФ**

Утверждена указом президента 5 декабря 2016 года.

Информационная сфера – это совокупность информации объектов информатизации, информационных систем, сайтов в сети интернет, сетей связи, информационных технологий, субъектов, совокупность механизмов регулирования этих общественных отношений.

Угроза информационной безопасности РФ – это совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Информационная безопасность РФ – это состояние защищенности личности и государства от внутренней и внешней информационной угроз, при котором обеспечиваются реализация конституционных прав личности, достойный уровень жизни граждан, суверенитет, территориальная целостность, устойчивое социально-экономическое положение России, оборона и безопасность.

Основные информационные угрозы:

1. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях
2. Усиление деятельности организаций осуществляющих техническую разведку
3. Используется для достижения террористических, экстремистских, криминальных целей
4. Увеличиваются масштабы использования специальными службами иностранных государств средств информационно-психологического воздействия направленного на подрыв суверенитета других государств
5. Террористические экстремистские группировки используют механизм информационного воздействия на индивидуальное и общественное сознание для разжигания этнической или религиозной вражды
6. Возрастают масштабы компьютерной преступности, прежде всего в финансовой сфере, в том числе касающиеся обработки ПД с использованием информационных технологий

Доктрина закрепляет стратегические цели и основные направления обеспечения информационной безопасности (раздел 4).

Раздел 5 доктрины закрепляет организационные основы обеспечения информационной безопасности и принципы деятельности государственных органов по обеспечению информационной безопасности.

**Информация ограниченного доступа.**

1. Государственная тайна
2. Коммерческая тайна

Федеральный закон «О государственной тайне» 1993 года дает определение государственной тайны.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной деятельности распространение которых может нанести Российской Федерации.

Наибольшими полномочиями в сфере защиты государственной тайны обладает президент. Именно он утверждает положения, структуру и состав межведомственной комиссии по защите государственной тайны. Президент утверждает перечень сведений, отнесенных к государственной тайне, в частности, в настоящее время, действует указ президента Российской Федерации 1995 года с изменениями в 2016 году «Об утверждении перечня сведений, отнесенных к государственной тайне».

Государственную тайну составляют:

1. Сведения в военной области
   1. Сведения о содержании оперативных планах
   2. Развертывание ВС
   3. ТТХ образцов вооружения и военной техники
2. Сведения в области экономики, науке и технике
   1. Мобилизационные мощности по изготовлению, ремонту техники и вооружения
3. Сведения в области внешней политики и экономике
   1. Внешнеполитическая деятельность
4. Сведения в области разведывательной, контрразведывательной, ОРД, противодействия терроризму
   1. О системе президентской, правительственной, шифрованной, кодированной и засекреченной связях
   2. О шифрах, методах и средствах защиты секретной информации
   3. Об организации и фактическом состоянии защиты государственной тайны

ФЗ устанавливает 3 степени грифов секретности:

1. Особой важности
2. Совершенно секретно
3. Секретно

Согласно статье 9 федерального закона лица, которые наделены полномочиями по отнесению сведений к государственной тайне, несут персональную ответственность.

Согласно статье 10 уполномоченные должностные лица в праве принимать решения о засекречивании информации, находящейся в собственности граждан, организаций или предприятий, если эта информация содержит сведения, содержащие государственную тайну. Материальный ущерб, наносимый собственнику информации в результате её засекречивания, возмещается государством.

Срок засекречивания сведений составляющих государственную тайну не должен превышать 30 лет, в исключительных случаях срок может быть продлен по заключению межведомственной комиссии по ряду оснований сведения могут быть рассекречены (изменение обстоятельств).

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

Судебная практика:

ВС был признан виновным в разглашении сведений, составляющих государственную тайну и привлечен к уголовной ответственности и дисциплинарной

**Коммерческая тайна.**

Федеральный закон от 2004 года «О коммерческой тайне» содержит определение – это режим конфиденциальности информации, позволяющей его обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных доходах, сохранить положение на рынке

Информация, составляющая коммерческую тайну – сведения любого характера, которые имеют действительную или потенциальную коммерческую тайну в силу неизвестности их третьим лицам.

Право на отнесение информации к коммерческой тайне и составлении её перечня принадлежит обладателю этой информации.

Статья 5 федерального закона о коммерческой тайне перечисляет сведения, в отношении которых не может быть установлен режим коммерческой тайны.

Запрещенные к сокрытию данные:

1. Показатели производственного травматизма
2. Профессиональной заболеваемости
3. О загрязнении окружающей среды

Статья 6 закрепляет порядок предоставления коммерческой тайны по требованию органа государственной власти или местного самоуправления на безвозмездной основе.

Статья 10 часть 2 содержит меры по охране конфиденциальности информации, которые должен предпринимать её обладатель:

1. Определение перечня информации, составляющих коммерческую тайну
2. Ограничение доступа к этой информации, через установления порядка обращения и контроля
3. Учет лиц, получивших доступ к такой информации
4. Регулирование отношений по коммерческой тайне на основании трудовых договоров
5. Нанесение на материальные носители грифа «коммерческая тайна» с указанием обладателя такой информации.

