**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.

ФЗ «О персональных данных» и защита персональных данных.

ФЗ-152 2006 года. Последнее изменение 03-07-2016.

Статья 1 закрепляет сферу действия данного закона.

Действие закона не распространяется на обработку персональных данных для личных и семейных нужд, если не затрагивает прав субъекта. Также на обработку архивных данных. На государственную тайну, и информацию деятельности судов.

Статья 3-1 ФЗ 152 дает определение термина персональные данные – это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

В статье 3 ФЗ 152 перечисляются операции при обработке персональных данных.

В статье 5 ФЗ 152 закрепляется важный принцип обработки персональных данных, а именно: она должна ограничиваться достижением заранее определенных конкретных и законных целей. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям.

1. Осуществляется с согласия субъекта персональных данных.
2. Необходимо для достижения целей, предусмотренных законом или международным договором.
3. Необходимо для осуществления правосудия, исполнения судебного акта или акта другого органа.
4. Необходимо для защиты жизни и здоровья субъекта персональных данных, если получение согласия субъекта невозможно.
5. Необходимо для осуществления профессиональной деятельности журналиста, для научной или творческой деятельности, но, если не нарушаются права субъекта персональных данных.

Статья 7 ФЗ 152 закрепляет обязанности операторов не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта, если иное не предусмотрено федеральным законом.

Статья 25 ФЗ 152 оговаривает ответственность за его нарушение. Лица, нарушившие закон, несут ответственность. Трудовым кодексом предусмотрена дисциплинарная ответственность за не надлежащее исполнение обязанностей, в том числе обязанности соблюдения порядка работы со сведениями конфиденциального характера.

Статья 90 ТК РФ предусматривает ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

Статья 86 ТК РФ содержит перечень требований к обработке персональных данных.

УК РФ статьи 137, 140, 272.

КОАП 13.11, 13.14.

Например, статья 13.11 КОАП предусматривает возможность привлечения работодателя к административной ответственности за передачу сведений третьим лицам без согласия субъекта.

Часть 2 статьи 24 указывает на обязанность нарушителя возместить моральный вред независимо от возмещения имущественного вреда.

Статья 8 ФЗ 152 содержит перечень общедоступных источников персональных данных. Например, справочники и адресные книги. С письменного согласия субъектов.

Статья 9 закрепляет порядок дачи субъектом согласия на обработку его ПД. Субъект принимает решение свободно, по своей воле и в своем интересе.

Статья 10 содержит специальные категории ПД. Религиозные, политические взгляды, состояние здоровья, интимная жизнь относятся к специальной категории ПД обработка которых НЕ ДОПУСКАЕТСЯ, за исключением нижеуказанных случаев:

1. Сам дал согласие.
2. Эти данные общедоступные.
3. В медико-профилактических целях.
4. Для осуществления правосудия.
5. В соответствии с законодательством о противодействии терроризму, коррупции, ОРД и исполнительном производстве.

Статья 14 и 17 ФЗ 152 закрепляют права субъекта на доступ к ПД и на обжалование действия или бездействия оператора.

Глава 4 закрепляет обязанности оператора. С точки зрения безопасности персональных данных наиболее весомой представляется 19 статья, которая содержит перечень мер по обеспечению безопасности персональных данных при их обработке. Всего 11 пунктов.

Меры:

1. Определение угроз
2. Применение организационных и технических мер

Правительство РФ устанавливает

* уровни защищенности ПД
* требования к защите
* требования к материальным носителям биометрических данных

Статья 23 закона закрепляет компетенцию уполномоченного органа, по защите прав субъектов персональных данных.

Федеральная служба по надзору в сфере связи информационных технологий и массовых коммуникаций.

1. Привлечение к административной ответственности.
2. Направление в правоохранительные органы материалы для возбуждения уголовных дел.
3. Обращаться в суд с исковыми заявлениями в защиту прав субъектов.
4. Принимать меры по приостановлению или прекращению обработки персональных данных, если она ведется с нарушениями.
5. Требовать от оператора уточнения или уничтожения недостоверных, или полученных незаконным путем сведений.
6. Хотите ли вы получить качественный программный продукт?
7. Хотите ли вы получать актуальное и поддерживаемое программное обеспечение?
8. Считаете ли вы правильным распространение взломанного программного обеспечения?
9. Считаете ли вы, что человек имеет право получать вознаграждение за свой труд?

**Правовая охрана интеллектуальной собственности:**

* **полезные модели**
* **производственные образцы**

**Охрана изображения гражданина**

Правовому регулированию этого вопроса посвящена статья 152.1 гражданского кодекса РФ, но и она содержит ряд пробелов в результате чего особое значение получило постановление пленума верховного суда РФ от 2015 года.

Согласно ГК, обнародование и дальнейшее использование изображения гражданина допускается только с согласия гражданина. Под изображением понимаются фотографии, видеозаписи или произведения изобразительного искусства.

После смерти гражданина его изображение может использоваться только с согласия детей и супруга, если нет детей и супруга – то с согласия родителей.

