

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Локтионова Оксана Геннадьевна

Должность: проректор по учебной работе

Дата подписания: 26.07.2022 10:13:58

Уникальный программный ключ:

0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

**А. Н. Леонтьев**

# КИБЕРПРАВО

**Волгоград  
2021**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ

А. Н. Леонтьев

*На правах рукописи*

# КИБЕРПРАВО

*Учебное пособие*



Волгоград  
2021

ББК Х401.114я7

Р е ц е н з е н т ы :

кафедра конституционного и административного права Волгоградского  
института управления (филиала) РАНХиГС при Президенте РФ, зав.  
кафедрой, канд. юр. наук доцент *Д. А. Абезин*;  
канд. экон. наук преподаватель кафедры «Математическое моделирование  
и информатика» Волгоградского ГАУ *Е. И. Конченкова*

Печатается по решению редакционно-издательского совета  
Волгоградского государственного технического университета

**Леонтьев, А. Н.**

Киберправо: учебное пособие/ А. Н. Леонтьев; ВолгГТУ. –  
Волгоград, 2021. – 80 с.  
ISBN 978-5-9948-4110-5

Учебное пособие содержит теоретические материалы, методические указания по подготовке к практическим занятиям и выполнению контрольной работы по дисциплине «Киберправо». Рассматриваются вопросы правового обеспечения и государственного регулирования информационных технологий в условиях формирования цифровой экономики.

Учебное пособие предназначено для магистров, обучающихся по программам магистратуры по профилю «искусственный интеллект» по направлениям 09.04.01 «Информатика и вычислительная техника», 09.04.03 «Прикладная информатика», 09.04.02 «Информационные системы и технологии». Учебное пособие выполнено в рамках реализации гранта на разработку программ бакалавриата и программ магистратуры по профилю «Искусственный интеллект», а также на повышение квалификации педагогических работников образовательных организаций высшего образования в сфере искусственного интеллекта (конкурс 2021-ИИ-01 от 10.06.2021).

Библиогр.: 52 назв.

ISBN 978-5-9948-4110-5

Волгоградский государственный  
технический университет, 2021  
А. Н. Леонтьев, 2021

## ВВЕДЕНИЕ

Дисциплина «Киберправо» нацелена на приобретение знаний, умений и навыков в сфере правового обеспечения информационной деятельности, развития цифровых технологий, цифровизации экономики и других сфер общественных отношений. Содержание учебной дисциплины раскрывает современное состояние системы российского законодательства в области регулирования информационных отношений, затрагивает некоторые аспекты международного права в сфере цифровых технологий, а также рассматривает перспективные направления развития информационных технологий.

В последнее время все чаще возникают термины, не известные в самом недавнем времени: «информационное общество», «искусственный интеллект», «большие данные», «облачные технологии», «электронное предприятие», «электронный бизнес», «цифровая экономика», «блокчейн», «криптовалюта», «интернет вещей», но которые не имеют должного отражения в действующих нормативно-правовых актах.

Общество вошло в новый этап развития. На смену индустриальному и постиндустриальному укладу пришел новый этап – этап информационного общества, когда на смену материальному производству приходит производство нового знания, информации. Экономика и социальная сфера переживает цифровизацию. Алгоритмы и кибернетические устройства занимают все более значительную роль в жизнедеятельности человека. Термин «кибернетика» переживает второе рождение, входит в состав новых терминов, связанных цифровыми технологиями, в том числе с использованием искусственного интеллекта.

Новое, цифровое, проникает, переплетается со старым, аналоговым. Исторически сложившаяся система поддержания равновесия, порядка в обществе, основанная на праве, встречается с динамичными вызовами. И не всегда это проходит гладко. Развитие робототехники оказывает

не меньшее воздействие, чем когда-то появление машин. Возникают риски массовой безработицы и социальной напряженности.

Конфликты, споры, проблемы, связанные с развитием и распространением информационных технологий, нуждаются в разрешении. Правовые системы государств с трудом успевают за техническим прогрессом и срочно нуждаются в развитии, гармонизации с возникающими технологиями. Но и сами технологии могут выполнять функции, которые исторически возложены на законодательство и органы правопорядка.

Киберправо еще не получило академического признания, нет учебников по этой отрасли знания. Однако изучение этой области знаний очевидно. Киберправо – это не повтор положений информационного права, под другим наименованием, а отрасль юридических знаний ориентированная исключительно на цифровые технологии.

За рамками дисциплины остается библиотечное и архивное дело, правовое обеспечение средств массовой информации. Основное внимание уделяется правовому обеспечению общественных отношений, связанных с цифровыми технологиями, формированию цифровой экономики, возможного возникновения новых объектов, субъектов и новых форм содержания правоотношений в цифровой сфере.

Киберправо как учебная дисциплина стремится так изучать существующую и перспективную правовую систему, в которой в качестве субъектов признаются права не только граждан (лица физические) и организаций (лица юридические), но обсуждается введение новых субъектов, чаще всего условно называемых «электронные лица», «роботы» или «автономные агенты». Это не человекоподобные электронно-механические изделия или киберфизические системы, а, качественно иное, ранее неизвестное. Это – вещи, наделенные восприятием и логикой, или сама логика (алгоритм, программа), без связи с материальной оболочкой.

