Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

ИНФОРМАЦИОННОЕ ПРАВО

сборник учебно-методических материалов

для направления подготовки: 40.03.01 Юриспруденция

Благовещенск 2017

Печатается по решению
редакционно-издательского совета
юридического факультета
Амурского государственного университета

Составитель: Галоян А.Р.

Информационное право: сборник учебно-методических материалов для направления подготовки 40.03.01 – Юриспруденция – Благовещенск: Амурский гос. ун-т, 2017.

Содержание

1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННОЕ ПРАВО»

Основными формами изучения дисциплины и проведения текущего и промежуточного контроля являются: лекции, практические занятия, решение задач, аналитическая работа с текстами нормативных правовых актов, тестирование. Итоговый контроль – зачет.

Важным условием успешного изучения дисциплины является системный подход в организации учебного процесса. При изучении дисциплины следует обращать особое внимание на освоение понятийного аппарата, а также на изучение содержания юридических норм.

С этими целями, помимо изучения лекционных материалов, необходимо использование текстов правовых актов. Для глубокого и качественного усвоения материала курса, прежде всего, рекомендуется внимательно ознакомиться с рабочей программой, тематическим планом дисциплины, планами практических занятий, заданиями для самостоятельной работы, рекомендованной литературой.

Аудиторная работа студента предполагает: во-первых, активную мыслительную деятельность во время посещения лекционных занятий, которые являются основной формой организации учебного процесса. Во-вторых, активное участие в проведении практических занятий. Аудиторная работа дополняется самостоятельной работой студентов с материалами лекций, подготовкой к практическим занятиям, выполнением заданий для самостоятельной работы по темам дисциплины.

Важной формой усвоения знаний по курсу является лекция. Работа студента над лекцией состоит из трех этапов. Первый из них подготовка к лекции, т. е. самостоятельное ознакомление с материалом следующей лекции при помощи учебника и др. источников. Подобный подход существенно облегчит восприятие материала, будет способствовать более глубокому его усвоению.

Главная стадия – это прослушивание лекции. Для того чтобы усвоить основные положения лекции, запомнить ее, необходимо конспектировать излагаемый материал. Следует помнить, что конспект – это не стенографирование лекции, а сокращенная запись главного. Подзаголовки разделов лекции, новые имена и понятия, определения и наиболее важные обобщающие выводы следует записывать полностью, иначе потом их будет трудно воспроизвести. Точно также должны быть полностью воспроизведены ссылки на правовые акты и специальную литературу. Аргументация общих юридических положений, обоснования и доказательства выводов, характеристика предметов или явлений могут быть записаны сокращенно. Важно также отчетливо представить себе и воспроизвести в записи внутреннюю связь между отдельными аргументами, чтобы вся аргументация или характеристика была записана как стройное целое. Иллюстративный материал-факт, примеры, казусы можно записывать совсем кратко. В тетради, предназначенной для конспектирования лекций, следует оставлять поля с таким расчетом, чтобы после прочтения лекционного материала можно было сделать примечания, исправления, дополнения, привести примеры.

Третий этап работы студента над лекцией – это своевременная работа над конспектом, которая позволит не только исправить неточности в записях, но и прочнее усвоить материал лекции.

2. СОДЕРЖАНИЕ КУРСА ЛЕКЦИЙ

Тема 1. Информационное право как отрасль права.

1. Информационное право: понятие, предмет и метод. Информационные правоотношения.
2. Источники информационного права.
3. Становление информационного права как науки и отрасли права, современное положение в системе российского права и перспективы.
4. Информационная сфера общества как объект правового регулирования.
5. Информационная функция государства.
6. Пределы деятельности государства в информационной сфере общества.
7. Система федеральных органов исполнительной власти в информационной сфере.

Лекции читаются по 1-2 вопросам.

Информационное право: понятие, предмет и метод. Информационные правоотношения.

Информационное право – как отрасль права представляет собой совокупность правовых норм, установленных и охраняемых государством, возникающих в информационной сфере производства, преобразования и потребления информации.

Информационное право изучает информационную сущность права.

Информационное право связано с другими отраслями права, т.е. имеет характер комплексной отрасли.

Предмет отрасли – это то, что она регулирует.

Предмет информационного права – это часть общественных отношений, которая связана с созданием, оформлением, хранением и обработкой, распространением, использованием информационных ресурсов, в том числе в области формирования и управления информационными ресурсами, в области использования новых технологических работ с информацией и технологий ее передачи в системах и сетях коммуникаций, в области установлением мер по обеспечению безопасности в информационных сферах, включая юридическую ответственность в названных областях.

Предметная область информационного права включает в себя процесс информатизации - организацию социально-экономических и научно-технических оптимальных условий для удовлетворения информационных потребностей и реализации прав субъектов на основе формирования и использования информационных ресурсов.

Процесс расширения границ информатизации современного общества, всех его государственных и негосударственных структур приводит к расширению сферы отношений, регулируемых нормами информационного права. Содержание таких отношений определяется постепенно под воздействием внешних объективно происходящих и исторически обусловленных процессов социально-экономического, политического и иного характера.

Предмет Информационного права составляют три группы отношений:

1. Отношения, связанные с производством, передачей, распространением, поиском и получением информации;
2. Отношения, связанные с применением информационных технологий;
3. Отношения, связанные с обеспечением защиты информации.

Метод отрасли – это определенные приемы, способы и средства юридического воздействия права на общественные отношения.

Информационная отрасль использует следующие методы в качестве правового регулирования:

1. Предписание – возложение прямой юридической обязанности совершать те или иные действия в условиях, предусмотренных правовой нормы.

2. Запрет – возложение прямой юридической обязанности не совершать те или иные действия в условиях, предусмотренных правовой нормой.

3. Дозволение – юридическое разрешение совершения в условиях, предусмотренных правовой нормой, те или иные действия либо воздержаться от их совершения по своему усмотрению.

В информационном праве используется вся совокупность способов регулирующего воздей-

ствия на информационные правоотношения, т.е. как диспозитивное регулирование (свобода выбора, равенство сторон, децентрализация, координация), так и императивное регулирование (централизованное осуществление властных полномочий, строгая субординация).

В теории государства и права под системой понимается упорядоченность по критерию единства предмета и метода правового регулирования совокупность правовых норм, которая складывается для регулирования данной области общественных отношений.

Функции информационного права:

1. Правотворческая – выражается в наделении субъектов информационной деятельности полномочиями по нормотворчеству.
2. Правоисполнительная – информационное право непосредственно регулирует общественные отношения, воздействуя на них при помощи установленных правом методов.
3. Организационная – информационная деятельность является организационной, т.е. направленной на упорядочение общественных отношений в информационной сфере.
4. Координационная – заключается в обеспечении разумного и эффективного взаимодействия всех субъектов информационных отношений.
5. Правоохранительная - обеспечивает соблюдение установленного правового режима и защиту законных интересов всех участников информационных отношений.

Принципы информационного права:

Принципы - это зафиксированные в правовых нормах основные начала, определяющие сущность и содержание данной отрасли права, придающие ей системный характер и позволяющие ей говорить о целостности механизма правового регулирования.

Под принципами информационного права понимаются основные исходные положения, юридически закрепляющие объективные закономерности общественной жизни, проявляющиеся в информационной сфере.

1. Принцип приоритетности прав. В информационном праве возможен как приоритет прав личности (ст. 2 Конституции РФ), так приоритет прав государства, например, при столкновении интересов государства и личности в правоотношениях, когда требуется установить пределы осуществления права на тайну государства и тайну отдельно взятой личности.

2. Принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом.

3. Принцип достоверности информации и своевременности ее предоставления.

4. Принцип ограничения доступа к информации только федеральным законом.

5. Принцип открытости информации о деятельности органов государственной власти и органов местного самоуправления. *Принцип прозрачности.*

6. Принцип обеспечения безопасности РФ при создании информационных систем, их эксплуатации и защите содержащейся в них информации.

7. Принцип равноправия языков народов РФ при создании информационных систем и их эксплуатации.

8. Принцип неприкосновенности частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Правовые отношения - это урегулированные правом и находящиеся под охраной государства общественные отношения, участники которых выступают в качестве носителей взаимно корреспондирующих друг другу юридических прав и обязанностей.

Информационные правоотношения - это общественные отношения, урегулированные нормами информационного права, субъекты которых являются носителями взаимных информационных прав и обязанностей.

Регулирование информационных отношений с помощью права осуществляется посредством установления определенных информационно-правовых норм, т.е. путем установления правил поведения субъектов информационных отношений и применения норм информационного права.

Информационные отношения возникают между разнообразными субъектами - гражданами, редакциями газет, телестудиями, предприятиями, организациями, фирмами и другими, в которых последние участвуют в качестве носителей прав и обязанностей, установленных нормами инфор-

мационного права.

Особенности (черты) информационных отношений:

- Возникают, изменяются и прекращаются только на основе информационных норм;
- Возникают, развиваются и прекращаются в информационной сфере при обращении информации только;
- Опосредуют государственную политику признания, соблюдения и защиты информационных прав и свобод человека и гражданина в информационной сфере;
- Отражают особенности применения публично-правовых и гражданско-правовых методов правового регулирования при осуществлении информационных прав и свобод с учетом специфических особенностей и юридических свойств информации и информационных объектов.

Виды правоотношений:

1. По назначению:
   - Материальные – эти отношения возникают на основе материальных норм, и складываются по поводу реализации прав и обязанностей участников отношений.
   - Процессуальные – это отношения, которые складываются в информационной сфере в связи с порядком разрешения конкретных дел, они регулируются процессуальными нормами.
2. По характеру:
   - Активные
   - Пассивные
   - Посреднические
   - Вспомогательные
   - Организационные
   - Имущественные
   - Неимущественные
3. По содержанию:
   - Регулятивные – дозволенная деятельность
   - Охранительные – возникают в результате восстановления нарушенных прав или в связи с правонарушением.
4. По соотношению прав и обязанностей участников:
   - Вертикальные – один из участников подчинен другому;
   - Горизонтальные – участники не находятся в подчинении друг друга.

5. По степени конкретизации и субъектному составу можно выделить следующие информационные правоотношения:

- абсолютные (точно определена лишь одна сторона, например, собственник информационных ресурсов, информационных систем, технологий и средств обеспечения, которому противостоят все те, кто с ним соприкасается или может соприкоснуться, и которые обязаны уважать это его право);
- относительные (строго определены обе стороны, например, учредитель средства массовой информации и главный редактор этого же СМИ: они в соответствии с требованиями закона обязаны заключить между собой договор и утвердить устав редакции СМИ)
- общерегулятивные (выражают юридические связи более высокого уровня между государством и гражданами, а также последних между собой по поводу гарантирования и осуществления основных прав и свобод личности, а равно обязанностей).

