

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Методические указания
по выполнению практических работ
по дисциплине «Правовое регулирование информационной
безопасности»
для студентов специальности 40.05.01 Правовое обеспечение
национальной безопасности
специализация «Государственно-правовая»**

Ставрополь, 2026

Предисловие

Актуальность изучения учебной дисциплины. Активное формирование и развитие институтов информационного общества в современном мире через повсеместное использование информационных технологий во всех сферах привели к созданию новой инновационной отрасли информационного права.

Учебный курс «Правовое регулирование информационной безопасности» призван закрепить теоретические и практические знания по изучению общего курса информационного права, сформировать научное представление о системе информационного законодательства, основных направлениях ее развития, правовых основах формирования и развития информационного общества в Российской Федерации, обеспечения информационной безопасности личности, общества и государства. В сферу учебного курса «Правовое регулирование информационной безопасности» входят такие важные и актуальные для развития общества направления, как право на информацию, правовой режим информации, правовой режим общедоступной информации, правовой режим информации ограниченного доступа, правовая охрана различных видов тайн, формирование и развитие единого нормативного регулирования в сфере информационной безопасности, правовое регулирование информационной безопасности в информационно-телекоммуникационной сети Интернет и др.

В результате освоения дисциплины «Правовое регулирование информационной безопасности» обучающийся должен приобрести следующие общекультурные и профессиональные компетенции:

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен разрабатывать нормативные правовые акты	ИД ПК-1.1. Выявляет пробелы и коллизии действующего законодательства и определяет способы их преодоления и устранения; ИД ПК-1.2. Понимает сущность и уровни нормотворческого процесса, выделяет стадии нормотворческой процедуры; ИД ПК-1.3. Аргументирует нормативное решение и прогнозирует последствия его реализации, в том числе с учетом возможных коррупционных рисков.	Определяет пробелы и коллизии действующего законодательства и определяет способы их преодоления и устранения Логически обосновывает и понимает сущность и уровни нормотворческого процесса, выделяет стадии нормотворческой процедуры. Обеспечивает нормативное решение и прогнозирует последствия его реализации, в том числе с учетом возможных коррупционных рисков.
ПК-6 Способен осуществлять	ИД ПК-6.1. Выявляет и принимает меры к	Способен выявлять и принимать меры к

профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению	устранению причин и условий, способствующих совершению преступлений и иных правонарушений	устранению причин и условий, способствующих совершению преступлений и иных правонарушений
	ИД ПК-6.2. Участвует в оценке проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, на предмет их соответствия действующему законодательству в рамках поставленной задачи	Проявляет способности участия в оценке проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, на предмет их соответствия действующему законодательству в рамках поставленной задачи

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Тема 1. Государственная политика и управление в сфере информационной безопасности

Цель занятия: сформировать у обучающихся знаний в области государственного управления информационной сферой, специальных структур, обеспечивающих инновационные процессы в государственном управлении.

Организационная форма занятия: Круглый стол

В результате освоения темы обучающийся должен **знать:** действующие нормативно-правовые акты и программы, направленные на реализацию государственной политики в информационной сфере; органы государственной власти осуществляющие управление в информационной сфере; приоритеты и цели современной государственной политики в сфере развития информационного общества; достоинства и недостатки информатизации института управления.

Уметь: ориентироваться в действующем законодательстве, устанавливающем основные направления государственной информационной политики, выделять полномочия органов государственной власти в информационной сфере, применять нормы материального права.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №1 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Обеспечение информационных прав человека - одна из основных задач в условиях формирования информационного общества и построения электронного государства. Формирование и развитие полноценного информационного общества является одним из приоритетных направлений современной государственной политики.

Теоретическая часть: Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти. Государственная политика по реализации плана мероприятий закреплена в нормативно-

правовых актах: «Стратегия развития информационного общества в Российской Федерации»; Государственной программа «Информационное общество (2011-2020 годы)».

Современная информационная правовая политика представляет собой комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленных на обеспечение конституционного права граждан на доступ и распространение информации, в соответствии с п. 4 ст. 29 Конституции РФ, указывающим, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом», которая должна быть направленной на обеспечение развития творческого потенциала личности».

Вопросы, выносимые на обсуждение:

1. Государственное управление в сфере информационной безопасности: понятие и общая характеристика.
2. Система и полномочия органов государственной власти в сфере информационной безопасности.
3. Современные тенденции государственной политики в сфере информационной безопасности.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Регулирующие органы в сфере телекоммуникаций и их воздействие на телекоммуникационные отношения в Российской Федерации и зарубежных странах
2. Информационная функция государства в сети Интернет
3. Информационная открытость государственных и муниципальных органов

Повышенный уровень

1. Информационное обеспечение органов власти на трех уровнях: государственном, региональном и местном
2. Информационная функция в системе функций государства

Тема 2. Правовой режим информационной безопасности документированной информации. Информационная безопасность электронного документооборота

Цель занятия: формирование профессиональных компетенций в области правового регулирования информационной безопасности документооборота, электронного документооборота, использования электронных документов и электронной подписи в правоприменительной деятельности.

Организационная форма занятия: семинар дискуссия.

В результате освоения темы обучающийся должен **знать:** условия юридической значимости электронного документа.

Уметь: толковать и применять информационное законодательство, составлять письменные процессуальные документы, анализировать нестандартные практических ситуаций и суметь найти различные варианты решений.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №2 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Юридическая важность и значимость документооборота усиливается в связи с современным уровнем развития информационных технологий, в том числе криптографических средств.

Теоретическая часть: В соответствии с действующим законодательством документ - материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения. Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. Документ в обязательном порядке должен обладать реквизитами, позволяющими определить информацию, содержащуюся в документе, или в установленных законом случаях материальный носитель документа. Реквизиты документа должны обеспечивать защиту от несанкционированных изменений в документе и устанавливать лицо, от которого документ исходит.

Законодатель ввел также такие категории как электронный документ, электронная подпись, электронный документооборот.

Электронные документы выделяются из общего понятия на основании особенностей источника, т.е. носителя информации, электронным является источник (носитель) доказательственной информации. Сама же информация остается прежней.

В соответствии с ст. 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» под электронным документом понимается документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Видами электронных подписей являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Вопросы, выносимые на обсуждение:

1. Документирование информации: понятие и значение.
2. Понятие и признаки электронного документа.
3. Понятие и виды документооборота. Правовой режим информационной безопасности электронного документооборота.
4. Правовой режим информационной безопасности электронной подписи
5. Проблемы правового регулирования в области информационной безопасности организации электронного документооборота.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Законодательство об электронных документах и их архивах: проблемы становления и перспективы развития
2. Электронные документы в сети Интернет как доказательства в российском судопроизводстве

3. Использование электронной подписи как форма реализации права

Повышенный уровень

1. Понятие электронного документа и его применение в качестве доказательства в гражданском и арбитражном судопроизводстве Российской Федерации
2. Применение электронной подписи в электронном документообороте

Тема 3. Правовой режим информации ограниченного доступа. Информационная безопасность информации ограниченного доступа

Цель занятия: изучить правовой режим государственной тайны, тайны частной жизни, личной тайны, семейной тайны, коммерческой тайны, банковской тайны, профессиональной тайны, служебной тайны и особенности обеспечения информационной безопасности сведений

Организационная форма занятия: семинар-опрос.

В результате освоения темы обучающийся должен **знать:** информационное законодательство, юридические механизмы обеспечения информационной безопасности конфиденциальной информации.

Уметь: работать с нормативными актами, применять их в практической деятельности; применять правовые механизмы обеспечения информационной безопасности конфиденциальной информации.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №3 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Важной частью информационного законодательства являются нормативно-правовые акты в сфере правовой охраны конфиденциальной информации. Ориентирование в правовом режиме конфиденциальной информации является необходимым как для правоприменения в предпринимательской среде, так и в системе государственной службы.

Теоретическая часть: К информации (сведениям), обладающей свойствами конфиденциальности Закон об информации относит: государственную тайну, коммерческую, служебную и иную тайну, обязательность соблюдения конфиденциальности которой устанавливается действующим законодательством. Ограниченный доступ устанавливается также в отношении сведений, составляющих персональные данные человека. Важным нормативным актом, упорядочивающим перечень конфиденциальных сведений, является Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера». В перечень входят: 1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях; 2) сведения, составляющие тайну следствия и судопроизводства; 3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна); 4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее); 5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и

федеральными законами (коммерческая тайна); 6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

В теории информационного права содержатся различные определения информации с ограниченным доступом (конфиденциальной информации). Под «информацией с ограниченным доступом следует понимать сведения (сообщения, данные), независимо от формы их представления, в отношении которых в порядке, установленном действующим законодательством, введен тот или иной режим конфиденциальной информации, определяющий порядок предоставления доступа к этим сведениям и меры ответственности за нарушения, возникающие в процессе отнесения, хранения, предоставления и распространения таких сведений».

