1. Факторы и условия формирования и развития информационного права.
2. Информация как правовая категория и объект права.
3. Электронная информация как объект права.
4. Информационная система как объект права.
5. Информационно-телекоммуникационная сеть как объект права.

1.Факторы и условия формирования и развития информационного права.

1)Научно-технические факторы:
Экспонентное развитие научно-технического прогресса, сформировавшее предпосылки для создания ЭВМ как самого важного технического средства социального прогресса в целом.
Использование на рубеже 1970-1980-х гг. новых технологических форм передачи информации, или цифровых линий связи.
Развитие нового класса наукоёмких (высоких) информационных технологий – мощного индикатора социальных преобразований
2)Социальные предпосылки (находят отражение в документах: Стратегия развития информационного общества; государственная программа «информационное общество»; концепция формирования электронного правительства) :
Массовая информатизация – организованный социально-экономический и научно-технический процесс удовлетворения информационных потребностей во всех сферах человеческой деятельности на основе внедрения ИТ и др.
Активное формирование информационного законодательства, развитие информатизации.
Внедрение в учебный процесс дисциплин информационно-правового цикла
Развитие науки правового обеспечения информационной сферы.
Проблемы информационного общества как фактор развития информационного права.
1)Углубление информационного противоборства как новая форма разрешения противоречий и общественного противостояния
2)Информационная безопасность и киберпреступность
3)Защита частной жизни человека в информационной сфере
4)Защита авторского права
5)Возможность «биологической революции»
Проблемы информационной свободы как фактор развития информационного права
Информационная свобода= право на информацию.
Информационная свобода определяется такими факторами, как:
1)Баланс соотношения прав и обязанностей
2)Взаимное уважение прав каждого человека
3)Высокий уровень информационной культуры

2. Информация как правовая категория и объект права.

ФЗ «об информации» зафиксировал определение информации как правовой категории:
Информация – это сведения, сообщения, данные, не зависимо от формы их представления. На основе данного определения информация и определяется как объект права.
Понятие – это слово, имеющее характерные признаки
Категория – это совокупность наиболее абстрактных признаков, т.е. научное языковое средство.
Слово и понятие информация обладает категориальными свойствами, т.е. является научной категорией.
Основные категориальные признаки информации имеют обобщенные выражения:
1)Предметы и объекты действительности
2)Отражённый образ предметов и объектов действительности
3)Сознание человека, с помощью которого отражается образ
4)Символ (внешняя форма образа) и его материальный носитель.
Информация, как категория, отражает наиболее существенные закономерные связи и взаимозависимости реальной действительности.
1)Персональные данные (ФЗ 2006г.)- информация личностного характера; информация о человеке, она включает в себя определенные признаки (индивидуальные). По этим признакам человек определяется в обществе, определяет его как физическое лицо.
Персональные данные – это информация о человеке, которая определяет его.
2)Рекламная информация (ФЗ 2006г. о рекламе) – строго экономическая категория, экономическая деятельность (коммерческая), адресованная неопределенному кругу лиц, с целью привлечения внимания.

3)Массовая информация (самый первый объект права – 1991г. ФЗ «о СМИ») – предназначенные неопределенному кругу лиц сведения и сообщения, а также другой материал (печатного, аудио- и телевизионного характера). Она характеризует свободу информации. Массовая информация как отражение свободы информации появилась в 1991г.
4)Кредитная история – она отражает процесс кредитора-заемщика, процесс исполнения кредитного договора (ФЗ «о кредитных историях» 2004г.).
5)Геномная информация (ФЗ 2008г. о государственной геномной регистрации в РФ) – некая кодированная информация персонального характера, в которой отражаются определенные фрагменты ДНК.

1.Информация как общенаучная категория, как образ жизни – это самый предельный уровень обобщения существующей действительности. Носит фундаментальный характер
2.Информация как правовая категория имеет обобщенные признаки конкретных фактов и объектов жизни (правоотношений). Выбранные правом и законодателем объекты, носящие актуальный характер.
3.Информация как объект права – правовая модель, обобщенный правовой образ конкретных благ материального и нематериального характера, но обязательно информация природы. Материальность – материальный носитель информации.

3. Электронная информация как объект права.

Электронная информация – образ существующей действительности, созданный и представленный в символьной (двоичной форме) с помощью специально созданного искусственного языка учётной записи в памяти ЭВМ.

Виды электронной информации: электронное сообщение, электронная подпись, универсальная электронная карта.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети
Телематическое электронное сообщение – одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом.

Спам – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, предоставленную без предварительного согласия абонента, не позволяющий определить отправителя).
Вирус – программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и пользователя, в т.ч. к сбору, обработке, передаче информации без согласия абонента и др.
Электронный документ – документированная информация, представленная в электронной форме, т.е. пригодной для восприятия человека с помощью ЭВМ, а также для передачи по информационно – телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (ЭП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Признаки:
1.Электронная цифровая форма
2.Присоединена к другой информации
3.Определение идентификация лица и документа.
Виды электронной подписи: простая и усиленная.
1.Простая электронная подпись – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
2.Усиленная (неквалифицированная) электронная подпись является электронной подписью, которая:
получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
позволяет определить лицо, подписавшее электронный документ;

позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи.
3.Усиленная квалифицированная электронная подпись – электронная подпись, при создании которой используются в специальное средство электронной подписи (ключ проверки электронной подписи), получившее подтверждение соответствия требованиям в квалифицированном сертификате ключа проверки электронной подписи.
Сертификат ключа проверки электронной подписи выдается аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти. Уполномоченным в сфере использования электронной подписи.

Универсальная электронная карта – электронный документ на материальном носителе в визуальной (графической) и электронной (машиносчитываемой) формах, содержащий информацию о пользователе картой, используемую для универсальных целей) (ч. 1 ст. 22 Федерального закона «О предоставлении государственных услуг»).
Признаки:
1.Универсальные цели использования карты.
2.Электронный документ, удостоверяющий личность граждан.
3.Материальный носитель, содержащий визуальную и электронную формы информации
4.Средство доступа к информации о пользователе картой и информационной системе.
УЭК является одним из технико-технологических средств, с помощью которых обеспечивается реализация прав, связанных с информационным воздействием в условиях функционирования систем «электронного правительства»

4. Информационная система как объект права.

Информационная система (ИС)– это совокупность баз данных, и обеспечивающих их обработку технических средств.
Виды информационных систем:
ФЗ «об информации»:
Государственные
Муниципальные
Иные (смежного характера)
ФЗ «об электронной подписи»:
Корпоративные
Общего пользования
Информация не является объектом собственности, она носит нематериальный характер (кроме объектов авторского права), а на информационные системы право собственности может быть.
Корпоративная информационная система – это информационная система, имеющая обязательный круг лиц, который определен законом (например, ГАС «Выборы»).
Информационные системы общего пользования – у данной системы неопределенный круг лиц и они не определяются законом, т.е. участником может стать любой человек (например, сеть Интернет).
Эти виды различаются для того, чтобы определить круг защиты информации.
Требования к информационным системам общего пользования при соединении с корпоративной информационной системой:
Защита информации;
Постоянный контроль над возможностью доступа к ним;
Работа этой системы должна быть устойчивой и бесперебойной и имела возможность быстрого восстановления в случае кризиса.
Субъекты участников информационных систем:
Оператор ИС – временно пользуется ИС, исполняя свою деятельность
Собственник ИС – постоянно пользуется ИС

5..Информационно-телекоммуникационная сеть как объект права.

В соответствии со ст. 2 Закона «Об информации» информационно-телекоммуникационная сеть — это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляете с использованием средств вычислительной техники.
Важнейшим признаком является свойство высокотехнологичности информационно-телекоммуникационной сети.
Следовательно, в состав информационно-телекоммуникационной сети обязательно должно входить три элемента:
•вычислительная техника, т.е. компьютеры;
•телефонные каналы связи;
•система доступа к каналам связи (коммутационное оборудование и регламенты их использования).
Информационно-телекоммуникационные сети могут быть:
•локальными(в одном здании, в какой-либо организации);
•ведомственными(охватывающими пользователей одного ведомства или корпорации);
•региональными(объединяющими пользователей городов, областей и других территориальных единиц);
•специального назначения (например, защищенная сеть государственной автоматизированной системы ГАС «Правосудие», государственной автоматизированной системы ГЛС «Выборы» и др.);
•глобальными(Интернет).
Признаки ИТС:
Технологичность (потому что сложное оборудование в сети)
Передача информации по техническим каналам связи (ФЗ «о связи»; ФЗ «об информации»)
Наличие доступа к информации
Ст.15 ФЗ «об информации» предусматривает правовые режимы использования сети.

1. Общие условия правового режима ИТС.
1.1. НПА об ИТС:
• ФЗ Об информации от 27.07.2006 №149-ФЗ
• ФЗ О связи от 7.07.2003 №126-ФЗ
• ФЗ О защите детей от информации, причиняющей вред их здоровью и развитию от 29.12.2010 №436-ФЗ
• КоАП РФ
• подзаконные акты (Указы ПРФ и постановления Правительства РФ)
• Указ Президента РФ от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности РФ»
• Постановление Правительства РФ от 31.07.2014 «О порядке взаимодействия Роскомнадзора и блогеров»

1.2. Основные понятия правового режима ИТС
1) Сайт в сети Интернет
2) Страница сайта в сети Интернет
3) Доменное имя
4) Сетевой адрес
5) Владелец сайта в сети Интернет
6) Провайдер хостинга
7) Обладатель информации
8) Оператор связи
9) Организатор распространения информации в сети Интернет
10) Блогер
11) Оператор информационной системы
12) Доступ к информации
13) Распространение информации
14) Предоставление информации

2. Правовой режим распространения информации в ИТС.
2.1. Общие условия распространения Информации в сети (ст.10 Закона Об информации).
1. В РФ распространение информации осуществляется свободно при соблюдении требований, установленных законодательством РФ.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.
3. При использовании для распространения информации средств, позволяющих определить получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.
4.
5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются ФЗ (ФЗ от 29.12.1994 №77 «Об обязательном экземпляре документов»).
6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная ответственность или административная ответственность.
Эти виды запрещенной информации дополнены случаи распространения информации, предусмотренные ст.10-2 (обязанности блогера) и 15-1 (Единый реестр доменов и сетевых адресов, запрещенной информации о защите детей) Закона об информации.

2.2. Основные субъекты правового режима распространения информации в ИТС.
1) Роскомнадзор - федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере СМИ, массовых коммуникаций, информационных технологий и связи.
2) Владелец в сети Интернет - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет, в том числе порядок размещения информации на таком сайте.
3) Провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет
4) Оператор связи – ЮЛ или ИП, оказывающие услуги связи на основании соответствующей лизенции.
5) Организатор распространения информации в сети Интернет - лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приёма, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет.
6) Блогер – владелец сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более 3тыс. пользователей сети Интернет.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор – http://RKN.GOV.RU/

3. Основные положения правового режима распространения информации в ИТС (со.10-1, 10-2, 15.3-15.5) ФЗ «Об информации».
Со.10-1. Обязанности организатора распространения информации в сети Интернет:
- уведомить Роскомнадзор о начале осуществления своей деятельности
- хранить голосовую информацию, письменный текст, изображения, звук или иные электронные сообщения пользователей сети Интернет информацию об этих пользователях в течение 6 месяцев
- обеспечивать реализацию установленных Роскомнадзором требований безопасности к оборудованию и программно-техническим средствам.

Ст.10-2. Обязанности блогера:
1) не допускать использование сайта или страницы сайта в сети Интернет в целях совершения уголовно наказуемым деяний, для разглашения сведений, составляющих государственную или иную специальную охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;
2) проверять достоверность размещаемой общедоступной достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;
3) не допускать распространение информации о частной жизни гражданина;

4) соблюдать запреты и ограничения, предусмотренные законодательством РФ о выборах;
5) соблюдать требования законодательства РФ, регулирующие порядок распространения массовой информации;
6) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

Ст.10-2. Особенности распространения информации блогером (запреты).
2. При размещении информации на сайте или странице сайта в сети Интернет не допускается:
1) использование сайта или страницы сайта в сети Интернет в целях сокрытия или фальсификации общественно значимых сведений, распространения заведомо недостоверной информации под видом достоверных сообщений;
2) распространение информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

Статья 10-2. Особенности распространения блогером общедоступной информации.
ст.15-4, п.3, п.7. Владельцы сайтов в сети Интернет, которые зарегистрированы в соответствии с Законом РФ от 27 декабря 1991 №2124 «О СМИ» в качестве сетевых изданий, не являются блогерами.

18. Понятие информационного права.
Информационное право – это комплексная структурно сложная система норм (нормативных актов), регулирующих общественные отношения оп поводу информации и связанных с ней систем, а также система знаний в области правового обеспечения ИО (наука и учебная дисциплина).
ИП как отрасль законодательства включает в себя специальные законы, подзаконные НПА и отдельные нормы отраслевых законодательных актов.
ИП как наука и учебная дисциплина
Наука Учебная дисциплина
Объект – закономерности правового обеспечения информационной действительности Объект – базовые, общие (элементарные_ знания и умения (навыки)
Предмет – модели решения проблем (нерешенные задачи и вопросы) науки ИП Предмет – вопросы, входящие в содержание общих знаний и умений (компетенций)

Задача – производство новых знаний в области правового обеспечения информационной сферы Задача – получение профессиональных знаний и умений (компетенций) в области правового обеспечения информационной сферы

Формальный результат – научная аттестация высшей категории и получение диплома кандидата (доктора) юридических наук
Формальный результат – профессиональная аттестация и получение диплома высшего профессионального образования
Содержание – исследование, анализ закономерностей развития правового обеспечения информационной сферы Содержание – изучение наиболее общих вопросов, входящих в состав учебной программы (лекции, учебные издания, практические занятия), а также контроль знаний и экзамены
Объем научных знаний не имеет пределов Объем учебных знаний ограничен рамками учебной программы

ИП как отрасль системы права.
Признаки отрасли:
1. Особый (уникальный) предмет – информационные правоотношения (уникальность их структуры – объекта, специальных субъектов и содержание информационных правоотношений). Ни одна из отраслей не выделяет такой предмет.
2. Самостоятельный понятийный аппарат правового регулирования информационных правоотношений.
3. Нормативные принципы ИП.
4. Комплексно используются правовые методы – императивный, диспозитивный и их сочетание.
5. Формируются комплексные (охватывают сразу несколько отраслей права) правовые режимы различных видов информации и информационной деятельности.

