# Правовые аспекты Информационных Технологий.

**Лекция 1.**

Информационное право.

Информационное право в системе российского права.

Информационное право – это относительно новая быстро развивающаяся комплексная отрасль российского права.

152 ФЗ – основной закон.

Предмет информационного права – это общественные отношения в сфере информации. Связано с передачей, распространением, созданием, использованием информации, с информационными технологиями, информационной безопасностью.

Метод информационного права – императивно-диспозитивный.

Императивный метод – предполагает строго определенный вариант поведения (обязать и запретить).

Диспозитивный метод – предоставляет участникам правоотношений выбрать вариант поведения (дозволение).

# Информационные технологии как объект правового регулирования.

1. Объекты права информационных технологий.
2. Субъекты права информационных технологий.
3. Содержания правоотношений.

Информационные технологии – это все, что связано с компьютерными технологиями, такими как: сети, аппаратные средства, программное обеспечение и интернет.

Право в сфере информационных технологий – это совокупность правовых норм, которые регулируют общественные отношения, связанные с созданием, переработкой и распространением информации в сфере аппаратного и программного обеспечения, телекоммуникационных и сетевых услуг, а также в сети интернет.

Список услуг, предоставляемых в отрасли:

1. Составление договоров по разработке ПО, лицензионных и авторских.
2. Юридическое сопровождение, открытие, передача или ликвидация домена в интернете и другое.

Субъекты права информационных технологий – физические и юридические лица. В частности, производители ПО, веб-студии, операторы телефонной связи и сети мобильных операторов, интернет провайдеры, а также потребители поставляемых ими услуг, государство и государственные органы и органы местного самоуправления.

Отношения, возникающие при создании информации.

1. Отношения по поводу авторского права.
2. Обязанности по созданию, сбору и хранению информации.
3. Ответственность за создание недоброкачественной информации и дезинформации.

Отношения, возникающие при передаче и распространении информации. Устанавливаются между заказчиком и потребителем.

Отношения, возникающие при реализации права на поиск, получение, передачу и потребление информации.

Отношения, возникающие при разработке и эксплуатации ИС и их сетей. Они устанавливаются между заказчиком, и разработчиком, и пользователем. Пример: договорные отношения, или отношения по поводу исполнения.

**Лекция 2.**

# Правовое регулирование информационных технологий в государственном управлении. Информатизация судебной сферы. Электронное правосудие.

Создание Государственной Автоматизированной Системы “Правосудие” было предусмотрено федеральной программой развития судебной программы России на 2002-2006 годы. Начало эксплуатации 2007 год.

1. Для общества информационные технологии могут дать преимущество в сфере общественного контроля над правосудием через информационную открытость.
2. Трансляция и запись судебных заседаний через интернет будет способствовать правовому воспитанию и формированию общественного мнения о правосудии.
3. Информационные технологии позволяют бороться с коррупцией благодаря электронному распределению дел, публикации сведений по доходам судий.

Изначально создаваемое для автоматизации работы судий, аппаратов судов и работы официальных интернет сайтов система ГАС “Правосудие” не предусматривала функционирование на своей платформе электронных сервисов для граждан и организаций, а также для ведомств, нуждающихся в информации от судебной системы.

Основным документом, определяющим стратегию внедрения ИТ и их взаимодействия с обществом, является концепция развития информатизации судов до 2020 года.

Этой концепцией предусмотрено создание объединенной картотеки всех судебных дел. В 2015 году состоялось первое, тестовое для судов общей юрисдикции, интернет трансляция судебного заседания.

**Лекция 3.**

# Источники информационного права (информационной безопасности и информационных технологий).

1. Конституция
2. Общепризнанные международные нормы и принципы
   1. Международные договоры РФ
   2. Всеобщая декларация прав человека (1948 года)
   3. Окинавская хартия глобального информационного общества от 2000 года.

В 2015 году генассамблея ООН на 70 сессии приняла резолюцию “Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности” разработанную Россией.