Информационные отношения возникают, изменяются и прекращаются на основе юридических фактов (событий или действий – правомерных и неправомерных).

Элементы информационного правоотношения (субъект + объект + содержание).

1. Субъекты – это участники информационных отношений: (правосубъектность: правоспособность + дееспособность + деликтоспособность):

- физические лица;
- юридические лица всех форм собственности;
- органы государственной власти;

- органы местного самоуправления
- должностные лица;
- общественные организации;
- государство;
- другие субъекты, признаваемые субъектами права.

2. Объект правоотношений - это все те материальные, духовные и иные социальные блага, явления и процессы, по поводу которых субъекты информационного права вступают в информационно-правовые отношения, и что является предметом их интересов, прав и обязанностей. Т.е. объектом информационных правоотношений является сама информация в ее многочисленных и многообразных формах (печатные издания, газеты, журналы, книги, аудио- и аудиовизуальные материалы, рекламная продукция, компьютерные программы, базы и банки данных, информационные сети и системы, средства связи и т.п.).

К особой группе объектов информационного права относят нематериальные блага, т.е. не имеющие экономического содержания и не отделимые от личности их носителя. Проявление нематериальных благ в качестве информации возможно в тех случаях, когда необходимо защищать честь, достоинство и личную репутацию гражданина, т.е. об информации, которая искажена и не соответствует личностным качествам данного человека. Нематериальные блага характеризуются двумя признаками: отсутствием материального содержания и неразрывной связью с личностью носителя.

3. Содержание правоотношения: права и обязанности субъектов. Они зависят от вида информационных правоотношений.

Под правами участников информационных отношений понимают меры возможного или дозволенного поведения. Состоит из трех правомочий: правомочие на собственные действия + правомочие на чужие действия + правомочие на защиту.

Под обязанностью понимается установленная законом мера должного или требуемого поведения. Состоит из трех элементов: необходимостью совершить определенные действия или воздержаться от них + необходимость исполнить требования управомоченного субъекта + необходимостью нести ответственность за нарушения или за неисполнение требований закона.

Источник информационного права – это внешняя форма выражения информационно-правовых норм.

Источниками информационного права являются:

1. Конституция РФ.
2. Международно-правовые акты.
3. Федеральные законы, в том числе кодексы.
4. Указы Президента РФ.
5. Постановления Правительства РФ.
6. Нормативные акты федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ.
7. Локальные правовые акты.

Тема 2. Понятие и основные принципы функционирования информационного общества.

1. Понятие и признаки информационного общества, цели формирования и развития в России.
2. Стратегия развития информационного общества в Российской Федерации.
3. Справочно-информационный портал «Государственные услуги».

Лекции читаются по 1-2 вопросам.

Понятие и признаки информационного общества, цели формирования и развития в России.

Информационное общество – это состояние развития общества, которое характеризуется высокоразвитой информационной инфраструктурой, информационной культурой и массовой информатизацией, широким доступом населения к информационным ресурсам, рынком информационных продуктов и приоритетным развитием информационного сектора экономики.

Признаки информационного общества:

1. Состояние развития общества (новое состояние). Это не просто этап развития общества. Состояние – это совокупность параметров, которые характеризуют данное общество.

Параметры: новая высокоразвитая инфраструктура (высокопроизводительные компьютеры, высокие информационные технологии)

2. Высокоразвитая информационная структура.
3. Высокоразвитая информационная культура. Знания используются во благо всеми пользователями информационной среды:
4. возможность овладения знанием
5. обязанность каждого пользователя информационной среды не злоупотреблять своими знаниями и правами, т.е. запрет на злоупотребление.
6. Массовая информатизация - информатизация во всех сферах человеческой деятельности.
7. Широкий доступ населения к информации
8. Информационный рынок, т.е. рынок информационных продуктов – свободный оборот информационных товаров и услуг, производство и реализация которых зависит от общественных потребностей.

Целями развития информационного общества в России являются:

1. Повышение устойчивости общественного развития, конкурентоспособности страны, благосостояния и качества жизни граждан.
2. Укрепление государственных гарантий реализации конституционных прав человека и гражданина в информационном обществе, создание равных возможностей по доступу к информации и информационно-коммуникационным технологиям.
3. Повышение качества образования и здравоохранения.
4. Создание условий для сохранения и развития культурного разнообразия и самобытности народов, проживающих на территории Российской Федерации.
5. Повышение эффективности государственного управления.
6. Противодействие угрозам использования потенциала информационно-коммуникационных технологий для нанесения ущерба национальным интересам России.

Развитие информационного общества в Российской Федерации базируется на следующих принципах:

1. сотрудничество и партнерство государства, бизнеса и гражданского общества;
2. опережающее развитие информационной инфраструктуры общества;
3. создание благоприятной среды для развития информационной инфраструктуры;
4. обеспечение гражданам доступа к информации, идеям и знаниям, к использованию информационно-коммуникационных технологий;
5. укрепление доверия и безопасности при использовании информационно-коммуникационных технологий;
6. обеспечение свободы массовой информации и независимости средств массовой информации; содействие развитию глобального информационного общества;
7. международное сотрудничество.

Для достижения целей развития информационного общества в России государство решает следующие задачи:

1. определяет систему основных мероприятий по развитию информационного общества и создает условия для согласования усилий государственных органов и негосударственных организаций по их выполнению;
2. совершенствует правовые механизмы регулирования общественных отношений, связанных с использованием информационно-коммуникационных технологий, в целях ускорения постиндустриального развития России;

осуществляет информатизацию государственного управления и местного самоуправления;

1. создает условия для ликвидации неравенства в доступе к информации и информационно-коммуникационным технологиям различных групп населения и субъектов Российской Федерации.

Стратегия развития информационного общества в Российской Федерации.

Стратегия развития информационного общества (далее - Стратегия) устанавливает цели и принципы этого развития, а также определяет наиболее важные мероприятия в области использования потенциала информационных технологий, науки и образования, национальной культуры и демократического устройства для улучшения качества жизни граждан России, повышения конкурентоспособности и укрепления обороноспособности страны, безопасности государства, обеспечения правопорядка, расширения взаимовыгодного международного сотрудничества, содействия решению задач по формированию глобального информационного общества.

Стратегия предназначена для использования при подготовке концептуальных, доктринальных, программных и иных документов, определяющих цели, принципы и направления деятельности государственных органов и негосударственных организаций по решению проблем интенсификации постиндустриального развития России.

Главной целью Стратегии является повышение качества жизни граждан. Впервые в практике государствоведения в официальном документе, в котором определяются базовые параметры государственной политики, заявлена именно такая, самая важная для общества и человека цель.

Другими целями Стратегии являются: обеспечение конкурентоспособности России, развитие всех основных сфер жизни общества (экономической, социально-политической, культурной и духовной), совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

К числу основных задач, требующих решения для достижения поставленных целей, относятся:

- формирование современной информационной и телекоммуникационной инфраструктуры, предоставление на ее основе качественных услуг и обеспечение высокого уровня доступности для населения информации и технологий;
- совершенствование системы государственных гарантий конституционных прав человека и гражданина в информационной сфере;
- развитие экономики Российской Федерации на основе использования информационных и телекоммуникационных технологий;
- повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг;
- повышение качества образования, медицинского обслуживания, социальной защиты населения на основе развития и использования информационных и телекоммуникационных технологий;
- развитие науки, технологий и техники, подготовка квалифицированных кадров в сфере информационных и телекоммуникационных технологий;
- сохранение культуры, укрепление нравственных принципов в общественном сознании, развитие системы культурного и гуманитарного просвещения;
- противодействие угрозам национальным интересам России, использованию потенциала информационных и телекоммуникационных технологий.

Развитие информационного общества в Российской Федерации базируется на следующих основных началах (принципах):

- партнерство государства, бизнеса и гражданского общества;
- свобода и равенство доступа к информации и знаниям;
- поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;
- содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;
- обеспечение национальной безопасности в информационной сфере.

Тема 3. Понятие и правовые принципы построения электронного правительства в РФ.

1. Электронное правительство как один из важнейших институтов формирования информационного общества и инструмент транспарентности деятельности органов власти: понятие, признаки, перспективы становления в Российской Федерации. Зарубежный опыт раз-

вития электронного правительства.
2. Проблемы законодательного обеспечения доступа к информации о деятельности органов государственной власти.

Одним из основных направлений формирования электронного государства является реализация концепции электронного правительства. *Электронное правительство* (англ. *e-Government*) – способ предоставления информации и оказания уже сформировавшегося набора государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное (вербальное) взаимодействие между государством и заявителем минимизировано, а информационные технологии используются максимально полно.

Электронное правительство – система электронного документооборота государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны, служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Создание электронного правительства предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.

Внедрение информационных технологий в практику государственного управления повышает его интенсивность, способствует качественному изменению отношений между властью и обществом. Информационные технологии могут способствовать развитию политической активности в обществе при условии заинтересованности в этом власти и общества. Тогда Интернет создает возможности для расширения публичного пространства и вовлечения в это пространство все новых и новых авторов и пользователей.

При этом возможны различные варианты. Так, если в традиционном обществе власть осуществляется в основном правительствами, бюрократиями и парламентами (то есть, достаточно традиционными политическими институтами), то в информационном обществе (то есть, в обществе сетевого типа) в публичную власть все больше включаются такие формы, как комиссии, форумы, большие демократически организованные группы. При этом, если ранее информация об управленческих действиях власти была в большей степени централизованной и засекреченной, то в информационном обществе она становится распределенной и открытой, а информационные процессы, связанные с интерфейсами и протоколами, становятся сетевыми, включают сетевые форумы и систему образования.

Органы государственной власти посредством электронных средств более оперативно и эффективно предоставляют услуги населению и бизнес-организациям, совершенствуют отношения между различными властными структурами. Обычно специалисты отмечают, что при этом достигаются общие (для власти и общества) цели деятельности государства:
– укрепляются и расширяются формы сотрудничества между обществом и государством;
– более эффективно осуществляется экономическое и социальное развитие общества и граждан;
– повышается эффективность реагирования власти на социальные проблемы;
– уменьшается стоимость услуг населению;
– развивается кадровый потенциал государственного управления;
– повышается ответственность государственных служащих, поощряется их инициатива и повышается уровень прозрачности государственного управления в целом.

Концепция электронного правительства развивается, как обычно отмечается учеными и специалистами, за счет «размещения правительства в сети Интернет», то есть путем *увеличения степени публичности действий органов государственной власти*.