19. Система информационного права.
Система информационного права
- это объективно существующая совокупность норм, регулирующих правоотношения в информационной сфере и сгруппированных в относительно самостоятельные структурные подразделения (правовые институты).
Правовой институт – это взаимосвязанная и относительно обособленная группа норм ИП, регулирующих однородные О/О.
ИП подразделяется на общую и особенную части. В общей сосредоточены нормы, имеющие базовое значение для всех институтов особенной части (базовые категории, понятия, предмет, особенности метода, принципы, источники и система законодательства…), и общие правовые институты: институт права на информацию; институт доступа к информации и ИС-ам.
Особенная часть состоит из отдельных правовых институтов – групп обособленных норм ИП, регулирующих однородные общественные отношения:
1)Нормы, определяющие правовой режим информационных ресурсов.
2)Нормы, определяющие правовой режим информации ограниченного доступа.
3)Нормы, определяющие правовой режим ИС.
4)Нормы, определяющие правовой режим деятельности в области телекоммуникаций.
5)Нормы, определяющие правовой режим распространения массовой информации.
6)Нормы, определяющие правовой режим обеспечения ИБ.
7)Нормы, определяющие правовой режим международного информационного обмена.

20. Информационное право как наука и учебная дисциплина.
ИП как наука и учебная дисциплина
Наука Учебная дисциплина
Объект – закономерности правового обеспечения информационной действительности Объект – базовые, общие (элементарные_ знания и умения (навыки)

Предмет – модели решения проблем (нерешенные задачи и вопросы) науки ИП Предмет – вопросы, входящие в содержание общих знаний и умений (компетенций)

Задача – производство новых знаний в области правового обеспечения информационной сферы Задача – получение профессиональных знаний и умений (компетенций) в области правового обеспечения информационной сферы

Формальный результат – научная аттестация высшей категории и получение диплома кандидата (доктора) юридических наук Формальный результат – профессиональная аттестация и получение диплома высшего профессионального образования

Содержание – исследование, анализ закономерностей развития правового обеспечения информационной сферы Содержание – изучение наиболее общих вопросов, входящих в состав учебной программы (лекции, учебные издания, практические занятия), а также контроль знаний и экзамены

Объем научных знаний не имеет пределов Объем учебных знаний ограничен рамками учебной программы

21. Место информационного права в системе правовых знаний.

Информационное право как комплексная отрасль, объединяющая в предметной области регулирования однородную группу общественных отношений, тесно взаимодействует с профилирующими отраслями права и прежде всего конституционным, гражданским и административным правом.

Эта взаимосвязь прослеживается, в частности, на следующих примерах.

Конституционное право оперирует понятиями, непосредственно связанными с предметом регулирования информационного права. Нормы Конституции РФ провозглашают свободу информации, закрепляют содержание конституционного права на информацию, гарантируют защиту информации, находящейся в режиме личной, семейной, государственной тайны.

Гражданское право связано с информационным посредством правила, закрепленного в п. 1 ст.5 Федерального закона «Об информации, информационных технологиях и о защите информации». Согласно указанному правилу информация может являться объектом публичных, гражданских и иных правовых отношений. Информация

может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.
Административное право взаимодействует с информационным правом прежде всего посредством наличия в том и другом отношений субординации. Например, запрещено допускать предприятия, учреждения и организации к проведению работ, связанных с использованием сведений, составляющих государственную тайну, без наличия соответствующей лицензии (ст. 27 Закона РФ «О государственной тайне»).
Взаимодействие информационного права с профилирующими и специальными отраслями права не стирает границ, которые объективно пролегают между сферой общественной жизни и деятельности, связанной с информацией, и другими сферами общественных отношений, урегулированных нормами иной отраслевой принадлежности.
От конституционного права информационное право отличается тем, что предметом последнего являются отношения, связанные с созданием условий реализации права на информацию, а не отношения по установлению пределов и характера государственного регулирования в основных сферах общественного развития и взаимоотношения государства с человеком и гражданином с точки зрения прав и свобод последнего. В Конституции РФ провозглашены и закреплены лишь основные устои информационных отношений, определенные через права и свободы человека и гражданина.
Отграничение гражданского права от информационного права состоит в том, что объектом информационных отношений является информация как благо особого рода, существующее в единстве со своим материальным носителем. Информация существует по особым объективным законам природы и человеческого бытия, поэтому отличается специфическим режимом юридического регулирования, не всегда основанным на равенстве участников информационных отношений и товарно-денежном характере этих отношений.
От административного права, являющегося отраслью, призванной регулировать управленческие отношения и обладающей устойчивым предметом регулирования, информационное регулирование отличается тем, что хотя в нем и присутствуют отношения власти и подчинения, но они касаются управления лишь частью спектра информационных отношений, за пределами которых соподчиненность прекращается. Элемент субординации, присутствующей в информационном праве, носит строго ограниченный законом характер, поскольку компетентные органы не вправе выходить за рамки своих полномочий и установленного для них регламента.
Подводя итог сказанному, сделаем следующий вывод: информационное право занимает самостоятельное место в системе российского права в качестве комплексной отрасли, его нормы регулируют специфические группы информационных отношений, составляющих обособленный, но тесно взаимосвязанный с иными отраслями права предмет регулирования.

22. Предмет информационного права.

Предмет информационного права - область общественных отношений, связанных с формированием и использованием информационных ресурсов, информатизацией, ИС-ми и телекоммуникационной деятельностью, а также обеспечением ИБ.
В предмет входят:
Правоотношения, возникающие при производстве, обработке, хранении, передаче и использовании информационных ресурсов независимо от формы из предоставления.
Информатизация, деятельность по формированию и использованию ИС, ИТ и др., а также общественные отношения, возникающие по поводу производства и использования ИТ как самостоятельных объектов и отношения, связанные с лицензированием различных видов информационной деятельности.
Информатизация – это организованный социально-экономический и научно-технический процесс удовлетворения информационных потребностей на основе формирования и использования ИР, применения ЭВМ и ИКТ.
Телекоммуникационные ПО – деятельность по поводу передачи информации по техническим каналам связи, в т.ч. по их созданию, эксплуатации и использованию.
Правоотношения по поводу обеспечения ИБ, т.е. защиты интересов ЛОГ в информационной сфере, а также защиты информации.

23. Многообразие методов информационного права.

В правовом регулировании применяются два взаимно противоположных базовых метода. Первый — метод субординации (императивный), когда положение субъектов характеризуется отношениями подчиненности. Регулирование в данном случае осуществляется на властных началах, в юридическом инструментарии преобладают приказы и распоряжения, а основными способами воздействия на отношения (способами регулирования) являются запреты и позитивные обязывания.
В информационном праве существует несколько групп отношений, которые складываются на началах власти и подчинения. Это прежде всего отношения по формированию государственных информационных систем, по управлению информационными процессами, по обеспечению информационной безопасности, по охране информации, находящейся в режиме государственной тайны.
Второй — метод координации (диспозитивный), который строится на основе равенства участников правоотношений и их автономии. В юридическом инструментарии этого метода преобладают соглашения, а среди способов регулирования ведущую роль играют дозволения. В информационном праве к отношениям, которые складываются на началах равенства сторон и их имущественной самостоятельности, прежде всего принадлежат отношения, возникающие по поводу информации, находящейся в режиме коммерческой тайны, и отношения по предоставлению информации.
Таким образом, в информационном праве проявляются оба базовых метода правового регулирования. При этом может иметь место их специфическое сочетание, которое дополняется конкретными методами правового воздействия и особым правовым инструментарием.
Взаимосвязь публичных и частных начал в регулировании общественных отношений, возникающих по поводу информации, свидетельствует не только о разносторонности правового регулирования этих отношений, но и о том, что информационное право следует рассматривать как целостное образование, регламентирующее специфический и сравнительно новый вид отношений.
В то же время своего специфического метода правового регулирования информационное право не имеет, для него характерны оба базовых универсальных метода — императивный и диспозитивный.

24. Понятие и система принципов информационного права.
Принципы ИП – это основные исходные идеи, руководящие положения, которые определяют содержание правового регулирования информационных правоотношений и других сторон правового обеспечения информационной сферы (нормотворчества, правоприменения и толкования).
Система принципов ИП:
Общеправовые (конституционные) принципы закреплены в КРФ: принцип уважения прав человека, принцип свободы информации, принцип защиты частной жизни, принцип законности.
Отраслевые принципы (характерны исключительно для ИП): принцип баланса интересов ЛОГ в информационной сфере, принцип открытости информации, принцип достоверности информации, принцип технологической обусловленности.
1.Принцип свободы информации (ч.4.ст. 29 К РФ) – каждый имеет право свободно искать, получать, производить и распространять информацию любым законным способом.
Принцип свободы информационных действий является первоначальным правом на информацию. Принцип свободы информации имеет значение для общечеловеческой культуры, независимо от их форм. Право на информацию является естественным правом человека. Свобода информации обладает цивилизационной ценностью для общеправовой культуры.
С точки зрения философии: свобода информации - это структурно-сложное, пространственно-волевое явление человеческой деятельности. Соизмерение в пространстве и волевом. Волевое – всеобщий формуляр нравственного императива: во всем поступай так и таким образом, как ты бы хотел, чтобы остальные поступали аналогично по отношению к тебе.
Свободу информации нужно понимать как, соотношение одного пространства человека с другим, а также волеизъявление. Свобода наша заканчивается там, где начинается свобода другого.
Свободу информации нужно соизмерять с категориями: свобода и необходимость, свобода и ответственность.
Данный принцип имеет исключение (п.3 ст.55 К РФ): предусматривает, что права и свободы гражданина могут быть ограничены ФЗ и в той мере, в какой необходимо в целях защиты:
1)Основ конституционного строя
2)Нравственности
3)Здоровья
4)Прав и законных интересов других лиц

5)Обеспечение обороны страны
6)Безопасность государства
Перечень исчерпывающий. Свобода информации может быть ограничена.
Конституционный принцип свободы информации реализуются в следующих законах: ФЗ «об информации»; ФЗ «об обеспечении доступа к информации» (официальной, судебной); ФЗ «о предоставлении государственных и муниципальных услуг»; КоАП РФ; УК РФ.
2.Принцип уважения прав человека. В ст. 30 Всеобщей декларации прав человека (впервые): никому не дозволено нарушать права и законные интересы человека.
П.3 ст. 17 К РФ: осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (те, кто не соблюдает, тот злоупотребляет правом).

3.Принцип законности. Он проявляется в двух началах: верховенство Конституции и ее законов, а также единство понимания, исполнения и применения Конституции и законов. Верховенство: Конституция имеет самую высшую власть. Верховенство конституции и законов обладают высшей юридической силу.
Единство: единство распространение на всей территории РФ. Ведомственное единство: не нарушение законов и иным НПА Конституции.
4.Принцип неприкосновенности частной жизни. Нормативная база: ст. 12 Всеобщей декларации прав человека фиксирует запрет на вмешательство в личную жизнь и семейную тайну, а также на тайну корреспонденции, честь, достоинство и репутацию. Ст. 23-24 К РФ также формулируют принцип неприкосновенности (ст. 23: защита семейной тайны, тайну переписки и телефонных переговоров, почтовых и телеграфных сообщений. Ограничение этого права только на основании судебного решения; ст. 24: фиксирует запрет неприкосновенности личной жизни человека, информации личностной информации. Сбор информации без согласия человека не допускается).

Отраслевые принципы
1.Принцип баланса интересов в информационной сфере.
п. 8 Доктрины информационной безопасности в РФ: баланс интересов личности, общества и государства в информационной сфере; ст. 6 ФЗ «о государственной тайне». Выбор сведений, которые включаются или исключаются из сведений государственной тайны, регулирующие данным принципом.
Баланс интересов – это уравновешивание интересов личности, общества и государства. Не должно быть приоритета одного из названных интересов. Приоритет личности не должен преобладать над интересами общества или государства. Баланс интересов - это критерий устойчивости информационной сферы.
По доктрине:
Интересы личности: свобода поиска информации (ст. 29 К РФ), защита персональных данных, духовное и культурное развитие личности.
Интересы общества: создание условий для общественного согласия, обеспечение распространение СМИ позитивного содержания информации.
Интересы государства: защита и укрепление конституционного строя, суверенитета и территориальной целостности государства; укрепление законности и правопорядка в информационной сфере (профилактика правонарушений).
Принцип баланса интересов может нарушаться: когда преобладают интересы личности, персоналии ставят свои интересы выше других; может нарушаться со стороны гос-ва, интересы гос-ва с помощью закона ставить свои интересы выше других.
2.Принцип открытости информации.
В ст. 3 ФЗ «об информации», закреплен в деятельности государственных органов, органов местного самоуправления, а также свобода доступа информации. Ст. 7 ФЗ «об информации»: общедоступной информация - общеизвестные сведения и иная информация, доступ к которой не ограничен. В ст. 8 установлено правило, согласно которому не может быть ограничен доступ к следующим видам информации:
к НПА и вообще ко всей правовой информации;
информация о состоянии окружающей среды (экологическая информация);
информация о деятельности государственных органов, органов местного самоуправления (за исключением сведений составляющих государственную тайну);
информация, накапливаемая в библиотечных, музейных и архивных фондах (за исключением персональных данных, сведений составляющих государственную тайну);

для всех видов иной информации, недопустимость ограничения которой оговаривается в ФЗ.
Исключения из принципа открытости информации: ст. 55 К РФ; ст. 9 ФЗ «об информации» дублирует эту статью.
Ограничение открытости информации допускается только на основании ФЗ, никакими подзаконными актами, ведомственными приказами не должен ограничиваться доступ к информации.
Основания для ограничения (перечень закрытый):
- защита основ конституционного строя;
- нравственность;
- здоровье человека;
- права и законные интересы других лиц;
- обеспечение обороны страны и безопасности государства.
Реализуется принцип открытости в двух ФЗ «о доступе к информации» (государственной и муниципальной информации, судебной информации).
Нормы правоохранительных законодательных актов (УК, КоАП) предусматривает ответственность за нарушение этого принципа 13.27, 13.28 – ответственность за нарушение к доступу информации; ст. 283, 183 - ответственность за получение сведений ограниченного доступа.
3.Принцип достоверности информации.
Вытекает из природы и сущности информации. ст. 42 К РФ: защиты окружающей среды и человека от загрязнений, право каждого человека на достоверную информацию об окружающей среде. Ст. 3 ФЗ «об информации»: право человека на своевременно предоставленную информацию. ФЗ «о персональных данных» в ст. 5 также закрепляет этот принцип: адекватность информации рассматривается как ее достоверность. ФЗ «об обеспечении доступа к официальной информации» ст. 11: достоверность представляемой для населения и каждого пользователя информации.