1. ФКЗ
2. ФЗ
   1. федеральный закон «Об информации, информационных технология и о защите информации» 2006 года #149-ФЗ. Последние изменения 19 декабря 2016 года.
   2. 152-ФЗ “О персональных данных”
   3. Закон Российской федерации 1993 года «О государственной тайне» отредактированный 2015. #5485-1
   4. Гражданский кодекс Российской Федерации (#4)
   5. Уголовный кодекс
   6. Кодекс об административных правонарушениях
   7. Уголовно-процессуальный кодекс РФ
   8. Гражданский процессуальный кодекс РФ
   9. Арбитражный процессуальный кодекс РФ
   10. Федеральный закон 2004 года #98-ФЗ «О коммерческой тайне»
3. Указ президента РФ.
   1. Указ президента РФ 1995 года №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»
   2. Указ президента РФ 5 декабря 2016 года №646 «Об утверждении доктрины информационной безопасности Российской Федерации»
   3. Указ президента 2013 года об утверждении «Основ государственной политики Российской Федерации» в области международной информационной безопасности на период до 2020 года
4. Постановления правительства.
   1. Постановление правительства Российской Федерации 2012 года №1101 «О единой автоматизированной системе «Единый реестр доменных имен»»
5. Нормативно-правовые акты министерств и служб.
   1. Приказ Роскомнадзора, ФСКН, Роспотребнадзор 2013 года «Об утверждении критериев оценки материалов и информации»

Нормативно-правовые акты в сфере информационных технологий и информационной безопасности, кроме того, могут быть приняты в субъектах российской федерации, органами местного самоуправления и внутри организации.

Федеральными целевыми программами предусмотрено проведение, финансирование, внедрение концепции информационного общества, электронного правительства. Под электронным правительством в концепции понимается новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий, качественно новый уровень оперативности и удобства получения гражданами и организациями государственных услуг и информации о результатах работы деятельности государственных органов. В правовой сфере последовал всплеск нормотворчества в электронной сфере.

1. Регулирование межведомственного электронного документооборота (постановление правительства 2009 года)
2. Регулирование электронных государственных услуг (распоряжение правительства 2009 года о плане перехода на предоставление государственных услуг и исполнение государственных функций в электронном виде федеральными органами исполнительной власти)

**Государственные-информационные ресурсы**

Обеспечение доступности государственных услуг и повышение эффективности электронного государства.

Информационное общество на 2011-2020 годы. Программа – информационное государство. Достижение этих целей возможно при решении двух задач.

1. Создание базовых государственных информационных ресурсов и инфраструктуры информационно-коммуникационных технологий
2. Профессионально-квалификационные данных о гражданах (образование, профессия)
3. Данные экономического характера
4. Иные юридические

БГИР предназначены для использования, при осуществлении межведомственного информационного взаимодействия в целях предоставления государственных и муниципальных услуг, или для исполнения функций.

Инфраструктура информационных технологий необходима для логистики формируемых информационных потоков. Сюда относятся:

1. Центры обработки
2. Сети передачи данных
3. Единая система межведомственного электронного взаимодействия
4. Рабочие станции

Выявлены недостатки, часть их устранена в связи с принятием очередной концепции «методологии, систематизации и …» 2014 года.

Постоянная корректировка требований к информационным ресурсам, что влечет за собой дополнительные затраты.

Десинхронизация процессов по разработке программного обеспечения, что осложняет их ввод в эксплуатацию.

Правовые проблемы электронной коммуникации (в сети интернет). ПРАКТИКИ. ПРИМЕРЫ. ПРИЧИНЫ и СТАТЬИ.

На администрацию города возложена обязанность в трехмесячный срок со дня работы государственной системы «Энергоэффективность» направить в министерство энергетики информацию и разместить на сайте. Органы не разместили, поскольку информация является конфиденциальной. Обратились к министерству энергетики с запросом по поводу правомерности размещения данной информации.

**Правовое регулирование в сфере финансов и банковской сфере.**

Правовое обеспечение по вопросам информационных технологий в этих сферах осуществляется по следующим направлениям:

1. Принятие новых нормативно-правовых актов
2. Внесение изменений и дополнений в действующее
3. Участие в выработке международно-правовых документов

Современная банковская система не может существовать без инновационного развития информационных технологий.

* Онлайн-услуги
* Использование банковских карт
* Электронные переводы

Все это нуждается в правовой защите и защите информационной безопасности банковских систем.

Безопасность банковских информационных систем является неотъемлемой стратегической функцией государства, призванной минимизировать финансовые потери, тем самым способствуя сохранению финансов.