Целями формирования в Российской Федерации электронного правительства являются:
– повышение качества и доступности предоставляемых организациям и гражданам государственных услуг, упрощение процедуры и сокращение сроков их оказания, снижение административных издержек со стороны граждан и организаций, связанных с получением государственных услуг, а также внедрение единых стандартов обслуживания граждан;
– повышение открытости информации о деятельности органов государственной власти и расши-

рение возможности доступа к ней и непосредственного участия организаций, граждан и институтов гражданского общества в процедурах формирования и экспертизы решений, принимаемых на всех уровнях государственного управления;
– повышение качества административно-управленческих процессов;
– совершенствование системы информационно-аналитического обеспечения принимаемых решений на всех уровнях государственного управления, обеспечение оперативности и полноты контроля за результативностью деятельности органов государственной власти и обеспечение требуемого уровня информационной безопасности электронного правительства при его функционировании.

«Электронное правительство», по сути, является единственным официальным источником информации о деятельности властных структур. Все другие источники информации о деятельности правительства либо имеют ограниченный доступ, либо не являются официальными.

Основные направления формирования электронного правительства:
а) снижение трудозатрат органов государственной власти на организацию обмена информацией на межведомственном уровне до 50 %;
б) уменьшение административной нагрузки на организации и граждан, связанной с представлением в органы государственной власти необходимой информации, снижение количества обращений граждан в органы государственной власти для оказания услуг и сокращение времени ожидания за счет повышения оперативности взаимодействия органов государственной власти на основе информационно-коммуникационных технологий исходя из принципов «одного окна», что, по экспертным оценкам, позволит в масштабах страны получить ежегодную экономию до 10 млрд. рублей;
в) обеспечение гарантированного уровня информационной открытости органов государственной власти, повышение уровня доверия и взаимодействия, сокращение затрат времени на реализацию гражданами своих конституционных прав и обязанностей за счет создания новых и модернизации действующих ведомственных сайтов в сети Интернет, развития их информационного наполнения и функциональных возможностей, а также обеспечение тематического доступа к размещаемой на них информации через специализированную информационную систему «Правительственный портал». В соответствии с этим направлением в декабре 2010 года открылся интернет-портал «Государственные услуги» (www.gosuslugi.ru).

В настоящее время данный интернет-портал выполняет информационно-справочные функции: содержит описание госуслуг, порядка их предоставления, списки документов, необходимых для их получения, бланки и образцы заявлений, квитанций, контакты соответствующих государственных органов. Сейчас на портале есть такой набор сведений о более чем 100 федеральных и 250 региональных государственных услугах. Информацию на портале размещают и актуализируют сами ведомства, предоставляющие те или иные услуги. Кроме этого, обеспечена возможность представлять в государственные органы через портал документы в электронном виде без личной явки. Затем заявитель сможет сам отслеживать на портале, как его документы «идут» по госорганам, где рассматриваются и какие решения по ним принимаются. В перспективе результат своего обращения за госуслугой заявитель будет получать на этом же портале, если это не запрещено федеральными законами. Данный портал разработан по заданию Министерства связи и массовых коммуникаций в рамках федеральной целевой программы «Электронная Россия»;
г) повышение оперативности и качества принимаемых решений, сокращение издержек на управление за счет создания соответствующих ведомственных информационно-аналитических систем;
д) повышение спроса на информационно-коммуникационные технологии со стороны органов государственной власти и, как следствие, рост отечественного производства их до 10 % в год за счет повышения готовности и мотивации работников органов государственной власти к использованию современных информационно-коммуникационных технологий в своей деятельности, а также за счет содействия разработке и обоснованию ведомственных программ и проектов информатизации;
е) развитие национальной инфокоммуникационной инфраструктуры и обеспечение информационного единства страны за счет формирования единой телекоммуникационной инфраструктуры для государственных нужд и подключения к ней государственных органов на всей территории Российской Федерации.

Таким образом, в любой современной, экономически развитой стране сформировано и функционирует электронное правительство. Его главной целью является повышение качества и увеличение скорости оказания государственных услуг собственным гражданам.

Тема 4. Информационная безопасность.

1. Понятие информационной безопасности.
2. Задачи обеспечения безопасности в информационной сфере.
3. Угрозы, риски, правонарушения в области информационной безопасности.

Информационная безопасность – это *состояние* защищённости информационной среды, *защита информации* представляет собой *деятельность* по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть *процесс*, направленный на достижение этого состояния.

Информационная безопасность – это состояние защиты жизненно важных национальных интересов от угроз в информационной сфере определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Для понимания сущности информационной безопасности нужно знать термины:

«безопасность» - отсутствие опасных воздействий, способных нарушить нормальное функционирование системы.

«национальная безопасность» - состояние защищённости личности, общества, государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы. Достойное качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие РФ, оборону и безопасность государства.

«национальные интересы РФ» - совокупность внутренних и внешних потребностей государства в обеспечении защищённости и устойчивого развития личности, общества и государства.

Элементы информационной безопасности:

- Состояние защищённости: предотвращение утечек, утраты, хищении, искажении, поддели и других форм незаконного вмешательства в информацию, сохранении государственной и коммерческой тайны, обеспечении доступа к офиц. информации, защите конституционных прав на неприкосновенность информации о частной жизни. Защищённость - не только сохранность, но и целостность, устойчивость.

Таким образом, состояние защищённости применительно к информационной безопасности – сохранение всех элементов информационной системы.

- Национальные интересы в информационной сфере.

Жизненно важные интересы личности: реализация конституционных прав и свобод на доступ к информации, на её использование, на защиту информации, обеспечивающей личную безопасность.

Жизненно важные интересы общества: обеспечение интересов личности в этой сфере, упрочение демократии, создание правового социального государства, общественное согласие, духовное обновление России.

Жизненно важные интересы государства: создание условий для гармоничного развития информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости строя, суверенитета и т.д.

- Внутренние и внешние угрозы.

Угроза информационной безопасности – это различные обстоятельства (условия, факторы и состояния), т.е. опасные воздействия на информацию и информационную инфраструктуру, реализацию правового статуса гражданина в информационной сфере, а также опасные воздействия, связанные с причинением вреда информационным интересам личности, обществу и государству.

Виды:

- Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному созна-

нию, духовному возрождению России;

- Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи. Обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Тема 5. Информация ограниченного доступа.

1. Тайна как разновидность информации. Государственная тайна: понятие и содержание. Порядок отнесения сведений к государственной тайне, а также их рассекречивания.
2. Порядок допуска к сведениям, составляющим государственную тайну.
3. Ответственность за правонарушения и преступления, связанные с государственной тайной.
4. Информация, составляющая коммерческую тайну: понятие, содержание и правовой режим.
5. Порядок засекречивания информации, составляющей коммерческую тайну.
6. Законные способы доступа к информации, составляющей коммерческую тайну.
7. Способы защиты прав обладателя информации, составляющей коммерческую тайну.
8. Юридическая ответственность за нарушение режима коммерческой тайны.
9. Основные гарантии приватности жизни граждан. Понятие и виды персональных данных.
10. Принципы и условия обработки персональных данных.
11. Правовое положение участников оборота персональных данных.
12. Юридическая ответственность за нарушение режима охраны персональных данных.

Лекции читаются по 1-2, 4 вопросам.

Тайна как разновидность информации. Государственная тайна: понятие и содержание. Порядок отнесения сведений к государственной тайне, а также их рассекречивания

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны (ч. 2 ст. 2 Закона РФ «О государственной тайне»). Характер этих сведений обусловливает их особый правовой статус, выражающийся в процедуре засекречивания и рассекречивания, а также допуска к секретной информации.

Закон РФ «О государственной тайне» определяет отнесение сведений к государственной тайне и их засекречивание как введение ограничений на их распространение и доступ. Статья 7 Закона РФ «О государственной тайне» закрепляет перечень сведений, не подлежащих ограничениям.

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях;
- о стихийных бедствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о ситуации с преступностью;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах РФ;
- о состоянии здоровья высших должностных лиц РФ;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Засекречивание должностными лицами перечисленных сведений в зависимости от причиненного обществу, государству и гражданам материального и морального вреда влечет уголовную, административную или дисциплинарную ответственность, гарантией чего служит право на обращение в суд.

Отнесение сведений к государственной тайне осуществляется в соответствии со ст. 9 и 11 Закона РФ «О государственной тайне» и определяется их отраслевой, ведомственной или программно-целевой принадлежностью. Основным условием засекречивания сведений является их соответствие общему (раздел II Закона РФ «О государственной тайне») и локальным перечням сведений, относимых к государственной тайне. Решение о засекречивании в каждом конкретном случае принимается компетентным должностным лицом, несущим за это персональную ответственность.

Согласно ст. 5 Закона РФ «О государственной тайне», к государственной тайне относятся сведения в военной области, в сфере экономики, науки и техники, внешней политики; материалы разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Степень секретности сведений, составляющих государственную тайну, соответствует размеру ущерба, который может быть нанесен национальной безопасности вследствие их распространения (ч. 1 ст. 8 Закона РФ «О государственной тайне»). Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие им грифы секретности для носителей указанных сведений: «особой важности»; «совершенно секретно»; «секретно» (ч. 2 ст. 8 Закона РФ «О государственной тайне»). Порядок определения размеров ущерба, который может быть нанесен безопасности страны вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством РФ (ч. 3 ст. 8 Закона РФ «О государственной тайне»).

Допуск к государственной тайне – это процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений (ч. 5 ст. 2 Закона РФ «О государственной тайне»). Эта процедура предусматривает санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну (ч. 6 ст. 2 Закона РФ «О государственной тайне»).

Установлены три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности (ч. 16 ст. 21 Закона РФ «О государственной тайне»).

Закон РФ «О государственной тайне» предусматривает основания для отказа должностному лицу или гражданину в допуске к государственной тайне (ст. 22), условия прекращения допуска должностного лица или гражданина к государственной тайне (ст. 23) и ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне (ст. 24).

Наряду с обычным порядком доступа к сведениям, составляющим государственную тайну, существует особый порядок допуска к государственной тайне (ст. 21): члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к таким сведениям без проведения проверочных мероприятий, предусмотренных ст. 21 Закона РФ «О государственной тайне». Сохранность государственной тайны в таких случаях гарантируется путем установления Законом ответственности указанных лиц.

Рассекречивание сведений означает снятие ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям (ч. 1 ст. 13).

Основаниями для рассекречивания сведений, составляющих государственную тайну, являются:

- принятие государством международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;
- изменение объективных обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной;
- истечение срока, установленного при засекречивании сведений, составляющих государственную

тайну, и их носителей (максимальный срок – 30 лет);
- необоснованность засекречивания сведений и их носителей;
- в исключительных случаях срок засекречивания сведений, составляющих государственную тайну, и их носителей может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Руководители органов государственной власти, наделенные полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности. Эти решения подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения. Граждане, предприятия, учреждения и органы государственной власти РФ вправе обратиться к компетентным должностным лицам с запросом о рассекречивании сведений, отнесенных к государственной тайне. Такой запрос должен быть рассмотрен в течение трех месяцев. При отсутствии полномочий для решения данного вопроса запрос в месячный срок с момента поступления передается в орган государственной власти, наделенный такими полномочиями, либо в межведомственную комиссию по защите государственной тайны, о чем уведомляется податель запроса. Уклонение должностных лиц от рассмотрения запроса по существу влечет за собой административную (дисциплинарную) ответственность в соответствии с действующим законодательством.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. В случае признания судом необоснованности засекречивания сведений, они подлежат рассекречиванию в установленном Законом РФ «О государственной тайне» порядке.