4.Принцип технологической обусловленности.
Вытекает из характера научно-технического процесса. Прослеживается связь ИП с технической и технологической средой информационной сферы. Электронное правительство – концепция. Единая система межведомственного информационного взаимодействия от 8 сентября (Постановление Правительства). Межведомственное информационное взаимодействие – это совокупность электронных сервисов построенных на общепринятых стандартах, использующие единые технологические решения, единые классификаторы электронных структур и электронных БД. ФЗ «о связи» употребляет такие термины как: нумерация, средства связи, трафик. Без этих терминов мы не сможем описать законы, связанные с информационной средой.

25. Конституционные принципы информационного права.
Принцип свободы информации (ч.4.ст. 29 К РФ) – каждый имеет право свободно искать, получать, производить и распространять информацию любым законным способом.
Принцип свободы информационных действий является первоначальным правом на информацию. Принцип свободы информации имеет значение для общечеловеческой культуры, независимо от их форм. Право на информацию является естественным правом человека. Свобода информации обладает цивилизационной ценностью для общеправовой культуры.
С точки зрения философии: свобода информации - это структурно-сложное, пространственно-волевое явление человеческой деятельности. Соизмерение в пространстве и волевом. Волевое – всеобщий формуляр нравственного императива: во всем поступай так и таким образом, как ты бы хотел, чтобы остальные поступали аналогично по отношению к тебе.
Свободу информации нужно понимать как, соотношение одного пространства человека с другим, а также волеизъявление. Свобода наша заканчивается там, где начинается свобода другого.
Свободу информации нужно соизмерять с категориями: свобода и необходимость, свобода и ответственность.
Данный принцип имеет исключение (п.3 ст.55 К РФ): предусматривает, что права и свободы гражданина могут быть ограничены ФЗ и в той мере, в какой необходимо в целях защиты:
7)Основ конституционного строя
8)Нравственности
9)Здоровья
10)Прав и законных интересов других лиц

11)Обеспечение обороны страны
12)Безопасность государства
Перечень исчерпывающий. Свобода информации может быть ограничена.
Конституционный принцип свободы информации реализуются в следующих законах: ФЗ «об информации»; ФЗ «об обеспечении доступа к информации» (официальной, судебной); ФЗ «о предоставлении государственных и муниципальных услуг»; КоАП РФ; УК РФ.
Принцип уважения прав человека. В ст. 30 Всеобщей декларации прав человека (впервые): никому не дозволено нарушать права и законные интересы человека.
П.3 ст. 17 К РФ: осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (те, кто не соблюдает, тот злоупотребляет правом).

Принцип законности. Он проявляется в двух началах: верховенство Конституции и ее законов, а также единство понимания, исполнения и применения Конституции и законов. Верховенство: Конституция имеет самую высшую власть. Верховенство конституции и законов обладают высшей юридической силу.
Единство: единство распространение на всей территории РФ. Ведомственное единство: не нарушение законов и иным НПА Конституции.
Принцип неприкосновенности частной жизни. Нормативная база: ст. 12 Всеобщей декларации прав человека фиксирует запрет на вмешательство в личную жизнь и семейную тайну, а также на тайну корреспонденции, честь, достоинство и репутацию. Ст. 23-24 К РФ также формулируют принцип неприкосновенности (ст. 23: защита семейной тайны, тайну переписки и телефонных переговоров, почтовых и телеграфных сообщений. Ограничение этого права только на основании судебного решения; ст. 24: фиксирует запрет неприкосновенности личной жизни человека, информации личностной информации. Сбор информации без согласия человека не допускается).

26. Отраслевые принципы информационного права.
5.Принцип баланса интересов в информационной сфере.
п. 8 Доктрины информационной безопасности в РФ: баланс интересов личности, общества и государства в информационной сфере; ст. 6 ФЗ «о государственной тайне». Выбор сведений, которые включаются или исключаются из сведений государственной тайны, регулирующие данным принципом.
Баланс интересов – это уравновешивание интересов личности, общества и государства. Не должно быть приоритета одного из названных интересов. Приоритет личности не должен преобладать над интересами общества или государства. Баланс интересов - это критерий устойчивости информационной сферы.
По доктрине:
Интересы личности: свобода поиска информации (ст. 29 К РФ), защита персональных данных, духовное и культурное развитие личности.
Интересы общества: создание условий для общественного согласия, обеспечение распространение СМИ позитивного содержания информации.
Интересы государства: защита и укрепление конституционного строя, суверенитета и территориальной целостности государства; укрепление законности и правопорядка в информационной сфере (профилактика правонарушений).
Принцип баланса интересов может нарушаться: когда преобладают интересы личности, персоналии ставят свои интересы выше других; может нарушаться со стороны гос-ва, интересы гос-ва с помощью закона ставить свои интересы выше других.
6.Принцип открытости информации.
В ст. 3 ФЗ «об информации», закреплен в деятельности государственных органов, органов местного самоуправления, а также свобода доступа информации. Ст. 7 ФЗ «об информации»: общедоступной информация - общеизвестные сведения и иная информация, доступ к которой не ограничен. В ст. 8 установлено правило, согласно которому не может быть ограничен доступ к следующим видам информации:
к НПА и вообще ко всей правовой информации;
информация о состоянии окружающей среды (экологическая информация);
информация о деятельности государственных органов, органов местного самоуправления (за исключением сведений составляющих государственную тайну);
информация, накапливаемая в библиотечных, музейных и архивных фондах (за исключением персональных данных, сведений составляющих государственную тайну);

для всех видов иной информации, недопустимость ограничения которой оговаривается в ФЗ.
Исключения из принципа открытости информации: ст. 55 К РФ; ст. 9 ФЗ «об информации» дублирует эту статью.
Ограничение открытости информации допускается только на основании ФЗ, никакими подзаконными актами, ведомственными приказами не должен ограничиваться доступ к информации.
Основания для ограничения (перечень закрытый):
- защита основ конституционного строя;
- нравственность;
- здоровье человека;
- права и законные интересы других лиц;
- обеспечение обороны страны и безопасности государства.
Реализуется принцип открытости в двух ФЗ «о доступе к информации» (государственной и муниципальной информации, судебной информации).
Нормы правоохранительных законодательных актов (УК, КоАП) предусматривает ответственность за нарушение этого принципа 13.27, 13.28 – ответственность за нарушение к доступу информации; ст. 283, 183 - ответственность за получение сведений ограниченного доступа.
7.Принцип достоверности информации.
Вытекает из природы и сущности информации. ст. 42 К РФ: защиты окружающей среды и человека от загрязнений, право каждого человека на достоверную информацию об окружающей среде. Ст. 3 ФЗ «об информации»: право человека на своевременно предоставленную информацию. ФЗ «о персональных данных» в ст. 5 также закрепляет этот принцип: адекватность информации рассматривается как ее достоверность. ФЗ «об обеспечении доступа к официальной информации» ст. 11: достоверность представляемой для населения и каждого пользователя информации.

8.Принцип технологической обусловленности.
Вытекает из характера научно-технического процесса. Прослеживается связь ИП с технической и технологической средой информационной сферы. Электронное правительство – концепция. Единая система межведомственного информационного взаимодействия от 8 сентября (Постановление Правительства). Межведомственное информационное взаимодействие – это совокупность электронных сервисов построенных на общепринятых стандартах, использующие единые технологические решения, единые классификаторы электронных структур и электронных БД. ФЗ «о связи» употребляет такие термины как: нумерация, средства связи, трафик. Без этих терминов мы не сможем описать законы, связанные с информационной средой.

27. Понятие и система источников информационного права.
Источники ИП – официальные формы закрепления и существования правовых норм, регулирующих информационные правоотношения.
Система:
* НПА;
* Договоры;
* Санкционированные обычаи.
По уровню:
1. Международные акты. Основные – международные договоры. В них могут фиксироваться основные принципы и нормы.
2. Федеральное законодательство: КРФ, ФКЗ, ФЗ, Кодексы, указы президента, постановления правительства и др. подзаконные акты.
3. Законодательные акты и подзаконные акты субъектов РФ.
4. НА ОМС относятся к локальному уровню правового регулирования, они определяют особенности правовых режимов муниципальных ИС.
5. Нормативные документы предприятий и организаций также относятся к локальному уровню. Это приказы и инструкции, в которых содержатся нормы, регулирующие общественные отношения по поводу объектов ИП. Они возникают между работодателем и работником или между работниками.
6. Постановления КС РФ и других высших судебных инстанций. Постановления КС являются источником, т.к. в их текстах содержатся правовые позиции суда, адресованные законодателю и всем судам. Ими устраняются пробелы в правовом регулировании.

7. Стандарты, технические правила и условия регулируют организационные отношения, связанные и информатизацией.
8. Административные и технические регламенты определяют правила информационного взаимодействия: человек-машина-человек – административные; машина-машина – технологические.
9. Юридические обычаи. Это сложившиеся и широко применяемые правила поведения, не предусмотренные законодательством.

28. Система информационного законодательства.

Вся система информационного законодательства состоит из:
Базовые законы
Специальные законы
Отраслевые законы
Базовые законы: в них содержатся общий нормативный правовой климат правовой сферы, формируется с помощью общих правовых положений. Содержатся в базовых положениях:
основные понятия и их определения;
принципы правового регулирования (ст.3 ФЗ «об информации»; ФЗ «о персональных данных»);
правовой статус основных субъектов информационных правоотношений: основные права и основные обязанности – оператор, владелец и пользователь информационной системы (ФЗ «об информации», ФЗ «о связи»);
общеправовой режим информации
ФЗ «об информации»: содержит основные определения терминов, действующих во всей правовой системе. Термины и определения распространяются на все ФЗ и НПА. Принципы (ст.3: принцип достоверности; принцип доступности; принцип защищенности; принцип информационной безопасности и др. Оператор, владелец, пользователь – общие условия (ст.12 и 14 ФЗ «об информации»).
ФЗ «об электронной подписи»: содержит основные понятия и термины (электронная подпись, ключ электронной подписи и др.), виды, принципы.
ФЗ «о связи»: содержит понятия (электротехническая связь, трафик, правовой статус оператора и абонента связи, тайна оператора связи).
ФЗ «о доступе к официальной информации».
ФЗ «о доступе к судебной информации»: содержит определения, термины (портал, сайт), принципы доступа к информации, права и обязанности тех субъектов, которые находятся в этом ФЗ.
ФЗ «о персональных данных»: содержит понятия и термины (оператор персональных данных, кто к ним относится, кто относится к владельцам персональных данных), принципы, права и обязанности основных субъектов. Особенности применения ФЗ «о персональных данных» содержатся в трудовом кодексе и в ФЗ «о государственной гражданской службе в РФ».
Базовые законы действуют на информационные правоотношения двуедино: они закрепляют общеправовой режим и общеправовое положение; с другой стороны они содержат конкретные правила поведения (ФЗ «об информации», ФЗ «о персональных данных», ФЗ «о связи», ФЗ «об электронной подписи»).

Специальные законы: они закрепляют в себя нормы, которые регулируют правоотношения в области отдельных видов информационной деятельности.
Виды информационной деятельности:
сфера государственного управления (государственная регистрация по дактилоскопической экспертизе, геномной информации);
деятельность по обеспечению избирательной системы (ГАС Выборы);
предпринимательская деятельность (ФЗ «о кредитной истории», ФЗ «о рекламе», ФЗ «об инсайдерской информации»);
деятельность по организации торгов;
деятельность по распространению массовой информации (ФЗ «О СМИ»);
Функции специальных законов:
1.определение специального правового режима отдельных видов информации;
2. определение специальных правовых требований к формированию отдельных объектов (информационно-телекоммуникационная сеть, информационная система);

3.закрепление тех основных правовых положений, которые дополняют базовые законы.
Отраслевые законы: к ним относятся отраслевые кодексы (ТК, ГК, УК, процессуальные кодексы, НК, КоАП, Таможенный К.). Они регулируют правоотношения по использованию отраслевых объектов информационного права (ч.4 ГК: правовая защита объектов авторского права. Ст. 494 и 495 ГК содержат требования к товарам и услугам: ст. 160 ГК закрепляет использование электронной подписи в гражданских сделках); УК закрепляет ответственность за совершение информационных преступлений (гл. 28); ТК содержит множество статей предусматривающих специальный правовой режим персональных данных, предусматривает дисциплинарную ответственность за нарушение в области персональных данных; КоАП предусматривает более 100 составов административных правонарушений (глава 13).
Подзаконные акты источников ИП: постановления правительства и указы президента.
Их насчитывается около 1000. Среди них выделяем:
Постановление Правительства РФ «о межведомственном электронном взаимодействии» (правовые требования, права и обязанности, все субъекты информационного взаимодействия, пользователи информационного взаимодействия)
Постановление Правительства РФ от 24 марта 2011 года «о технических требованиях к электронной карте»
Постановление Правительства РФ «о порядке ввода в эксплуатацию государственных информационных систем» (правовые требования к эксплуатации информационных систем государственного назначения; реестр федеральных государственных систем. Реестр – это специальная информационная система, содержащая сведения о государственных информационных системах, предназначенных для предоставления услуг и использования государственных функции.
Указ Президента РФ от 17 марта 2008 года «о мерах по обеспечению информационной безопасности в сетях Интернет»: предусматривает требования подключения к информационной системе; если в информационной системе государства содержится информация ограниченного доступа, то запрещено подключать такую систему к сети интернет; использование сертифицированных средств защиты информации.
Постановление Правительства РФ от 3 ноября 1994 года «об утверждении положения о порядке обращения со служебной информации, ограниченного распространения федеральных органов государственной власти» («положение о служебной информации»): понятие служебной информации, правовой режим создания и использования служебной информации; порядок обращения со служебной информацией; порядок защиты служебной информации

29. Базовые законы информационного права.
Базовые законы: в них содержатся общий нормативный правовой климат правовой сферы, формируется с помощью общих правовых положений. Содержатся в базовых положениях:
основные понятия и их определения;
принципы правового регулирования (ст.3 ФЗ «об информации»; ФЗ «о персональных данных»);
правовой статус основных субъектов информационных правоотношений: основные права и основные обязанности – оператор, владелец и пользователь информационной системы (ФЗ «об информации», ФЗ «о связи»);
общеправовой режим информации
ФЗ «об информации»: содержит основные определения терминов, действующих во всей правовой системе. Термины и определения распространяются на все ФЗ и НПА. Принципы (ст.3: принцип достоверности; принцип доступности; принцип защищенности; принцип информационной безопасности и др. Оператор, владелец, пользователь – общие условия (ст.12 и 14 ФЗ «об информации»).
ФЗ «об электронной подписи»: содержит основные понятия и термины (электронная подпись, ключ электронной подписи и др.), виды, принципы.
ФЗ «о связи»: содержит понятия (электротехническая связь, трафик, правовой статус оператора и абонента связи, тайна оператора связи).
ФЗ «о доступе к официальной информации».
ФЗ «о доступе к судебной информации»: содержит определения, термины (портал, сайт), принципы доступа к информации, права и обязанности тех субъектов, которые находятся в этом ФЗ.
ФЗ «о персональных данных»: содержит понятия и термины (оператор персональных данных, кто к ним относится, кто относится к владельцам персональных данных), принципы, права и обязанности основных субъектов. Особенности применения ФЗ «о персональных данных» содержатся в трудовом кодексе и в ФЗ «о государственной гражданской службе в РФ».