К числу основных стратегических угроз национальной безопасности относится такой фактор как кризис мировой и государственной финансовой системы, что определяет значимость защиты безопасности информационных систем.

Регулирование ИТ производится следующими нормативно-правовыми актами:

1. Стандарт «Обеспечение информационной безопасности организации банковской системы российской федерации» (обеспечение эффективного и бесперебойного функционирования платежной системы РФ является задачей банка России и это зависит от уровня безопасности банковских технологических процессов (платежных и информационных)). Этот стандарт распространяется на все банки.
2. Гражданский кодекс РФ затрагивает такой аспект, как банковская тайна. Указывается, что банковская тайна отличается характерными особенностями и специфическим порядком охраны и защиты.
3. Федеральный закон «О контрактной системе в сфере закупок» регулирует закупки, участниками которых являются банки.

**Информационная политика предприятия, связанная с технологиями.**

Для руководителя важно выработать положение о информационной безопасности, поскольку все направления деятельности предприятия, связаны с информационными технологиями.

Принципы информационной политики:

1. Ей должны следовать все без исключения работники организации.
2. Целостность информационной системы и устойчивость функционирования, поскольку сбой на одной стадии информационного процесса может повлечь разрушению всей системы. В то же время излишнее нагромождение технических средств защиты может осложнить доступ к информационной системе.
3. Разумное соотношение открытости информации.
4. Постоянное изменение её режима (обновление должны подвергаться не только технологические условия защиты информации, но и общие организационно-правовые правила).
5. Введение контроля за реализацией разработанной политики (пользователь корпоративно-информационной системы должен помнить о том, что любая операция в вычислительной сети фиксируется и контролируется на технологическом уровне и организационном уровне).
6. Оптимальность финансовых затрат.
7. Профессионализм – весь персонал, имеющий доступ к корпоративной информационной системе, должен обладать навыками в сфере применения информационных технологий и безопасности.

Придумать фирму и разработать политику информационной безопасности.

1. Общее состояние защиты фирмы
2. Разработать нормативный документ, например, «Приказ руководителя или положение об ИБ фирмы»
3. Должностная инструкция по ИБ
4. Для всех работников разработать памятку об информационной безопасности

**Правовое регулирование**

Правовое регулирование информационных технологий в государственной сфере регулируется ФЗ «Об информации …».

Статья 12 «Государственное регулирование в сфере применения информационных технологий» предусматривает цели, а также обязанности государственных органов и органов местного самоуправления в сфере применения информационных технологий.

Статья 12.1 регулирует особенности государственного регулирования в сфере использования российских программ для ЭВМ и БД.

Статья 14 «О государственных ИС», которые создаются в целях реализации полномочий, госорганов и обеспечения обмена информацией между ними, а также в других целях.

Статья 11.1 регулирует обмен информацией в форме электронных документов при осуществлении полномочий органов государственной власти.

**Информационные конфликты.**

1. Информация как объект информационного конфликта.
2. Первоисточники конфликта.
3. Виды конфликтов в информационно-телекоммуникационной сфере.

Окинавская хартия – 2000 год – определяет, что люди, все без исключения, повсеместно должны пользоваться преимуществами глобального информационного общества. Однако информация вышла за территориальные рамки, и для отношений в информационной сфере стал применяться термин трансграничность. Например, это охват лиц, находящихся в различных национальных сегментах сети интернет. Этот признак порождает правовые проблемы регулирования отношений. Ученые к технологиям в этой сфере причисляют: пиринговые сети, крипто деньги, tor-протоколы и анонимные сети. Использование этих технологий ставит под сомнение об анонимности субъектов, признаках государства и etc.

Возникли новые информационные субъекты – хостинг-провайдеры, информационные посредники, блоггеры, интернет-сообщества, транснациональные интернет-корпорации. Возникли новые формы обмена информацией и её распространения – электронные СМИ, блоги, ЖЖ, электронная торговля. Появились новые формы платежей. Электронные деньги и крипто валюта. Новые формы подтверждения личности – ЭЦП. Институтом РАН выявлен перечень проблем правового регулирования отношения в сети интернет.