Вопросы, выносимые на обсуждение:

1. Понятие и категории информации ограниченного доступа
2. Цели и основания ограничения свободного доступа к информации
3. Комплекс мер по защите информации ограниченного доступа
4. Правовые механизмы обеспечения информационной безопасности детей

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Эволюция правового регулирования в отношении сведений конфиденциального характера в Российской Федерации
2. Ограничение права несовершеннолетних на доступ и получение информации
3. Понятие и признаки врачебной (медицинской) тайны по законодательству Российской Федерации

Повышенный уровень

1. Административная ответственность за нарушение прав на сведения, составляющие коммерческую тайну
2. Система и классификация тайн в российском законодательстве и юридической науке
3. Принципы определения налоговой тайны в законодательстве России и зарубежных стран

Тема 4. Правовое регулирование информационной безопасности сведений, составляющих государственную тайну

Цель занятия: изучить правовой режим государственной тайны.

В результате освоения темы обучающийся должен **знать:** информационное законодательство, юридические механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну.

Форма проведения практического занятия: семинар-опрос

Уметь: работать с нормативными актами, применять их в практической деятельности; применять правовые механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №4 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Отнесение тех или иных сведений к государственной тайне продиктовано необходимостью обеспечения безопасности

государства, что влечет за собой законодательное ограничение права граждан, закрепленного в ст. 29 (ч. ч. 1, 4) Конституции Российской Федерации (19) о том, что каждому гарантируется свобода мысли и слова. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Но эта же статья содержит указание на то, что перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Теоретическая часть: В настоящее время действует целый комплекс нормативно - правовых актов, регулирующих отношения в сфере государственной тайны. Легальное определение сведений, составляющих государственную тайну содержится в Законе Российской Федерации «О государственной тайне». Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Определение государственной тайны, установленное законодательством, позволяет установить ряд важных признаков, которыми обладает информация, составляющая государственную тайну: во-первых, строгое законодательное установление сфер деятельности государства (военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности) в которой сведения имеют место быть; во-вторых, это сведения не известные широкому кругу лиц, и именно в силу своей неизвестности и ограниченной доступности сведения представляют интерес; в-третьих, распространение сведений, может нанести ущерб безопасности РФ; в-четвертых, это сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» определяет совокупность информации, в отношении которой может быть установлен правовой режим государственной тайны. Основным критерием отнесения сведений к государственной тайне является необходимость обеспечения обороноспособности, безопасности государства и правоохранительной деятельности в Российской Федерации и на основании Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности, установленных Постановлением Правительства РФ.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью и должностными лицами органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

Необходимость отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений должны обосновать органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны). Если эти сведения подпадают под перечень сведений, подлежащих засекречиванию, действующий в данном органе, на данном предприятии, в данном учреждении и организации, то вопрос об их засекречивании решает руководитель данного органа, предприятия, учреждения, организации. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности. Указанное должностное лицо должно обладать полномочиями по засекречиванию сведений.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Органами государственной власти, утвержденными Распоряжением Президента «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне», руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности.

Действующее законодательство устанавливает степени секретности сведений и грифы секретности носителей этих сведений.

Установлено три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно». Основным критерием при отнесении сведений к тому или иному грифу секретности служит степень тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Сведениям, составляющим государственную тайну, требующим наибольшую защищаемость, присваивается гриф «особой важности», требующим меньшую степень защищаемости – «совершенно секретно», затем «секретно».

Вопросы, выносимые на обсуждение:

1. Понятие и правовое регулирование института государственной тайны.
2. Перечень сведений, отнесенных к государственной тайне.
3. Порядок отнесения сведений к государственной тайне.
4. Порядок рассекречивания сведений и их носителей.
5. Правовые механизмы защиты государственной тайны.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Основные направления организационной и правовой защиты государственной тайны в истории России
2. Современные проблемы правового регулирования государственной и служебной тайны в России

Повышенный уровень

1. Защита государственной тайны в Российской Федерации на современном этапе ее развития
2. Правовой статус государственной тайны в системе обеспечения безопасности страны и общей совокупности информационных ресурсов

Тема 5. Правовое регулирование информационной безопасности сведений, составляющих коммерческую тайну

Цель занятия: изучить правовой режим коммерческой тайны.

В результате освоения темы обучающийся должен **знать:** информационное законодательство, юридические механизмы обеспечения информационной безопасности информации, составляющей коммерческую тайну.

Форма проведения занятия: семинар-опрос.

Уметь: работать с нормативными актами, применять их в практической деятельности; применять правовые механизмы обеспечения информационной безопасности сведений, составляющих коммерческую тайну.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №5 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: В российском законодательстве существует особый институт информации, составляющей коммерческую тайну, призванный не допустить утечки коммерчески значимых данных. Институт коммерческой тайны имеет длительную историю развития, он не раз становился предметом научных исследований, однако при этом целый ряд аспектов его понимания носит дискуссионный характер, а некоторые вопросы являются слабо изученными, например о системе и механизмах защиты коммерческой тайны в корпоративных отношениях, а также в отношениях с третьими лицами (контрагентами и органами власти), в судебной практике возникают трудности при разграничении сведений, составляющих коммерческую тайну и «ноу-хау», «секрет производства».

Теоретическая часть: Коммерческая тайна относится к конфиденциальной информации, направлена на защиту прав на осуществление предпринимательской деятельностью.

Информация, составляющая коммерческую тайну, - это сведения любого характера, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, в отношении которых обладателем таких сведений введен режим коммерческой тайны, обеспечивающий возможность извлечения прибыли от использования подобной информации.

В настоящее время закон определяет коммерческую тайну через такую категорию как режим конфиденциальности. В то время как раньше она определялась как научно-техническая, производственная, финансово-экономическая или иная информация. Новый подход законодателя не упростил, а усложнил рассматриваемый вопрос, так как само словосочетание «режим коммерческой тайны» содержит скрытую тавтологию.

В Федеральном законе «О коммерческой тайне» существует достаточно много пробелов, например не урегулирован порядок подачи сведений, относящихся к коммерческой тайне при реорганизации и ликвидации юридического лица, детально не урегулирован порядок передачи сведений, составляющих государственную тайну, государственным органам, органам местного самоуправления.

Особенностью защиты подобного вида информации является выбор защитительных мер, который делает не государственный орган, а сами обладатели прав. При этом нарушением права на коммерческую тайну должно считаться не всякое получение третьим лицом ранее неизвестной и ценной для него информации, а только завладение такой информацией с помощью незаконных методов. В этой связи можно выделить несколько уровней возможных угроз в данной сфере. Первый уровень - это внутренние угрозы (акционеры, наемные работники, которые не имеют доступа к коммерческой тайне в силу выполняемых ими функций) и второй уровень - это внешние нарушители (контрагенты, конкуренты и др.). Исходя из этого, в зависимости от правомочий субъекта этого права можно выделить внутренние и внешние охранительные правоотношения. Внутренние отношения возникают с наемными работниками, с акционерами компаний в отношении охраны коммерческой тайны. Внешние правоотношения возникают, например, с регистрирующими, контролирующими органами, по запросу которых может предоставляться информация. Сами же нарушения гражданских прав возможны не только со стороны контрагентов, но и со стороны третьих лиц. Одно и то же правонарушение может быть не только нарушением гражданско-правовых норм и договорных обязательств, но и преступлением и проступком. Отсюда выделяются две группы возможностей - самостоятельно, в одностороннем порядке предпринимать фактические и юридические действия или обратиться в юрисдикционный орган за защитой собственного права.

Вопросы, выносимые на обсуждение:

1. Понятие и правовое регулирование коммерческой тайны.
2. Особенности предоставления сведений, составляющих коммерческую тайну.
3. Юридические меры по защите конфиденциальности информации, составляющей коммерческую тайну.
4. Юридическая ответственность за нарушение права на коммерческую тайну.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Особенности правовой охраны секретов производства и информации, составляющей коммерческую тайну
2. Охрана и защита информации, составляющей коммерческую тайну

Повышенный уровень

1. Актуальные вопросы охраны коммерческой тайны в отношениях с органами государства
2. Соотношение ноу-хау с коммерческой тайной
3. Особенности формирования и использования режима коммерческой тайны

Занятие 6. Правовая охрана информационной безопасности персональных данных

Цель занятия: изучить правовое регулирование института персональных данных, условия обработки, передачи, правовой охраны и мер юридической ответственности за нарушение законодательства о персональных данных.

Организационная форма занятия: опрос, семинар-дискуссия.

В результате освоения темы обучающийся должен **знать:** законодательство о персональных данных, условия обработки, передачи сведений, права и обязанности субъекта персональных данных, правовой статус лиц участвующих в обработке персональных данных, меры правовой защиты сведений, составляющих персональные данные.

Уметь: квалифицировать факты и обстоятельства с точки зрения действующего права; принимать решения и давать юридическую оценку по факту нарушения персональных данных; составлять основные процессуальные документы по охране нарушенных прав; давать квалифицированные юридические заключения и консультации по нарушению прав субъектов персональных данных.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №6 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: В век информационных технологий информация, составляющая персональные данные человека является важной частью неприкосновенности его частной жизни. Всеобъемлющая информатизация имеет негативные стороны, в частности, она приводит к грубому нарушению информационных прав. Для будущих юристов является важным рассмотрение государственно-правового механизма защиты информации, а именно института обращения персональных данных.