Базовые законы действуют на информационные правоотношения двуедино: они закрепляют общеправовой режим и общеправовое положение; с другой стороны они содержат конкретные правила поведения (ФЗ «об информации», ФЗ «о персональных данных», ФЗ «о связи», ФЗ «об электронной подписи»).

30. Специальные законы информационного права

Специальные законы: они закрепляют в себя нормы, которые регулируют правоотношения в области отдельных видов информационной деятельности.

Виды информационной деятельности:

сфера государственного управления (государственная регистрация по дактилоскопической экспертизе, геномной информации);

деятельность по обеспечению избирательной системы (ГАС Выборы);

предпринимательская деятельность (ФЗ «о кредитной истории», ФЗ «о рекламе», ФЗ «об инсайдерской информации»);

деятельность по организации торгов;

деятельность по распространению массовой информации (ФЗ «О СМИ»);

Функции специальных законов:

4.определение специального правового режима отдельных видов информации;

5. определение специальных правовых требований к формированию отдельных объектов (информационно-телекоммуникационная сеть, информационная система);

6.закрепление тех основных правовых положений, которые дополняют базовые законы.

31. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».

ФЗ «Об информации, информационных технологиях и защите информации».

Такое же значение для отраслевых норм информационного зак-ва имеют зафиксированные в законе «Об информации» принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст.3).

Классификация информации по разным основаниям (ст.5).

В частности, по категориям доступа (общедоступную и ограниченного доступа), в зависимости от порядка ее предоставления или распространения (свободно распространяемую, предоставлению по соглашению, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще).

Причем, при этом делается оговорка о том, что законодательством РФ могут быть установлены и иные виды информации в зависимости от ее содержания или обладателя.

ФЗ «Об информации» определяет:

• правовой статус основных субъектов ИП – обладателя информации (ст.6), организатора и блогера (ст.10-1 и 10-2), оператора информационных систем (ст.13,14,16), владельца сайта в сети «Интернет» и провайдера хостинга (ст.15.1 Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов).

• общие условия правового режима создания и использования ИС и сетей (ст.13,14,15).

• общие условия доступа к информации (ст.8) и его ограничения (ст.9 – защиты конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства).

• общие условия распространения информации (ст.10) и документирования информации (ст.11).

• общие условия защиты информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также ответственности.

32.Основные положения Федерального закона «Об электронной подписи»

Он регламентирует отношения в области использования эл. подписей при совершении гражданско-правовых сделок, оказании гос. и мун. услуг, исполнении гос. и мун. функций, при совершении иных юридически значимых действий.

Он закрепляет основные понятия и определения, принципы использования ЭП, правовой статус субъектов информационных ПО в области использования ЭП, правовой режим различных видов ЭП.
Он определяет круг субъектов данных отношений:
Участники эл. взаимодействия (ОГВ, ОМС, физ. и юр. лица);
ФОИВ в сфере использования ЭП;
Удостоверяющие центры.
Свобода выбора конкретного вида ЭП – специфичный принцип Закона.

33. Основные положения Федерального закона «О персональных данных».
1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.
2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:
1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

ФЗ определяет принципы обработки ПД (законность, справедливость, целесообразность, дифференцированность, точность, достаточность, актуальность), условия обработки (с согласия субъекта, для определённых целей, для осуществления правосудия, для деятельности огв, для исполнения договора, защиты жизни и здоровья и др.), категории ПД (общие, специальные, биометрические), права субъекта ПД, обязанности оператора, порядок контроля и надзора за обработкой ПД, ответственность за нарушения требований настоящего ФЗ.

34. Основные положения Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
Сфера действия настоящего Федерального закона
Действие настоящего Федерального закона распространяется на отношения, связанные с обеспечением доступа пользователей информацией к информации о деятельности государственных органов и органов местного самоуправления.

2. Если федеральными конституционными законами, федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации предусматриваются особенности предоставления отдельных видов информации о деятельности государственных органов и органов местного самоуправления, положения настоящего Федерального закона применяются с учетом особенностей, предусмотренных этими федеральными конституционными законами, федеральными законами и иными нормативными правовыми актами Российской Федерации.
3. Если законами и иными нормативными правовыми актами субъектов Российской Федерации, принятыми по предметам ведения субъектов Российской Федерации, предусматриваются особенности предоставления отдельных видов информации о деятельности государственных органов субъектов Российской Федерации и органов местного самоуправления, положения настоящего Федерального закона применяются с учетом особенностей, предусмотренных этими законами и иными нормативными правовыми актами субъектов Российской Федерации.
4. Действие настоящего Федерального закона распространяется на отношения, связанные с предоставлением государственными органами и органами местного самоуправления информации о своей деятельности по запросам редакций средств массовой информации, в части, не урегулированной законодательством Российской Федерации о средствах массовой информации.
5. Действие настоящего Федерального закона не распространяется на:
1) отношения, связанные с обеспечением доступа к персональным данным, обработка которых осуществляется государственными органами и органами местного самоуправления;
2) порядок рассмотрения государственными органами и органами местного самоуправления обращений граждан;
3) порядок предоставления государственным органом, органом местного самоуправления в иные государственные органы, органы местного самоуправления информации о своей деятельности в связи с осуществлением указанными органами своих полномочий.

о Правовое регулирование отношений, связанных с обеспечением доступа к информации о деятельности государственных органов и органов местного самоуправления
о Основные принципы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления
о. Информация о деятельности государственных органов и органов местного самоуправления, доступ к которой ограничен
о Способы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления
оФорма предоставления информации о деятельности государственных органов и органов местного самоуправления
о Права пользователя информацией

35. Основные положения ФЗ «О связи»
Цель-установление правовых основ в области связи, определение полномочий огв в области связи, а также права и об-ти лиц, участвующих в указанной деятельности или пользующимися услугами связи.
Субъкеты:1_)абонент-пользователь услугами связи, с которым заключен договор об оказании таких услуг, предоставлен абонентский номер и т.д.Виды пользователей: а)пользователь радиочастотным спектром-лицо,которому выделена полоса радиочастот либо присвоение радиочастота или канал б)пользователь услугами связи….2)оператор связи-юл или ип, оказываающие услуги связи на основании лицензии.
Объекты: сеть связи, сооружение связи. средства связи и т.д.
Трафик-нагрузка, создаваемая потоком вызовов, сообщений и сигналов, поступающих на средства связи.

36.Основные положения ФЗ «О рекламе»
Он регулирует общественные отношения по поводу рекламы.
Реклама – это информация, распространяемая любым способом, в любой форме и с использованием любых средств, адресованной неограниченному кругу лиц и направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.
Ст. 5 устанавливает общие требования к рекламе: запрещены недобросовестная и недостоверная реклама.
Субъекты:

Рекламодатель – изготовитель или продавец товара либо иное определившее объект рекламирования и/или содержание рекламы лицо;
Рекламопроизводитель – лицо, осуществляющее полностью/частично приведение информации в готовую для распространения в виде рекламы форму;
Рекламораспространитель – лицо, осуществляющее распространение рекламы любым способом, в любой форме и с использованием любых средств;
Потребители рекламы – целевая аудитория, лица, на привлечение внимания которых к объекту рекламирования направлена реклама;
Спонсор – лицо, предоставившее средства либо обеспечившее предоставление средств.

Также ФЗ определяет особенности отдельных способов распространения рекламы (теле, радио, рекламные конструкции, реклама в транспорте и др.), особенности рекламы отдельных видов товаров (алкоголь, Лекарства, биологические добавки, ценные бумаги и др.), порядок саморегулирования в сфере рекламы, государственного надзора в сфере рекламы и ответственность за нарушение законодательства Российской Федерации о рекламе.

37.Основные положения ФЗ «О СМИ»

Цель-урегулирование отношений в сфере массовой информации
Массовая информация-предназначена для неопределенного аруга лиц печатн.аудио,видео сообщения и материалы.
СМИ-периодическое печатное,сетевое издание,телеканал,аудио/,видео канал и т.д.,под постоянным наименованием.(не реже 1 раза в год д.б.)
Субъекты:1)Редакция сми-организации,граждане,осущ.выпуск и распространение периодической продукции.2)главный редактор-возглавляет редакцию независимо от занимаемой должности, 3)журналист-занимается сбором,редактированием инф для зарег.сми, 4)издатель-осущ.материельно техн производство продукции СМИ,для него эта деятельность-не главный источник дохода.,5)распространитель,6)вещатель-российское юл, 7)УЧРЕДИТЕЛЬ СМИ
Не могут быть учредителями-до 18 лет, осужденные и т.д.
Свобода массовой информации:
В Российской Федерации
поиск, получение, производство и распространение массовой информации,
учреждение средств массовой информации, владение, пользование и распоряжение ими,
изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации, не подлежат ограничениям, за исключением предусмотренных законодательством Российской Федерации о средствах массовой информации.
ФЗ регламентирует организации деятельности СМИ (учредитель, регистрация, гос. Пошлина, порядок приостановления и прекращения деятельности, возникновение прав и обязанностей, статус учредителя, статус редакции и др), порядок распространения МИ (выход в эфир, лицензия на вещание, лицензионный контроль, порядок приостановления и прекращения лицензии, хранение материалов и др.), определяет порядок взаимодействия СМИ с гражданами и организациями, права и обязанности журналиста, порядок межгосударственного сотрудничества в области массовой информации и ответственность за нарушение законодательства о СМИ.

38. Основные положения Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»

Настоящий Федеральный закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.
Настоящий Федеральный закон не распространяется на отношения в сфере:
1)оборота информационной продукции, содержащей научную, научно-техническую, статистическую информацию;

2)распространения информации, недопустимость ограничения доступа к которой установлена Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и другими федеральными законами;
3)оборота информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества;
4)рекламы.
ФЗ определяет Виды информации, причиняющей вред здоровью и (или) развитию детей, классификацию информационной продукции (для детей, не достигших 6 лет, достигших 6 лет, достигших 12 лет, достигших 16 лет), требования к обороту информационной продукции (знак информационной продукции), условия экспертизы информационной продукции, порядок государственного надзора и общественного контроля, а также ответственность за правонарушения в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

39. Правовое регулирование предоставления публичных услуг в электронном виде.

Порядок правового регулирования определяется гл. 5 ФЗ от 27.07.2010 N 210-ФЗ (ред. от 13.07.2015) "Об организации предоставления государственных и муниципальных услуг" (с изм. и доп., вступ. в силу с 15.09.2015)
Предоставление государственных и муниципальных услуг в электронной форме, в том числе взаимодействие органов, предоставляющих государственные услуги, органов, предоставляющих муниципальные услуги, организаций, участвующих в предоставлении государственных и муниципальных услуг и заявителей, осуществляется на базе информационных систем, включая государственные и муниципальные информационные системы, составляющие информационно-технологическую и коммуникационную инфраструктуру.
Правила и порядок информационно-технологического взаимодействия информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, а также требования к инфраструктуре, обеспечивающей их взаимодействие, устанавливаются Правительством Российской Федерации.
Технические стандарты и требования, включая требования к технологической совместимости информационных систем, требования к стандартам и протоколам обмена данными в электронной форме при информационно-технологическом взаимодействии информационных систем, устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.
Единый портал государственных и муниципальных услуг является федеральной государственной информационной системой, обеспечивающей предоставление государственных и муниципальных услуг.
Органы государственной власти субъектов Российской Федерации вправе создавать региональные порталы государственных и муниципальных услуг, являющиеся государственными информационными системами субъектов Российской Федерации, обеспечивающими предоставление государственных услуг субъектов Российской Федерации и муниципальных услуг
Обращение за получением государственной или муниципальной услуги и предоставление государственной или муниципальной услуги могут осуществляться с использованием электронных документов, подписанных электронной подписью в соответствии с требованиями Федерального закона "Об электронной подписи" и требованиями настоящего Федерального закона.
Виды электронных подписей, использование которых допускается при обращении за получением государственных и муниципальных услуг, и порядок их использования устанавливаются Правительством Российской Федерации.
Универсальная электронная карта представляет собой материальный носитель, содержащий зафиксированную на нем в визуальной (графической) и электронной (машиносчитываемой) формах информацию о пользователе картой и обеспечивающий доступ к информации о пользователе картой, используемой для удостоверения прав пользователя картой на получение государственных и муниципальных услуг, а также иных услуг, оказание которых осуществляется с учетом положений настоящей главы, в том числе для совершения в случаях, предусмотренных законодательством Российской Федерации, юридически значимых действий в электронной форме. Пользователем универсальной электронной картой может быть гражданин Российской Федерации, а также в случаях, предусмотренных федеральными законами, иностранный гражданин либо лицо без гражданства (далее, если не указано иное, - гражданин).

40.Перспективы развития информационного законодательства.