1. Возможность государства установить контроль над субъектами сети интернет.
2. Определение местоположения субъектов в сети.
3. Идентификация анонимного субъекта.
4. Определение перечня норм для решения конфликтных вопросов.
5. Определение частноправового и публично правового пространства
6. Определение достоверности информации

В 2012-2016 годах были предприняты меры для регулирования сети интернет и информации в ней:

1. Принято постановление 2012 года «О единой автоматизированной системе «Единый реестр доменных имен…» содержащих информацию, распространение которой в РФ запрещено».
2. В ГК РФ введен новый субъект «Информационный посредник» в 2014 году. В федеральный закон об информации было введено понятие блоггер, особенности распространения им информации и его ответственность.
3. В 2013 году был принят приказ Роскомнадзора и ФСКН, который раскрывает специфику такой информации, как суицид, наркотики, детская порнография и определяет критерии для отнесения информации к указанным категориям. #666 – ПРОЧИТАТЬ!11

**Первоисточники конфликта**

Ученые выделяют 2 способа реализации информационных противоречий – это информационный конфликт и информационная война.

Параметры информационных противоречий:

1. Поведение участников определяется их областью интересов и их моделью мира.
2. Используются методы, основанные на знаниях и информации.
3. Средством является информационное воздействие.
4. Средой является информационные технологии.
5. Участники могут быть как реальные, так и виртуальные.
6. Объектами являются смысловые модели, технологии.

Информационное воздействие направлено на человека. Информационное противоречие связано распространяемой информацией, информационными технологиями, которые позволяют создавать, передавать, уничтожать, модифицировать и похищать информацию.

В целях защиты детей от информации был принят соответствующий ФЗ, а с целью его реализации постановление правительства от 2013 года, на основании которого создан единый реестр доменных имен, позволяющих идентифицировать сайты, содержащие запрещенную информацию.

В зависимости от роли и функции каждый может стать либо активным, либо пассивным субъектом конфликтных отношений.

Источники конфликтов – в основе конфликта обмен информации, т.е. движение информации между двумя или более субъектами, вызывающее реакцию взаимодействующих субъектов.

**Обращение информации.**

Обмен информации – если есть реакция взаимодействующих субъектов.

Примеры конфликтов в аппаратно-программной среде:

1. Применение закрытого программного обеспечения приводит к невозможности его адаптации в уже установленную программную среду. Как указывает ГК РФ #12.80 – декомпилирование программ для ЭВМ разрешено лицам, правомерно владеющим экземпляром программы для ЭВМ, однако правообладатель может запретить такие действия, и пользователь программы лишается этой возможности. Для исключения таких ситуаций стали широко применяться программы с открытым кодом.
2. Конфликты могут возникнуть из-за ошибок, заложенных изначально разработчиками технологий.
3. Конфликты могут возникнуть при взаимной технологической несовместимости моделей из-за применения новых стандартов или отсутствия технических норм. В дальнейшем такие конфликты в сфере аппаратно-программного обеспечения.

Противоречие, возникающее при обмене в социальной среде.

Конфликт могут повлечь следующие действия:

1. Создание информации
2. Распространение информации
3. Информационный обмен
4. Передача информации
5. Использование информационных технологий
6. Разработка информационных технологий

Например, конфликт может возникнуть может возникнуть из-за неопределенности понятия достоверные сведения об обладателе информации.

Согласно конституции, на органы государственной власти местного самоуправления возлагается обязанность обеспечить каждому возможность ознакомления с документами, затрагивающими его права. В связи с этим были приняты федеральные законы, например, 2009 года «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

Ответственность – уголовная (статья 140 УК РФ), административная (статья 5.39 КОАП, статья 13.27 КОАП и 13.28 КОАП).

Другой пример конфликта, связанный с использованием информации – это отставание в использовании новейших технологий.

Третье направление конфликтов – это конфликты в смешанной правовой и технической среде. Например, конфликты, связанные с правообладателями. Например, для защиты кинофильмов, телефильмов был принят регламент по статье 15.2 ФЗ «Об информации».

Федеральный закон «Об электронной подписи» 2011 года ФЗ-63.

Виды электронных подписей в статье 5. Различаются:

* усиленная неквалифицированная
* усиленная квалифицированная
* простая электронная подпись

Квалифицированная электронная подпись обладает дополнительными признаками.