Режим коммерческой тайны считается установленным только после принятия обладателем информации перечисленных мер.

Статья 11 закрепляет порядок охраны коммерческой тайны в рамках трудовых отношений.

1. Обязанности работодателя
   1. Ознакомить работника под расписку с перечнем и режимом коммерческой тайны
2. Обязанности работника
   1. Обязан не разглашать коммерческую тайну
   2. Обязан возместить убытки

Работник имеет право обжаловать в суде незаконное установление режима коммерческой информации в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Нарушение федерального закона «О коммерческой тайне» влечет уголовную, административную, дисциплинарную или гражданско-правовую ответственность, в соответствии с законодательством Российской Федерации. Работник, если нет состава преступления, в случае разглашения информации несет дисциплинарную ответственность.

Органы государственной власти и местного самоуправления, получившие доступ к коммерческой тайне, несут гражданско-правовую ответственность за разглашение или незаконное использование этой информации.

Статья 183 УКРФ устанавливает наказание за незаконное получение и разглашение сведений, составляющих коммерческую тайну.

В 2014 году суд впервые назначил уголовное наказание за разглашение коммерческой тайны.

Иванов ответчик по гражданскому делу о разглашении коммерческой тайны. Истец фирма.

Истец:

* Ответчик принят на должность менеджера по продажам.
* При поступлении был ознакомлен с «Положением о конфиденциальной информации» и подписал обязательство о неразглашении.
* За разглашение информации предусмотрен штраф.
* Истец узнал, что ответчик передал информацию своему знакомому.

Ответчик:

* Это не информация, имеющая коммерческую ценность.
* Не является ноу-хау.
* В должностной инструкции у него этого нет.

Фирма занимается розничной и оптовой торговлей.

Суд:

* Истец не обеспечил режим охраны конфиденциальной информации (статья 10 ФЗ «О коммерческой тайне»)
* Гражданским правом ответственность работником за разглашение коммерческой тайны не предусмотрена. За это трудовой кодекс предусматривает дисциплинарную ответственность (замечание, выговор, увольнение).

**Правовой режим информации**

1. Понятие и признаки правового режима информации.
2. Элементы правового режима.
3. Виды правовых режимов. Тайна и конфиденциальность.

Правовой режим информации – объектный режим, вводимый нормативным актом и позволяющий обеспечить комплексность воздействия в информационной сфере, посредством совокупности регулятивных, охранительных, процессуальных средств, характеризующих особое сочетание дозволений, запретов и обязываний и гарантий по его соблюдению.

Признаки:

1. Основной объект права – информация, которая отличается нематериальным характером.
2. Устанавливается для достижения определенного социального эффекта.
3. Отражается в правилах, закрепленных нормативно-правовыми актами.
4. Эти правила санкционируются государством.

Элементы правового режима информации:

1. Целевое назначение прав и обязанностей субъектов по поводу информации и её защиты.
2. Информационная безопасность интересов государства, общества, человека.
3. Объект правового регулирования – информация.
4. Субъекты правового режима и их правовое положение – круг субъектов очень широк:
   1. Физические лица
   2. … (юридические, самоуправление, и т.д.)
   3. Государство
5. Определить круг субъектов правового режима информации – важно, т.к. от этого зависит установление на кого возложить обязанности, кого привлечь к ответственности.
6. Комплекс способов правового регулирования и средств воздействия (конкретный состав этих способов зависит и сам влияет на жесткость этих режимов):
   1. Обязывание.
   2. Дозволение.
   3. Запрет.

Одна из главных задач законодателя правильно регламентировать правовой режим конкретного вида информации.

Тайна – это сведения, не предназначенные для широкого круга. Есть ограничение доступа использования и распространения. Есть государственная защита. Нарушение требований ведет к неблагоприятным последствиям (юридическим).

Существенной характеристикой информации к какому-то виду тайн в рамках правового режима условий, ограничивающих её предоставление и распространение.

Статья 2 закона «О защите информации» - конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

**Виды режимов.**

Есть 2 основных правовых режима.

1. Общий – характеризуется открытостью, доступностью информации для всех лиц, этот режим складывается из права свободно получать, передавать и распространять информацию. Исключения из общего режима информации могут устанавливаться только законом. Режим открытой информации предоставляет максимально возможную свободу не только доступа, но и использования информации. К открытой информации относится информация, являющаяся общественным достоянием. Складывается из двух групп:
   1. Информация, защита права на которую истекла или снята добровольно.
   2. Информация о деятельности государственных и муниципальных органов.
2. Смешанный (инсайдерская информация) – существенная, публично не раскрытая служебная информация компании, которая в случае её раскрытия способна повлиять на рыночную стоимость ценных бумаг компании.
3. Специальный

Общий режим характеризуется:

1. Неограниченность лиц, получивших информацию
2. Различие форма предоставления информации
3. Отсутствие цели предоставления информации
4. Открытый доступ
5. Неограниченный объем
6. Предусмотрены гарантии соблюдения режима

Специальные правовые режимы информации направлены на охрану сведений, свободное распространение которых нарушает права и законные интересы человека, общества, государства.