В соответствии с Указом Президента РФ от 9 марта 2004г. "О системе и структуре ФОИВ" в сферу полномочий таких ФОИВ, как Минкультуры, Минсвязи, Минэкономразвития, и др. вошли различные аспекты информационных отношений, что обусловило включение вопросов информации и информатизации в сферу интересов и полномочий различных органов исполнительной власти, в том числе связанных с разработкой законопроектов. В целях предупреждения возникновения конфликта интересов между ФОИВ нужна разработка государственной концепции развития законодательства в информационной сфере. Одним из документов, направленных на выработку согласованной государственной политики в сфере информационного законодательства, является утвержденная 9 сентября 2000г. Президентом РФ Доктрина информационной безопасности РФ. В ее развитие был разработан документ рекомендательного характера под названием "Основные направления нормативно-правового обеспечения информационной безопасности РФ". Основные направления развития законодательства в сфере информации и информатизации. В связи с интенсивным развитием информационных технологий, средств и способов производства, хранения и распространения информации, а также в связи с ратификацией ГД Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных существует потребность в совершенствовании законодательства в сфере информации и информатизации. ФЗ "Об информации, информационных технологиях и защите информации", который позволит приблизить российское законодательство к международной практике регулирования информационных отношений, установить правила и перечень способов защиты публичных и гражданских прав на информацию, законодательно закрепить принципы использования информационно-телекоммуникационных сетей, в том числе при международном информационном обмене, а также заложить правовую основу создания и эксплуатации государственных и иных информационных систем. Предусматривается, что в результате принятия указанного законопроекта утратят силу: ФЗ "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", Указ Президента РФ "Об утверждении Перечня сведений конфиденциального характера" и другие нормативные правовые

41.Тайна как правовая категория и ее место в информационном обществе.

Слово «тайна» русского происхождения и имеет языковые истоки таких слов, как "тай" (глушь, территориальная отдаленность), "тайнба" (помещения для ведения сокровенных бесед).
Отсюда и употребления слов "тайная комната", " тайный приказ", "тайная канцелярия".
В словаре Даля оно имеет достаточно однозначное обозначение скрытности, неведения, сокровенности, неизвестности: " кто чего не знает, то для него тайна, все покрытое, неизвестное, неведомое".
Тайна нами рассматривается как понятие категориального свойства, поскольку оно обладает обобщёнными признаками.
Для понимания природы понятия "тайны" необходимо рассмотреть его с точки зрения смысла сущности информации.

В обычных отношениях Действительность напрямую отражается в Сознании человека, то есть адекватно.
Но в отдельных случаях, Личность, Общество или Государство заинтересованы в сохранении отдельных жизненных ситуаций в состоянии конфиденциальности (секретности).

Таким образом, Л, О. и Г. заинтересовано в создании преграды или защиты между тайными фактами и событиями и сознанием иных субъектов.
Тайна – создание защиты для отражения в сознании третьих лиц!
Создание такой преграды является совокупностью действий по созданию условий защиты отдельных событий в жизни Л. О. и Г., а информация о таких событиях при этом получает новое состояние, новые признаки.
Субъекты принимают меры к защите особенностей жизни в форме маскировки, придание им признаков скрытности – нового качества информации, т.е. состояния конфиденциальности.
Поэтому первым и главным признаком понятия «тайна» является конфиденциальность сведений о жизни, которые подлежат защите от внимания третьих лиц. Доступ (возможность ознакомления) к таким сведениям со стороны третьих лиц с помощью системы маскировки становится невозможной.

Конфиденциальность сведений (информации) – совокупность маскирующих признаков, характеризующих состояние информации.

Вторым признаком понятия тайны является - охрана её законом, то есть установленное законом состояние конфиденциальности информации о важных сторонах жизни и деятельности Л. О. и Г.
В этом проявляется правовой смысл тайны как категории. Правовой смысл придается всегда такому понятию, которое фиксируется в тексте закона.
Обязательность правовой защиты сохранности конфиденциальности сведений о жизни Л. О. и Г. является легитимностью сведений о важных сторонах жизни и деятельности личности, общества и государства.
Легитимность тайны подчеркивает:
• заинтересованность законодателя в установлении специального правового режима для сохранения в неприкосновенности названных сведений;
• исключительность правовой защиты информации о важных сторонах жизни из общего правила о свободе информации;
Поэтому в тексах законов об отдельных видах тайн нередко упоминается понятие «охраняемая законом тайна».

Третьим признаком понятия "тайна" является особая важность отдельных направлений, событий и объектов человеческой деятельности.
Интерес к покрытию таких областей жизни всегда возникает у всех субъектов: личности, общества и государства.
Потребности человека к сокрытию информации о личной и частной жизни.
Потребности общественного сектора заключаются в тайном характере ведения бизнеса, стремлении сохранить устойчивость предпринимательских структур: финансово-банковский раздел, коммерческая тайна и технологии промысла («ноу-хау»).
Государство реализует свои тайные потребности с помощью института «секретности» сведений о наиболее важных сторонах деятельности в области обороны и безопасности.
Следовательно, правовой охране подлежат не все сведения, а только наиболее важные, представляющие особый интерес личности, общества и государства.

Охраняемая законом тайна - установленное законом состояние конфиденциальности информации об особо важных сторонах жизни и деятельности личности, общества и государства.

42.Ответственность за нарушение правового режима информации ограниченного доступа

.

Информационное правонарушение – это общественно-опасное, противоправное и виновное деяние (действие, бездействие), совершаемое в сфере информации, либо в области любой человеческой деятельности, но с использованием информационных систем.

Нарушение требований по защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица. В случае, если распространение определённой информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несёт лицо, оказывающее услуги:
либо по передаче информации, предоставленной другим лицом, при условии её передачи без изменений и исправлений;
либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Данные мероприятия за правонарушения в области защиты информации устанавливают нормативные правовые акты и предусматривают следующие виды ответственности:
дисциплинарную (замечание; выговор; увольнение) Трудовой кодекс РФ, ст. 192 (ФЗ 2001 г.№ 197-ФЗ)
гражданскую (возмещение причинённого ущерба) Гражданский кодекс РФ (ст. 15, 16) ФЗ «О защите прав потребителя» (ФЗ 1999 г. № 2-ФЗ)
административную (предупреждение, административный штраф) КоАП (от 30.12.2001 г. №195-ФЗ) (ст.13.11-13.14) Трудовой кодекс РФ (от 30.12.2001 г. № 197-ФЗ) (ст. 57, 86, гл. 39 и др.) ФЗ «О защите прав потребителя»
уголовную (штраф, лишение свободы) Уголовный кодекс РФ (от 13.06.1996 г. №63-ФЗ) (ст.138, 140, 183, 238, гл. 28 (ст. 272-274) и др.)

43.Понятие государственной тайны.

1. Понятие государственной тайны.
Определение государственной тайны сформулировано в ст.2 Закона РФ от 21.07.1993 "О государственной тайне".
Государственная тайна - защищаемые государством сведения в области его специфической деятельности, связанной с обеспечением безопасности, распространение которых может нанести ущерб безопасности РФ.
Первым признаком понятия ГТ является значение выделяемого в тексте названного закона словообразования «защищаемые государством сведения», т.е. находящаяся под правовой защитой информация, обеспеченная государством.
Мы уже отмечали, что маскируемые с помощью специальных мер и находящиеся в защищенном состоянии сведения приобретают новое качество, именуемое конфиденциальностью.
Следовательно, «защищаемые государством сведения» являются их конфиденциальное состояние.

Вторым признаком понятия «гостайна» являются специфичные виды государственной деятельности и её объекты, которые государство стремится сохранить в защищённом состоянии.
Но не все сведения о видах гос. деятельности подлежат защите, а только те, которые представляют для государства особую важность в военной, экономической, внешнеполитической, разведывательной, контрразведывательной и оперативно-розыскной областях.
Такие сведения особой важности составляют содержание государственной тайны.
Правовой режим ГТ имеет специфику материальных носителей конфиденциальной информации, характерных для сведений об особо важных областях деятельности государства.
К носителям сведений, составляющих ГТ, относятся материальные объекты, в том числе физические поля, в которых сведения, составляющие ГТ, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Третьим признаком является реальная возможность нанесения ущерба безопасности РФ в результате распространения сведений, составляющих государственную тайну.
Вначале кратко остановимся на слове распространение.
Закон «Об информации» приводит определение понятия «распространение информации» как действия, направленные на получение или передачу информации неопределенным кругом лиц.
Итак, распространение информации – это результат активных действий: получение информации и передача информации, адресованные всем.
Формы распространения могут быть разными:
• разглашение – действие или бездействие, в результате которых информация, составляющая ГТ, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам;
• утрата - выход содержания информации из владения субъекта помимо его воли либо исчезновение материального носителя документа помимо его воли (например, его неосторожное уничтожение);
• передача – совершение действия (бездействия), направленного на перемещение символьной формы информации или ее материального носителя;
• получение – принять для использования либо ознакомления содержания информации;
• копирование (размножение) – создание одной или нескольких копий имеющейся информации, т.е. перенос информации на другой обособленный материальный носитель при сохранении оригинала информации в любой

форме: от руки, путем фотографирования текста, а также считывания информации путем перехвата электромагнитных излучений и т.д.

Второе важное слово в определении понятия ГТ - наличие ущерба безопасности государства - обычно рассматривается как наиболее негативные последствия для существования и развития государства:
• в области военной деятельности – срыв военных операций вооруженных сил России либо поддержке незаконных военных формирований на ее территории;
• в области разведки – расшифровка разведывательных операций, провал агентуры и др;
• во внешнеполитической области – в срыве мирных переговоров, разрыве дипломатических отношений;
• в экономической области – в срыве выгодных межгосударственных деловых контактов, экономической блокаде;
• в оперативно-розыскной деятельности – в существенных затруднениях в борьбе с преступностью и коррупцией.

44.Условия допуска к государственной тайне.

Допуск к ГТ - процедура оформления права граждан на доступ к сведениям, составляющим ГТ, а организаций - на проведение работ с использованием таких сведений.
Доступ к ГТ - санкционированное полномочный должностным лицом ознакомление конкретного лица со сведениями, составляющими ГТ.
Допуск должностных лиц и граждан РФ к ГТ осуществляется в добровольном порядке.
При этом граждане, которым по характеру занимаемой ими должности необходим доступ к ГТ, могут быть назначены на эти должности только после оформления допуска по соответствующей форме в установленном порядке.
Существуют следующие формы допуска:
1ая – для граждан, допускаемых к сведениям особой важности;
2ая – для граждан, допускаемых к совершенно секретным сведениям;
3я – для граждан, допускаемых к секретным сведениям.

Процедура оформления доступа к ГТ - сложный юридический состав, элементами которого являются:
1) принятие на себя обязательств перед государством по нераспространению доверенных сведений, составляющих гостайну;
2) согласие на частичные, временные ограничения прав;
3) письменное согласие на проведение проверочных мероприятий;
4) определение видов, размеров и порядка предоставления льгот, предусмотренных законодательством РФ о ГТ (надбавка от 10% до 70% к окладу + надбавка за стаж);
5) ознакомление с нормами законодательства РФ о ГТ, предусматривающим ответственность за его нарушение;
6) принятие решения руководителем органа государственной власти (УФСБ) или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Условия допуска к ГТ.
Условия проведения проверочных мероприятий (ст.21-22 Закона РФ «О государственной тайне»):
1. Объем проверочных мероприятий зависит от степени секретности сведений;
2. Основания для отказа в допуске к гос.тайне:
• признание лица недееспособным, ограниченно дееспособным;
• наличие неснятой судимости за тяжкие преступления;
• наличие медицинских противопоказаний для работы с использованием сведений, составляющих ГТ, согласно перечню, утвержденному Министерством здравоохранения РФ;
• постоянное проживание (более 6 месяцев) и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства – жена (муж), отец, мать, дети, усыновители, усыновленные, полнородные и неполнородные (имеющие общих отца или мать) братья и сестры;
• уклонение от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Особый порядок доступа к ГТ отдельных лиц установлен в ст.21.1 Закона «О государственной тайне».
• Члены Совета Федерации

• депутаты Государственной Думы
• судьи на период использования ими своих полномочий
• адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими гос.тайну.
Перечисленные лица допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных ст.21 Закона «О ГТ».
Указанные лица предупреждаются о неразглашении государственной тайны, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случаях ее разглашения, о чем у них отбирается соответствующая расписка.

Порядок допуска должностных лиц и граждан РФ к ГТ осуществляется в порядке, установленном Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденной Постановлением Правительства РФ от 6 февраля 2010 №63.
Инструкцией определены правила и порядок допуска, его оформление и переоформление, установлен порядок доступа граждан к особой важности, совершенно секретным и секретным сведениям при командировании их в другие организации.
Проверочные мероприятия, связанные с допуском граждан по первой и второй форме, осуществляются ФСБ РФ и ее территориальными органами во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.
Допуск граждан по третьей форме, за исключением случая, когда имеются обоснованные сомнения в достоверности их анкетных данных, осуществляется руководителем организации без проведения проверочных мероприятий органами ФСБ РФ. Руководители организаций допускаются к секретным сведениям по третьей форм, только попе проведения проверочных мероприятий органами безопасности

45.Виды государственной тайны.

Указ Президента РФ от 30.11.1995 № 1203 « об утверждении перечня сведений, отнесённых к ГТ».
!!!Виды сведений зависят от вида деятельности по обеспечению безопасности!!!
В военной области к особой важности относятся сведения:
1)Раскрывающие планы применения войск в мирное время в специальных (контртеррористических) операциях или мероприятиях по обеспечению защиты государства, общества и личности от антиконституционных действий и противоправного вооруженного насилия
2)о содержании документов по приведению войск в различные степени боевой готовности, о составе или состоянии систем управления войсками
3)раскрывающие организацию или функционирование всех видов связи, радиолокационного, радиотехнического обеспечения войск
В области внешней политике к особой важности относятся сведения:
1)раскрывающие стратегию, тактику внешней политики Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства
2)Сведения о подготовке, заключении, ратификации, подготовке денонсации, содержании или выполнении договоров, конвенций, соглашений с иностранными государствами, преждевременное распространение которых может нанести ущерб безопасности государства
3)Сведения об источнике информации по политическим, военным, научно-техническим или экономическим вопросам в отношении одного или ряда иностранных государств, полученные в доверительном порядке
Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму к особой важности относятся сведения:
1)Сведения, раскрывающие принадлежность конкретных лиц к кадровому составу подразделений, непосредственно осуществляющих борьбу с терроризмом, организованной преступностью и коррупцией, специальным оперативным подразделениям
2)Сведения, раскрывающие силы, средства, методы, планы, состояние или результаты проведения контртеррористических специальных операций, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения

3)Сведения, раскрывающие силы, средства, источники, методы, планы, результаты деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения
4)О сотрудниках, выполняющих или выполнивших специальные задания в специальных службах (организациях) иностранных государств или в преступных групах

46.Понятие и режим служебной тайны.