При этом сама программа не обязательно присутствует в целом виде внутри самого изделия (вещи). Программа может быть и вне устройства, а связь между элементами осуществляется посредством сети Интернет. Способ принятия решения становится многоуровневым, глобальным. Алгоритм алгоритмов – программа, направляющая или изменяющая работу других программ. Алгоритмы (программы) становятся все более изолированными. Роль программного обеспечения приближается к роли человека как руководителя или лица, принимающего решения.

Для успешного изучения киберправа как учебной дисциплины необходимо знать дисциплину «Основы правовых знаний» или «Правоведение» в объеме федерального образовательного стандарта для неюридических вузов, быть знакомым с основными положениями информационного права как отрасли действующего законодательства. Для восполнения знаний рекомендуется знакомство с учебными пособиями автора, указанными в списке рекомендуемой литературы.

Также желательно иметь представления об организации профессиональной деятельности и происходящих процессах в информационной сфере, быть знакомым с вопросами и ситуациями, которые не отрегулированы или недостаточно отрегулированы современным правом.

Учебное пособие состоит из трех разделов. В первом разделе, состоящем из восьми тем, излагаются теоретические материалы по дисциплине. Во втором разделе раскрываются вопросы подготовки и проведения практических занятий, в том числе и дистанционно, с использованием электронной информационной обучающей системы вуза. В третьем разделе даются методические указания по выполнению контрольной работы.

**Раздел 1**  
**ТЕОРЕТИЧЕСКИЕ МАТЕРИАЛЫ**

**Тема 1. КИБЕРПРАВО – ПОДОТРАСЛЬ ИНФОРМАЦИОННОГО ПРАВА**

Как известно из курса дисциплины «Основы правовых знаний», право – это система обязательных для исполнения норм (правил), установленных или санкционированных государством и охраняемых от нарушения возможностью применения государственного принуждения. Параллельно с нормами права существуют и функционируют другие виды норм, например, моральные или религиозные. В общем виде они не противоречат правовым нормам, но дополняют их. Абсолютное большинство правовых норм - это признанные государством уже существующие нормы и закрепленные в законах.

Информационное общество порождает более радикальные изменения области права. Информационные технологии не противостоят, а переплетаются с правом. Можно найти схожесть между структурой программного кода и правовой нормой.

Конструкция, которая существует во всех языках программирования: «если..., то ....., иначе ...», соответствует элементам нормы права: гипотеза, диспозиция и санкция. Гипотеза – это условие, при котором действует норма – аналог элемента «если». Диспозиция – собственно правило – аналог элемента «то», а санкция соответствует элементу «иначе».

Таким образом, правовые нормы легко алгоритмизируются, но применяются только в редких случаях. Например, фиксация превышения скорости автоматическими камерами и наложение штрафа. Или другой пример: все электронные платежи – не что иное, как заключение, оформление и исполнение договоров с соблюдением всех существующих требований законодательства, но в электронном виде.

Для анализа сферы правового обеспечения информационной эпохи есть возможность и необходимость использовать общетеоретические под-

ходы, сформировавшиеся на заре информационной эпохи, в том числе кибернетический. Кибернетический подход возник в 40-е годы XX века, прошел определенные этапы своего развития и породил системный подход 1960-х годов. Системный подход в науке остается основным до настоящего времени. Любой объект изучения, его поведение можно изучать как систему. Система понимается как единство взаимодействующих элементов, каждый из которых также является системой. Поведение системы любого вида (человека, группы, общества, живого организма) определяется как результат всех взаимодействий между всеми элементами системы.

В рамках парадигмы системного подхода, доминирующего в современной науке, каждый из элементов системы также представляет собой систему, состоящую из элементов. Правовая система состоит из своих элементов. Для удобства изучения и применения единая система права разделена на элементы: отрасли, институты и нормы права. Между элементами нет четких границ. Они иногда пересекаются и переплетаются, но подобное деление на отрасли, институты, нормы показало свою доступность и применимость.

В российской правовой системе сложились шесть устоявшихся и разработанных отраслей права: конституционное, гражданское, трудовое, семейное, административное, уголовное. Выделяют еще несколько других отраслей по предметам правового регулирования, например, налоговое, хозяйственное, земельное, воздушное, водное и т. п. В последнее время сформировались как актуальные отрасли экологического и информационного права.

В настоящее время все большее значение приобретает правовое обеспечение отношений, связанных с информацией. Информационное право возникло и закрепилось в качестве самостоятельной отрасли. Информация как объект правового обеспечения обладает уникальными качествами, что отличает ее от предметов материального мира. Это требует развития ин-



формационного права, определения собственных подотраслей, институтов и норм.

В общем и целом информационное право развивается в рамках сложившихся методов правовой науки, но постепенно становится все более заметно различие с правовой парадигмой. Например, норма действует по трем измерениям: во времени, в пространстве и по кругу лиц.