Анализ правовых норм об информации ограниченного доступа показывает, что многие из них носят декларативный и противоречивый характер. При этом следует учитывать, что если в советский период осуществлялась правовая защита только государственных секретов, то в настоящее время на законодательном уровне урегулирована защита различных видов информации с ограниченным доступом, разглашение (утечка) которой может причинить материальный и моральный вред интересам личности, общества и государства.

Порядок допуска к сведениям, составляющим государственную тайну.

Согласно ст. 2 Закона о государственной тайне допуск к государственной тайне – это процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений. Допуск организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляется путем получения ими лицензий на проведение работ со сведениями соответствующей степени секретности. Лицензия выдается предприятиям при выполнении ими следующих условий:

• выполнение требований нормативных документов по обеспечению защиты сведений, составляющих государственную тайну;

• наличие подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

• наличие сертифицированных средств защиты информации.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности только после оформления допуска по соответствующей форме в установленном порядке. Под доступом к сведениям понимается санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

1. первая форма – для граждан, допускаемых к сведениям особой важности;
2. вторая форма – для граждан, допускаемых к совершенно секретным сведениям;

3. третья форма – для граждан, допускаемых к секретным сведениям.

При этом наличие допуска к сведениям более высокой степени секретности является основанием для доступа к сведениям более низкой степени секретности.

Порядок допуска должностных лиц и граждан к государственной тайне определяется Законом о государственной тайне, а также Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденной постановлением Правительства РФ № 1050 (далее – Инструкция о порядке допуска).

Итак, допуск должностных лиц и граждан к государственной тайне осуществляется в добровольном порядке и предусматривает:

1. Принятие на себя гражданином или должностным лицом обязательств перед государством по нераспространению доверенных сведений, составляющих государственную тайну.

2. Согласие гражданина или должностного лица на частичные, временные ограничения прав. В соответствии со ст. 24 Закона о государственной тайне должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах.

Ограничения могут касаться:

• права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

• права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

• права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

3. Письменное согласие гражданина или должностного лица на проведение в его отношении проверочных мероприятий полномочными органами. Проверочные мероприятия, связанные с оформлением граждан по первой и второй формам допуска, осуществляются ФСБ РФ и ее территориальными органами во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность (далее – органы безопасности). Допуск граждан по третьей форме, за исключением случаев, когда имеются обоснованные сомнения в достоверности данных, предоставленных гражданином, осуществляется руководителем организации без проведения проверочных мероприятий органами безопасности. Однако это не касается руководителей организаций, допуск которых оформляется только после проведения проверочных мероприятий органами безопасности (п. 6 Инструкции о порядке допуска).

Объем проверочных мероприятий зависит от степени секретности сведений, к которым оформляется допуск. Проверка проводится с целью выявления оснований, которые могут послужить причиной отказа в допуске к государственной тайне.

Согласно ст. 22 Закона о государственной тайне для гражданина или должностного лица такими основаниями являются:

• признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

• наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;

• постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;

• выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;

• уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Если при проверке обнаруживается хотя бы одно из указанных оснований, гражданину или должностному лицу должно быть отказано в допуске к государственной тайне. Решение об отказе

принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

4. Определение видов, размеров и порядка предоставления гражданину или должностному лицу социальных гарантий.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие социальные гарантии:

• преимущественное право при прочих равных условиях на оставление на работе при проведении организационных и (или) штатных мероприятий;

• процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым сотрудник имеет доступ;

• дополнительная процентная надбавка к заработной плате за стаж работы для сотрудников структурных подразделений по защите государственной тайны.

Правила выплаты ежемесячных процентных надбавок к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе, и сотрудников структурных подразделений по защите государственной тайны утверждены постановлением Правительства Российской Федерации № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны». Данные гарантии отражаются в трудовом договоре (контракте) работника (должностного лица), заключаемом исключительно по окончании проведения проверочных мероприятий.

5. Ознакомление гражданина или должностного лица с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение. Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством (ст. 26 Закона о государственной тайне).

6. Принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну. Следует учесть, что согласно ст. 25 Закона о государственной тайне руководители несут персональную ответственность за подбор лиц, допускаемых к сведениям, составляющим государственную тайну, а также за создание условий, при которых граждане знакомятся только с теми сведениями и в таких объемах, которые необходимы для выполнения ими должностных (функциональных) обязанностей.

Оформление допуска. Подготовка материалов на граждан, оформляемых на допуск к особой важности, совершенно секретным и секретным сведениям, осуществляется управлениями (отделами) кадров, а в случае их отсутствия – работниками, ведущими кадровую работу в организации. Направлять граждан в подразделения по защите государственной тайны и органы безопасности по вопросам оформления допуска запрещается (п. 16 Инструкции о порядке допуска).

При оформлении допуска используются следующие формы документов, образцы которых приведены в Приложении к Инструкции о порядке допуска:

форма 1. Номенклатура должностей работников, подлежащих оформлению на допуск к особой важности, совершенно секретным и секретным сведениям (по заполнении секретно);

форма 1.1. Список членов организации, которым оформляется допуск к государственной тайне (утверждается руководителем организации);

форма 2. Анкета (заполняется оформляемым гражданином собственноручно);

форма 3. Карточка (по заполнении секретно);

форма 4. Список на оформляемого гражданина и его близких родственников;

форма 5. Учетная карточка на допуск по первой и второй формам допуска;

форма 6. Список лиц, подлежащих допуску к секретным сведениям по организации;

форма 7. Отметка органов ФСБ России о проведении проверочных мероприятий для оформления допуска по третьей форме допуска;

форма 8. Карточка на допуск гражданина по третьей форме допуска;

форма 9. Типовой договор (контракт) об оформлении допуска к государственной тайне (приложение к трудовому договору);

форма 10. Журнал учета карточек на допуск работников по первой и второй формам.

Оформление допуска на практике вызывает немало вопросов, обусловленных большим количеством форм и строгим порядком их заполнения, отправки в органы безопасности и последующего хранения. Рассмотрим процедуру оформления поэтапно.

Создание в организации перечня должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну. Данный перечень определяется номенклатурой должностей (форма 1), утверждаемой руководителем организации или его заместителем, после согласования ее с органом безопасности. В номенклатуру включаются только те должности, по которым допуск граждан к указанным сведениям действительно необходим для выполнения ими должностных (функциональных) обязанностей. В номенклатуру могут включаться должности работников, допуск которых к сведениям соответствующей степени секретности обусловлен выполнением ими заданий в других организациях, куда они командируются на основании распоряжений вышестоящих организаций, соглашений или договоров, предусматривающих выполнение совместных работ. Изменения и дополнения в номенклатуру должностей вносятся по мере необходимости, согласовываются и утверждаются в установленном порядке. Номенклатура должностей пересматривается не реже одного раза в пять лет (п. 13 Инструкции о порядке допуска).

Граждане, оформляемые на допуск к государственной тайне, заполняют анкету (форма 2), в которой они обязаны указывать достоверные данные. Анкета оформляемого на допуск гражданина подписывается работником кадровой службы и заверяется печатью организации.

Работники отдела кадров в ходе беседы с оформляемым гражданином сверяют указанные в анкете данные с его личными документами (паспорт, военный билет, трудовая книжка, диплом об образовании, свидетельство о рождении и т.д.), уточняют ответы на отдельные вопросы анкеты, выявляют представляющие интерес сведения, не предусмотренные вопросами анкеты, выясняют у гражданина, имел ли он за последний год отношение к секретным работам, документам и изделиям, давал ли он обязательство по неразглашению сведений, составляющих государственную тайну, работал ли (служил) на режимных объектах, запрашивают необходимые справки и документы, знакомят гражданина с содержанием типового договора (контракта) об оформлении допуска к государственной тайне (форма 9).

О результатах беседы работники кадровой службы обязаны информировать в устной или письменной форме руководителя подразделения по защите государственной тайны, особенно если в ходе беседы или в анкетных данных выявлены обстоятельства, влияющие на принятие решения о допуске гражданина к государственной тайне, или установлено, что он ранее работал с особой важности или совершенно секретными сведениями.

Подразделение по защите государственной тайны организации дает оценку первичным материалам на оформляемого гражданина, представляемым кадровой службой. При необходимости оно запрашивает дополнительные сведения с прежних мест работы и карточку (форма 3) из подразделения по защите государственной тайны организации, где оформляемый гражданин работал в течение последнего года, и также анализируют их в целях определения целесообразности проведения проверочных мероприятий органами безопасности.

При оформлении третьей формы допуска

На граждан, оформляемых на третью форму допуска, отделом кадров составляются общие (в алфавитном порядке) списки лиц, подлежащих допуску к секретным сведениям (форма 6).

Помимо этого, руководители организаций, не включенных в перечень объектов, на которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности, могут направлять в органы безопасности материалы на граждан, допускаемых по третьей форме допуска, в случае, когда имеются обоснованные сомнения в достоверности их анкетных данных. При этом в орган безопасности направляется сопроводительное письмо с указанием обстоятельств, влияющих на принятие решения о допуске соответствующего

гражданина, его анкета (форма 2), три экземпляра списка на оформляемого гражданина (форма 4), один экземпляр списка лиц, подлежащих допуску к секретным сведениям (форма 6), и другие материалы, необходимые для принятия решения по данному вопросу. При этом о проведении проверочных мероприятий органами безопасности делается отметка в листе согласования (форма 7) или на списках (форма 6), возвращаемых в организацию вместе с сопроводительным письмом. В этом случае входящий номер, проставляемый соответствующим органом безопасности на списке (форма 6), является и номером допуска.

После этого решение о допуске гражданина по третьей форме допуска оформляется распоряжением руководителя организации, при этом делается отметка в списке лиц, подлежащих допуску к секретным сведениям (форма 6), с соответствующей записью в графе 10 карточки на допуск (форма 8).

При оформлении гражданина по первой или второй форме допуска помимо анкеты гражданина (форма 2) организацией подготавливаются и направляются в органы безопасности следующие документы:

1. Мотивированное письмо о необходимости оформления допуска гражданина к государственной тайне (готовится подразделением по защите государственной тайны). В письме указываются должность, на которую оформляется гражданин, ее порядковый номер в утвержденной номенклатуре должностей, количество лиц, допущенных по данной должности к сведениям, составляющим государственную тайну, отмечаются обстоятельства, влияющие на принятие решения о допуске, и дается их оценка. Если оформляемый гражданин ранее был допущен к данным сведениям, указывается номер допуска, дата окончания проведения проверочных мероприятий и наименование органа безопасности, который их проводил, а в случае -переоформления допуска – причина переоформления.

