# 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.