Теоретическая часть: Институт персональных данных является относительно новым в отечественной правовой системе. Персональными данными является любая

информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Основные принципы обработки персональных данных граждан закреплены в ст. ст. 23, 24 Конституции РФ - каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Вопросы обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных нашли детальное регулирование в Федеральном законе от 27 июля 2006 г. №152-ФЗ «О персональных данных».

Общим правилом обработки персональных данных, в том числе и в Российской Федерации, является наличие согласия субъекта персональных данных на их обработку. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Данное субъектом персональных данных согласие на их обработку не является необратимым. Оно может быть отозвано. При этом не нужно объяснять причины такого решения или выполнять какие-либо условия, необходимо только уведомить оператора персональных данных о принятом решении.

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Уполномоченным органом по защите прав субъектов персональных данных, на которого возлагается обеспечение контроля и надзора за соответствием действующему законодательству обработки персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), которая находится в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Важным элементом правового механизма защиты прав субъектов персональных данных является институт юридической ответственности. Юридическая ответственность - составная часть большинства правоотношений, в том числе в сфере охраны персональных данных.

Статья 24 Закона о персональных данных регулирует вопросы установления юридической ответственности за нарушение законодательства о персональных данных и закрепляет: «Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность». Поскольку указанная норма является отсылочной, то установление конкретных видов правонарушений и применение соответствующих мер ответственности должно регулироваться иными нормативными актами

Вопросы, выносимые на обсуждение:

1. Персональные данные: понятие и общая характеристика.
2. Законодательство о персональных данных.

3. Принципы и условия обработки персональных данных.
4. Права субъекта персональных данных.
5. Ответственность за нарушение законодательства о персональных данных.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Категории персональных данных
2. Защита персональных данных посредством права на забвение
3. Биометрические персональные данные: определение и сущность

Повышенный уровень

1. Пути совершенствования законодательства и практики о персональных данных /
2. Законодательство о персональных данных в зарубежных странах и России
3. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника

Тема 7. Правовые основы информационной безопасности отношений в информационно-телекоммуникационной сети Интернет

Цель занятия: раскрыть юридическую природу информационно-телекоммуникационной сети Интернет, а также отношений протекающих в глобальной сети.

Организационная форма занятия: семинар дискуссия.

В результате освоения темы обучающийся должен **знать:** правовые основы информационных отношений в сети Интернет; круг отношений подлежащих правовому воздействию, т.е. входящие в предмет интернет права.

Уметь: применять информационно-правовые нормы в практической деятельности; выявлять нарушения норм информационного законодательства; составлять процессуальные документы, необходимые для защиты нарушенных прав; определять вид правовой ответственности и размер соответствующих санкций.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №7 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: информационно-правовая сфера ставит перед государством, научным сообществом, правоприменителями множество не решенных вопросов. Через информационные сети, трансформируются отношения между государством и гражданским обществом, государственными структурами и бизнесом, образуются новые уровни и виды правовых пространств. Правовые механизмы информационных отношений активно глобальной сети Интернет развиваются и трансформируются в правовое поле.

Теоретическая часть: Согласно положениям Федерального закона «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть - это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Исходя из ст. 16 Закона об информации, информационно-телекоммуникационные сети разграничиваются на информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, а также иные информационно-телекоммуникационные сети.

Существующие нормативные акты регулируют лишь отдельные аспекты функционирования Сети.

В настоящее время ни в одной из стран мира нет кодифицированного законодательства, регулирующего правоотношения в сети Интернет.

Нормы, которые можно было бы применить к отношениям по поводу Интернета, «разбросаны» по законодательным актам иных отраслей права. В первую очередь они содержатся в нормах об интеллектуальной и промышленной собственности, гражданском и уголовном законодательстве, а также в разделе, условно именуемом «компьютерным правом».

Сеть Интернет обладает рядом признаков: доступность сети, открытость (транспарентность) информации. Указанные признаки необходимо учитывать при решении вопроса о необходимости регулирования отношений, складывающихся в ней по поводу массовых коммуникаций.

Правовое регулирование отношений в сети Интернет обусловлено рядом проблем: нарушение интеллектуальных прав на результаты интеллектуальной деятельности и средства индивидуализации; распространение ненадлежащей рекламы, оскорбительных и непристойных материалов и доступ к ним несовершеннолетних; несанкционированный доступ к информации ограниченного доступа; нарушение прав и законных интересов личности, общества и государства в процессе информационного обмена, и другие.

Появление в сети Интернет ряда новых отношений, видов массовых коммуникаций, их активное развитие и проблемы функционирования обуславливают необходимость расширения сферы правового регулирования, увеличении ряда областей и сторон правового регулирования применительно к сети Интернет.

Вопросы, выносимые на обсуждение:

1. Правовая природа отношений, возникающих, изменяющихся и прекращающихся в области использования сети Интернет.
2. Понятие и признаки и структура интернет-отношений.
3. Правовой статус участников правоотношений в Интернет.

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Основы правового регулирования информационной безопасности сети Интернет.
2. Правовое регулирование распространения информации в сети Интернет
3. Проблемы правового регулирования оборота неправомерной информации в Интернете

Повышенный уровень

1. Правовая природа и нормативно-правовое регулирование интернет-услуг по законодательству Российской Федерации
2. Проблемы правового регулирования информационной безопасности в сети Интернет и их причины
3. Особенности правового регулирования распространения рекламы в сети Интернет

Практическое занятие 8. Актуальные проблемы информационной безопасности объектов интеллектуальной собственности в информационно-телекоммуникационной сети Интернет

Цель занятия: раскрыть юридическую природу информационно-телекоммуникационной сети Интернет, а также отношений протекающих в глобальной сети.

В результате освоения темы обучающийся должен **знать:** правовые основы информационных отношений в сети Интернет; особенности их информационной безопасности, круг отношений подлежащих правовому воздействию, т.е. входящие в предмет интернет права.

Уметь: применять информационно-правовые нормы в практической деятельности; выявлять нарушения норм информационного законодательства; составлять процессуальные документы, необходимые для защиты нарушенных прав; определять вид правовой ответственности и размер соответствующих санкций.

Владеть: материальными и процессуальными нормами информационного и смежных отраслей права.

Актуальность темы: «Антипиратский закон» определил порядок ограничения доступа к информационным ресурсам, посредством которых осуществляется распространение аудиовизуальных произведений с нарушением интеллектуальных прав правообладателей.

Теоретическая часть: На основании действующего законодательства правообладатель в случае обнаружения в информационно-телекоммуникационных сетях фильмов или информации, необходимой для их получения с использованием таких сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в уполномоченный федеральный орган исполнительной власти с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие фильмы или информацию, на основании вступившего в силу судебного акта.

Предусмотрена возможность досудебного урегулирования претензий правообладателей. Так, если оператор связи в добровольном порядке исполнил требование правообладателя об удалении спорного контента, он освобождается от ответственности перед правообладателем.

В случае если в досудебном порядке не удастся достичь соглашения, правообладатель вправе обратиться за защитой своих прав в судебном порядке. При этом на время судебного разбирательства доступ к сайту блокируется.

Вопросы, выносимые на обсуждение:

1. Правовая природа отношений, возникающих, изменяющихся и прекращающихся в области использования объектов интеллектуальной собственности в сети Интернет.
2. Проблемы, связанные с информационной безопасностью прав интеллектуальной собственности в сети Интернет
3. Компетенция Роскомнадзора по обеспечению безопасности объектов интеллектуальной собственности в информационно-телекоммуникационной сети Интернет

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Актуальные проблемы совершенствования законодательства в сфере защиты интеллектуальных прав в информационно-телекоммуникационных сетях
2. Ответственность за незаконное использование объектов интеллектуальной собственности в сети Интернет. Зарубежный опыт
3. Правовое регулирование доменных имен и их информационная безопасность

Повышенный уровень

1. Особенности рассмотрения интернет-споров
2. Свободный и бесплатный доступ к произведениям физических и юридических лиц при условии соблюдения целевого назначения доступа: правовое регулирование

Практическое занятие 9. Актуальные проблемы международного- правового регулирования обеспечения информационной безопасности

Цель занятия: изучить основные информационные права и свободы человека и гражданина и правовые механизмы их обеспечения на внутригосударственном и международном уровне.

В результате освоения темы обучающийся должен **знать:** юридические нормы, закрепляющие информационные права и свободы на международном уровне; правовые механизмы защиты информации нормами международного права.

Уметь: применять материальные и процессуальные нормы права, обеспечивающие информационные права и свободы человека, гражданина; применять правовые механизмы защиты информации нормами международного права.

Владеть: материальными и процессуальными нормами информационного и смежных отраслей права.

Актуальность темы: Сфера безопасности в глобальном информационном обществе, к которой приковано наше внимание, обуславливает необходимость обеспечения баланса интересов государства, общества и каждой отдельной личности.

Теоретическая часть: В условиях глобального информационного общества проблема соотношения и взаимозависимости интересов личности, информационного общества и информационного государства требует взвешенного подхода в решении. Вопрос определения места правового обеспечения информационной безопасности личности предопределяет целесообразность сбалансированного подхода, учитывающего публичные интересы, общественные интересы и личные интересы на паритетных началах. Глобальный трансграничный характер информационно-телекоммуникационных технологий приводит к масштабности правонарушений в информационной сфере, что, в свою очередь, ведет к серьезному нарушению прав и интересов личности.