2. Один экземпляр карточки (форма 3) (готовится подразделением по защите государственной тайны). Данная карточка с момента заполнения является секретным документом и регистрируется в журнале учета карточек на допуск работников по первой и второй формам допуска (форма 10) ответственными за их хранение лицами. На каждого гражданина, оформляемого по первой или второй формам допуска, заводится только одна карточка, которая при его переходе на работу в другие организации пересылается по получении письменного запроса от соответствующего подразделения по защите государственной тайны. Новая карточка заводится на работника, только если ранее заведенная карточка была уничтожена по причинам, определенным Инструкцией о порядке допуска.

3. Два или три экземпляра списка на оформляемого гражданина и его близких родственников (отца, мать, братьев, сестер и детей старше 16 лет), а также на жену (мужа), в том числе бывших (форма 4) (готовятся отделом кадров по согласованию с органом безопасности).

4. Один или два экземпляра учетной карточки на допуск по первой и второй формам допуска (форма 5) (готовится подразделением по защите государственной тайны по согласованию с органом безопасности).

Карточка (форма 3) с отметкой органа безопасности о проведении проверочных мероприятий, связанных с допуском гражданина по первой или второй форме допуска, возвращается без сопроводительного письма в организацию. Ее следует хранить в подразделении по защите государственной тайны организации в специальной картотеке, составленной в алфавитном порядке (при необходимости такие картотеки могут вестись по структурным подразделениям организации). После этого решение о допуске гражданина по первой или второй форме допуска оформляется распоряжением руководителя организации с отметкой в графе 8 карточки (форма 3) и заверяется его подписью и печатью организации.

Взаимные обязательства организации и оформляемого лица отражаются в специальном договоре (контракте) об оформлении допуска к государственной тайне, заключение которого осуществляется с соблюдением всех требований гражданского и трудового законодательства РФ. Данный документ служит приложением к трудовому договору.

На каждое лицо, получившее третью форму допуска, подразделение по защите государственной тайны на основании письменного ходатайства руководителя структурного подразделения

организации заводит карточку (форма 8) с указанием номера списка (форма 6) и даты утверждения руководителем организации этого списка. Заполненные карточки заверяются подписью руководителя подразделения по защите государственной тайны и печатью этого подразделения, регистрируются в журнале учета карточек на допуск работников (форма 10) отдельно от карточек на допуск граждан по первой и второй формам и вместе со списками на лиц, подлежащих допуску к секретным сведениям (форма 6), и договорами (контрактами) об оформлении допуска к государственной тайне хранятся в подразделении по защите государственной тайны в течение всего периода работы в данной организации граждан, допущенных к секретным сведениям. Карточки (форма 8) в другие организации не пересылаются и уничтожаются по истечении одного года после увольнения граждан, на которых они были заведены. При небольшом количестве граждан, оформляемых на допуск по третьей форме, карточки (форма 8) могут не заводиться. Списки (форма 6) также хранятся в организации в течение одного года, после чего они могут быть уничтожены в установленном порядке.

В отношении граждан, которые свыше года после оформления им допуска по первой, второй или третьей форме не соприкасались со сведениями, составляющими государственную тайну, а также граждан, которые уволились из организации, ушли на пенсию или закончили обучение в учебном заведении и на которых в течение года не затребованы карточки (форма 3), действие допусков прекращается. При этом договоры (контракты) об оформлении допуска к государственной тайне и карточки (форма 3) хранятся в подразделении по защите государственной тайны не менее пяти лет, после чего они уничтожаются по акту.

Следует иметь в виду, что при оформлении на работу уволенного с военной службы в запас гражданина при наличии в его военном билете специальной записи о допуске к государственной тайне в период прохождения им службы отдел кадров организации обязан направить запрос в военкомат по месту жительства этого гражданина для получения карточки (форма 3). При этом руководитель организации имеет право в течение одного года со дня увольнения гражданина с военной службы в запас допускать его к государственной тайне без проведения дополнительных проверочных мероприятий органами безопасности. При этом в графе 8 карточки (форма 3), полученной из военкомата, делается соответствующая запись. О факте допуска гражданина к государственной тайне информируется орган безопасности, в его адрес подразделение по защите государственной тайны организации направляет -учетную карточку (форма 5).

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. Решение о допуске к государственной тайне руководителей организаций, впервые привлекающихся для проведения работ со сведениями, составляющими государственную тайну, принимается руководителями организаций – заказчиков работ. Карточки (форма 3 или 8) в этом случае хранятся в подразделении по защите государственной тайны организации – заказчика работ.

Кроме того, необходимо учесть, что работники кадровой службы обязаны своевременно информировать подразделения по защите государственной тайны обо всех изменениях в анкетных данных граждан, допущенных к соответствующим сведениям по любой из форм допуска, для решения вопроса о целесообразности переоформления им допуска в соответствии с установленным порядком.

Информация, составляющая коммерческую тайну: понятие, содержание и правовой режим

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

Информация, составляющая коммерческую тайну (секрет производства), - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную

или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны. Следовательно, коммерческая тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, в связи с чем предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования.

Коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Вся имеющаяся информация по степени конфиденциальности, утрата которой может вызвать различные по тяжести последствия, может быть распределена по следующим группам:

- Высшая степень конфиденциальности. Данная информация является ключевой в деятельности фирмы, основой ее нормального функционирования. Утрата или разглашение этой информации нанесет непоправимый ущерб деятельности фирмы. Это – угроза высокой степени тяжести, последствия реализации которой могут ликвидировать саму фирму.

- Строго конфиденциальная информация. Утечка этой информации может вызвать значительные по тяжести последствия. Это информация о стратегических планах фирмы, о перспективных соглашениях и т.п.

- Конфиденциальная информация – ее разглашение наносит фирме ущерб, сопоставимый с текущими затратами фирмы, ущерб может быть преодолен в сравнительно короткие сроки.

- Информация ограниченного доступа – ее утечка оказывает незначительное негативное воздействие на экономическое положение фирмы (должностные инструкции, структура управления).

- Открытая информация. Ее распространение не представляет угроз экономической безопасности фирмы. Наоборот, отсутствие данной информации может оказать негативное воздействие на экономическое положение фирмы.

По функционально-целевому признаку выделяются следующие составляющие коммерческой тайны:

1. Деловая информация:
сведения о контрагентах;
сведения о конкурентах;
сведения о потребителях;
сведения о деловых переговорах;
коммерческая переписка;
сведения о заключенных и планируемых контрактах.
2. Научно-техническая информация:
содержание и планы научно-исследовательских работ;
содержание “ноу-хау”, рационализаторских предложений;
планы внедрения новых технологий и видов продукции;
3. Производственная информация:
технология;
планы выпуска продукции;
объем незавершенного производства и запасов;
планы инвестиционной деятельности.
4. Организационно-управленческая информация:
сведения о структуре управления фирмой не содержащиеся в уставе;
оригинальные методы организации управления;
система организации труда.

5. Маркетинговая информация:
рыночная стратегия;
планы рекламной деятельности;
планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм;
методы работы на рынках;
планы сбыта продукции;
анализ конкурентоспособности выпускаемой продукции.
6. Финансовая информация:
планирование прибыли, себестоимости;
ценообразование – методы расчета, структура цен, скидки;
возможные источники финансирования;
финансовые прогнозы.
7. Информация о персонале фирмы:
личные дела сотрудников;
планы увеличения (сокращения) персонала;
содержание тестов для проверки вновь принимаемых на работу.
8. Программное обеспечение:
программы;
пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях.

Тема 6. Юридическая ответственность в информационной сфере.

1. Понятие, виды, функции и принципы юридической ответственности в информационной сфере.
2. Основные составы преступлений в сфере компьютерной информации.
3. Особенности информационных правонарушений и их выявления.
4. Усиление значимости ответственности в информационной сфере.
5. О подходах к разработке методологии ответственности в информационном праве.

Лекции читаются по 1 вопросу.

Понятие юридической ответственности относится к числу общетеоретических и применяемых в различных отраслях права. Это понятие неоднозначное и, в известной мере, спорное для юридической науки. Доктринальному единству подхода к данной категории препятствуют различия в исходных правовых позициях ученых, которые нашли отражение в многочисленных работах, посвященных проблемам юридической ответственности.

Являясь одним их юридических средств, нейтрализующих последствия ненадлежащего поведения субъекта, нарушающего права и охраняемые законом интересы других лиц, юридическая ответственность выступает как реакция государства на совершенное правонарушение. Исходя из этого, содержанием юридической ответственности будет выступать государственное властное принуждение, проявляющее себя в различных формах. Однако не всякое государственное принуждение следует считать ответственностью. Например, принудительное (судебное) воздействие, побуждающее нарушителя к исполнению своих обязанностей, не будет мерой ответственности, поскольку в данном случае отсутствует элемент дополнительных неблагоприятных последствий для нарушителя, т.е. тех самых лишений, которые выходят за рамки принудительно исполненной обязанности.

Юридическая ответственность за нарушения законодательства, регулирующего отношения в информационной сфере, имеет ряд специфических особенностей. Эти особенности заключаются в следующем:

- правонарушения, подпадающие под применение тех либо иных мер воздействия на совершившего их субъекта, всегда связаны с информацией;
- правонарушения можно рассматривать в качестве информационно-правовых, если их связь с информацией является не только непосредственной, но и опосредованной наличием ее

материального носителя.

Как и любая юридическая ответственность, ответственность за правонарушения в информационной сфере реализуется в рамках правоохранительных правоотношений, субъектами которых выступают нарушитель информационно-правовых норм и государство в лице уполномоченных на применение санкций органов. Лицо, привлекаемое к ответственности, имеет право на защиту от незаконного привлечения.

В доктрине выделяют принципы юридической ответственности, которые в полной мере распространяются и на ответственность в информационной сфере. К их числу относятся:

- принцип законности, означающий, что ответственность имеет место лишь за правонарушения в информационной сфере, признаваемые в качестве таковых законом;
- принцип обоснованности, заключающийся в установлении факта совершения лицом конкретного правонарушения;
- принцип справедливости, означающий, в частности, что ответственность должна быть соизмерима тяжести совершенного правонарушения;
- принцип неотвратимости, предполагающий неизбежность наступления для правонарушителя неблагоприятных последствий;
- принцип целесообразности, заключающийся в индивидуализации мер воздействия на правонарушителя и соответствии этих мер целям юридической ответственности.