Из этих трех базовых признаков в информационном праве имеют проблему два последних. Интернет ставит необходимость посмотреть на пространство юрисдикции, место действия законодательства, государственных законов и области государственной поддержки. Круг лиц также требует внимательного отношения. Характерным для отрасли информационного права является неопределенный круг лиц, например, при регулировании рекламной деятельности или средств массовой информации.

Следует признать, что информационное право в настоящее время вполне эффективно функционирует в рамках сложившейся правовой традиции, успешно применяет сложившиеся способы и методы правового регулирования правоотношений. Например, информация преобразуется в документ и дальше регулируется как вещь, используя все тысячелетние наработки регулирования оборота предметов материального мира.

Одним из величайших изобретений правовой науки является введение понятия «юридическое лицо». В отличие от лица физического, юридическое лицо не обладает телесностью (телом), но в правовом пространстве отождествляется с человеком, признавая стороной правоотношений со всеми вытекающими последствиями. Эта правовая фикция, искусственное образование, которое впервые появилось в еще несовершенно виде около 500 лет назад, позволило резко упростить регулирование правоотношений в области хозяйственной деятельности, торговле, промышленности, социальной сфере. Оно стало одной из основ правового обеспечения промышленной революции. Юридическое лицо стало привычным элементом пра-

восознания, но уже практически исчерпало свои возможности и инновационный потенциал.

В настоящее время все четче проявляется необходимость развивать эту линию, создавать новый вид субъекта правоотношений – «электронное лицо». Этот вопрос уже несколько лет присутствует в научном дискурсе, но публичную актуальность приобрело в последнее время в связи с появлением беспилотных транспортных средств, прежде всего автомобилей.

Вопрос о том, кто несет ответственность в случае аварии, ущерба, смерти пешехода или водителя, остается открытым. Правовая традиция рассматривает три варианта: владелец, изготовитель, разработчик. Но все три варианта имеют логическую неполноту. Признать само устройство (беспилотный автомобиль) ответственным, значит наделить его правосубъектностью, но этого не позволяют правовые доктрины.

Можно привести исторические аналогии, рассмотрев этапы постепенной правовой трансформации древнеримского раба, который по законам Римской империи являлся вещью, через статус крепостного в свободного крестьянина, горожанина конца европейского Средневековья и далее в гражданина правового государства. Процесс занял около 1500 лет, но аналогия обоснована.

При решении о наделении беспилотного транспортного средства правосубъектностью прослеживаются и фискальные интересы государства. Конечно, трудно представить робота-пылесоса равноправным гражданином общества, но гражданские права роботов уже обсуждаются в Интернете. Но там где есть права, там есть и налоги. Очевидно, что здесь подразумеваются дополнительные налоги на владельцев предприятий, использующих на производстве роботов, но в политическом, публичном аспекте выглядит заманчиво.

Кибернетика как наука об управлении выделяет и изучает информационные потоки - сигналы прямой и обратной связи. Другими словами,

в центре внимания находятся управляющие сигналы (приказы, законы) и реакция системы (поведение), что позволяло предсказывать поведение объекта и повышать эффективность управления.

Следует рассмотреть организацию (предприятие) через призму кибернетической модели. В организации есть управляющий орган, который выдает сигналы управления и через обратную связь наблюдает реакцию. После этого следует уточняющий сигнал и наблюдается следующий результат. Эту модель построил Норберт Винер. Он обратил внимание, что с помощью подобной модели можно описать работу органов живого организма и машины (автомата). Из этой идеи развилась наука кибернетика. Модель стали применять ко всем системам, в том числе высшего уровня - экономическим, политическим.

Выводы кибернетики очень хорошо подтверждались на уровне достаточно простых устройств – автоматов или вычислительных устройств – первых ЭВМ. С более сложными системами, а тем более живыми организмами, методы кибернетики работали не так точно, что потребовало привлечь для анализа дополнительные факторы: информационные шумы, помехи, энтропию. Это позволило выделить эффекты самоорганизации или влияния окружающей среды, но усложнило поиск решения. Поэтому верхний уровень применения кибернетики – это уровень предприятия, фирмы. И если предприятие промышленное или коммерческое, построено на обмене исчисляемыми сигналами, цифровыми данными. Для управления другими организационными структурами (например, театром, творческим или научным коллектив) кибернетический подход применим слабо.

После первых десятилетий бурного развития метод достаточно быстро исчерпал свой потенциал. Метод хорошо работал для уровня развития науки и техники той эпохи. Это способствовало возникновению следующих, продвинутых подходов.

Системный подход к изучению сферы политики впервые применил Толкотт Парсонс. Опираясь на методологию общей теории систем Людвига фон Берталанфи, он рассматривал общество в качестве сложной системы, состоящей из относительно автономных частей: экономической, политической, духовной и интегративной. Последний термин обозначал государство. Правовая сфера также понималась как система, состоящая из элементов и входящая в систему более высокого уровня - государство. Системный подход отказывается от количественной определенности в пользу качественной. Для науки того времени это был большой шаг вперед. Степень точности был вполне достаточной.