Статья 152.1 ГК РФ перечисляет случаи, когда такое согласие не требуется. Указывает, что эта норма работает, например, когда гражданин является публичной фигурой. А именно – занимает государственную или муниципальную должность, является выдающимся политиком, спортсменом.

Студент пришел в библиотеку КГУ и попросил сделать копии из научного журнала.

Исполнение произведения литературы искусства или народного творчества посредством чтения, игры, декларации, постановки в живом исполнении или с помощью технических средств.

**Уголовная ответственность за преступления в сфере информации.**

1. Понятие и состав преступления
2. Преступление в сфере информации и ответственность за них
3. Ответственность за компьютерные преступления
4. Особенности совершения и расследования компьютерных преступлений

Преступлением признается виновно совершенное общественно опасное деяние, совершенное деликтоспособным субъектом, за которое предусмотрено за которое предусмотрена ответственность и которое запрещено УК РФ.

Состав преступления конструируется из четырех элементов, достаточных и необходимых в совокупности, для квалификации деяния как преступления.

1. Субъектом преступления может быть признано только физическое лицо, достигшее возраста уголовной ответственности и являвшееся вменяемым в момент совершения преступления. (уголовная ответственность наступает с 16 лет, а за отдельные виды преступлений с 14 лет)
2. Объектом является правоотношение охраняемые уголовным законом. Объект можно увидеть в названии главы. Например, «правоотношения в сфере компьютерной безопасности», «право собственности».
3. Субъективная сторона – психическое отношение субъекта к совершенному им деянию. Основным признаком субъективной стороны является вина, а факультативными цель и мотив. Существуют 2 формы вины: умысел и неосторожность. Умысел может быть прямой и косвенный. При прямом умысле лицо, осознавало, что совершает преступное деяние и что могут наступить общественно опасные последствия и желало их наступления. При косвенном умысле лицо осознавало возможность общественно опасных последствий и относилось к ним, как к безразлично. По легкомыслию, лицо осознавало возможность наступления общественно опасных последствий, но по самонадеянности рассчитывало на их предотвращение. По небрежности, лицо не осознавало возможности наступления последствий.
4. Объективная сторона – деяние может быть совершено путем действия или бездействия. Учитываются обстоятельства, влияющие на степень общественной опасности. Наличие причинно-следственной связи между деянием и наступившими общественно опасными последствиями.

Уголовно правовые санкции прямо или косвенно связанные с информацией. Клевета и оскорбление сейчас не являются уголовными преступлениями.

**Публичные призывы к развязыванию агрессивной войны (354 УК РФ).**

Незаконное разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (183 УК РФ).

Хищение предметов, имеющих особую ценность (164 УК РФ).

Статьи 189, 190, 233, 284, 324, 325.

За преступления в сфере информации может быть наказание в виде штрафа, лишения права занимать определенные должности, исправительных работ. Более строгое наказание предусмотрено за преступление в сфере государственной тайны за что предусмотрено лишение свободы.

Диспозиция – часть нормы, которая отражает права, обязанности и запреты.

Субъект – общий/специальный с 16 лет.

Объект – конституционные права и свободы личности.

Субъективная сторона характеризуется умыслом.

Внедрение информационных технологий автоматизированных систем компьютерных программ создает и угрозу безопасности. Значимость таких преступлений в том, что они могут повлечь за собой аварии, катастрофы, паралич банковской системы.

Преступления против общественной безопасности и порядка. В данной главе 3 статьи (272, 273, 274 УК РФ).

«Неправомерный доступ к компьютерной информации» статья 272 УК РФ. Ответственность наступает, если неправомерный доступ повлек уничтожение или копирование информации.

Частью третьей статьи 272 УК РФ предусмотрены квалифицирующие признаки. Совершенная группой лиц или лицом с использованием служебного положения. Часть четвертая содержит признак наступления тяжких последствий или угрозы их наступления.

Статья 273 УК РФ предусматривает ответственность за создание, распространение и использование вредоносных компьютерных программ. Объектом являются общественные отношения, обеспечивающие безопасность компьютерной безопасности и компьютера. Предметом посягательства является сама вредоносная программа.

Вредоносная программа – программное средство, которые было создано для выполнения несанкционированных собственником функций (модификация, блокирование, копирование, уничтожение информации и нарушение работы ПК).

Объективная сторона – факт создания компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации.

Способ совершения – действия, выраженные в создании, распространении и использовании вредоносной программы или информации.

Состав по части первой является формальным по части второй и третьей – материальным. Субъектом может быть любое вменяемое физическое лицо, достигшее 16-ти лет. Часть 2 статьи предусматривает повышенную ответственность, если преступление совершено группой лиц или с использованием служебного положения. Субъективная сторона выражается в виде прямого умысла, что подчеркивается термином – «заведомо». Часть 3 характеризуется двумя формами вины: умысел по отношению к преступному деянию и неосторожность по отношению к наступившим последствиям. Разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей подготовки могут и должны предвидеть возможные последствия использования этих программ. Поэтому уголовная ответственность установлена не только к умыслу, но и к неосторожности по отношению к последствиям. Степень тяжести последствий устанавливается по постановлению суда.