Государственное принуждение осуществляется путем применения к нарушителю различных мер воздействия. От характера этих мер и характера последствий их применения зависит отраслевая принадлежность юридической ответственности за нарушения законодательства в информационной сфере. Если неблагоприятные последствия носят имущественный характер и выражаются в возмещении убытков, уплате неустойки, возмещении вреда, имеет *место* гражданско-правовая ответственность.

Если неблагоприятные последствия выражаются в санкциях, предусмотренных нормами административного или уголовного законодательства, имеет *место* административно-правовая или уголовная ответственность.

В механизме правового обеспечения в информационной сфере значимое место занимают борьба с нарушениями информационного законодательства и их предупреждение. Для этого действует так называемый институт юридической ответственности, закрепленный в российском законодательстве.

Понятно, что любой вид информационных отношений только тогда приобретает реальные свойства (характеристики), когда существуют гарантии того, что они будут исполнены субъектами, а также если нормативным правовым актом установлена юридическая ответственность за их неисполнение или ненадлежащее исполнение.

В настоящее время практически сформирована основная нормативная база по предупреждению и пресечению правонарушений в информационной сфере, предусматривается как гражданско-правовая, дисциплинарная (включая материальную), административная ответственность, так и уголовная ответственность за совершение правонарушений и преступлений в информационной сфере, разработаны и действуют многочисленные законы и подзаконные акты в информационной сфере. Но их практическое применение довольно слабое, отсутствуют конкретные механизмы применения и соблюдения законодательства на практике, существуют трудности по наложению взысканий за его нарушения, отсутствует систематизация действий правоохранительных органов по осуществлению своих обязанностей и прав в информационной сфере.

Как уже говорилось, основополагающие положения законодательства в информационной сфере содержатся в Конституции РФ. В ней закреплено право каждого на неприкосновенность частной жизни, личную и семейную тайну, указано, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются и т.д. Федеральным законом «Об информации, информатизации и защите информации» сведения о гражданах (персональные данные), т.е. о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, отнесены к конфиденциальной информации. Законодательством также определены сведения, право свободного доступа к которым не может быть ограничено.

Российское государство усиливает свое внимание к проблеме укрепления информационного правопорядка. В Концепции национальной безопасности Российской Федерации отмечено, что «важнейшими задачами обеспечения информационной безопасности Российской Федерации являются: реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности; совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство; противодействие угрозе развязывания противоборства в информационной сфере».

При этом особо отмечается, что национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

В Уголовном кодексе РФ к преступлениям в информационной сфере можно отнести более 50 статей, причем отдельная глава УК РФ (глава 28) посвящена составам преступлений в сфере компьютерной информации. В ней содержатся три статьи преступлений (ст. 272 - 274). В Кодексе РФ об административных правонарушениях, существенным новшеством которого является возможность привлечения за правонарушения к административной ответственности юридических лиц, также имеется глава 13 и отдельные статьи в ряде глав, посвященные административным правонарушениям в информационной сфере.

Основанием для возникновения юридической ответственности является совершенное субъектом (участником) информационных правоотношений правонарушение в информационной сфере.

Правонарушением в информационной сфере принято считать виновное, противоправное деяние (действие, бездействие) конкретного субъекта, посягающее на установленный информационный правопорядок и причиняющее вред информационной сфере либо создающее реальную угрозу такого причинения.

Для реализации юридической ответственности важно установить причинно-следственные связи между негативными последствиями, наступившими в результате правового предписания, и действиями (бездействием) предполагаемого правонарушителя. Основной целью применения юридической ответственности к правонарушителям является поддержание информационного правопорядка, основанного на соблюдении большинства субъектов информационных правоотношений установленным материальным нормам информационного права, а не только наказание виновного субъекта.

К сожалению, не все субъекты правоотношений соблюдают информационный правопорядок. Многие из них нарушают этот правопорядок и подвергаются воздействию норм информационного права, устанавливающих юридическую ответственность. Однако на часть субъектов сам факт наличия таких норм права, которые устанавливают юридическую ответственность, действует как сдерживающий фактор, предупреждающий их неправомерные действия в информационной сфере. Отсюда вытекает, что установление юридической ответственности носит еще и некое нравственно-воспитательное значение.

Таким образом, юридическая ответственность за правонарушения в информационной сфере - это применение к виновному лицу, совершившему правонарушение, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке.

Юридическим основанием привлечения к ответственности является наличие в деянии (действии, бездействии) правонарушителя состава правонарушения в информационной сфере, предусмотренного нормами права.

Состав правонарушения, в том числе и информационного, включает в себя четыре обязательных элемента (признака): объект, объективную сторону, субъект и субъективную сторону.

Объектом правонарушения является совокупность общественных отношений в информационной сфере. В качестве объектов могут выступать отношения в области обеспечения информационной безопасности, в области массовой информации, авторского права, библиотечного дела, в области законодательно установленных правил создания, сохранения и использования Архивного

фонда Российской Федерации и архивов, отношения в сфере установленного правового режима распространения сведений, составляющих государственную, коммерческую, служебную тайну, тайну частной жизни и т.д.

Информация (сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления), документированная информация, компьютерная информация могут являться предметом правонарушения в информационной сфере.

Сложность регулирования информационных правоотношений заключается также в том, что здесь применяются все виды ответственности: административная, гражданско-правовая, уголовная, дисциплинарная.

Объективная сторона правонарушения в информационной сфере характеризует внешнее выражение процесса незаконного посягательства на информацию. В целом ее образуют следующие признаки:

1) нарушение норм права в информационной сфере путем деяния (действия, бездействия);

2) причинение вреда информационным интересам личности, общества или государства либо создание реальной опасности такого вреда;

3) наличие причинной связи между опасным деянием в информационной сфере и наступившими последствиями в виде причинения вреда информационным интересам личности, общества или государства.

По конструкции объективной стороны, составы правонарушений в информационной сфере подразделяются на формальные и материальные.

Формальными называются такие составы правонарушений, объективная сторона которых в законе характеризуется с помощью только одного признака - нарушение норм права в информационной сфере путем деяния (действия, бездействия). Материальные составы - это составы, в объективную сторону которых законодатель включил в качестве обязательных все три выше перечисленных признака объективной стороны.

С субъективной стороны могут иметь место две формы вины - умышленная или неосторожная. Признать лицо виновным - означает установление того, что правонарушение в информационной сфере совершено либо умышленно, либо по неосторожности.

В Уголовном кодексе РФ предусматривается деление умысла на прямой и косвенный (ст. 25), а неосторожности - на легкомыслие и небрежность (ст. 26). Формы вины в конкретных преступлениях либо указываются в диспозициях статей, либо подразумеваются. Причем умышленная форма вины подразумевается во всех случаях, когда при описании преступления нет прямого указания на неосторожность (ч. 2 ст. 24).

В Кодексе РФ об административных правонарушениях указаны две формы вины - административное правонарушение признается совершенным умышленно или по неосторожности (ст. 2.2).

Субъектами правонарушения в информационной сфере могут быть физические и юридические лица в зависимости от вида юридической ответственности.

Российская правовая система предусматривает четыре вида ответственности физических лиц за правонарушения - дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную. Юридические лица (предприятия, учреждения и организации) привлекаются лишь к административной и гражданско-правовой ответственности.

Ответственность наступает в соответствии как с Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации», так и с иными законами РФ - Трудовым кодексом, Кодексом об административных правонарушениях, Уголовным кодексом, Гражданским кодексом, другими актами трудового, административного, уголовного, гражданского законодательства, включая законы субъектов Федерации.

В гражданском праве в области имущественных отношений основным источником является Гражданский кодекс РФ.

Отнесение правонарушения к тем или иным видам зависит в основном от степени причиненного природе и обществу вреда, личности правонарушителя, иных обстоятельств дела, влияющих на уровень ответственности. В Уголовном кодексе Российской Федерации и в Кодексе РФ об административных правонарушениях предусматриваются смягчающие и отягчающие обстоятельст-

ва, учитываемые при наказании. В определенной степени они имеются также в Трудовом кодексе РФ и Гражданском кодексе РФ.

Тема 7. Электронный документ и электронный документооборот.

1. Понятие, функции и основные принципы работы электронной подписи.
2. Статус субъектов правоотношений с электронной подписью. Факсимиле как аналог собственноручной подписи.
3. Правовой статус электронных документов. Законодательная база электронного документооборота в Российской Федерации.

Лекции читаются по 1 вопросу.

В мире электронных документов подписание файла с помощью графических символов теряет смысл, так как подделать и скопировать графический символ можно бесконечное количество раз. **Электронная Цифровая Подпись (ЭЦП)** является полным электронным аналогом обычной подписи на бумаге, но реализуется не с помощью графических изображений, а с помощью математических преобразований над содержимым документа.

Особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами,

чем достигается неопровержимость авторства.

ЭЦП – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

ЭЦП представляет собой определенную последовательность символов, которая формируется в результате преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения. ЭЦП добавляется к исходному документу при пересылке. ЭЦП является уникальной для каждого документа и не может быть перенесена на другой документ. Невозможность подделки ЭЦП обеспечивается значительным количеством математических вычислений, необходимых для её подбора. Таким образом, при получении документа, подписанного ЭЦП, получатель может быть уверен в авторстве и неизменности текста данного документа.

Применение ЭЦП обеспечивает: простое разрешение спорных ситуаций (регистрация всех действий участника системы во времени), невозможность изменения заявки участника до даты окончания закупки.

Кроме того, ЭЦП способствует: снижению затрат на пересылку документов, быстрому доступу к торгам, проходящим в любой точке России.

Пользоваться электронной подписью достаточно просто. Никаких специальных знаний, навыков и умений для этого не потребуется. Каждому пользователю ЭЦП, участвующему в обмене электронными документами, генерируются уникальные открытый и закрытый (секретный) криптографические ключи.

Закрытый ключ – это закрытый уникальный набор информации объемом 256 бит, хранится в недоступном другим лицам месте на дискете,

смарт-карте,ru-token. Работает закрытый ключ только в паре с открытым ключом.

Открытый ключ - используется для проверки ЭЦП получаемых документов/файлов. Технически это набор информации объемом 1024 бита.

Открытый ключ передается вместе с Вашим письмом, подписанным ЭЦП.

Дубликат открытого ключа направляется в Удостоверяющий Центр, где создана библиотека открытых ключей ЭЦП. В библиотеке Удостоверяющего Центра обеспечивается регистрация и надежное хранение открытых ключей во избежание попыток подделки или внесения искажений.

Вы устанавливает под электронным документом свою электронную цифровую подпись. При этом на основе секретного закрытого ключа ЭЦП и содержимого документа путем криптографического преобразования вырабатывается некоторое большое число, которое и является электрон-

ноцифровой подписью данного пользователя под данным конкретным документом. Это число добавляется в конец электронного документа или сохраняется в отдельном файле.

В подпись, в том числе, записывается следующая информация: имяфайла открытого ключа подписи, информация о лице, сформировавшем подпись, дата формирования подписи.