На высшем уровне анализа, в общем приближении, кибернетический подход вполне состоятелен. Норму права, закон можно понимать как управляющий, выходящий сигнал для объекта управления - общества (лиц физических и юридических). Объект управления, в свою очередь формирует сигнал обратной связи – реакцию. Сигналы обратной связи могут быть многомерными. От безразличия (отсутствия сигнала обратной связи) до бунта (распада управляемого объекта).

Как правило, сигналы обратной связи отражают динамику определенной сферы жизни общества, регулируемой принятым законом или нормативным актом. После этого формируется следующий управляемый сигнал (поправки к закону) и снова ожидается реакция. Потом новая поправка, другое правило или отмена закона. Предложенная модель проста, но наглядна.

Однако право реализуется в чрезвычайно сложной и динамичной системе – обществе. Наука описывает общество как процесс взаимодействия больших социальных групп – классов, наций, страт, поколений. Современные информационные технологии формируют возможность определить и проанализировать поведение (реакцию) на уровне отдельных индивидов. Более того, на уровне ролей, которые изменяются в течение дня. Например, поведение в роли работника, в роли покупателя (потребителя), в роли

участника компьютерной игры или социальной сети. Мобильное устройство (смартфон) способен приобретать возможности «карманного полицейского», наблюдать за поведением и фиксировать правонарушения, определять меру соответствия требованиям законодательства, то есть определять поведение. Кибернетика проникает в сферу права.

### ***Контрольные вопросы:***

1. Какими отличиями обладает информационное общество?
2. Что является отличительным признаком киберправа?
3. Какие потоки выделяет кибернетический подход?
4. Какова главная цель и функция государства?
5. Какие отрасли российского права являются основными?
6. Как понимать «электронное лицо»?

## **Тема 2. КОНСТИТУЦИОННЫЕ ГАРАНТИИ ИНФОРМАЦИОННЫХ ПРАВ**

В тексте основного закона государства - Конституции Российской Федерации зафиксированы основные права и свободы человека и гражданина. Каждому гарантируется свобода мысли и слова (п. 1 ст. 29). Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п. 4. ст.29).

Одновременно Конституция определяет и ограничения на распространение информации. Это конституционные права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также защиту государственной тайны, противодействие пропаганде экстремистской идеологии.

Право свободного поиска и получения информации означает право каждого обращаться к органам государственной власти, общественным объ-

единениям, органам и организациям, частным фирмам, другим структурам по вопросам, затрагивающим основные права и свободы, провозглашенные Конституцией РФ, а также получения у них запрашиваемой информации.

Право передавать информацию означает право свободного обмена информацией каждого с каждым. Право производить и распространять информацию означает свободу каждого на творчество и интеллектуальную деятельность, сопровождаемую созданием новой или производной информации, а также на свободу широкого распространения произведенной информации всеми законными способами. Эти права могут быть ограничены только законом, а не указом, постановлением, решением или другим подзаконным актом.

Институт права на информацию – это совокупность правовых актов и отдельных норм, определяющих порядок реализации прав субъектов информационного права в области производства (создания) информации, поиска и получения (доступа) информации, сбора, хранения, передачи, использования, распространения информации в целях, не противоречащих свободам, правам и интересам человека, государства, общества и обеспечивающих создание информационных ресурсов, необходимых для реализации других прав и обязанностей субъектов права, предусмотренных и гарантированных законодательством РФ и нормами международного права.

Институт права на информацию следует отличать от институтов информационного права. Институты информационного права многообразны. Это - информация, сведения, сообщения, данные, тайна, правовой режим информации, информационная система, информационный ресурс и другие. Институты могут быть общеправовыми (правовой режим, право на информацию, защита информации) и межотраслевыми (институт собственности на результаты интеллектуальной деятельности). Институты могут делиться на подинституты. Так, институт правового режима отражает метод регулирования, и далее разделяется на подинституты по признакам предметов ре-

гулирования: информационные объекты и ресурсы; информационные системы; информационно-коммуникативные технологии.

Информационное право Российской Федерации в наибольшей степени испытывает влияние международных принципов информационного права. Развитие коммуникационных технологий в условиях трансграничной, транснациональной природы сети Интернет, с одной стороны, порождает требование унификации норм правового регулирования информационной сферы, с другой стороны, порождает риски информационной безопасности. Необходимо понимать, что международное право не обладает прямым действием, так как независимость и приоритет национального законодательства сохраняется. В этом заключается суверенитет государства.

Международное право по своему содержанию – это набор деклараций, положений, выработанных экспертами авторитетных международных организаций, которые рекомендуется включить (имплементировать) полностью или частично в законодательство государства. Но допустимо и игнорирование, что порождает политическую, экономическую, социальную и технологическую изолированность.