Вопросы, выносимые на обсуждение:

1. Правовая защита информации: понятие, содержание.
2. Международно-правовое регулирование информационной безопасности.
3. Международно-правовое регулирование отношений в области обеспечения информационной безопасности личности, общества и государства

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Транснациональный характер сети Интернет: правовая характеристика
2. Международно-правовое регулирование информационно-телекоммуникационных технологий
3. Правовое обеспечение информационной безопасности личности в международном праве

Повышенный уровень

1. Правовое обеспечение безопасности информации в международном праве
2. Международные подходы правового регулирования борьбы с кибертерроризмом

Тема 10. Юридическая ответственность в сфере информационной безопасности

Цель занятия: заключается в познании студентами правовой природы юридической ответственности в информационной сфере, а также в применении полученных на лекциях, семинарских занятиях и в ходе самостоятельной работы знаний в правоприменительной практике.

Организационная форма занятия: семинар-опрос

В результате освоения темы обучающийся должен **знать:** нормы информационного, уголовного, административного, уголовного законодательства, устанавливающие меры юридической ответственности за правонарушения в информационной сфере.

Уметь: толковать, соблюдать, исполнять и применять нормы права, устанавливающие меры юридической ответственности за совершение информационных правонарушений в профессиональной деятельности, в том числе квалифицировать юридически значимые факты; давать консультации по правовым вопросам; применять нормы материального и процессуального права.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №10 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Правовое обеспечение информационной безопасности является гарантией соблюдения прав субъектов информационных правоотношений. Институт юридической ответственности в информационном праве является действенным механизмом гарантий информационной безопасности. В информационных отношениях институт юридической ответственности оснащается специальными методами и средствами.

Теоретическая часть: Юридическая ответственность означает применение компетентным государственным органом санкции правоохранительной нормы и наступление отрицательных действий в рамках закона для правонарушителя в виде установленных вида и меры наказания, соразмерных нанесенному ущербу (вреду). Юридическая ответственность наступает за неправомерное поведение субъектов, выражающееся в совершении информационных правонарушений.

Юридическая ответственность характеризуется тем, что она: опирается на государственное принуждение; наступает за совершенное правонарушение; выражается в определенных отрицательных последствиях для правонарушителя, являющихся для него новой юридической обязанностью, которой не существовало до совершения противоправного деяния, и представляющих собой лишения личного, организационного либо имущественного характера; воплощается в процессуальной форме.

Информационные правонарушения – это противоправное, виновное действие (бездействие) физического или юридического лица, за которое действующим законодательством установлена юридическая ответственность.

В настоящее время за правонарушения в информационной сфере, предусматривается как гражданско-правовая, дисциплинарная (включая материальную), административная ответственность, так и уголовная ответственность. В связи с многоотраслевой правовой природой информационных правонарушений, ответственность за их совершение устанавливается целым комплексом нормативных актов, в том числе Уголовным кодексом РФ, Кодексом РФ об административных правонарушениях, Гражданским кодексом и др.

Юридическая ответственность возможна за совершение административных правонарушений, уголовных преступлений, служебных и дисциплинарных проступков в информационной сфере.

Административные правонарушения в информационно-правовой сфере это деяние, за которое предусмотрена административная ответственность, административные наказания, состоящие как в имущественных, в частности административный штраф, так и в неимущественных ограничениях правонарушителя, в частности предупреждение и др.

В Кодексе РФ об административных правонарушениях устанавливается административная ответственность, за: нарушение права гражданина на ознакомление со списком избирателей, участников референдума (ст. 5.1); нарушение порядка участия средств массовой информации в информационном обеспечении выборов, референдумов (ст. 5.5); изготовление, распространение или размещение агитационных материалов с нарушением требований законодательства о выборах (ст. 5.12); умышленное уничтожение или повреждение печатных материалов, относящихся к выборам, референдуму (ст. 5.14); непредоставление или неопубликование отчета, сведений о поступлении и расходовании средств, выделенных на подготовку и проведение выборов, референдума (ст. 5.17); непредоставление сведений об итогах голосования или о результатах выборов (ст. 5.25); нарушение порядка или сроков предоставления сведений о несовершеннолетних, нуждающихся в передаче на воспитание в семью либо в учреждение для детей-сирот или детей, оставшихся без попечения родителей (ст. 5.36); отказ в предоставлении гражданину информации (ст. 5.39); незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53); сокрытие или искажение экологической информации (ст. 8.5); невыполнение правил ведения судебных документов (ст. 8.16); сокрытие сведений о внезапном падеже или об одновременных массовых заболеваниях животных (ст. 10.7); самовольную установку или эксплуатацию узла проводного вещания (ст. 13.1); воспрепятствование распространению продукции средств массовой информации (ст. 13.16); нарушение правил распространения обязательных сообщений (ст. 13.17); воспрепятствование уверенному приему радио- и телепрограмм (ст. 13.18); нарушение порядка предоставления статистической информации (ст. 13.19); непредоставление информации для составления списков присяжных заседателей (ст. 17.6); нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11.); нарушение правил защиты информации (ст. 13.12.); разглашение информации с ограниченным доступом (ст. 13.14.); нарушение порядка размещения информации в государственной информационной системе жилищно-коммунального хозяйства (ст. 13.19.1.); нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети «Интернет» (ст. 13.27.); нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления (ст. 13.28.).

Анализ вышеперечисленных составов позволяет говорить о разнообразии административных правонарушений, объектом посягательства которых является информация. Как отмечает И.Л. Бачило, «сложность отнесения некоторых составов к области информационных правонарушений связана с тем, что они являются пограничными и касаются не только информации, но и той области отношений, где информация работает и является предметом отношений».

Субъектами ответственности по Кодексу РФ об административных правонарушениях являются физические, должностные и юридические лица, совершившие общественно опасное и противоправное деяние. Объектом посягательства являются охраняемые правом общественные отношения в информационной сфере, на которые посягает административное правонарушение.

В рамках юридической ответственности необходимо рассмотреть уголовные преступления в информационной сфере. Наиболее тяжкие преступления сосредоточены в главе 28 Уголовного кодекса РФ «Компьютерные преступления».

Статья 272. Неправомерный доступ к компьютерной информации; Статья 273. Создание, использование и распространение вредоносных компьютерных программ; Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объектом данных преступлений выступают общественные отношения в сфере обеспечения безопасности охраняемой законом компьютерной информации. Под

компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В других главах Уголовного кодекса РФ размещены нормы, предусматривающие уголовную ответственность за нарушения режима информации. Например: Статья 276. Шпионаж; Статья 283. Разглашение государственной тайны; Статья 283.1. Незаконное получение сведений, составляющих государственную тайну; Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну; Статья 185. Злоупотребления при эмиссии ценных бумаг; Статья 185.1. Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах; Статья 185.6. Неправомерное использование инсайдерской информации; Статья 237. Соккрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей; Статья 128.1. Клевета; Статья 137. Нарушение неприкосновенности частной жизни; Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений; Статья 140. Отказ в предоставлении гражданину информации; Статья 159.6. Мошенничество в сфере компьютерной информации.

Практически все анализируемые преступления относятся к преступлениям средней тяжести. При характеристике объективной стороны рассматриваемых составов отмечается, что большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также установление причинной связи между этими двумя признаками.

Из всех признаков субъективной стороны значение будет иметь только один - вина.

Ряд информационных объектов защищается средствами гражданского права. Ст. 5 Закона об информации установлено, что информация может являться объектом публичных, гражданских и иных правовых отношений. В основном это объекты права интеллектуальной собственности.

Гражданско-правовая ответственность - возникающая на основании гражданского правонарушения обязанность правонарушителя совершить определенное имущественное действие (возместить убытки, уплатить неустойку), удовлетворяющее законный интерес лица, чье право нарушено, к исполнению которой правонарушитель может быть присужден по иску потерпевшего, т.е. которая может быть возложена судом на правонарушителя.

Пресечение действий правонарушителя только приостанавливает нарушение права, но не компенсирует возможные материальные потери потерпевшего. Поэтому данная мера применяется совместно с иными.

Возмещение убытков. Суд может принять решение о возмещении убытков, взыскании дохода или выплате компенсации по выбору истца и в пользу истца. Истец может требовать полного возмещения причиненных ему убытков, если законодательством или договором не предусмотрено иное.

Выплата компенсации вместо возмещения убытков. В соответствии с п. 1 ст. 1252 Гражданского кодекса Российской Федерации правообладатель вправе вместо возмещения убытков требовать от нарушителя выплаты компенсации за нарушение указанного права. Компенсация подлежит взысканию при доказанности факта правонарушения. При этом правообладатель, обратившийся за защитой права, освобождается от доказывания размера причиненных ему убытков.

Размер компенсации определяется судом в пределах, установленных Гражданским кодексом, в зависимости от характера нарушения и иных обстоятельств дела с учетом требований разумности и справедливости. Правообладатель вправе требовать от нарушителя выплаты компенсации за каждый случай неправомерного использования

результата интеллектуальной деятельности или средства индивидуализации либо за допущенное правонарушение в целом.