* Ключ проверки указан в квалификационном сертификате
* Для создания и проверки электронной подписи используются средства электронной подписи, соответствующие требованиям

Статья 6 закона закрепляет при каких условиях документы, подписанные электронной подписью, приравниваются к документам, подписанным собственноручно.

Статьи 9-10 закрепляют процедуры использования простой и усиленной электронных подписей.

Статья 13 закрепляет полномочия удостоверяющего центра.

Пример привлечения биометрических технологий.

Программный продукт и его защита.

1. Программа для ЭВМ.
2. Особенности государственного регулирования в сфере использования российских программ для ЭВМ.
3. Правовая защита программных продуктов и баз данных.
4. Ответственность за незаконное использование программного обеспечения.

Нормативную основу составляют статьи 1261, 1262 ГК РФ.

Программа для ЭВМ – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, в целях получения определенного результата, включая подготовительные материалы и порождаемые аудиовизуальные отображения.

Авторские права на все виды программ для ЭВМ в том числе на операционные системы и программные комплексы, которые могут быть выражены на любом языке и в любой форме (включая исходный текст и объектный код) охраняются также, как авторские права на произведения литературы.

Различают 2 категории прав в сфере использования программных продуктов:

1. Экономические права, дающие их обладателю право на получение экономических выгод от продажи или использования программных продуктов.
2. Моральные права, обеспечивающие защиту личности, автора программного продукта.

Авторское право действует с момента создания продукта или БД в течение всей жизни автора и 70 лет после смерти. Правомочия автора:

1. Выпускать в свет;
2. Воспроизводить в любой форме и любыми способами;
3. Распространять;
4. Модифицировать;
5. Использовать программный продукт;

Имущественные права на программный продукт могут быть переданы по договору другим лицам, физическим или юридическим. Имущественные права наследуются. Если программный продукт создан в порядке выполнения служебных обязанностей, то имущественные права принадлежат работодателю.

Лицо, правомерно владеющее экземпляром программы, имеет право осуществлять любые действия, связанные с функционирование программного продукта в том числе:

1. Устанавливать один экземпляр
2. Исправлять явные ошибки
3. Адаптировать программный продукт
4. Изготавливать страховые копии

Что является доказательством законности использования ПО:

1. Лицензионные договор
2. Документ, свидетельствующий об оплате программного продукта

Особенности регулирования отношений, связанных с программами для ЭВМ:

1. В 2015 году в ФЗ «Об информации …» введена статья 12.1 «Особенности государственного регулирования в сфере использования Российских программ для ЭВМ и баз данных».
2. Создается единый реестр российских программ для ЭВМ и баз данных.
3. <30% для российских не коммерческих и иностранных коммерческих организаций.
4. Если сведения о программе не составляют государственную тайну.

Срок исковой давности 3 месяца.

Статья 1262 ГК РФ регламентирует государственную регистрацию программ для ЭВМ и БД.

Правообладатель может по своему желанию зарегистрировать программу в Роспатенте.

Не подлежат регистрации программы, в которых содержатся сведения, составляющие государственную тайну.

Сведения о правообладателе и программе вносятся в реестр программ для ЭВМ. Ответственность за достоверность представленных для регистрации сведений несет заявитель.

В 2015 году было принято было принято постановление правительства РФ «Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств для целей осуществления государственных и муниципальных нужд». Теперь заказчики обязаны закупать российское программное обеспечение, кроме случаев, когда программное обеспечение с необходимыми функциональными, техническими или эксплуатационными характеристиками в России отсутствует, но такую необходимость надо обосновать.

Представляет интерес письмо МинОбрНауки от 2008 года «Об использовании пакета свободного ПО для общеобразовательных учреждений РФ».

Защита программного обеспечения предусматривает следующие цели:

1. Ограничение не санкционированного доступа к программам или их преднамеренное разрушение и хищение.
2. Исключение несанкционированного копирования программ.
3. Программный продукт должен быть защищен по нескольким направлениями от воздействия человека (хищение, нарушение работоспособности и etc.)

Воздействие аппаратуры для считывания программ или физического уничтожения, воздействие специализированных программ.

Самый простой способ защиты программных продуктов – это ограничение доступа.

Ограничение и контроль доступа могут проводиться путем парольной защиты программ при их запуске, использование ключевой дискеты, ограничение функций доступных пользователям. Более сложные – это криптографические методы защиты. На Западе наиболее популярны следующие методы правовой защиты программных продуктов.