Международные принципы информационного права изложены в следующих документах:

- Всеобщая декларация прав человека (1948 г.);
- Конвенция Совета Европы о защите прав человека и основных свобод (1950 г.);
- Международный пакт о гражданских и политических правах (1966 г.);
- Окинавская хартия глобального информационного общества (2000 г.).
- Всеобщая декларация прав человека утверждена и провозглашена Генеральной Ассамблеей ООН 10 декабря 1948 г. В этой декларации изложены ряд положений и принципов, связанных и информационной сферой.

В ст. 12 Всеобщей декларации записано: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произ-

вольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию».

Таким образом, провозглашаются принципы:

- неприкосновенность личной и семейной жизни;
- неприкосновенность тайны переписки (корреспонденции);
- неприкосновенность чести и репутации.

Здесь приводится пример сокращенного и упрощенного изложения положений для студентов неюридических вузов. Детальное рассмотрение терминов, в том числе различий содержания и значений понятий «вмешательство» и «посягательство», симметричных формулировок на других официальных языках ООН, может продемонстрировать всю сложность трансляции идеи в текст, сложность определения и понимания международных правовых принципов.

Статья 19 гласит: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

Тем самым определяются информационные свободы:

- свобода иметь убеждения, их придерживаться и выражать;
- свобода искать, получать и распространять информацию и идеи любыми средствами;
- трансграничность получения и распространения информации.

Необходимо помнить, что речь идет о правах отдельного человека, личности, но не об организациях или корпорациях. Также необходимо помнить и понимать исторический контекст принятия этого документа. Рассматривая понятие «любые средства» распространения информации, необходимо понимать, что в 1948 году трудно было предвидеть возможности сети Интернет по распространению недостоверной информации. В то время основным



источником информации для населения были периодическая печать, радиовещание и кинохроника перед началом фильмов в кинотеатрах.

Статья 27 Всеобщей декларации гласит: «Каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами». Из всего спектра перечисленных и подразумеваемых в этой статье свобод можно выделить только один - о том, что результаты достижений науки свободны для распространения, то есть не могут приватизироваться. Кажется, что это входит в противоречие с принципами патентного права. Получается, что изобретения, защищенные патентом, не являются наукой в понимании ООН 1948 года. Выходом является разделение науки на два вида: фундаментальную и прикладную. Водоразделом между фундаментальной и прикладной наукой является различие в содержании понятий «открытие» и «изобретение». Определяющим здесь является признак «промышленно применимо» (ст. 1350 ГК РФ).

Право есть не что иное, как механизм поиска и поддержания баланса интересов и действий участников правоотношений. Так, противостоят, с одной стороны, принципы свободы получения и распространения информации, свободы слова и творчества, а с другой стороны, неприкосновенность частной жизни и обеспечение информационной безопасности государства. При поверхностном взгляде эти принципы взаимоисключающие, но в реальности, в сфере правового обеспечения они сбалансированы нормами правовых актов.

- Следующим признанным международным актом является «Конвенция Совета Европы о защите прав человека и основных свобод» (Рим, 4 ноября 1950 г.). В этой конвенции провозглашены не только свободы, но определены ограничения в сфере распространения информации. В ст. 10 рассматриваемой конвенции прямо записано: «Настоящая статья не препятствует государствам осуществлять лицензирование радиовещательных,

телевизионных или кинематографических предприятий», то есть признается право государств на регулирование информационных потоков, что создает баланс для свободы распространения информации.

Далее в Конвенции указывается, что осуществление свобод «может быть сопряжено с формальностями, условиями, ограничениями или санкциями, которые установлены законом и которые необходимы в демократическом обществе в интересах государственной безопасности, территориальной целостности или общественного спокойствия, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия».

Таким образом, процессы законодательного обеспечения информационных отношений и формирования информационного права Российской Федерации не имеют существенных отличий от признанных международным сообществом правовых норм.

- Еще один акт, который необходимо рассмотреть в рамках этой темы, является «Международный пакт о гражданских и политических правах», принятый на Генеральной Ассамблее ООН 19 декабря 1966 г. Этот пакт также формирует баланс свободы и безопасности. При этом защитительные нормы находятся выше, чем разрешительные. В ст. 17 устанавливается: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию». То есть осуществление прав и свобод одного человека и гражданина не должно нарушать права и свободы других лиц.

В статье 19, которая начинается с утверждения свободы мнения: «Каждый человек имеет право на свободное выражение своего мнения; это пра-

во включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору», но заканчивается перечнем причин для ограничения указанных свобод: «... сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

- а) для уважения прав и репутации других лиц,
- б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения».

Статья 20 устанавливает прямые запреты на некоторые темы для обсуждения: «Всякая пропаганда войны должна быть запрещена законом. Всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом». Аналогичные принципы практически дословно повторяются в Конституции Российской Федерации.

Помимо международных конвенций существуют и региональные соглашения в информационной сфере. Одним из таких документов является «Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности».

### ***Контрольные вопросы:***

1. Каковы конституционные гарантии прав на информацию?
2. Существуют ли ограничения на свободу распространение информации?
3. Какие существуют правовые основания ограничения на свободу распространение информации?
4. В чем состоит институт права на информацию?