В соответствии со ст. ст. 1301, 1311, п. 4 ст. 1515 и п. 2 ст. 1537 Гражданского кодекса Российской Федерации в случаях нарушения исключительного права на произведение, объект смежных прав, товарный знак, наименование места происхождения товара обладатель исключительного права вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации: в размере от 10 тыс. рублей до 5 млн. рублей, определяемом по усмотрению суда; в двукратном размере стоимости экземпляров произведения, фонограммы, товаров, на которых незаконно размещен товарный знак или наименование места происхождения товара, или в двукратном размере стоимости права использования произведения, объекта смежных прав, товарного знака, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения, объекта смежных прав или товарного знака.

Изъятие контрафактных товаров из гражданского оборота происходит по решению суда. Кроме того, изъятые контрафактные товары подлежат уничтожению без какой бы то ни было компенсации в соответствии с п. 4 ст. 1252 Гражданского кодекса Российской Федерации.

Изъятие оборудования и материалов, используемых или предназначенных для совершения нарушений исключительного права на объекты интеллектуальной собственности, осуществляется по решению суда. Кроме того, в соответствии с п. 5 ст. 1252 Гражданского кодекса Российской Федерации изъятое оборудование и материалы подлежат уничтожению за счет нарушителя, если законом не предусмотрено их обращение в доход государства.

Вопросы, выносимые на обсуждение:

1. Понятие и виды юридической ответственности в сфере информационной безопасности
2. Правонарушения, посягающие на информационную безопасность: понятие и формы
3. Актуальные проблемы совершенствование форм и методов борьбы с различными видами правонарушений в сфере информационной безопасности

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Ответственность за нарушения информационного законодательства
2. Проблемы юридической ответственности в информационном праве

Повышенный уровень

1. Административная ответственность при нарушении информационной безопасности
2. Формы и методы борьбы с различными видами правонарушений в сфере информационной безопасности

Занятие 11. Актуальные проблемы правового регулирования информационной безопасности

Цель занятия: изучение направлений развития правовой охраны информационной безопасности.

Организационная форма занятия: семинар - занятие в форме практической подготовки.

В результате освоения темы обучающийся должен **знать:** систему информационного права, информационное законодательство, актуальные направления развития современного правового регулирования информационной безопасности.

Уметь: применять приобретенные теоретические знания на практике, решать практические задачи, применять практические сведения в области информационного права, умело оперировать информационно-правовыми нормами для аргументации профессиональных оценок и защиты интересов граждан.

Владеть: понятийным аппаратом информационного права, нормами информационного законодательства.

В результате освоения темы №11 обучающийся должен приобрести следующие общекультурные и профессиональные **компетенции:** ПК-1, ПК-6

Актуальность темы практического занятия: Актуальность изучения актуальных проблем развития проблем информационного права как относительно новой отрасли российского права обусловлена, прежде всего, повышением роли информации в жизни государства, личности и общества, а также широким распространением информационно-компьютерных технологий и внедрением глобальных информационно-телекоммуникационных сетей, создающих новые формы информационных отношений, что, в свою очередь, приводит к необходимости создания адекватной нормативно-правовой базы.

Теоретическая часть: Информационное право выделилось в самостоятельное научное направление, при этом право на продление ее отраслевой самостоятельности до сих пор вызывает оживленные дискуссии. Информационное право в настоящее время переживает переходный период от становления к развитию. Информационное право представляет собой структурно-сложное правовое явление, состоящее из множества элементов: информационное законодательство, отрасль юриспруденции, учебная дисциплина и отрасль системы права. Причем траектория развития каждого из названных элементов синхронно не совпадает не только по времени, но и по организационным основаниям. В образовательные программы практически всех юридических вузов уже введена учебная дисциплина «Информационное право». Информационное законодательство является одним из динамично развивающихся, в связи с этим нередко возникают разногласия с правоприменительной практикой. Теоретические и прикладные проблемы информационного права традиционно находятся в фокусе юридической науки и практики. Продолжает формироваться понятийно-категориальный аппарат, предметное содержание теории и науки информационного права.

Вопросы, выносимые на обсуждение:

Актуальные проблемы развития информационного законодательства как главного компонента информационного права

Основные тенденции становления и развития правового регулирования информационной безопасности

Задания и вопросы для формирования и контроля владения компетенциями:

Вопросы для собеседования:

1. Актуальные проблемы системологии законодательства в сфере информационной безопасности
2. Формирование понятийного аппарата информационной безопасности как подотрасли информационного права

Повышенный уровень

1. Научно-образовательные проблемы современной информационной безопасности
2. Понятийный аппарат информационного и телекоммуникационного права: проблемы правоприменения

Рекомендуемая литература

Основная литература:

1. Корнилова, А.А. Защита персональных данных: учебное пособие: [16+] / А.А. Корнилова, Д.С. Юнусова, А.С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2021. – 119 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=611314> (дата обращения: 15.04.2021). – Библиогр. в кн. – Текст: электронный.
2. Максуров, А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование / А.А. Максуров. – Москва: Дашков и К, 2021. – 198 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=600313> (дата обращения: 15.04.2021). – ISBN 978-5-394-03262-2. – Текст: электронный.

Дополнительная литература:

1. Арзуманян, А.Б. Международные стандарты правовой защиты информации и информационных технологий: учебное пособие: [16+] / А.Б. Арзуманян; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – 140 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612162> (дата обращения: 15.04.2021). – Библиогр.: с. 129-133. – ISBN 978-5-9275-3546-0. – Текст: электронный.
2. Современные информационные технологии и право / А.С. Ворожечин, Е.В. Зайченко, Е.Е. Кирсанова и др.; отв. ред. Е.Б. Лаутс; Московский государственный университет им. М. В. Ломоносова. – Москва: Статут, 2019. – 288 с. – (Труды Юридического факультета: книга 15). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=571922> (дата обращения: 15.04.2021). – Библиогр. в кн. – ISBN 978-5-8354-1578-6. – Текст: электронный.
3. Крахин А.В. Информационные технологии и системы в управленческой деятельности: учебное пособие: [16+] / А.В. Крахин. – Москва: ФЛИНТА, 2020. – 256 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=607279> (дата обращения: 15.04.2021). – ISBN 978-5-9765-4392-8. – Текст: электронный.

Интернет-ресурсы

1. Справочная правовая система «Консультант плюс» <https://www.consultant.ru/>
2. ЭБС «Университетская библиотека онлайн». <http://biblioclub.ru>
3. Электронно-библиотечная система IPRsmart . <https://www.iprbookshop.ru/>
4. Российская государственная библиотека <https://www.rsl.ru/>
5. Электронно-библиотечная система «Знаниум»: <https://znanium.com/>
6. Электронно-библиотечная система «Лань» <https://e.lanbook.com/>
7. Электронно-библиотечная система «Консультант студента» <https://www.studentlibrary.ru/>
8. Электронно-библиотечная система «Национальный цифровой ресурс «Руконт» <https://lib.rucont.ru/>
9. Библиотека профессионала №1 <https://profspo.ru/>
10. Русский язык как иностранный РКИ <https://www.ros-edu.ru/>

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по организации и проведению самостоятельной работы
по дисциплине «Правовое регулирование информационной безопасности»
для студентов направления подготовки 40.05.01. Правовое обеспечение
национальной безопасности
специализация «Государственно-правовая»

Ставрополь, 2026

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целями курса являются:

- ❖ Рассмотрение совокупности правовых норм, регулирующих информационные отношения.
- ❖ Изучение отдельных подотраслей и институтов информационного права, регулирующих отношения в сфере информационной безопасности;
- ❖ Формирование у будущих специалистов теоретических знаний и компетенций в области применения норм в сфере информационной безопасности; проблем правового регулирования информационной безопасности в сети Интернет, международной информационной безопасности.

Задачами освоения дисциплины «Правовое регулирование информационной безопасности» являются:

- раскрытие места и значения подотрасли информационного права в правовом регулировании общественных отношений в сфере информационной безопасности;
- рассмотрения общих и специальных вопросов в области информационно-правовой дисциплины, соотношения общего и специального законодательства.
- анализ теории и правоприменительной практики информационного права, и информационной безопасности;
- уяснения студентами системы научных знаний об информационном праве и информационной безопасности как отрасли права, его предмете, методах, принципах правового регулирования информационных отношений, истории развития, его основных институтах, сравнительно-правовом анализе норм права и общественных отношений в сфере информационной безопасности зарубежных стран.

Все темы курса выстроены в единой логической последовательности, образуя целостную структуру внутрипредметных связей.

Учебная дисциплина «Правовое регулирование информационной безопасности» включена в профессиональный цикл базовые дисциплины по направлению подготовки 40.05.01.