1. Патентная защита
2. Законодательство о производственных секретах
3. Законодательство об авторском праве
4. Лицензионные соглашения и контракты

Лицензионные соглашения распространяются на все аспекты правовой охраны программных продуктов включая авторское право, патентную защиту.

Лицензий – это договор на передачу одним лицом (лицензиаром) другому лицу (лицензиату) право на пользование программой.

Лицензиар увеличивает свои доходы сбором лицензионных платежей, расширяет область распространения программного продукта.

Лицензиат извлекает пользу из использования.

Статья 1280 ГК РФ регулирует права пользователя программы для ЭВМ, а именно:

1. Осуществлять действия необходимые для функционирования программы, включая запись и хранение в памяти ЭВМ, внесение изменений исключительно в определенных целях и, если иное не предусмотрено договором с правообладателем.
2. Пользователи имеют право изготовить копию программы при условии, что эта копия предназначена только для архивных целей или для замены экземпляра в случае его утери, уничтожения или непригодности.

Лицензия может быть исключительной и простой.

Исключительная лицензия предполагает продажу всех имущественных прав на программный продукт, а автор или владелец патента отказывается от применения программы или предоставления другим лицам.

Простая лицензия – лицензиар предоставляет право лицензиату использовать программный продукт, оставляя за собой право применять его и предоставлять на аналогичных условиях не ограниченному кругу лиц.

**Ответственность за незаконное использование программного обеспечения.**

Предусмотрено административная, уголовная и гражданско-правовая ответственность за незаконное использование программного обеспечения.

1. Административная ответственность предусмотрена за ввод, продажу или другое незаконное использование контрафактного программного обеспечения, если это происходит в целях извлечения дохода.
2. Статья 7.12 КОАП. Должностное лицо, разрешившее сотрудниками применение контрафакта, будет оштрафовано, а не лицензионные программы конфискованы. Конфискованы будут и компьютеры, на которых программы установлены.
3. Авторское право и исключительное право
4. Ограничение доступа к информации, распространяемой с нарушением авторских прав
5. Правовое регулирование служебного произведения

Следует различать авторское право и исключительное право. Авторское право принадлежит непосредственно автору, оно не отчуждаемо и не передаваемо. Исключительное право может передаваться. Регулируются частью четвертой ГК РФ. Интеллектуальные права включают в себя исключительное право, которое относится к имущественным правам, а также личные неимущественные права. Интеллектуальное право не зависит от права собственности на материальный носитель. В случае, когда изготовление, распространение и иное использование интеллектуального права осуществляется с нарушением исключительного права, то материальные носители признаются контрафактными.

Пример нарушения авторского права при проведении предвыборной агитации. Признается нарушение авторского права, публикации или иное использование изображения, фотографии без согласия правообладателя, даже если эта информация находится в свободном доступе.

Статья 1281 ГК РФ регулирует срок действия исключительного права на произведение – 70 лет после смерти автора.

1. Должен определить провайдера.
2. Направить провайдеру уведомление (на русском и английском языках) о нарушении исключительных прав.

Провайдер в течение рабочего дня с получения уведомления, обязан уведомить обслуживаемого ими владельца информационного ресурса о необходимости ограничить доступ к незаконно размещенной информации.

Служебное произведение – статья 1295 ГК РФ содержит правовое регулирование служебного произведения. Авторское право на произведения науки, литературы и искусства, созданные в рамках трудового договора, принадлежит автору, а исключительные права принадлежат работодателю, если по договору не установлено иное.

Автор имеет право на вознаграждение. Статья 1296 ГК РФ регулирует исключительное право на произведения, созданные по заказу. Если, по заказу была создана программа для ЭВМ, БД или иное произведение, то исключительное право на них принадлежит заказчику. Исполнителю необходимо не использовать программу в коммерческих целях. Автор имеет право на вознаграждение.