5. Какие существуют институты информационного права?
6. Какие существуют международные конвенции, затрагивающие информационную сферу?
7. Какие принципы международного права в сфере информации имплементированы в российское законодательство?

### **Тема 3. ОБЪЕКТЫ, СУБЪЕКТЫ И СОДЕРЖАНИЕ ПРАВООТНОШЕНИЙ В ЦИФРОВОЙ СФЕРЕ**

Объекты информационных правоотношений в широком понимании, указанные в Федеральном законе 149-ФЗ - это информация, информационные технологии, информационная система, информационно-телекоммуникационная сеть.

*Информация* - сведения (сообщения, данные) независимо от формы их представления. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). Информация в зависимости от порядка ее предоставления или распространения подразделяется:

- 1) на информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В Российской Федерации предусмотрен порядок ограничения доступа к информации, если:

- выражается в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, проявляет явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации;

- распространяется с нарушением авторских и (или) смежных прав;

- распространяется с нарушением закона;

- распространяется с нарушением требований законодательства Российской Федерации о выборах и референдумах, и (или) агитационным материалам, изготовленным и (или) распространяемым с нарушением требований законодательства Российской Федерации о выборах и референдумах;

- обрабатывается с нарушением законодательства Российской Федерации в области персональных данных.

Ограничение доступа осуществляется:

- к информационному ресурсу организатора распространения информации в сети Интернет;

- к сайтам в сети Интернет, на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет;

- к копиям заблокированных сайтов.

Блокирование сайтов осуществляется без судебного процесса. Внесудебные меры по прекращению нарушения авторских и (или) смежных прав в информационно-телекоммуникационных сетях, в том числе в сети Ин-

тернет принимаются по заявлению правообладателя. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Характерными для информационного права понятиями являются термины «информационные технологии» и «информационные система». *Информационные технологии* - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. *Информационная система* - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Информационные технологии являются необъемлемой составляющей информационных систем.

Закон выделяет следующие информационные системы: Единая система идентификации и аутентификации, имеющая особое место в государственном регулировании; поисковые системы как особый вид информационных систем, а также Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

- Единая система идентификации и аутентификации – это федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

- Поисковая система - информационная система, осуществляющая по запросу пользователя поиск в сети Интернет информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети Интернет для доступа к запрашиваемой информации,

расположенной на сайтах в сети Интернет, принадлежащих иным лицам. Из этого понятия исключаются информационные системы, используемые для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

Сеть Интернет имеет сложности в правовом поле. Технически, интернет – это одна из возможных технологий передачи сигналов (сообщений, сведений) на расстояние. Однако правовое обеспечение не должно быть привязано к определенной технологии, поэтому используется универсальный термин «информационно-телекоммуникационная сеть». *Информационно-телекоммуникационная сеть* - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Помимо объектов информационных правоотношений, имеющих широкое толкование, характеризующих родовое разнообразие информационных ресурсов, выделяют и видовые, единичные объекты. Все видовые объекты информационных правоотношений попадают под определение документированной информации.

*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. Несмотря на то, что сообщение существует в электронной форме, предполагается наличие материального носителя, например жесткого диска. Главное здесь – это возможность идентифицировать обладателя, несущего ответственность.

Документированная информация в цифровом пространстве может выступать в форме электронного сообщения, электронного документа, сайта в сети Интернет в целом или в форме отдельной страницы.

*Электронное сообщение* - информация, переданная или полученная пользователем информационно-телекоммуникационной сети. *Электронный документ* - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

- Сайт в сети Интернет понимается не как собрание текста и мультимедиа, а как программно-информационный комплекс с системой доступа. По определению, приведенному в 149-ФЗ, сайт – это совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет. Страница сайта – это часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта.

Важнейшую часть характеристики информационных правоотношений является определение сторон таких правоотношений, субъектов. Специальные наименования субъектов указывает на принадлежность к информационной сфере. В качестве субъектов информационных правоотношений, каждый из которых обладает собственным набором прав, обязанностей и ответственностью, 149-ФЗ выделяет обладателя информации и посредников, обеспечивающих информационный обмен, но не обязательно являющихся обладателями информации. Это оператор информационной системы, владелец сайта и провайдер. Ранее в качестве субъекта признавался блогер.

Основным субъектом информационных правоотношений, согласно 149-ФЗ, определяется обладатель информации. Обладатель информации – универсальный термин, характеризующий держателя всех видов докумен-



тированной информации, как в бумажной, так и в электронной форме. Термин «обладатель» противостоит термину «собственник». Признано, что институт права собственности не сочетается с информацией. Информация не может отождествляться ни с вещью, ни с обязательством, сопровождающим право собственности. Поэтому используется другое слово – «обладатель», благо богатство русского языка позволяет такое слово подобрать.

*Обладатель информации* - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Обладателем информации может выступать гражданин (физическое лицо), юридическое лицо (предприятие, организация), Российская Федерация, субъект Российской Федерации, муниципальное образование. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются государственными органами и органами местного самоуправления.