В результате освоения дисциплины «Правовое регулирование информационной безопасности» обучающийся должен приобрести следующие компетенции:

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен разрабатывать нормативные правовые акты	ИД ПК-1.1. Выявляет пробелы и коллизии действующего законодательства и определяет способы их преодоления и устранения; ИД ПК-1.2. Понимает сущность и уровни нормотворческого процесса, выделяет стадии нормотворческой процедуры; ИД ПК-1.3. Аргументирует нормативное решение и прогнозирует последствия его реализации, в том числе с	Определяет пробелы и коллизии действующего законодательства и определяет способы их преодоления и устранения Логически обосновывает и понимает сущность и уровни нормотворческого процесса, выделяет стадии нормотворческой процедуры. Обеспечивает нормативное решение и прогнозирует

	учетом возможных коррупционных рисков.	последствия его реализации, в том числе с учетом возможных коррупционных рисков.
ПК-6 Способен осуществлять профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению	ИД ПК-6.1. Выявляет и принимает меры к устранению причин и условий, способствующих совершению преступлений и иных правонарушений	Способен выявлять и принимать меры к устранению причин и условий, способствующих совершению преступлений и иных правонарушений
	ИД ПК-6.2. Участвует в оценке проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, на предмет их соответствия действующему законодательству в рамках поставленной задачи	Проявляет способности участия в оценке проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, на предмет их соответствия действующему законодательству в рамках поставленной задачи

Общая характеристика самостоятельной работы студента при изучении дисциплины «Правовое регулирование информационной безопасности»

Цель самостоятельной работы студентов в процессе изучения дисциплины – научиться осмысленно и самостоятельно работать:

- 1) с учебным материалом по дисциплине,
- 2) с научной информацией, актуальными исследованиями в области теории и практики информационной безопасности,
- 3) с эмпирическими данными, получаемыми в ходе экспериментальных исследований,
- 4) нормативными документами, как историческими, так и актуальными, регулирующими названную сферу.

Задачи самостоятельной работы:

- сформировать и развить навыки ведения самостоятельной работы и овладения методикой исследования при решении разрабатываемых в учебной деятельности проблем и вопросов;

- повысить уровень подготовленности к самостоятельной работе в соответствии с избранным направлением обучения с учетом современного состояния науки и культуры.

Таким образом, самостоятельная работа позволяет повысить общий образовательный уровень студента, приобщает к научно-исследовательскому творчеству.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Тема 1. Государственная политика и управление в сфере информационной безопасности

Цель занятия: сформировать у обучающихся знания в области государственного управления информационной сферой, специальных структур, обеспечивающих инновационные процессы в государственном управлении.

Форма контроля: *Подготовка докладов*

Вопросы и задания для развития и контроля владения компетенциями

1. Составьте схему системы и полномочий органов государственной власти, обеспечивающих право доступа к информации.
2. Составьте схему системы и компетенций органов, обеспечивающих охрану государственной тайны.
3. Определите компетенцию органов государственной власти по обеспечению правового режима конфиденциальной информации.
4. Взаимодействие органов местного самоуправления и органов государственной власти в условиях информационного общества.
5. Организационно-правовое обеспечение инновационных процессов.
6. Характеристика документов, которыми определяются основные приоритеты, принципы и направления модернизации государственного управления и административной реформы: Концепция формирования в Российской Федерации электронного правительства; Федеральная целевая программа «Информационное общество»; Концепция региональной информатизации; Концепция использования информационных технологий в деятельности федеральных органов государственной власти.

Тема 2. Правовой режим информационной безопасности документированной информации. Информационная безопасность электронного документооборота

Цель занятия: формирование профессиональных компетенций в области правового регулирования документооборота, электронного документооборота, использования электронных документов и электронной подписи в правоприменительной деятельности.

Форма контроля: *Подготовка электронных презентаций*

Вопросы и задания для развития и контроля владения компетенциями

1. Могут ли договор и документы, подтверждающие выполнение работ (акт приема-передачи), оформляться в электронной форме и передаваться по сети Интернет?
2. Допустима ли по российскому праву выдача банковской гарантии в электронной форме (по электронной почте) с использованием электронной подписи?
3. Возможно ли использование факсимиле в договорах на оказание услуг и других документах, касающихся данного договора?
4. Будет ли иметь юридическую силу договор поставки, подписанный покупателем путем факсимильного воспроизведения подписи? Может ли он быть принят в качестве доказательства в суде?
5. При заключении письменного договора поставки поставщик предлагает включить пункт о том, что дополнительные соглашения к договору могут совершаться путем обмена письмами по электронной почте. Будут ли такие дополнительные соглашения иметь юридическую силу? Как можно доказать, что такое соглашение было заключено?
6. Обязан ли подрядчик приостановить работы в случае получения уведомления о приостановлении работ, направленного заказчиком в адрес подрядчика факсимильной связью? Каковы правовые последствия неисполнения документов, полученных посредством факсимильной связи?

7. Товарищество собственников жилья обратилось в Арбитражный суд г. Москвы с иском к банку о взыскании убытков, вызванных несанкционированным списанием денежных средств со счета истца. В ходе рассмотрения дела было установлено, что платежные поручения, на основании которых списывались указанные денежные средства, подписывались электронной подписью с использованием закрытого ключа, зарегистрированного на имя руководителя и главного бухгалтера истца, электронная подпись верна, в связи с чем у банка отсутствовали основания для неисполнения платежных поручений. Решением суда первой инстанции в иске было отказано, суд кассационной инстанции оставил решение суда без изменения, а кассационную жалобу - без удовлетворения. Дайте юридическую оценку возникшей ситуации. Оцените правовые позиции сторон спора.

Тема 3. Правовой режим информации ограниченного доступа. Информационная безопасность информации ограниченного доступа

Цель занятия: изучить правовой режим государственной тайны, тайны частной жизни, личной тайны, семейной тайны, коммерческой тайны, банковской тайны, профессиональной тайны, служебной тайны.

Форма контроля: *Подготовка докладов*

Задания для развития и контроля владения компетенциями

1. Определите соотношение понятий «сведения о частной жизни», «тайна личной жизни», «сведения об интимных сторонах жизни лица», «личная и семейная тайна».

2. Прокуратура Ленинского района г. Ставрополя сочла журнал «Вокруг света» опасным для детей. В библиотеке лица, прокуроры нашли выпуск журнала за 2006 год, где рекламировался табак и алкоголь. А это противоречит закону о защите детей от вредной информации, решили они. Являются ли действия сотрудников прокуратуры законными?

3. Вправе ли Фонд социального страхования РФ требовать от кредитной организации предоставления сведений о лице, получившем денежные средства со счета вкладчика, на который были излишне начислены суммы страховых выплат. Возможно ли такие действия банка считать нарушением банковской тайны. Обоснуйте ответ со ссылкой на действующее законодательство.

4. Возможно ли привлечь к административной ответственности коммерческие организации, не раскрывшее информацию об аффилированных лицах? Обоснуйте ответ со ссылкой на действующее законодательство.

5. Заместителем Генерального прокурора Российской Федерации в адрес Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций было направлено требование о принятии мер по ограничению доступа к информационным ресурсам, согласно которому в ходе мониторинга сети «Интернет» выявлен ряд веб-ресурсов (блогов и сообществ), в том числе в социальной сети «Facebook.com» по указателям страниц сайтов: ... В ходе изучения информационных массивов, размещенных на страницах указанных ресурсов, установлена их единая тематическая направленность - освещение публичных мероприятий неправомерного характера на территории РФ.

Прокурор В. потребовал принять меры по ограничению доступа к распространяющим призывы к участию в массовых публичных мероприятиях. Какова суть претензий? Какие нормы материального и процессуального права необходимо принять сторонам спора для обеспечения интересов?

Тема 4. Правовое регулирование информационной безопасности сведений, составляющих государственную тайну

Цель занятия: изучить правовой режим государственной тайны.

В результате освоения темы обучающийся должен **знать:** информационное законодательство, юридические механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну.

Форма контроля: *Подготовка к практическим занятиям*

Вопросы и задания для развития и контроля владения компетенциями

1. Гражданин Ш. в форме электронного документа с использованием Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» обратился в архив УФСБ России по Ставропольскому краю с заявлением о предоставлении сведений об оформлении в отношении него допуска к сведениям особой важности или совершенно секретным сведениям, отнесенным к государственной тайне, в случае, если такой допуск был оформлен, сообщить организацию и год. В запросе был указан домашний адрес и телефон заявителя. Письмом Центрального архива ФСБ России заявителю разъяснено, что запрашиваемыми им сведениями Центральный архив ФСБ России не располагает, данный архивный запрос направлен для рассмотрения в УФСБ России по Ставропольскому краю.

Из ответа УФСБ России по Ставропольскому краю последовала, что запрос рассмотрен, сообщить запрашиваемую информацию не представляется возможным, данными об оформлении допуска к государственной тайне, поскольку данными должно располагать предприятие, учреждение, в т.ч. образовательное, где заявитель осуществлял трудовую деятельность или обучался. Нарушено ли право гражданина Ш. на информацию? Составляют ли запрашиваемые сведения государственную тайну? Дайте юридическую оценку возникшей ситуации.

2. Кто осуществляет контроль и надзор за обеспечением защиты государственной тайны?

3. Охарактеризуйте систему защиты государственной тайны.

4. Раскройте порядок отнесения сведений к государственной тайне.