**Юридическая ответственность за нарушение авторских и патентных прав**

За нарушение авторских, смежных, изобретательских и патентных прав предусмотрены 3 вида юридической ответственности:

1. Административная
2. Уголовная
3. Гражданско-правовая

Нормы уголовного и административного права – это публичное право. Юридическое последствие за нарушение или не исполнение нормы наступает в виде уголовного или административного наказания. Если наказание в виде штрафа – то он взыскивается в пользу государства. Гражданское право относится к отраслям частного права, здесь неблагоприятные последствия за нарушение или не исполнение/не надлежащее исполнение формы в виде возмещения ущерба или штрафа в пользу истца. Применение к нарушителю авторского и изобретательского права мер уголовного или административного наказания не исключает привлечение виновного по заявлению истца к гражданско-правовой ответственности.

Статья 7.12 КОАП предусматривает ответственность за нарушение авторских и смежных прав, изобретательских и патентных прав. Ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм **в целях извлечения дохода** в случае если экземпляры являются контрафактными, либо на них указана ложная информация о производителях… влечет административную ответственность для граждан от 1500 до 2000 штрафа с конфискацией контрафактных экземпляров и оборудования, на юридических лиц от 30 до 40 тысяч рублей с конфискацией контрафакта и оборудования.

Вторая часть статьи предусматривает ответственность за незаконное использование изобретения, полезной модели или промышленного образца присвоение авторства или принуждение к соавторству. Ответственность в виде штрафа в размере аналогично предыдущему.

Статья 14.33 КОАП предусматривает ответственность за недобросовестную конкуренцию, выразившуюся во введении в оборот товара с незаконным использованием результатов интеллектуальной деятельности для юридических лиц – от 0.01 до 0.15 суммы выручки правонарушителя, но не менее 100000.

В рамках дела об административном правонарушении в соответствии со статьей 27.14 КОАП может быть применена мера обеспечения производства по делу об административном правонарушении в виде ареста товара. По статье 29.10 вещи, изъятые из оборота, подлежат передаче в соответствующие органы или уничтожение.

Статья 14.58 КОАП предусматривает ответственность за осуществление проката и/или показа фильма без прокатного удостоверения на фильм.

Уголовная ответственность наступает только при наличии крупного ущерба.

Статья 146 УК РФ содержит наказание за нарушение авторских и смежных прав. Присвоение авторства, если это деяние причинило крупный ущерб автору или иному правообладателю. Наказывается штрафом до 200 тысяч рублей или арестом до 6-ти месяцев.

Незаконное использование объектов авторского прав или смежных прав равно как приобретение, хранение, перевозка контрафактных экземпляров в целях сбыта в крупном размере (100000) наказывается штрафом до 200 тысяч рублей или лишением свободы до двух лет. Если эти деяния совершены в особо крупном размере (1 миллион рублей) или группой лиц или с использованием служебного положения наказываются лишением свободы до 6-ти лет и штрафом до 500 тысяч рублей.

Статья 147 УК РФ предусматривает ответственность за нарушение изобретательских и патентных прав. Незаконное использование изобретения и полезной модели или промышленного образца разглашение без согласия автора сущности изобретения… до официальной публикации сведений и них, присвоение авторства или принуждение к соавторству, если это причинило крупный ущерб, может наказываться до двух лет лишения свободы.

Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой – лишение свободы до пяти лиц. Для вычисления крупного ущерба учитывается реальный ущерб, упущенная выгода, но не должен учитываться моральный вред потерпевшему в том числе связанный с подрывом его деловой репутации. Может быть проведена конфискация. На основании обвинительного приговора может быть произведена конфискация денег и имущества, полученных в результате совершения преступления, предусмотренного 147 УК РФ, а пока обвинительный приговор не вынесен на это имущество может быть наложен арест.

Гражданско-правовая ответственность.

В соответствии с частью первой статьи 1252 ГК РФ защита исключительных прав на результаты интеллектуальной деятельности осуществляется путем предъявления требований:

1. О пресечении действий, нарушающих право или создающих угрозу его нарушения
2. О возмещении убытков
3. О публикации решения суда о допущенном нарушении с указанием действительного правообладателя

По части второй статьи 1252 могут быть приняты обеспечительные меры в том числе может быть наложен арест на материальные носители, оборудование.

В соответствии с частью три статьи 1252 истец в праве требовать от нарушителя либо возмещения убытков, либо выплаты компенсации законом предусмотрена в трех вариантах:

1. От 10 тысяч до 5 миллионов рублей на усмотрение суда
2. В двукратном размере стоимости контрафактных экземпляров

Часть 4 статьи 1252 определяет какие материальные носителя являются контрафактными и что по решению суда они подлежат уничтожению без компенсации.