Обладатель информации имеет право:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению; передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;

- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Правовое регулирование доступа в сеть Интернет необходимо рассматривать с трех сторон: со стороны производителя информации, со стороны потребителя информации и со стороны поставщика (посредника, владельца или оператора информационных систем и технологий). Особо выделяются так называемые *новостные агрегаторы* – собиратели информации, поставляющие ее в систематизированном виде, но при этом не являющиеся создателями.

Участники, субъекты информационных правоотношений за свои действия несут ответственность, мера которой определяется законом. Например, глава 15.1 Кодекса об административных правонарушениях определяет состав правонарушений в информационной сфере и меры ответственности за них.

Пользователь как участник информационных отношений упоминается в тексте 149-ФЗ, но специально не определяется, его мера ответственности не определяется. При этом необходимо помнить, что пользователь может выступать в пассивной роли как потребитель информации, а также в активной роли как обладатель информации (создатель), когда размещает информацию на сайте.

*Оператор информационной системы* - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. При этом оператор может выступать обладателем информации, несмотря на то, что он не создает и потребляет сведения, но обеспечивает информационный обмен, неся свою долю ответственности.

Наиболее распространенной и достаточно простой для правового анализа информационной системой является сайт в сети Интернет. *Сайт* – это информационно-программный комплекс, имеющий несколько уровней

представляемых возможностей. В законе не рассматривается техническая сторона, но выделяются только лица, на которых закон накладывает обязанности. Это владелец сайта, провайдер хостинга. На них распространяются требования закона, четко определяются обязанности. Прежде всего, это касается обеспечения возможности федерального органа исполнительной власти в области обеспечения безопасности путем просмотра содержания сообщений, в том числе и зашифрованных.

Как уже было сказано ранее, институт права собственности с трудом реализуется в информационном пространстве. В информационное право вводятся понятия «обладатель» и «владелец». Обладание относится к информации, а владение к информационным ресурсам.

Владелец сайта в сети Интернет - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет, в том числе порядок размещения информации на таком сайте. Провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет.

### ***Контрольные вопросы:***

1. Как разделяется информация по уровню доступа?
2. При каких условиях доступ к информации ограничивается?
3. Каким образом осуществляется ограничение доступа к информации?
4. Как именуются родовые объекты информационных правоотношений?
5. Что относится к видам объектов информационных правоотношений?
6. Каковы признаки обладателя информации?
7. Каково отличие между сайтом и страницей сайта в сети Интернет?

#### **Тема 4. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Государственное регулирование в сфере применения информационных технологий предусматривает:

а) регулирование отношений, связанных с поиском, получением, передачей, производство и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

б) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

в) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей;

г) обеспечение информационной безопасности детей.

Органы государственной власти, органы местного самоуправления в соответствии со своими полномочиями: участвуют в разработке и реализации целевых программ применения информационных технологий, создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается Единый реестр российских программ для электронных вычислительных машин и баз данных (сокращенное наименование - реестр российского программного обеспечения).

Правила формирования и ведения реестра российского программного обеспечения устанавливаются Правительством Российской Федерации. В Постановлениях правительства определяется состав сведений, включаемых в реестр российского программного обеспечения. К таким сведениям, прежде всего, относятся:

- сведения об основаниях возникновения исключительного права у правообладателя (правообладателей);
- включения в реестр российского программного обеспечения;
- исключения из реестра российского программного обеспечения;
- порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливается.

Постановлением Правительства от 16 ноября 2015 года № 1236 вводятся ограничения для государственных заказчиков на закупку программного обеспечения, отсутствующих в реестре.

Для успешного государственного регулирования правоотношений в цифровой сфере Закон определяет основных участников информационного обмена и их обязанности. Таковыми являются организатор распространения информации в сети Интернет, владелец сайта и (или) страницы сайта в сети Интернет, оператор поисковой системы, владелец новостного агрегатора, владелец аудиовизуального сервиса, владелец социальной сети. Именно они несут административную ответственность за неправомерные действия в цифровой сфере. На них налагается обязанность выявлять и пресекать негативные явления.

Организатор распространения информации в сети Интернет обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет, дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети Интернет возможности дополнительного кодирования электрон-

ных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений (п. 4.1. ст. 10.1 149-ФЗ).

Владелец сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети Интернет (далее - блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данном сайте или странице сайта иными пользователями сети Интернет, обязан обеспечивать соблюдение законодательства Российской Федерации.

На оператора поисковой системы налагается обязанность обеспечить чести и достоинства граждан путем информационного забвения, то есть удаления из поискового запроса ссылок на недопустимые ресурсы, ущемляющие права заявителей с ограничениями.

Оператор поисковой системы, распространяющий в сети Интернет рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, по требованию гражданина (физического лица) (далее в настоящей статье - заявитель) обязан прекратить выдачу сведений об указателе страницы сайта в сети Интернет (далее также - ссылка), позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя, за исключением информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость (п. 1 ст. 10.3 149-ФЗ).