Служебная тайна – конфиденциальность сведений несекретной информации о механизме разработки и принятия гос-ых управленческих решений, распространение которой причинить ущерб эффективности деятельности ОГВ.
Конфиденциальность – состояние защищённости от третьих лиц (ограничения распространения) документов, содержащими несекретные сведения (т.е. не составляющие ГТ)
Жизненная важность сведений о механизме принятия гос-ого управленческого решения (в подготавливаемых федеральными ОГВ проектах указов, постановлений и распоряжений Президента РФ, Правительства РФ и других служебных документов)
Негативные ущербные последствия – препятствия нормальному осущ-нию функция гос. власти
ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ от 3 ноября 1994 г. N 1233 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ПОРЯДКЕ ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В ФЕДЕРАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ»
Положение определяет общий порядок обращения со служебной информацией ограниченного распространения: с документами и другими материальными носителями информации (далее - документами), содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях.
На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка "Для служебного пользования".
Необходимость проставления пометки "Для служебного пользования" на документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется исполнителем и должностным лицом, подписывающим или утверждающим документ.
Без санкции соответствующих должн.лиц информация не подлежит разглашению и распространении.
Не может быть отнесена к служебной тайне информация:
акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;
документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

47.Порядок работы с информацией, составляющей служебную тайну.

Условия сохранения конфиденциальности СТ включает:
Порядок определения режима конфиденциальности и порядок обработки (использования) сведений, составляющих СТ.
1.Руководитель федерального органа исполнительной власти в пределах своей компетенции определяет:
категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения

порядок передачи служебной информации ограниченного распространения другим органам и организациям
порядок снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения
организацию защиты служебной информации ограниченного распространения.
Порядок обработки и использования документов, составляющих СТ (самостоятельно)
Документы с пометкой "Для служебного пользования":.
печатаются в машинописном бюро. На обороте последнего листа каждого экземпляра документа машинистка должна указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах;
учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка "ДСП";
передаются работникам подразделений под расписку;
пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
размножаются (тиражируются) только с письменного разрешения соответствующего руководителя. Учет размноженных документов осуществляется поэкземплярно;
хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

48.Понятие профессиональной тайны и особенности ее правового режима и субъекты профессиональной тайны.

Нормативное основание
Ст.9 закона Об информации П.6 - информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
П.4 Указ Президента от 6 марта 1997 №188 «Об утверждении перечня сведений конфиденциального характера» - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
Нормы о тайнах Федеральных законов о видах профессиональной деятельности.

1. Понятие профессиональной тайны
Охраняемая законом профессиональная тайна - конфиденциальность информации о жизненно важных обстоятельств личности либо деятельности организаций, полученной гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых профессиональных видов деятельности.

Поверенный (гражданин): личность, доверитель
Профессиональная функция: налоговая, адвокатская, усыновления и тайна исповеди
Поверенный (юридическое лицо): организация, доверитель
Профессиональная функция: банковская тайна, аудиторская, судебная и следственная.

Личность/доверитель передает тайну поверенному – осуществляется профессиональная функция (доверие или требование законом).
Организация/доверитель передает тайну поверенному – осуществляется функция (доверие или требование законом).

Признаки ПТ.
1) конфиденциальность - состояние защищённости от третьих лиц информации о жизненно важных событиях и обстоятельствах личности либо деятельности организаций.

Такими обстоятельствами для личности являются, например, факты усыновления, финансовое состояние (банковская тайна) и состояние здоровья (врачебная тайна).
Для деятельности организаций ими могут быть особенности реализации их полномочий, например, в сфере финансов (банковская тайна и аудиторская тайна), налогообложения (налоговая тайна) и др.
2) легитимность ПТ является обязательность защиты сведений физическими лицами или организациями в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
3) факт передачи физическим лицам при исполнении ими профессиональных обязанностей или организациям при осуществлении ими определённых видов профессиональной деятельности информации о жизненно важных обстоятельствах личности либо деятельности организаций. Необходимость передачи сведений о важных обстоятельствах частной жизни обусловлена особенностями реализации потребностей, например, в воспитании детей (тайна усыновления), в ходе судебной защиты (адвокатская тайна), о финансовом благополучии (банковская тайна), в духовной сфере (тайна исповеди).
Передача сведений, составляющих ПТ, основана на условиях максимального доверия либо требованиях закона.
4) особенности реализации профессиональной функции физических лиц и организаций, которым доверитель (обладатель сведений) передает, т.е. доверяет сведения о важных обстоятельствах своей жизни и деятельности.
Название "профессиональная тайна" определяется особенностями профессии работников, которые реализуют функции физических лиц и организаций, которым доверитель (обладатель) сведений доверяет свои секреты.
Реализация профессиональной функции во многом зависит от деловых качеств работников, т.е. способностей выполнять определенную трудовую функцию с учетом имеющихся у них профессионально-квалификационных качеств (наличие базового образования, определенной профессии, специальности и квалификации, опыт работы по данной специальности и т.д.)

Следовательно, природа профессиональной тайны обусловлена:
1. Особенностями реализации определенной профессиональной функции, в рамках которой возникает необходимость у личности и организации реализовать личные либо общественные интересы и при этом сохранить их в конфиденциальном состоянии.
Поэтому она именуется профессиональной.
2. Природа ПТ обусловлена доверием либо требованием закона.

2. Правовой режим профессиональной тайны.
ПРПТ включает нормы права, которые определяют:
- состав сведений, составляющих ПТ
- состав субъектов ПТ, и их правовой статус
- условия передачи сведений, составляющих профессиональную тайну третьим лицам
- условия и требования сохранности в конфиденциальном состоянии информации ограниченного доступа
- меры ответственности за нарушения конфиденциальности.
Нормативно-правовые основания ПРПТ: ФЗ «Об информации» определяет общий правовой режим (ст.9). Другие ФЗ и иные НПА о профессиональной деятельности определяют виды профессиональной тайны – специальный правовой режим.

Состав сведений, составляющих профессиональную тайну, зависит от обстоятельств и условий:
- особенностей важных обстоятельств личности либо деятельности организаций, которые подлежат защите;
- конкретного вида профессии, в рамках которых реализуются личные либо общественные интересы;
- цели и содержание реализации профессиональных функций;
- характера публичного интереса поверенных (обладателей) в получении сведений, составляющих профессиональную тайну.

Например, для банковской тайны состав таких сведений ограничивается рамками банковских операций по счету и вкладу своих клиентов и корреспондентов, т.е. сведениями по операциям и счетам юридических лиц и граждан (сведения о доходах, об имуществе и обязательствах имущественного характера).
Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону (ст.26 ФЗ «О банковской деятельности»).

Субъектами профессиональной тайны являются:
• доверитель – личность либо организация, которым принадлежит информация, составляющая профессиональную тайну:
• обладатель (поверенный) – граждане (физические лица) при исполнении ими профессиональных обязанностей или организация при осуществлении определенных видов деятельности, которые получают на основании закона или договора информацию, составляющую ПТ;
• пользователь – работник, специалист, выполняющий трудовую функцию в области определенной профессии, в рамках которой возникает необходимость у доверителя реализовать личные либо общественные интересы и при этом сохранить их в конфиденциальном состоянии.

Третьи лица – государственные органы или органы местного самоуправления, которым может быть предоставлена информация, составляющая ПТ, в соответствии с федеральными законами и (или) по решению суда (п.7 ст.9 Закона «Об информации»).

2.3. Условия передачи сведений ПТ.
• Условия передачи от доверителя поверенному (обладателю) информации, составляющей профессиональную тайну, сформулированы федеральным законом или договором (адвокатская, аудиторская и др.);
• Условия передачи информации, составляющей профессиональную тайну, от обладателя третьим лицам по запросу определяются только федеральным законом либо по решению суда (п.7 ст.9 ФЗ Об информации);
• Условиями являются уполномоченность представителя госоргана; целесообразность и мотивированность запроса.

Особенности правового режима отдельных видов профессиональной тайны.

Банковская тайна (ст.26 ФЗ о банковской деятельности)
Справки по операциям и счетам юр.лиц и граждан выдаются кредитной организацией им самим, судам(судьям), Счетной палате РФ, налоговым органам, ФОИВ в области финансовых рынков, Пенсионному фонду РФ, Фонду социального страхования РФ и органам принудительного исполнения суд.актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их Д-ти, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве.
Справки по операциям, счетам и вкладам физ.лиц выдаются кредитной организацией руководителям (должн.лицам) федеральных гос.органов при наличии запроса, направленного в порядке, определяемом Президентом РФ, в случае проверки в соот-вии с ФЗ « О противодействии коррупции» сведений о доходах, об имуществе и обязательствах имущ-ого характера:
Граждан, претендующих на замещение гос-ых должностей РФ, должностей глав муниц.образований, муниц.должностей, замещаемых на постоянной основе
Граждан, претендующих на должность судьи
Граждан, претендующих на замещение гос.должностей субъектов РФ, должностей глав МО, муниц.должностей, замещаемых на постоянной основе
Граждан, претендующих на замещение должностей федеральной гос.службы, должностей гос-ой гражданской службы субъектов РФ, должностей муниц.слежбы
Гос.органы и ОМС не вправе раскрывать третьим лицам инф-ию, полученную от кредитных организаций в соот-вии с ФЗ.
Адвокатская тайна (ст. 8 ФЗ об адвокатской д-ти)
1. Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.
2. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

3. Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.
Полученные в ходе оперативно-розыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей. Указанные ограничения не распространяются на орудия преступления, а также на предметы, которые запрещены к обращению или оборот которых ограничен в соответствии с законодательством Российской Федерации.
Аудиторская тайна(ст. 9 ФЗ об аудит-ой д-ти)
1. Аудиторскую тайну составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг, предусмотренных настоящим Федеральным законом, за исключением:
1) сведений, разглашенных самим лицом, которому оказывались услуги, предусмотренные настоящим Федеральным законом, либо с его согласия;
2) сведений о заключении договора оказания аудиторских услуг;
3) сведений о величине оплаты аудиторских услуг.
2. Аудиторская организация и ее работники, индивидуальный аудитор и работники, с которыми им заключены трудовые договоры, обязаны соблюдать требование об обеспечении конфиденциальности информации, составляющей аудиторскую тайну.
Налоговая тайна (ст.90, 102 и др Налогового кодекса РФ)
1. Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:
1) являющихся общедоступными, в том числе ставших таковыми с согласия их обладателя - налогоплательщика;
2) об идентификационном номере налогоплательщика;
3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;
4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам);
5) предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности;
6) предоставляемых в Государственную информационную систему о государственных и муниципальных платежах, предусмотренную Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг";
7) о специальных налоговых режимах, применяемых налогоплательщиками, а также об участии налогоплательщика в консолидированной группе налогоплательщиков;
8) предоставляемых органам местного самоуправления в целях осуществления контроля за полнотой и достоверностью информации, представленной плательщиками местных сборов, для расчета сборов, а также о суммах недоимки по таким сборам.
2. Налоговая тайна не подлежит разглашению налоговыми органами, органами внутренних дел, следственными органами, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом.
3. Поступившие в налоговые органы, органы внутренних дел, следственные органы, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа.
Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица, определяемые соответственно федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов, федеральным органом исполнительной власти, уполномоченным в области внутренних дел, федеральным государственным органом, осуществляющим полномочия в сфере уголовного судопроизводства, федеральным органом исполнительной власти, уполномоченным в области таможенного дела.

Тайна связи (ст. 63 ФЗ О связи)

1. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение этого права допускается только в случаях, предусмотренных федеральными законами.

Тайна усыновления (ст.139 Семейного кодекса РФ и др)

1. Тайна усыновления ребенка охраняется законом.

Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка.

2. Работники органов записи актов гражданского состояния не вправе без согласия усыновителей (усыновителя) сообщать какие-либо сведения об усыновлении и выдавать документы, из содержания которых видно, что усыновители (усыновитель) не являются родителями (одним из родителей) усыновленного ребенка.

Тайна завещания (ст.1123 ГК РФ)

Нотариус, другое удостоверяющее завещание лицо, переводчик, исполнитель завещания, свидетели, нотариусы, имеющие доступ к сведениям, содержащимся в единой информационной системе нотариата, и лица, осуществляющие обработку данных единой информационной системы нотариата, а также гражданин, подписывающий завещание вместо завещателя, не вправе до открытия наследства разглашать сведения, касающиеся содержания завещания, его совершения, изменения или отмены.

В случае нарушения тайны завещания завещатель вправе потребовать компенсацию морального вреда, а также воспользоваться другими способами защиты гражданских прав, предусмотренными настоящим Кодексом.

Не является разглашением тайны завещания представление нотариусом, другим удостоверяющим завещание лицом сведений об удостоверении завещания, отмене завещания в единую информационную систему нотариата в порядке, установленном Основами законодательства Российской Федерации о нотариате.

Врачебная тайна (ст. 13 ФЗ Об основах охраны здоровья граждан в РФ)

1. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

2. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 настоящей статьи.

3. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю,

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания
9) в целях осуществления учета и контроля в системе обязательного социального страхования;
Тайна следствия (ст. 9 ФЗ О гос-ой защите потерпевших, свидетелей)
1. По решению органа, осуществляющего меры безопасности, может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств.
2. В исключительных случаях, связанных с производством по другому уголовному либо гражданскому делу, сведения о защищаемом лице могут быть представлены в органы предварительного расследования, прокуратуру или суд на основании письменного запроса прокурора или суда (судьи) с разрешения органа, принявшего решение об осуществлении государственной защиты.

Профессиональная тайна - ответственность

49. Понятие, природа и правовой режим коммерческой тайны.