5. Существуют ли ограничения для организации (ООО), имеющей иностранных учредителей, на получение лицензии ФСБ в части доступа к государственной тайне?

6. Вправе ли организация, имеющая лицензию на работу со сведениями, составляющими гостайну, оформить на гражданина-подрядчика допуск к таким сведениям?

7. Должны ли организации, данные на сотрудников которых относятся к секретной информации, представлять сведения о доходах таких сотрудников в налоговые органы?

Тема 5. Правовое регулирование информационной безопасности сведений, составляющих коммерческую тайну

Цель занятия: изучить правовой режим коммерческой тайны.

В результате освоения темы обучающийся должен **знать:** информационное законодательство, юридические механизмы обеспечения информационной безопасности информации, составляющей коммерческую тайну.

Форма контроля: *Конспектирование и комментирование источников*

Вопросы и задания для развития и контроля владения компетенциями

1. Следователь СУ МУ МВД России обратился в суд с ходатайством о производстве обыска офиса коммерческой фирмы, по тем основаниям, что там могут находиться предметы, документы и иные ценности, имеющие значение для уголовного дела, возбужденному по признакам преступления, предусмотренного УК РФ, а также у следствия имеются основания полагать, что в найденной в ходе обыска документации и на

электронных носителях информации может содержаться государственная или иная охраняемая федеральным законом тайна, а также содержаться информация о вкладах и счетах граждан в банках и иных кредитных организациях.

Суд, рассмотрев материалы, разрешил производство обыска, поскольку представленные суду материалы подтверждают обоснованность ходатайства следователя, что по делу имеются достаточные основания полагать, что по вышеуказанному адресу могут находиться предметы, документы и иные ценности, имеющие значение для уголовного дела. Представители коммерческой фирмы обратились в суд, так как, разрешение о проведении обыска считают незаконно, а действия следователя при проведении обыска и изъятия компьютерной техники нарушают права и законные интересы организации, в том числе гарантированные права на охраняемую законом коммерческую тайну и на неприкосновенность частной собственности, гарантированную [Конституцией](#) РФ всем участникам гражданского оборота в РФ, указывает на то, что незаконное изъятие компьютерной техники и серверного оборудования привело к фактической остановке работы компании, невозможности своевременной сдачи налоговой отчетности и выплаты заработной платы сотрудникам. Дайте юридическую оценку сложившейся ситуации. Проведите правовую оценку позиции сторон спора.

2. Вправе ли закрытое акционерное общество установить режим коммерческой тайны в отношении сведений, содержащихся в документах о премировании работников?

3. Общество определило перечень информации, составляющей коммерческую тайну, и установило порядок обращения с ней. Однако на документах, содержащих такую информацию, не был нанесен гриф «Коммерческая тайна». Может ли это стать основанием для отказа в удовлетворении требований общества о взыскании убытков с работника, разместившего на своем интернет-ресурсе сведения, составляющие коммерческую тайну?

4. Имеет ли право участник общества с ограниченной ответственностью вправе знакомиться с документами, содержащими информацию, относящуюся к коммерческой тайне общества. Обоснуйте ответ с ссылкой на действующее законодательство.

5. Должностному лицу налогового органа в ходе проведения выездной налоговой проверки налогоплательщика-организации стала известна коммерческая тайна - информация о способах ведения организацией предпринимательской деятельности, приносящих значительно больший доход по сравнению с конкурентами, находящимися в сходных экономических условиях. Может ли указанное должностное лицо в случае разглашения такой информации третьим лицам без согласия организации быть привлечено к административной ответственности и дисциплинарной ответственности в виде увольнения с государственной гражданской службы, а также к уголовной ответственности?

Тема 6. Правовая охрана информационной безопасности персональных данных

Цель занятия: изучить правовое регулирование института персональных данных, условия обработки, передачи, правовой охраны и мер юридической ответственности за нарушение законодательства о персональных данных.

Форма контроля: Подготовка докладов. Выступление в рамках занятия

Задания для развития и контроля владения компетенциями

1. Организация ведет обычную хозяйственную деятельность, которая не связана с профессиональными коммерческими интересами в области разработки, продажи, внедрения информационных систем по обработке персональных данных. Является ли такая организация оператором персональных данных? Нужно ли уведомлять орган Роскомнадзора об обработке указанных данных?

3. Разрешите юридическую ситуацию: Гражданка М.И. обратилась в Промышленный районный суд г. Ставрополя с иском к товариществу собственников

жилья (далее - ТСЖ) «Чайка» и заявила требование и признании незаконными действия ТСЖ «Чайка» в лице председателя NNN, выразившиеся в распространении ее персональных данных и передаче их ООО «Юго-западная» без ее согласия. Заявленные требования обосновала тем, что является собственником жилья по адресу NNN. Оплату коммунальных услуг осуществляет по квитанциям, получаемым в бухгалтерии ТСЖ «Чайка», однако в сентябре - октябре 2012 г. стала получать письма от ООО «М.Б.А. Деньги» с требованием заплатить сумму долга за период с 1 мая 2010 г. по 1 мая 2013 г.

С ООО «Юго-западная» у нее какие-либо отношения отсутствуют, договор на оказание услуг по отоплению она не заключала. Истец полагает, что информация о наличии у нее имущества относится к персональным данным, согласие на распространение которых она ни ТСЖ «Чайка», ни ООО «Юго-западная», ни ООО «Деньги» не давала.

Решением Заводского районного суда г. Саратова от 7 мая 2013 г. в удовлетворении исковых требований М.И. к ТСЖ «Чайка» о признании незаконными действий по распространению персональных данных и их передаче без согласия и компенсации морального вреда отказано. Является законными требования о нарушении правил обработки персональных данных? Оцените решение суда с точки зрения правомерности и обоснованности применения материальных норм права.

4. Судебная коллегия по гражданским делам Ставропольского краевого суда рассмотрела 25 октября 2012 г. гражданское дело по апелляционной жалобе Н. на решение Невинномысского от 19 июня 2012 г. об оспаривании бездействия органа местного самоуправления Невинномысской городской администрации, создавшего препятствия к осуществлению гражданином его прав. Намереваясь приобрести во владение земельный участок, примыкающий к принадлежащему ей участку, Н. обратилась к главе Невинномысской городской администрации с заявлением, в котором просила сообщить ей сведения о владельцах интересующего ее участка. Она получила отказ по основаниям, предусмотренным Федеральным [законом](#) «О персональных данных», согласно которому персональные сведения граждан распространению без их согласия не подлежат. Решением Невинномысского городского в удовлетворении заявления Н. отказано. Судебная коллегия также отказала в удовлетворении заявления М.

Оцените позиции сторон? Являются ли объективными и обоснованными иски требования? Какое решение объективно должен принять суд?

5. В рамках исполнительного производства, возбужденного на основании исполнительного листа, выданного Серышевским районным судом в отношении физического лица, судебным приставом-исполнителем в адрес филиала ОАО «МТС» направлен запрос о предоставлении информации о номере абонента, денежных средствах, затраченных должником в счет оплаты связи, и месте жительства данного физического лица.

Руководствуясь статьями 53 и 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», статьями 3, 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», ОАО «МТС» отказало службе судебных приставов в предоставлении указанной информации, мотивировав тем, что запрашиваемые сведения являются конфиденциальными и без согласия абонента могут предоставляться лишь уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, к числу которых судебные приставы-исполнители не относятся. Указанные сведения являются персональными данными и без согласия лица, которому они принадлежат, третьим лицам передаваться не могут.

Сочтя отказ в предоставлении указанной информации неисполнением законных требований судебного пристава-исполнителя, служба судебных приставов постановлением привлекла ОАО «МТС» к административной ответственности, предусмотренной частью 3

статьи 17.14 КоАП РФ, назначив обществу наказание в виде административного штрафа в размере 50 000 руб.

Данные обстоятельства явились поводом для обращения общества в арбитражный суд с заявлением о признании незаконным и отмене постановления службы судебных приставов.

Оцените позиции сторон? Какое решение объективно должен принять суд?

6. Предприниматель В. обратился в Управление Роскомнадзора по Москве и Московской области с жалобой на действия ОАО «МТС», заключающиеся в обработке его персональных данных, а также оставлении без ответа запроса предпринимателя о разъяснении ему механизма и цели такой обработки. В обоснование жалобы В. сослался на нарушение такими действиями оператора мобильной связи требований статей 9, 18 Закона «О персональных данных».

Письмом Управление Роскомнадзора направило в адрес заявителя о результатах рассмотрения указанного обращения. В указанном ответе руководитель Управления Роскомнадзора со ссылкой на статью 3, подпункт 2 пункта 2 статьи 6 Закона «О персональных данных» сообщил заявителю о том, что нарушений указанного Закона со стороны ОАО «МТС» не установлено.

Предприниматель В. обратился в суд. Оцените позиции сторон? Какое решение объективно должен принять суд?

Тема 7. Правовые основы информационной безопасности отношений в информационно-телекоммуникационной сети Интернет

Цель занятия: раскрыть понятие распространения информации в законодательстве, а также отношений протекающих в глобальной сети.