Пользователь, получивший подписанный документ и имеющий открытый ключ ЭЦП отправителя на основании текста документа и открытого ключа отправителя выполняет обратное криптографическое преобразование, обеспечивающее проверку электронной цифровой подписи отправителя. Если ЭЦП под документом верна, то это значит, что документ действительно подписан отправителем и в текст документа не внесено никаких изменений. В противном случае будет выдаваться сообщение, что сертификат отправителя не является действительным.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Удостоверяющий центр - юридическое лицо, выполняющее функции по: изготовлению сертификатов ключей подписей, созданию ключей электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи, приостановлению и возобновлению действие сертификатов ключей подписей, а также аннулированию их, ведению реестра сертификатов ключей подписей, обеспечению его актуальности и возможности свободного доступа к нему участников информационных систем, проверке уникальности открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра, выдаче сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии, осуществлению по обращениям пользователей сертификатов ключей подписей подтверждения подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей, предоставлению участникам информаци-

онных систем иных связанных с использованием электронных цифровых подписей услуг.

При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Принципами использования электронной подписи являются:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Тема 8. Право и Интернет.

1. Правовое содержание понятия «Интернет-сайт». Доменное имя как объект правовой охраны. Юридическая ответственность за рассылку не запрошенных электронных сообщений (спама).
2. Удостоверение права автора на произведение в Интернете.

3. Правовое регулирование рекламы в Интернете.
4. Особенности дистанционной купли-продажи товаров через Интернет.
5. Перспективы правового регулирования отношений в сети Интернет.

Сайт в сети «Интернет» - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет».

Согласно этому определению любой сайт включает в себя:

1. технические (программные) средства;
2. содержание (информация, контент);
3. доменное имя и (или) сетевой адрес.

Доменное имя - обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет».

Сетевой адрес - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.

Домен и сайт очень тесно связаны друг с другом. Понятие доменного имени об этом свидетельствует. В сознании большинства людей представление о сайте складывается через его доменное имя. Репутация сайта переносится на доменное имя. И не только в сознании людей, но и технически.

Например, поисковые системы Google и Яндекс могут накладывать на веб-ресурсы определенные санкции. Они могут быть наложены исходя из самых различных показателей. Основную роль играет качество контента. Если контент некачественный согласно представлениям поисковой системы, то накладывается фильтр. Например, у Яндекса есть такой очень известный фильтр АГС. Технически он накладывается на доменное имя.

Все содержание сайта можно довольно легко перенести на другой домен, к которому санкции не применялись. Зачастую так и делают. Попав по неосмотрительности под фильтр, база данных и файлы прикрепляются к новому домену. Уже после этого ведется работа по устранению причин, которые привели к наложению санкций поисковых систем к первоначальному домену.
Если улучшать качество сайта, оставив его на первоначальном домене, то промежуток времени между началом работы над устранением причин, повлекших наложение санкций, до снятия последних может быть очень большим.

Поэтому многие не мучаются, а просто переносят сайт на другой домен. Если только первоначальное доменное имя не является брендом, товарным знаком.

По поводу товарных знаком разворачиваются целые доменные войны, когда кто-то регистрирует доменное имя, сходное с каким-либо товарным знаком. Но это уже тема отдельной статьи, сейчас не об этом речь.

Что можно сказать по поводу правовой сущности сайта исходя из положений закона № 149-ФЗ? Она все-равно осталась неопределенной - приведенные выдержки из закона характеризуют в основном его техническую сторону. Правовой режим сайта остается неопределенным.

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ (УКАЗАНИЯ) К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Одной из важнейших форм учебной работы выступают практические занятия. Они призваны закрепить, углубить знания студентов, полученные на лекциях, консультациях и в результате самостоятельной работы над литературой, нормативно-правовыми актами, развить у них аналитическое, научное мышление.

При подготовке к практическому занятию по определенной теме студенту следует просмотреть материалы лекции, а затем начать изучение учебной литературы и нормативных правовых актов. Необходимый материал по теме практического занятия следует законспектировать.

Рекомендации по подготовке к практическому занятию (конспектированию текста):

1) читая изучаемый материал в первый раз, подразделяйте его на основные смысловые части, выделяйте главные мысли, выводы;

2) если составляется план-конспект, сформулируйте его пункты, подпункты, определите, что именно следует включить в план-конспект для раскрытия каждого из них;

3) наиболее существенные положения изучаемого материала (тезисы) последовательно и кратко излагайте своими совами или приводите в виде цитат;

4) в конспект включаются не только основные положения, но и доводы, их обосновывающие, конкретные факты и примеры, но без их подробного описания;

5) составляя конспект, можно отдельные слова и целые предложения писать сокращенно, выписывать только ключевые слова, вместо цитирования делать лишь ссылки на страницы цитируемой работы, применять условные обозначения;

6) располагайте абзацы «ступеньками», применяйте цветные карандаши, маркеры, фломастеры для выделения значимых мест.

Практические занятия проводятся в форме устного опроса студентов по вопросам темы, а также в виде решения практических задач или моделирования практических ситуаций.

Во время практического занятия для выяснения уровня усвоения учебного материала могут проводиться экспресс-опросы с помощью тестов, контрольных вопросов.

4. ПЛАН ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 1. Информационное право как отрасль права.

1. Информационное право: понятие, предмет и метод. Информационные правоотношения.
2. Источники информационного права.
3. Становление информационного права как науки и отрасли права, современное положение в системе российского права и перспективы.
4. Информационная сфера общества как объект правового регулирования.
5. Информационная функция государства.
6. Пределы деятельности государства в информационной сфере общества.
7. Система федеральных органов исполнительной власти в информационной сфере.

Вопросы для обсуждения на семинаре

1. Какие права в информационной сфере закреплены в Конституции РФ?
2. Перечислите основания для ограничений конституционных прав граждан, которые установлены законами Российской Федерации?
3. Каковы конституционные гарантии реализации права на доступ к информации?
4. Назовите основных субъектов информационных правоотношений при реализации конституционного права на поиск, получение и передачу информации.
5. От чего зависит субъективное право каждого конкретного субъекта?
6. В чем выражается принцип информационной открытости?
7. Назовите законы, в которых закреплены обязанности по информированию субъектов информационного права.

Тема 2. Понятие и основные принципы функционирования информационного общества.

1. Понятие и признаки информационного общества, цели формирования и развития в России.
2. Стратегия развития информационного общества в Российской Федерации.
3. Справочно-информационный портал «Государственные услуги».

Вопросы для обсуждения на семинаре

1. Дайте понятие информационного общества.
2. Какие признаки присущи информационному обществу?
3. Какие задачи ставит Стратегия развития информационного общества в Российской Федерации?

Тема 3. Понятие и правовые принципы построения электронного правительства в РФ

1. Электронное правительство как один из важнейших институтов формирования информационного общества и инструмент транспарентности деятельности органов власти: понятие, признаки, перспективы становления в Российской Федерации. Зарубежный опыт развития электронного правительства.
2. Проблемы законодательного обеспечения доступа к информации о деятельности органов государственной власти.

Вопросы для обсуждения на семинаре

1. Дайте определение понятию «Электронное правительство».
2. Основные компоненты инфраструктуры электронного правительства.
3. Перечислите основные информационно-коммуникационные технологии.
4. Что такое информационная система?
5. Какие услуги может оказывать Электронное правительство?
6. Каковы принципы предоставления услуг Электронным правительством?
7. Что является главным приоритетом Электронного правительства?
8. Дайте характеристику порталу Электронного правительства?

9. Какие службы можно отнести к Web-службам?

Тема 4. Информационная безопасность

1. Информационная сфера как объект информационной безопасности.
2. Доктрина информационной безопасности: значение и основные этапы формирования.
3. Информационная безопасность в сфере экономики, обороны, науки и техники, внутренней и внешней политики, духовной жизни, правоохранительной и судебной деятельности.
4. Источники угроз информационной безопасности. Информационное оружие и информационные войны.

Вопросы для обсуждения на семинаре

1. Что понимается под информационной безопасностью?
2. Имеется ли законодательное определение информационной безопасности? Если имеется, то укажите его формулировку?
3. Что понимается под жизненно важными интересами личности, общества и государства в информационной сфере?
4. Как соотносятся понятия «информационная безопасность», «безопасность информации» и «защита информации»?
5. Сформулируйте основные задачи в области обеспечения информационной безопасности.
6. Назовите общие методы обеспечения информационной безопасности Российской Федерации.
7. Перечислите нормы Конституции РФ, провозглашающие основные права личности, касающиеся частной жизни.
8. В чем заключается системный подход к защите информации?
9. Что такое информационное оружие, информационный терроризм и информационная война?

Тема 5. Информация ограниченного доступа

1. Тайна следствия и судопроизводства.
2. Врачебная тайна.
3. Банковская тайна.
4. Нотариальная тайна.
5. Адвокатская тайна.
6. Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений.

Вопросы для обсуждения на семинаре

1. В чем состоят особенности информационных отношений в области государственной тайны?
2. В чем состоит правовой режим государственной тайны?
3. Каков порядок отнесения сведений к государственной тайне?
4. Какие степени секретности устанавливаются для сведений, составляющих государственную тайну?
5. Что является основанием для рассекречивания сведений?
6. Каков срок засекречивания сведений, составляющих государственную тайну?
7. В чем заключаются проблемы собственности в связи с информацией, составляющей государственную тайну?
8. Какие органы осуществляют защиту государственной тайны?
9. Как осуществляется допуск должностных лиц и граждан Российской Федерации к государственной тайне?
10. Как осуществляется контроль за обеспечением защиты государственной тайны?
11. В чем состоят особенности информационных отношений в области коммерческой тайны?

12. В чем состоит правовой режим коммерческой тайны?

13. Как охраняется коммерческая тайна в трудовых отношениях?

14. В чем состоят особенности информационных отношений в области персональных (конфиденциальных) данных?

15. Каковы правовые основания работы с персональными данными?

16. В чем заключается государственное регулирование в области персональных данных?

17. Что собой представляет понятие «частная жизнь»?

Тема 6. СМИ как институт гражданского общества

1. Роль СМИ в формировании и развитии информационной сферы общества.
2. Конституционный запрет цензуры: понятие, признаки и гарантии.
3. Защита чести, достоинства и деловой репутации от нарушений в СМИ.

Вопросы для обсуждения на семинаре

1. Как определяются понятия «массовая информация» и «средство массовой информации» согласно ст. 2 Закона РФ "О средствах массовой информации"?

2. Какие случаи злоупотребления свободой массовой информации приведены в ст. 4 Закона РФ «О средствах массовой информации»?

3. В каких случаях может быть прекращена деятельность средства массовой информации согласно ст. 11 Федерального закона «О противодействии экстремистской деятельности»?