Убытки, причиненные поставкой товара с нарушением исключительного права, могут быть взысканы с поставщика.

Вывод: гражданская ответственность за нарушение авторского прав может наступить и при одновременном привлечении нарушителя к административной или уголовной ответственности.

Административная ответственность наступает только при условии преследования цели извлечения прибыли и, если размер меньше 100 тысяч рублей. Примечательно, что по уголовному праву ответственность наступает и без указания цели и извлечения прибыли, если автору причинен крупный ущерб (законом не определено), устанавливается судом или сумма продукции больше 100 тысяч.

В уголовном праве действует принцип презумпции невиновности. Он же распространяется и на административное право. В гражданском праве наоборот – презумпция виновности. Нарушитель авторского и изобретательского права несет ответственность, если не докажет свою невиновность.

**Правовое регулирование, распространение общедоступной информации сети интернет блогером и новостным агрегатором.**

1. Распространение блогером общедоступной информации
2. Распространение информации новостным агрегатором

Распространение блогером общедоступной информации. Статья 10.2 ФЗ «Об информации…» посвящена этому вопросу.

Блогером назван владелец сайта или страницы сайта в интернете, на которых размещается общедоступная информация и доступ к которой в течение суток составляет более 3 тысяч пользователей. Роскомнадзор ведет реестр сайтов и страниц сайтов в сети интернет, указанных параметров (общедоступная информация, 3к пользователей).

Обязанности блогера:

1. обязан проверять достоверность размещаемой информации
2. не должен допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства

Новостной агрегатор - владельцем новостного агрегатора назван владелец программы для ЭВМ, владелец сайта или страницы сайта в интернете, который используется для обработки и распространения новостей, доступ к которым в сутки более миллиона посетителей в сутки. В случае обнаружения такого информационного ресурса роскомнадзор признает новостным агрегатором и включает его в реестр новостным агрегаторов.

Новостному агрегатору хранить саму информацию и сведения о источнике её получения.

**Формирование и использование информационных ресурсов.**

Могут формироваться как органами государственной власти и предприятиями, так и организациями разного вида. В этой сфере проблема заключается в том, что информатизация органов государственной власти до сих пор ориентирована на повышение эффективности собственной деятельности, что приводит к созданию ведомственных автоматизированных систем для ограниченного круга пользователей.

Решение проблема: формирование единого информационного пространства, организация информационного взаимодействия при решении комплексным проблем управления обществом.

Информация эта должна быть прокомментирована, приближена к пользователю, а порядок её получения должен быть упрощен. Считается, что такую задачу должны взять на себя министерства культуры и юстиции.

Необходимо разработать комплекс мер по повышению информационной и компьютерной грамотности населения: от чтения курсов в ВУЗах, до пропаганды в СМИ.

Значительная часть информационных ресурсов формируется в негосударственном секторе экономики, где действуют организации, специализирующиеся на информационном обслуживании.

Задачи государственной политики включить не государственные структуры в единое информационное пространство.

В особых случаях государство должно иметь право выкупа информационных ресурсов у юридических и физических лиц.

Государственные информационные ресурсы.

Работу по формированию государственных информационных ресурсов могут выполнять негосударственные организации, за счет государственного бюджета по договору.

Государственные и не государственные информационные ресурсы, в конечном итоге, должны организовать систему использующую, как традиционные технологии, так и автоматизированные. Система должна быть открытой для включения в неё новых ресурсов.

**Тенденции развития информационных технологий (Рассолов)**

Последовательное развитие законодательства о системах блокировки вредной информации, размещаемой в интернете. Важным стало внесение изменений в ФЗ «Об информации…» и гражданский процессуальный кодекс. Так называемый закон «О право на забвение в интернете».

1. Не достоверная
2. Не актуальная

Информация о совершении преступления, по которому не погажена судимость и о преступлениях. Удалять заставили и иностранных операторов поисковых систем, распространяющих рекламу, адресованную россиянам.

Считается, что в ближайшие годы приоритетным сектором экономики станет промышленность и это повлияет на оборот информационной продукции.

Связано с правовым обучением в сфере развития информационных технологий.

1. PR
2. Регистратор
3. Программист

К продуктам такой деятельности относятся сайты и социальные сети.