В каждом случае, установления специальных режимов, имеются факторы, требующие режимного регулирования.

По объектному составу информация различается:

1. Государственная тайна
2. Коммерческая тайна
3. Аудиторская тайна
4. …

По субъектному составу несколько групп правовых режимов:

1. Для безопасности государства и общества
2. Для безопасности личности
3. Для обеспечения интересов предпринимательской деятельности

Цели введения специальных режимов в информации.

1. В интересах национальной безопасности
2. Для общественного порядка
3. Для охраны здоровья и нравственности
4. Защита репутации
5. Обеспечение правосудия

Специальный режим не просто ограничивает доступ к информации, её использование и распространение, а определяет степень жесткости регулирования, порядок введения и прекращения действия режима.

К специальному режиму отнесена информация – государственная тайна, конфиденциальная информация. Профессиональная тайна, информация о частной жизни лица, в том числе личная и семейная тайна. Перечень тайн не является ограниченным.

В этой же статье говорится о ПД физических лиц.

Признаки специального режима:

1. Ограничение доступа
2. Запрет на передачу третьим лицам без согласия обладателя информации
3. Запрет на распространение информации
4. Возможность обладателя информации по общему правилу самостоятельно решать вопрос

Диспозитивный режим – субъекты сами определяют для себя варианты поведения.

Правовой режим информации определяется нормами, которые устанавливают следующие.

1. Порядок документирования информации
2. Право собственности на отдельные документы и массивы документов, в том числе в информационных системах
3. Категория информации по уровню допуска к ней
4. Порядок правовой защиты информации

Закон о персональных данных ФЗ 152.

1. Проблемы реализации ФЗ о персональных данных.
2. Юридическая ответственность за нарушение требований закона.

Информационный посредник – понятие появилось в ГК РФ в 2013 году. В часть 4 была введена статья 12.53.1 ГКРФ «Особенности ответственности информационного посредника».

Информационным посредником является лицо осуществляющее передачу материала в информационного-телекоммуникационной сети, а также лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием сети, или лицо, предоставляющее возможность доступа к материалу в этой сети.

Информационный посредник несет ответственность за нарушение интеллектуальных прав в сети на общих основаниях, но при этом он не несет ответственность за нарушение интеллектуальных прав при одновременном соблюдении условий:

1. Не является инициатором этой передачи. Не определяет получателя.
2. Не изменяет указанный материал.
3. Не знал и не должен был знать о неправомерности передачи.

Также не несет ответственности за размещение материала, если:

1. Не знал и не должен был знать, что это неправомерно.
2. В случае получения в письменной форме заявления правообладателя о нарушении интеллектуальных прав с указанием страницы сайта или адреса, где размещен этот материал, своевременно принял меры для прекращения нарушения интеллектуальных прав.

Статья 1302 ГКРФ «Обеспечение иска по делаем о нарушении авторских прав» была дополнена пунктом 3, который предусматривает принятие обеспечительных мер, направленных на ограничение доступа к информации, нарушающей исключительные права, и к ресурсам, в отношении которых было выдвинуто обвинение в нарушении авторских прав.

Суды фактор безвозмездности услуг информационных посредников используют как дополнительный аргумент при отказе в удовлетворении исков. Например, если пользователь электронного почтового сервиса не доволен взломом его ящика, это не дает ему права заявлять иск компании, владеющей данным сервисом, поскольку в пользовательском соглашении указано на то, что пользователь сам несет ответственность за безопасность, т.е. устойчивость к угадыванию выбранного им пароля и сам обеспечивает конфиденциальность пароля.

Понятие информационного посредничества затронута и в ФЗ «Об информации…» в статье 2 дается определение провайдера хостинга и владельца сайта в сети интернет. Судебная практика показывает, что основную ответственность за размещение материалов несут пользователи, также, как и за обеспечение безопасности.

Информационный посредник не несет ответственности за размещаемые на своей площадке материалы

При нарушении личных и авторских прав граждан информацией, размещаемой на сайтах, размещением их фотографий, личных данных, произведений, они имеют средства правовой защиты. Например, иск о запрете использования результатов интеллектуальный деятельности, о компенсации морального вреда, о возмещении убытков. Владелец электронного почтового ящика вправе поставить вопрос о запрете информационному посреднику читать его электронную переписку с другими пользователями с требованием компенсировать моральный вред, если он обнаружит, что рекламные объявления, встраиваемые в тексты его писем, а также размещаемые в интерфейсе почтового ящика соответствуют содержанию его переписки, что можно подтвердить протоколами осмотра нотариусом интернет страниц.