4. Назовите учредителей (соучредителей) средства массовой информации.

6. Что является основным условием легитимного функционирования средства массовой информации?

7. Приведите основания отказа в регистрации средства массовой информации.

8. Что является основанием для прекращения судом деятельности средства массовой информации?

9. Какие права и обязанности определены ст. 18 Закона РФ «О средствах массовой информации»2?

10. Что должно быть определено в уставе редакции средства массовой информации?

11. Какие сведения должен содержать каждый выпуск периодического печатного издания; каждая копия аудио-, видео- или кинохроникальной программы?

12. Какие сообщения и материалы редакция должна опубликовать бесплатно и в предписанный срок?

13. Кто обязан предоставлять информацию по запросу редакции средства массовой информации?

14. Какие сведения редакция не вправе разглашать в распространяемых сообщениях и материалах?

15. Что представляет собой право на опровержение?

16. Какие права имеет журналист?

17. Что представляет собой аккредитация журналиста?

18. Какие обязанности возлагаются на журналиста?

Тема 7. Юридическая ответственность в информационной сфере

1. Понятие, виды, функции и принципы юридической ответственности в информационной сфере.
2. Основные составы преступлений в сфере компьютерной информации.

Вопросы для обсуждения на семинаре

1. Какие нормативные правовые акты являются основополагающими в информационной сфере?

2. Что является основанием для возникновения юридической ответственности за правонарушение в информационной сфере?

3. Сформулируйте определение «информационное правонарушение» или «правонарушение в информационной сфере».

4. Назовите и дайте характеристику элементам состава информационного правонарушения.

5. Назовите предмет правонарушения в информационной сфере.

6. Какие виды юридической ответственности предусмотрены за несоблюдение информационно-правовых норм?

7. Перечислите признаки объективной стороны информационного правонарушения.

8. На какие виды подразделяются составы правонарушений в информационной сфере по конструкции объективной стороны?

9. Что понимается под информационным преступлением?

10. Перечислите и дайте краткую характеристику составов уголовных преступлений в информационной сфере.

11. Какие составы преступлений в сфере экономики можно отнести к информационным?

12. Какие составы преступлений против общественной безопасности и общественного порядка следует отнести к информационным?

13. Дайте законодательное определение административного правонарушения.

14. Почему с принятием и вступлением в силу КоАП РФ были отменены многочисленные нормы законов?

15. Содержится ли в КоАП РФ самостоятельная глава, посвященная административным правонарушениям в информационной сфере?

16. Дайте общую характеристику составов административных правонарушений, которые относятся к информационным.

17. Приведите примеры норм законов субъектов Российской Федерации, которые устанавливают административную ответственность за информационные правонарушения.

18. Приведите примеры привлечения субъектов (участников) информационных правоотношений к гражданско-правовой ответственности.

19. Имеются ли по поводу привлечения к различным видам юридической ответственности в информационной сфере разъяснения судов? Приведите примеры.

Тема 8. Электронный документ и электронный документооборот

1. Понятие, функции и основные принципы работы электронной подписи.
2. Статус субъектов правоотношений с электронной подписью. Факсимиле как аналог собственноручной подписи.
3. Правовой статус электронных документов. Законодательная база электронного документооборота в Российской Федерации.

Вопросы для обсуждения на семинаре

3. Какими нормами устанавливается порядок документирования информации?

4. Какими нормами устанавливается право собственности на отдельные документы и массивы документов?

5. Какую информацию запрещено относить к информации с ограниченным доступом?

6. Что является целями защиты информации?

7. Для каких целей формируется система обязательного бесплатного экземпляра документов?

8. Какие виды документов входят в состав бесплатного и обязательного платного экземпляра документов?

9. С какой целью используется электронная цифровая подпись в электронных документах?

10. При каких условиях электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе?

11. Какие сведения должен содержать сертификат электронной цифровой подписи?

12. В чем состоят особенности использования электронной цифровой подписи?

13. Какими законами регулируются отношения в сфере электронного документооборота?

Тема 9. Право и Интернет

1. Правовое содержание понятия «Интернет-сайт». Доменное имя как объект правовой охраны. Юридическая ответственность за рассылку не запрошенных электронных сообщений (спама).
2. Удостоверение права автора на произведение в Интернете.
3. Правовое регулирование рекламы в Интернете.
4. Особенности дистанционной купли-продажи товаров через Интернет.
5. Перспективы правового регулирования отношений в сети Интернет.

Вопросы для обсуждения на семинаре

1. Какие отношения регулируются Федеральным законом "О рекламе"?
2. Какие общие требования предъявляются к рекламе?
3. Какая реклама является недобросовестной?
4. Какая реклама является недостоверной?
5. В чем состоят особенности рекламы в радио- и телепрограммах?
6. В чем состоят особенности рекламы отдельных видов товаров?
7. Как и в каком контексте употребляется понятие «Интернет» в российском законодательстве?
8. Каким образом происходит правовое регулирование интернет-предложений?
9. Какие нормы права необходимо установить для улучшения общественных отношений в киберпространстве?

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа является внеаудиторной и предназначена для самостоятельного

ознакомления студента с определенными разделами дисциплины по рекомендованным преподавателем материалам и подготовки к выполнению индивидуальных заданий по дисциплине.

Самостоятельная работа студентов по курсу Информационное право выражается в изучении Конституции России и других источников информационного права. Изучение учебной и научной литературы по информационному праву. Подготовка к практическим занятиям, конспектирование, решение ситуационных задач, подготовка докладов.

6. НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ К ОТДЕЛЬНЫМ ТЕМАМ

Тема 1. Информационное право как отрасль права

1. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
2. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
3. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
4. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
5. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О.И. Шкаратана. – М.: ГУ ВШЭ, 2000. – 608 с.
6. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш.Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
7. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.
8. Мелюхин И. С. Информационное общество: истоки, проблемы, тенденции развития. – М.: Изд-во МГУ, 1999. – 208 с.
9. Михеева Е. В. Информационные технологии в профессиональной деятельности : учеб. пособие. – Москва : Проспект, 2015. – 448 с.

Тема 2. Понятие и основные принципы функционирования информационного общества

1. Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ) // Собрание законодательства РФ. 2009. № 4. ст. 445.
2. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» Собрание законодательства Российской Федерации от 2017 г., № 20, ст. 2901.
3. Стратегия развития информационного общества в России, утверждена Президентом РФ 7 февраля 2008 года № Пр-212 // Российская газета. № 34. 16.02.2008.
4. Постановление Правительства РФ от 15.04.2014 № 313 (в действ. редакции) «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)» // Собрание законодательства РФ, 05.05.2014, № 18 (часть II), ст. 2159.
5. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
6. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
7. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
8. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
9. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
10. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
11. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Про-

спект, 2015. – 312 с.

Тема 3. Понятие и правовые принципы построения электронного правительства в РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
2. Стратегия развития информационного общества в России, утверждена Президентом РФ 7 февраля 2008 года № Пр-212 // Российская газета. № 34. 16.02.2008
3. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
4. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
5. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
6. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
7. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
8. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
9. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.

Тема 4. Информационная безопасность

1. Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ) // Собрание законодательства РФ. 2009. № 4. ст. 445.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
3. Указ Президента РФ от 5 декабря 2016 г. № 646 2Об утверждении Доктрины информационной безопасности Российской Федерации»
4.
5. ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/71456224/#ixzz594rUBUBJ
6. Варлатая С. К., Шаханова М. В. Криптографические методы и средства обеспечения информационной безопасности : учебно-методический комплекс. – Москва : Проспект, 2015. – 152 с.
7. Варлатая С. К., Шаханова М. В. Защита и обработка конфиденциальных документов: учебно-методический комплекс. – Москва : Проспект, 2015. – 184 с.

Тема 5. Информация ограниченного доступа

1. Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ) // Собрание законодательства РФ. 2009. № 4. ст. 445.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

3. Закон РФ от 21.07.1993 № 5485-1 (ред. от 26.07.2017) «О государственной тайне» // Собрание законодательства РФ, 13.10.1997, № 41, стр. 8220-8235.
4. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» // Собрание законодательства РФ, 09.08.2004, № 32, ст. 3283.
5. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) «О персональных данных» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3451.
6. Федеральный закон от 07.07.2003 № 126-ФЗ (в действ. редакции) «О связи» // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895.
7. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
8. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
9. Варлатая С. К., Шаханова М. В. Защита и обработка конфиденциальных документов: учебно-методический комплекс. – Москва : Проспект, 2015. – 184 с.
10. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. – М.: Статут, 2011. – 134 с.
11. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
12. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
13. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
14. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
15. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.

Тема 6. СМИ как институт гражданского общества

1. Закон РФ от 27.12.1991 № 2124-1 (в действ. редакции) «О средствах массовой информации» // Российская газета, № 32, 08.02.1992.
2. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
3. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
4. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
5. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
6. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
7. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
8. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.

Тема 7. Юридическая ответственность в информационной сфере

1. Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ) // Собрание законодательства РФ. 2009. № 4. ст. 445.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954.
4. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 1.
5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ, 05.12.1994, № 32, ст. 3301.
6. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
7. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
8. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
9. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
10. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
11. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
12. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.

Тема 8. Электронный документ и электронный документооборот

1. Федеральный закон от 06.04.2011 № 63-ФЗ (в действ. редакции) «Об электронной подписи» // Собрание законодательства РФ, 11.04.2011, № 15, ст. 2036.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
3. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
4. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
5. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
6. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
7. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
8. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.

9. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.

Тема 9. Право и Интернет

1. Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ) // Собрание законодательства РФ. 2009. № 4. ст. 445.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (в действ. редакции) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
3. Актуальные проблемы информационного права : учебник / коллектив авторов : под ред. И.Л. Бачило, М.А. Лапиной. – М. : ЮСТИЦИЯ, 2016. – 534 с. – (Магистратура и аспирантура).
4. Бачило И. Л. Информационное право : учебник для магистров / И. Л. Бачило. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 564 с. – Сери : Магистр.
5. Информационное право: учебник для бакалавров / отв. ред. И. М. Рассолов. Москва : Проспект, 2016. – 352 с.
6. Информационное право : учебник для академического бакалавриата / И.Л. Бачило. – 5-е изд., перераб. и доп. – М. : Издательство Юрайт, 2016. – 419 с. – Серия : Авторский учебник.
7. Информационные правоотношения: теоретические аспекты : коллективная монография / под ред. И. М. Рассолова. – Москва : Проспект, 2017. – 208 с.
8. Килясханов И. Ш. Информационное право в терминах и понятиях: учеб. пособие для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / И.Ш. Килясханов, Ю.М. Саранчук. – М.: ЮНИТИ-ДАНА: Закон и право, 2009. – 136 с.
9. Кузнецов П. У. Основы информационного права : учебник для бакалавров. – Москва : Проспект, 2015. – 312 с.
10.