Коммерческая тайна - это конфиденциальность информации, имеющей «действительную или потенциальную коммерческую ценность», позволяющей ее обладателю в силу недопустимости для третьих лиц, увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получать иную коммерческую выгоду.
• 1. Первым из них является конфиденциальность информации, составляющей коммерческую тайну, т.е. придание ей тайных признаков, не позволяющих посторонним лицам ознакомиться с ее содержанием.
• 2. Вторым признаком является «действительная или потенциальная коммерческая ценность» сведений, если они неизвестны третьим лицам.
Ценность заключается в том, что обладатель получает материальное преимущество над конкурентом и наибольшую экономическую выгоду.
Действительная ценность - может быть оценена суммой затрат на обеспечение конфиденциальности либо причиненных убытков либо упущенной выгодой в результате утраты конфиденциальности.
Потенциальная ценность - расчетная или прогнозируемая ценность.
Ценность информации определяет экономическую природу коммерческой тайны, источник таинства вытекает из предпринимательства, секрета технологии бизнеса.
Потенциально ценные сведения, имеющие коммерческое значение - информация о реальных проектных затратах и инвестировании средств, расчетная информация о будущей реализации продукции, которая может принести положительный коммерческий успех на перспективу.
• 3. Следующим признаком, необходимым для признания сведений коммерческой тайной, является факт недопустимости, т.е. отсутствие условий реального свободного доступа к информации на законном основании.
Недоступность для третьих лиц означает необходимость введения режима КТ, т.е. совершения активных действий от ее обладателя по введению режима коммерческой тайны, т.е. по разработке необходимых мер, направленных на защиту КТ.

2. Режим коммерческой тайны - совокупность организационных, правовых и технических мер по охране конфиденциальности.
Таким образом, закон возлагает на обладателя обязанность самому принимать меры к охране ее конфиденциальности, то есть, к защите информации.
Такие меры включают в себя несколько условий:
• В соответствии со ст.10 Закона «О коммерческой тайне» эти меры должны включать в себя организационные:
1) определение перечня информации, составляющей коммерческую тайну;
2) установления порядка обращения с этой информацией и контроля за его соблюдением, т.е. ограничение доступа к информации, составляющей коммерческую тайну, путем;
3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
4) нанесение грифа «Коммерческая тайна» на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию,

5) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
К организационным мерам относится и выделение финансовых средств и т.д.;

К правовым мерам относится:
• принятие нормативных актов (Положения о КТ, Инструкций о работе с КТ, в т.ч. инструкции О конфиденциальном делопроизводстве)
• разработка должностных инструкций для отдельных групп работников - бухгалтеров, юристов, ИТ-сотрудников, службы ИБ и т.д.
• контрактная работа с персоналом (своевременное дополнение к контрактам с лицами допущенными и ответственными за сохранность КТ);
• договорная работа с партнерами и контрагентами (подготовка и заключение гражд.-правовых договоров).
Причем, и в трудовом договоре и в гражданско-правовом договоре пользователи информации, составляющих КТ, обязаны соблюдать режим конфиденциальности.

50.Субъекты коммерческой тайны.

Состав субъектов КТ.
Обладатель коммерческой тайны – (к ним закон относит, в том числе, собственников и владельцев таких сведений) - все юридические физические лица, руководители организаций, имеющие монопольное право на информацию, составляющей коммерческую тайну.
Сюда же относятся лица, определяющие правовой статус организации и принимающие важные (стратегические) решения о перспективах развития организации.
Пользователи (конфиденты) - лица, которые в силу своего служебного положения или трудового договора имеют доступ к сведениям, составляющим коммерческую тайну.
Контрагенты - лица, представляющие сторону гражданско-правового договора, которым обладатель коммерческой тайны передаёт такую информацию.
Государственные органы и органы местного самоуправления, их руководители и официальные представители, т. е. те, кому в силу закона дано право запрашивать и получать информацию, составляющую коммерческую тайну, у её обладателей.

51.Условия передачи информации, составляющей коммерческую тайну.

Закон О КТ включает нормы о возможности передачи сведений, составляющих КТ органам исполнительной власти для использования в соответствии с реализацией ими функций.
Ст.6 ФЗ «О Коммерческой тайне» - Условия передачи такой информации представителям органа государственной власти, иного государственного органа, органа местного самоуправления:
- уполномоченность должностного лица
- целесообразность запроса
- мотивированное требование (фактические основания)
- правовые основания требования
- безвозмездность
- обязательную сохранность конфиденциальности информации, составляющую коммерческую тайну.

Кроме того, ФЗ О КТ установил обязанности для ОГВ и ОМС:
1) ОГВ и иные государственные органы, ОМС обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.
2) Должностные лица ОГВ, иных государственных органов, ОМС, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей КТ, не вправе разглашать или передавать другим лицам (в т.ч. другим ОГВ и ОМС ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую КТ, за исключением случаев, предусмотренных настоящим ФЗ, а также не вправе использовать эту информацию в корыстных или … целях.

3) в случае нарушения конфиденциальности информации должностные лица ОГВ и ОМС несут ответственность в соответствии с законодательством РФ:
- дисциплинарную (ст.81 п.«В» ТК РФ – расторжение трудового договора);
- гражданско-правовую (ст.15 ГК рФ Возмещение убытков – п.1. Лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков);
- административную (ст.13.14 Разглашение информации с ограниченным доступом – штраф до 1 тыс. на д.л. – до 5 тыс.);
- уголовную (ст.183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну – повлекшие тяжкие последствия, наказываются в т.ч. лишением свободы на срок до 7 лет).

Условия освобождения от ответственности.
Ст.2 1472 ГК РФ - лицо, которое использовало секрет производства и не знало и не должно было знать о том, что его использование незаконно, в том числе в связи с тем, что оно получило доступ к секрету производства СЛУЧАЙНО или ПО ОШИБКЕ, не несет ответственность в соответствии с п.1 настоящей статьи.

52.Понятие и признаки персональных данных.

Персональные данные (научное определение) - сведения о жизненно важных фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.
Это определение приводится в п.1 Указа ПРФ от 6 марта 1997.
Поскольку режим ограничения доступа должен быть установлен федеральным законом, то это определение не является легальным.
Легальное определение ПД приводится в ст.3 ФЗ О ПД - это любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных).
Определенное лицо - это выделение его из числа других.
Определяемое - это наделение лица определёнными индивидуальными признаками.

Признаки ПД
1. ПД - информация ограниченного доступа, но это не тайна.
Здесь три важных замечания.
Во-первых, в отличие от тайны, конфиденциальность ПД не носит абсолютный характер, поскольку при согласии субъекта сведения, составляющие ПД, могут распространяться и передаваться 3-тьим лицам.
Во-вторых, человек или физическое лицо нередко сам желает, чтобы окружающие узнали его ПД и отменили индивидуальность человека.
В-третьих, в законе названы условия, при которых ПД могут распространяться и без согласия граждан.
2. Это информация ограниченного доступа о жизненно важных фактах, событиях и обстоятельствах частной жизни гражданина.
Это самый содержательный признак - информация (сведения), в которой раскрываются индивидуальные признаки личности, а потому ФЗ О ПД устанавливает слово "определяемый".
В первой редакции ФЗ О ПД называл и типовые отличия ПД – «в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».
Действующая редакция Закона не определяет состав сведений, составляющих ПД, однако анализ норм федеральных законов, в которых сформулированы условия специального режима ПД, позволяет их определить их именно так.

Персональные данные:
1) жизненно важные факты и события частной жизни - от них зависит существование человека (физическая целостность, здоровье, финансовое состояние, социальная устойчивость и т.д.);
2) иные факты, события и обстоятельства частной жизни - от них не зависит существование человека - это его индивидуальные признаки, таланты, профессиональные навыки.

ПД - набор индивидуальных признаков, на основе которых человек выделяется (определяется) среди многих других.
Новый человек приходит в мир с набором индивидуальных признаков, имеющих свою исходную природу, традиции, мораль, нравственность, финансовое состояние, медицинские данные.
Через родителей индивид изначально несёт запас информации не только через ДНК, но и в своём сознании.
Человек постепенно формируется как конкретная личность с определённым потенциалом креативности, культуры, навыков и проведения.
Его персональная характеристика – не что иное, как визитная карточка в среде, в которой ему приходится пребывать в течение своего века.
Персональные данные – это социальный портал человека.

Трудовой кодекс РФ.
Под персональными данными понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ст.85).
Сведения о личности работника, занесенные в его личное дело (анкета, автобиография, характеристики, сведения о составе семьи, сведения о родственниках работника, сведения о профессиональных качествах и о движении по службе, сведения о поощрениях и взысканиях и др.).

Виды ПД:
1) Ст.8 - общедоступные персональные данные.
П.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).
В общедоступные источники включаются его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные профессиональные данные, сообщаемые субъектом персональных данных.
2) Ст.10 - специальные категории персональных данных.
П.1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья интимной жизни, неё допускается, за исключением случаев, предусмотренных законом.
3) Ст.11 - биометрические ПД.
1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.
Субъект ПД - физические лица (человек, личность), которым принадлежат сведения, составляющие ПД.
Оператор ПД - государственный орган, муниципальный орган, юридические или физические лица, осуществляющие обработку ПД, а также определяющие цели обработки ПД, состав ПД, подлежащих обработке, действия (операции), совершаемые с ПД.
Функции оператора осуществляет исполнительный орган организации (руководитель).
Организатор обработки (ст.22.1 ФЗ о ПД) - лица, ответственные за организацию обработки ПД в организациях он назначается оператором (юридическим лицом) и обеспечивает контроль за соблюдением требований об обработке ПД внутри организации. Организатор получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетного ему.
Пользователь - работники гос и муниципальных органов, которые в силу своих трудовых функций допущены к сведениям составляющим ПД.
Уполномоченный государственный орган - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является ФОИВ, осуществляющим функции по контролю и надзору в сфере ПД.

Условия правового режима ПД.
1. Конфиденциальность ПД (ст.7).
Операторы и иные лица, получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД, если иное не предусмотрено ФЗ.
Сведения о субъекте общедоступных ПД должны быть в любое время исключены из общедоступных источников ПД (справочников) по требованию субъекта ПД либо по решению суди или иных уполномоченных гос.органов (ст.8).
2. Обработка только с согласия субъекта ПД (главное условие).

3. Обработка ПД - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации (ЭВМ), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление ПД.

53.Общие и специальные условия обработки персональных данных.

Ст.9. Общие условия согласия субъекта ПД на обработку его ПД:
1. Субъект ПД даёт согласие на их обработку свободно, своей волей и в своём интересе - то есть согласие должно быть конкретным и сознательным.
2. Согласие на обработку ПД даётся субъектом ПД или его представителем в любой форме, если иное не установлено ФЗ (проверяется оператором).
3. В случаях, предусмотренных ФЗ, обработка ПД только с согласия в письменной форме субъекта ПД на бумажном носителе либо в форме электронного документа, подписанного в соответствии с ФЗ электронной подписью.
4. Порядок получения в форме электронного документа согласия субъекта ПД в целях предоставления государственных и муниципальных услуг, устанавливается Правительством РФ.
5. В случае недееспособности субъекта ПД согласие на обработку его персональных данных даёт законный представитель субъекта.
6. В случае смерти субъекта ПД согласие на обработку его ПД дают наследники субъекта ПД, если такое согласие не было дано субъектом ПР при его жизни.

Условия обработки специальных категорий ПД (ст.10).
Основное условие - обработка специальных категорий ПД (о национальной принадлежности, политических и религиозных взглядах, состоянии здоровья, интимной жизни) не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.
Случаи обработки специальных категорий ПД:
1) субъект персональных данных дал согласие в письменной форме на обработку своих ПД,
2) общедоступные ПД (по воле субъекта ПД),
3) обработка ПД осуществляется для переписи населения,
4) обработка ПД для социальной помощи и пенсий,
5) обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов, если получение согласия субъекта ПД невозможно,
6) обработка ПД осуществляется в медицинских целях,
7) обработка ПД осуществляется соответствующими общественной или религиозной организацией в отношении своих членов (участников),
8) обработка ПД необходима в связи с осуществлением правосудия и прокурорского надзора,
9) обработка ПД осуществляется в целях обороны, безопасности, противодействия терроризму, противодействии коррупции, ОРД, исполнительного производства, исполнения уголовных наказаний,
10) обработка ПД осуществляется в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

Статья 11. Биометрические персональные данные.
1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПД) и которые используются оператором для установления личности субъекта, могут обрабатываться только при наличии согласия в письменной форме субъекта ПД.
2. Обработка биометрических ПД может осуществляться без согласия субъекта ПД, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством РФ об обороне, безопасности, противодействии терроризму, транспортной безопасности, противодействии коррупции, ОРД, государственной службе, исполнения уголовных наказаний, о выезде из России и въезде в РФ.

54.Правовое регулирование деятельности в области защиты информации.

Правовое обеспечение информационной безопасности (ПОИБ) как суботрасль информационного права.

В системе ИП ПОИБ по своей значимости занимает ведущее место.

Во-первых, исторически - это "исторически первый" правовой комплекс.

Во-вторых, это самый крупный блок норм ИП, он занимает более 30% всех нормативных актов.

В-третьих, это системообразующий суперправовой институт, определяющий характер информационного права. Неслучайно, в Доктрине ИБ провозглашен главный объект угроз, то есть воздействия на национальные интересы в информационной области человеческой деятельности является сфера духовной жизни.

ПОИБ – совокупность норм права, регулирующих правовой режим доступа к информации, защиты прав и интересов Л., О. и Г., в информационной сфере, защиты информации и информационной инфраструктуры, а также ответственности за информационные правонарушения.

Структура ПОИБ:

• Институт правового режима доступа к информации (обеспечение правомерного доступа к информации и правовой режим информации ограниченного доступа – конфиденциальной информации);
• Институт защиты прав и интересов Л., О. и Г. в информационной сфере (права на информацию, защита интересов Л., О., Г. от негативного воздействия социально вредной информации и агрессивной информационной среды и др.);
• Институт защиты информации и информационной инфраструктуры (правовой режим деятельности по обеспечению защиты конфиденциальности информации и инфраструктуры, а также лицензирования такой деятельности);
• Институт ответственности за информационные правонарушения.

Согласно статье 16 ФЗ об информации защита информации - это деятельность по принятию организационных, правовых и технических мер, направленных на:

• обеспечение защиты общедоступной информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
• соблюдение конфиденциальности информации ограниченного доступа;
• реализацию права на доступ к общедоступной информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации.