Форма контроля: *Подготовка докладов*

Вопросы и задания для развития и контроля владения компетенциями

1. Составьте схему системы и полномочий органов государственной власти, обеспечивающих контроль и надзор в сети Интернет.
2. Составьте схему осуществления саморегулирования в сети Интернет.
3. Проведите анализ судебной практики по делам, связанным с распространением запрещенной информации в Интернет.
4. Подготовьте анализ особенностей распространения информации новостным агрегатором, установленных законодательством.
5. Подготовьте анализ особенностей распространения блогером общедоступной информации, установленных законодательством.

Тема 8. Актуальные проблемы информационной безопасности объектов интеллектуальной собственности в информационно-телекоммуникационной сети Интернет

Цель занятия: раскрыть юридическую природу информационно-телекоммуникационной сети Интернет, а также отношений протекающих в глобальной сети.

Форма контроля: *Подготовка к практическим занятиям*

Вопросы и задания для развития и контроля владения компетенциями

1. Является ли введением в оборот без согласия правообладателя продукции, фотографии которой размещены на интернет-сайте с предложением о продаже, но в фактическом ассортименте эта продукция отсутствует?

2. Существует ли в России ответственность за распространение спама в Интернете в виде рекламы, получение которой пользователь не заказывал на свой электронный адрес в данной сети, а распространитель рекламы известен?

3. Провайдер предоставляет пользователю услуги по доступу в Интернет и пространство для хранения информации. Несет ли провайдер ответственность за распространение таким пользователем спама?

Тема 9. Актуальные проблемы международно - правового регулирования обеспечения информационной безопасности

Цель занятия: изучить основные информационные права и свободы человека и гражданина и правовые механизмы их обеспечения на внутригосударственном и международном уровне.

Форма контроля: Конспектирование и комментирование источников

Вопросы и задания для развития и контроля владения компетенциями

1. Подготовить доклад на тему: «Современные тенденции развития международной информационной безопасности как института международного права».
2. Провести анализ научной статьи «Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве»
3. Проанализировать положения «Конвенции о преступности в сфере компьютерной информации» (ETS N 185).

Тема 10. Юридическая ответственность в сфере информационной безопасности

Цель занятия: заключается в познании студентами правовой природы юридической ответственности в информационной сфере, а также в применении полученных на лекциях, семинарских занятиях и в ходе самостоятельной работы знаний в правоприменительной практике.

Форма контроля: *Подготовка электронных презентаций*

Вопросы и задания для развития и контроля владения компетенциями

1. Можно ли привлечь к ответственности распространителей информации, запрещенной к распространению на сайтах в сети Интернет?
2. Какие требования установлены законодательством Российской Федерации о рекламе по факту распространения на интернет-сайтах или в социальных сетях рекламы?

Тема 11. Актуальные проблемы правового регулирования информационной безопасности

Цель: изучение проблем правового регулирования информационной безопасности.

Форма контроля: собеседование, защита доклада, выполнение индивидуальных творческих заданий, проверка задач.

Задания для самостоятельной работы студентов.

Задание 1. Составьте презентацию: «Информационная безопасность как объект уголовно-правовой охраны».

ФОРМЫ ОТЧЕТНОСТИ И ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ И ОФОРМЛЕНИЮ РЕЗУЛЬТАТОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контроль результатов самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия и самостоятельную

работу по дисциплине / профессиональному модулю, может проходить в письменной, устной или смешанной форме с предоставлением изделия или продукта творческой деятельности.

Контроль самостоятельной работы должен отвечать следующим требованиям:

- систематичность проведения;
- максимальная индивидуализация контроля;
- соответствие формы контроля виду задания для самостоятельной работы.

Для контроля самостоятельной работы студентов могут быть использованы разнообразные формы, методы и технологии контроля.

- Формы: тестирование, самоотчет, презентации, кейсы, защита творческих работ, контрольные работы и др.;

- Методы контроля: семинарские занятия, зачеты, коллоквиумы, лабораторные работы, практические работы, собеседование, экзамены;

- Технологии контроля: рейтинговая оценка, портфолио, самооценка и др.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения учебного материала;
- умение использовать теоретические знания и практические умения при выполнении профессиональных задач;
- уровень сформированности общих и профессиональных компетенций;
- оформление отчетного материала в соответствии с требованиями;
- творческий подход к выполнению самостоятельной работы;
- уровень владения новыми технологиями, понимание их применения, их сила и слабости, способность критического отношения к информации;
- уровень ответственности за свое обучение и самоорганизацию самостоятельной познавательной деятельности.

Критерии оценивания

Собеседование и коллоквиум:

Оценка «отлично» выставляется студенту, если он раскрыл вопрос в полной мере на основе учебной, методической, дополнительной литературы, а также необходимых нормативно-правовых актов.

Оценка «хорошо» выставляется студенту, если он раскрыл вопрос в полной мере на основе только учебной литературы, а также необходимых нормативно-правовых актов.

Оценка «удовлетворительно» выставляется студенту, если он раскрыл вопрос лишь частично на основе только учебной литературы, сделав при этом ряд существенных ошибок.

Оценка «неудовлетворительно» выставляется студенту, если ответ по существу отсутствует, несмотря на наводящие вопросы преподавателя

Доклад:

Оценка «отлично» выставляется студенту, если он раскрыл тему в полной мере на основе учебной, методической, дополнительной литературы, а также необходимых нормативно-правовых актов; текст доклада оформлен в соответствии с требованиями, предъявляемыми к письменным работам студентов (курсовая, ВКР).

Оценка «хорошо» выставляется студенту, если он раскрыл тему в полной мере на основе только учебной литературы, а также необходимых нормативно-правовых актов; текст доклада оформлен в соответствии с требованиями, предъявляемыми к письменным работам студентов (курсовая, ВКР), но имеются недочеты.

Оценка «удовлетворительно» выставляется студенту, если он раскрыл тему лишь частично на основе только учебной литературы, сделав при этом ряд существенных ошибок; текст доклада оформлен с существенными нарушениями требований, предъявляемых к письменным работам студентов (курсовая, ВКР).

Оценка «неудовлетворительно» выставляется студенту, если сделанный доклад не раскрывает тему по существу; оформлен без учета требований, предъявляемых к письменным работам студентов (курсовая, ВКР).

Индивидуальное творческое задание:

Оценка «отлично» выставляется студенту, если он выполнил задание в полной мере на основе учебной, методической, дополнительной литературы, а также необходимых нормативно-правовых актов.

Оценка «хорошо» выставляется студенту, если он выполнил задание в полной мере на основе только учебной литературы, а также необходимых нормативно-правовых актов.

Оценка «удовлетворительно» выставляется студенту, если он выполнил задание частично на основе только учебной литературы, сделав при этом ряд существенных ошибок.

Оценка «неудовлетворительно» выставляется студенту, если задание по существу не выполнено.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ

Основная литература:

1. Корнилова, А.А. Защита персональных данных: учебное пособие: [16+] / А.А. Корнилова, Д.С. Юнусова, А.С. Исмаилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2021. – 119 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=611314> (дата обращения: 15.04.2021). – Библиогр. в кн. – Текст: электронный.
2. Максуров, А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование / А.А. Максуров. – Москва: Дашков и К, 2021. – 198 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=600313> (дата обращения: 15.04.2021). – ISBN 978-5-394-03262-2. – Текст: электронный.

Дополнительная литература:

1. Арзуманян, А.Б. Международные стандарты правовой защиты информации и информационных технологий: учебное пособие: [16+] / А.Б. Арзуманян; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – 140 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612162> (дата обращения: 15.04.2021). – Библиогр.: с. 129-133. – ISBN 978-5-9275-3546-0. – Текст: электронный.
2. Современные информационные технологии и право / А.С. Ворожечин, Е.В. Зайченко, Е.Е. Кирсанова и др.; отв. ред. Е.Б. Лаутс; Московский государственный университет им. М. В. Ломоносова. – Москва: Статут, 2019. – 288 с. – (Труды Юридического факультета: книга 15). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=571922> (дата обращения: 15.04.2021). – Библиогр. в кн. – ISBN 978-5-8354-1578-6. – Текст: электронный.

3. Крахин А.В. Информационные технологии и системы в управленческой деятельности: учебное пособие: [16+] / А.В. Крахин. – Москва: ФЛИНТА, 2020. – 256 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=607279> (дата обращения: 15.04.2021). – ISBN 978-5-9765-4392-8. – Текст: электронный.

Интернет-ресурсы

1. Справочная правовая система «Консультант плюс» <https://www.consultant.ru/>
2. ЭБС «Университетская библиотека онлайн». <http://biblioclub.ru>
3. Электронно-библиотечная система IPRsmart . <https://www.iprbookshop.ru/>
4. Российская государственная библиотека <https://www.rsl.ru/>
5. Электронно-библиотечная система «Знаниум»: <https://znanium.com/>
6. Электронно-библиотечная система «Лань» <https://e.lanbook.com/>
7. Электронно-библиотечная система «Консультант студента» <https://www.studentlibrary.ru/>
8. Электронно-библиотечная система «Национальный цифровой ресурс «Руконт» <https://lib.rucont.ru/>
9. Библиотека профессионала №1 <https://profspo.ru/>
10. Русский язык как иностранный РКИ <https://www.ros-edu.ru/>