Сравним 272 и 273. Есть общие черты и отличным.

Сходство: ведут к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации.

Различия: статья 272 состав материальный, статья 273 – материальный.

Предметом статьи 272 является только информация, охраняемая законом.

Статья 274 предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей.

Выход из строя компьютерного оборудования или информационно телекоммуникационных сетей может привести к катастрофическим последствиям и поэтому за нарушение правил установлена уголовная ответственность. Данная норма является отсылочной, т.е. она отсылает к нормативным и техническим актам и правилам, устанавливающим порядок работы с сетями и оборудованием.

Федеральный закон «О связи», санитарные нормы и правила для работников, техническая документация на компьютерную технику.

Объективная сторона – действие или бездействие (нарушение правил). Субъективная сторона – нарушение правил эксплуатации.

Субъективная сторона – нарушение правил эксплуатации может быть совершено как умышленно, так и по неосторожности – лицо предвидит уничтожение и т.д. информации в результате нарушения им правил, но без оснований рассчитывает на предотвращение этих последствий. Лицо не предвидит последствий. Субъект – специальный, лицо, которое по должностной инструкции имеет доступ к информации, сетям или оборудованию.

**Правовая ответственность за правонарушения в информационной сфере.**

Специфика гражданско-правовых отношений заключается в имущественном характере принудительных мер воздействия.

Статья 17 ФЗ «Об информации»: лица, законные интересы которых были нарушены, в связи с неправомерным пользованием информацией ограниченного доступа могут обратиться за судебной защитой своих прав, в том числе в рамках гражданского процесса.

Гражданско-правовая ответственность подразделяется на договорную и внедоговорную.

Договорная возникает при нарушении условий договора, внедоговорная возникает при причинении вреда.

Состав гражданского правонарушения – причем они противоправны, наличие причинной связи между деянием нарушителя и причинением вреда или убытков потерпевшему. Наличие вины правонарушителя, наличие вреда или убытков у потерпевшего, наличие субъекта. Противоправность может заключаться в следующих действиях – несанкционированный сбор и разглашение сведений, составляющих коммерческую тайну. При оценке наличия убытков учитывается принцип полноты возмещения причиненных убытков. При оценке наличия убытков учитывается принцип полноты возмещения причиненных убытков. Оценивая убытки обладателя коммерческой тайны надо учитывать факторы – неизвестность информации конкурентам, потребителям, возможность продажи, влияние на конъюнктуру рынка. Необходимым условием для привлечения лица незаконно получившего информацию, находящуюся в режиме коммерческой тайны, является его вина. В отличие от уголовного процесса, где действует принцип презумпции невиновности, в гражданском процессе действует обратный принцип.

По общему правилу правонарушитель сам должен доказать отсутствие своей вины в разглашении сведений, отнесенных к коммерческой тайне.

**Административная ответственность за правонарушения в сфере информационной безопасности.**

1. Понятие административного правонарушения
2. Виды административных правонарушений в сфере информационной безопасности

Административное правонарушение – это виновно-совершенное общественно-вредное деяние, предусмотренное административным законодательством. Административная ответственность наступает с 16 лет. Законодательство об административных правонарушениях состоит из кодекса об административных правонарушениях и законов субъектов РФ об административных правонарушениях.

Административные правоотношения отличаются субъектом и содержанием. Одной стороной всегда является представитель власти.

Уголовное законодательство содержит преступления в сфере информационной безопасности, как правило с материальным составом, т.е. с причинением определенного ущерба. Этот пробел заполняется в КоАП.

Статья 13.12 предусматривает административное наказание за правонарушение в отношении сведений составляющих государственную тайну. Использование не сертифицированных средств, предназначенных для защиты государственной тайны или нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой государственной тайны.

КоАП включает наказание по статье 13.12 «Нарушение правил защиты информации» до 20 тысяч рублей.

Имеются 3 обязательных признака по этой статье:

1. Обязательность лицензирования для ведения деятельности связанной с защитой информации.
2. Использование нелицензированных информационных систем, а также средств защиты информации, если они подлежат обязательной сертификации.
3. Грубое нарушение условий, предусмотренных лицензией.

Статья 5.39 предусматривает ответственность за отказ в предоставлении информации, статья 7.12 дополняет меры уголовного наказания за нарушение права на интеллектуальную собственность, если эти правонарушения причинили потерпевшим вред меньший, чем указано в уголовном кодексе. Ввоз, продажа или иное незаконное использование экземпляров произведений контрафактных, в целях извлечения дохода.

Незаконное использование изобретения, полезной модели или промышленного образца, присвоение авторства или принуждение к соавторству.

Статья 13.12 запрещает незаконную деятельность в области защиты информации.

Статья 13.14 предусматривает наказание за разглашение информации с ограниченным доступом. Предусматривается административное наказание за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение влечет уголовную ответственность). Лица, получившего доступ к такой информации в связи с исполнением служебных и профессиональных обязанностей.