Целями установления требований о защите информации:

• Целостность информации - это устойчивость;
• Конфиденциальность;
• Доступность.

Достижение этих целей является качественными признаками и свойствами безопасности информации. Поэтому правовой режим защиты информации направлен на достижение именно названных свойств.

Обязанности обладателя И. и оператора ИС.

П.4 ст.16 ФЗ об информации обладатель информации, оператор информационной системы обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) постоянный контроль за обеспечением уровня защищенности информации.

Силы и средства правового обеспечения ИБ.

Основные НПА ПОИБ:

• Конституция РФ

• ФЗ «Об информации, информационных технологиях и о защите информации»
• ФЗ «О связи»
• ФЗ «Об электронной подписи»
• ФЗ «О государственной тайне»
• ФЗ «О коммерческой тайне»
• ФЗ «О персональных данных»
• Уголовный кодекс РФ, Трудовой кодекс РФ, КоАП РФ
• Указ Президента РФ от 17 марта 2003 №351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
• Постановление Правительства РФ №1233 от 3 ноября 1994 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти»
• Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. Приказом ФСТЭК РФ от 1 февраля 2013 №17.

Силы обеспечения информационной безопасности:
• Президент РФ
• Федеральное собрание РФ
• Правительство РФ
• Совет Безопасности РФ
• Федеральные органы исполнительной власти (ФСБ России, ФСО России, МО РФ, МВД РФ, Минкомсвязь России, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
• ФСТЭК РФ является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней.

55.Понятие информационного правонарушения

Информационное правонарушение – общественно опасное, противоправное и виновное деяние (действия и бездействия) совершаемые в сфере информации либо совершаемые в иных областях человеческой деятельности с использованием информационных систем.

Общие признаки ИП – общественно опасное, противоправное и виновное деяние.

Специальные признаки ИП – информационная сфера и информационные средства совершения.

Общие признаки ИП.

Общественно опасное деяние. Это один из самых содержательных признаков правонарушения, обычно выражающийся в количестве вреда, причиненного для определенных ценностей для личности, общества и государства.

Но в информационной сфере необходимо выделять еще и качественную сторону вреда, поскольку нередко дать количественную оценку информации и информационного ресурса весьма затруднительно.

Тем не менее, названные признаки (количественный и качественный) дают основание отделять деяния друг от друга по степени опасности.

Виновность деяния. Этот признак несет в себе смысловые характеристики психического отношения субъекта к нарушению и к последствиям таких действий, а также совокупность условий, выражающих отношение лица (юридического лица – по административным правонарушениям) к соблюдению закона и установленным запретам в информационной сфере.

Как правило, существует 2 форма вины – умышленные и неосторожные деяния. В информационной сфере нередки неосторожные действия, связанные с нарушениями режима обработки информации, которые закон относит к правонарушениям (особенно с информацией ограниченного доступа).

Специальные признаки.

Информационная сфера (область деятельности, связанная с поиском, производством, хранением и использованием информации, вне зависимости от ее форма – традиционной или электронной (компьютерной)).
Информация – особый предмет посягательства позволяет выделить правонарушения в особый разряд исключительно информационных.
Информация ограниченного доступа чаще всего становится таким объектом – сведения, составляющие тайну, персональные данные.
Особое значение имеет электронная форма (компьютерная информация). Причем КИ может быть как объектом посягательства, так и средством совершения правонарушения (спам, вредоносная программа и др.).
Важное значение имеет такой объект посягательства как электронный документ (именно он чаще всего является целью для злоумышленника – платежные документы, электронные карты, электронные деньги и др.).
Информационные системы и их элементы (инфраструктура).
Особый арсенал средств совершения правонарушений – средства вычислительной техники и связи, информационные технологии и другие вспомогательные системы сбора, обработки и передачи информации.
Информационные системы также могут быть как объектом посягательства, так и средством совершения правонарушения.
• Базы данных
• Средства вычислительной техники и связи
• Информационные технологии (программы)
• Сайты и порталы в сети Интернет
• другие вспомогательные системы сбора, обработки и передачи информации.

56.Виды информационных правонарушений.

Гражданско-правовые информационные правонарушения.
- это общественно вредное, противоправное, виновное деяние, посягающее на нематериальные блага информационной природы.
Главный отличительный признак ГП правонарушений – общественные отношения по поводу информационных нематериальных благ – честь и доброе имя, достоинство, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, коммерческая тайна, результаты интеллектуальной деятельности и др. (ст.150 ГК РФ).
Отдельный вид информационных нематериальных благ – информационная продукция – предназначенная для оборота продукции СМИ, печатная продукция, программы для ЭВМ и базы данных, а также информация, распространяемая и размещаемая в сети Интернет и др.
Оборот информационной продукции – предоставление и (или) распространение информационной продукции, включая ее продажу, аренду, выдачу из фондов общедоступных библиотек, публичное исполнение, размещение в сети Интернет и др.
Гражданско-правовые правонарушения могут возникать:
• из закона (ответственность за нарушение коммерческой тайны, в сфере интеллектуальной деятельности);
• договора (договор о передаче сведений КТ, лицензионный договор);
• вследствие неосновательного обогащения (реализация без данных, товарных знаков, программ для ЭВМ и др);
• причинения вреда (вследствие нарушения доступа к информационным системам).

Статья 1253.1 ГК РФ. Особенности ответственности информационного посредника – лицо:
• осуществляющее передачу материала в сети Интернет;
• предоставляющее возможность размещения материала или информации в сети Интернет;
• предоставляющее возможность доступа к материалу в этой сети.
Существенные особенности установлены для информационного посредника.
Общее правило – ответственность его за нарушение интеллектуальных прав в сети Интернет наступает на общих основаниях.

п.2 ст.1253.1 ГК РФ. Основания освобождения от ответственности информационного посредника при передаче материалов (оператор сети) в сети Интернет:
1) не является инициатором этой передачи и не определяет получателя указанного материала;
2) не изменяет указанный материал при оказании услуг связи;

3) не знал и не должен был знать о том, что использование соответствующих материалов является неправомерным (оператор связи и провайдер хостинга);
4) своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав, предусмотренные законом (провайдер хостинга).

Статья 152 ГК РФ. Защита чести, достоинства и деловой репутации.
1. Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.
5. Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети Интернет, гражданин вправе требовать удаления соответствующей информации, а также опровержение указанных сведений способом, обеспечивающим доведение опровержения до пользователей сети Интернет.

Дисциплинарные информационные правонарушения.
Дисциплинарные – трудовой сфере при работе с информацией при выполнении трудовых функций и профессиональных обязанностей.
Дисциплинарное информационное правонарушение (проступок) – виновное, противоправное деяние (действия и бездействия), то есть неисполнение или ненадлежащее исполнение работником возложенных на него трудовых обязанностей, совершенное в сфере информации либо с использованием информационных систем.
Исходя из данного определения, можно отметить главные особенности дисциплинарных информационных правонарушений:
• в сфере труда при обработке и использовании информации (сфере сбора, хранения, обработки, передачи и использовании информации);
• неисполнение или ненадлежащее исполнение трудовых обязанностей (а не бытовых действий);
• работник должен находиться с работодателем в трудовых отношениях – а не в гражданско-правовых;
• ответственность наступает за нарушение возложенных на работника трудовых обязанностей (в соответствии с трудовым договором и локальными актами);
• требование о возмещении вреда может быть удовлетворено только в случае, если работодатель принимал меры по соблюдению конфиденциальности информации (п.2 ст.14 ФЗ Об информации, информационных технологиях и о защите информации).

Особенности дисциплинарных информационных правонарушений:
1. Они всегда носят локальный характер, который проявляется в том, что:
• на каждом предприятии и в любой организации могут быть установлены специфичные разные по характеру, уникальные трудовые обязанности, в зависимости от рода деятельности организации;
• в каждом случае необходимо руководствоваться установленными в организации особыми правилами.
2. П.6 ст.81 ТК РФ предусмотрено в качестве самостоятельного основания увольнения работника – разглашение охраняемой законом информации, отнесенной к государственной, коммерческой, или иной тайне, а также персональных данных.

АИП – посягающее на установленный порядок государственного управления общественно опасное, противоправное и виновное действие (бездействие) физического или юридического лица, совершаемые в сфере информации либо с использованием информационных систем при осуществлении государственных функций.
Сфера государственного управления – сфера общественного порядка и установленного порядка государственной власти и безопасности.
Общественно опасное деяние – выражается в количестве вреда, причиненного ценностям для личности, общества и государства.

В зависимости от причиненного вреда различают не только виды правонарушений, но и отграничивают административные правонарушения от уголовных преступлений.
3. Противоправное деяние – выражает нарушение запретов, установленных КоАП РФ, который относит проступки к числу административных правонарушений. В ст.2.1 Кодекса подчеркивается, что только им или законами субъектов РФ устанавливается административная ответственность.

4. Нередко в нормах, предусматривающих ответственность, делается ссылка на конкретные правила, существующие в той или иной сфере управления. Например, ст.13.11 предусматривает ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных.

В главе 13 КоАП общим объектом правонарушения выделен один общий объект – общественные отношения в области информации и информационной деятельности (связи, защиты информации, СМИ и др).
Видовыми объектами в главе 13 Кодекса названы 31 таких объектов (или целей информационных правонарушений).
Кроме того, в Кодексе поименованы еще более 80 статей, в которых предусмотрена административная ответственность за информационные правонарушения в других областях, но тесно священных с информационной сферой.
В них, специальный объект (информационные ОО) одновременно совпадают с другими родовыми объектами (например, ОО в области общественного порядка).

Статья 13.31. неисполнение обязанностей организатором распространения информации в сети Интернет.
2.Неисполнение организатором распространения информации в сети Интернет обязанности хранить и (или) предоставлять уполномоченным государственным органам, осуществляющим ОРД или обеспечение безопасности РФ, информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию о таких пользователей -
влечет наложение административного штрафа на граждан в размере от 3тыс до 5тыс рублей; на ДЛ – от 30тыс до 50тыс рублей; на ЮЛ – от 300тыс. до 500тыс. рублей.

Специальный объект (информационная сфера) является дополнительным объектом посягательства наряду с основным – обычно указанным в названии главы КоАП.
Область охраны ОС.
Статья. 8.5. сокрытие или искажение экологической информации.

Порядок управления.
ст.19.7.3. Непредставление информации в Банк России.

Общественный порядок и общественная безопасность.
ст.20.23. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.

Информационное преступление (ИП) – общественно-опасное, виновное деяние (действие или бездействие), совершенное в сфере информации либо с использованием информационных систем и причинившее существенный вред охраняемым законом правам и интересам личности, общества и государства.
Всего в УК РФ предусмотрены 58 составов информационных преступлений, расположенных в отдельных главах.

ИП против личности (глава 17) – ст.128.1. Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

ИП против конституционных прав и свобод человека и гражданина (глава 19) – ст.137-138 (тайна связи), ст.140 (отказ в предоставлении информации), ст.155 (разглашение тайны усыновления).
Статья 137. Нарушение неприкосновенности частной жизни.
1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении или СМИ.
Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

Глава 21. Преступления против собственности.
Статья 159.3. Мошенничество с использованием платежных карт – до 10 лет лишения свободы.
Статья 159.6. Мошенничество в сфере компьютерной информации.
1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей – до 10 лет лишения свободы.

ИП в сфере экономической деятельности (глава 22 УК РФ).
Статья 171.2. Незаконные организация и проведение азартных игр с использованием сети Интернет.
Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую тайну, налоговую или банковскую.
Статья 185.6. Неправомерное использование инсайдерской информации – до 6 лет лишения свободы.

ИП против общественной безопасности (глава 24 УК РФ):
Ст.207. Заведомо ложное сообщение об акте терроризма.
Ст.237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (экологическая информация).
Ст.242. Незаконное распространение порнографических материалов или предметов…с использование сети Интернет – до 6 лет лишения свободы.

ИП в сфере компьютерной информации (глава 28 УК РФ).
Ст.272. Неправомерный доступ к компьютерной информации.
Примечание 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
Ст.274. Старая редакция – Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
Новая редакция ст.274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

ИП против основ конституционного строя и государственной власти (глава 29 УК РФ).
Статья 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ с использованием сети Интернет.
Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства с использованием сети Интернет.
Статья 283. Разглашение государственной тайны.
Статья 283.1. Незаконное получение сведений, составляющих государственную тайну.
Статья 284. Утрата документов, содержащих государственную тайну.

ИП против правосудия (глава 31 УК РФ).
Статья 310. Разглашение данных предварительного расследования.
Статья 311. Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса.

57.Система ответственности за совершение информационных преступлений.

Общие условия ответственности (ст 17 фз об информации)
Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.
В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:
либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;
либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.
Провайдер хостинга, оператор связи и владелец сайта в сети "Интернет" не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

58.Правовые проблемы борьбы с компьютерными преступлениями.
Наиболее характерными, обостряющими проблемы борьбы с информационными преступлениями, являются следующие обстоятельства:
1)Сложность юридических конструкций и употребляемых в законе терминов и понятий. Эта сложность отражает технологическую сложность окружающей человека информационной среды.
2)Недостаточная строгость уголовного закона в отношении большинства составов преступлений (максимальное-6 лет лишения свободы по ч.2. ст.272 УК) – явное несоответствие между распространённостью явления и строгостью наказания
3)Сложность расследования таких преступлений. Это проявляется, прежде всего, в том, что в законе не закреплены электронные формы доказательств. Проблемой также является недостаточная квалификация следователей и судей, которые принимают участие в расследовании компьютерных преступлений и рассмотрении уголовных дел в суде
4)Проблема определения юрисдикции, т.е. неопределённость в определении правовых мер ответственности за совершение информационных преступлений в ситуациях трансграничности информационного пространства. Возникает сложность при определении точного времени, места, субъекта совершения преступления в сети Интернет. В связи с этим сложно определить закон, подлежащий применению. Также в разных странах действуют разные технологические и технические условия использования информационных систем, разные стандарты безопасности.
5)Международные проблемы борьбы с информационными преступлениями. Информационные преступления, особенно совершаемые в сети Интернет, носят глобальный характер. Для согласования и координации действий по борьбе с ними заключаются международные договоры и иные соглашения
Конкретные формы противодействия информационной преступности в настоящее время совершенствуются и постепенно находят закрепление в российском законодательстве.