Владелец новостного агрегатора, по тесту закона - владелец программы для электронных вычислительных машин, владелец сайта и (или) страницы сайта в сети Интернет, которые используются для обработки и распространения новостной информации в сети Интернет на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети Интернет, обязаны соблюдать требования законодательства Российской Федерации (п. 1 ст. 10.4 149-ФЗ).

Аудиовизуальные сервисы и социальные сети признаются ресурсами, наиболее часто нарушающими интеллектуальные права, негативно влияющими на финансовые показатели индустрии развлечений (музыка, кино и т. п.). В законе указывается, что владелец сайта и (или) страницы сайта в сети Интернет, и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые используются для формирования и (или) организации распространения в сети Интернет совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети Интернет, находящихся на территории Российской Федерации, обязан соблюдать требования законодательства Российской Федерации (п. 1 ст. 10.5 149-ФЗ).

Владелец сайта и (или) страницы сайта в сети Интернет, и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством соз-

данных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более пятисот тысяч пользователей сети Интернет, находящихся на территории Российской Федерации, обязан соблюдать требования законодательства Российской Федерации (п.1 ст. 10.6149-ФЗ)

Доступ к информации - возможность получения информации и ее использования. Граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законом. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (ст. 9 149-ФЗ).

В Законе «Об информации, информационных технологиях и защите информации» вводится новое понятие «профессиональная тайна». *Профессиональная тайна* - информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (п. 5 ст. 9 149-ФЗ).

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Необходимо различать предоставление информации и распространение информации. *Предоставление информации* - действия, направленные на получение информации определенным кругом лиц или передачу информа-



ции определенному кругу лиц. *Распространение информации* – те же действия, только для неопределенного круга лиц.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию (п. 2. ст. 10 149-ФЗ). Если есть возможность определить получателя информации, то лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации (п. 3. ст. 10 149-ФЗ).

Важнейший способ поддержания правопорядка в цифровой сфере – это исключение анонимности участников цифрового взаимодействия. Предусматриваются процедуры определения лиц (идентификация и аутентификация) и информационных ресурсов по доменному имени и сетевому адресу.

*Идентификация* - совокупность мероприятий по установлению сведений о лице и их проверке и сопоставлению данных сведений с уникальным обозначением, необходимым для определения такого лица.

*Аутентификация* - совокупность мероприятий по проверке лица на принадлежность ему идентификатора.

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

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

### ***Контрольные вопросы:***

1. В чем состоит государственное регулирование в сфере информационных технологий?

2. Кем устанавливаются правила формирования и ведения реестра российского программного обеспечения?
3. Как устанавливается ограничение доступа к информации?
4. В чем различие между распространением информации и предоставлением информации?
5. В чем различие между идентификацией и аутентификацией лица?
6. Какие требования предъявляются к информации, распространяемой без использования средств массовой информации?
7. В чем состоит отличие идентификации и аутентификации?

### **Тема 5. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ ЭКОНОМИКИ**

В разгар мирового финансового кризиса 2008 года в одном малоизвестном электронном журнале под псевдонимом была опубликована небольшая статья с формулами и блок-схемами, написанная по всем правилам научной публикации, которая положила первую криптовалюту биткоин, что стало начало эпохи криптовалют.

Неизвестный автор предложил алгоритм, который потенциально ставил под вопрос основные принципы функционирования и само существование современной мировой финансовой системы с банками, страховыми компаниями, государственными регуляторами. Функцию поддержания порядка в финансовой сфере брал на себя алгоритм и практически бесплатно. Это наиболее яркий пример проникновения кибернетики в экономику. Только этот пример обосновывает необходимость киберправа.

К моменту написания статьи программная реализация биткоина уже существовала и всем желающим можно было присоединиться, что и произошло. Первые несколько лет проблема активно обсуждалась специалистами, но носила малозначительный характер. Яркие проявления датированы 2017 и 2021 годами, когда обменный курс возростал в разы за корот-

кий промежуток времени (полгода), что привлекло внимание не только профессиональных финансовых спекулянтов, но обычных людей. Для такой деятельности не обязательно получать специальные разрешения.

Необходимо различать биткоин и блокчейн. *Биткоин* - одна из криптовалют, которых уже тысячи, хотя самая крупная. Капитализация составляет примерно 1 трлн долларов США.

*Блокчейн* (blockchain – цепочка блоков) – это технология, алгоритм, лежащий в основании всех криптовалют. Полное и более правильное название блокчейна (distributed ledger technology - DLT) – технология распределенного реестра. *Криптовалюты* – применение этой технологии в финансовой сфере. Но эта технология может применяться и во многих других сферах, в том числе и сфере государственного регулирования правового обеспечения. Наибольшую угрозу получил институт нотариата. Блокчейн буквально заменяет нотариуса, но быстрее, дешевле и надежнее. Технически, но не юридически.

Актуальность в финансовой сфере технология блокчейн приобрела буквально несколько лет назад. Основным посылом послужила возможность привлечения инвестиций на глобальном рынке финансового капитала. Особый прогресс в сфере инвестиций показывало увеличение объемов ICO (первичное размещение коинов), темпы которого превышали IPO (первичное размещение бумаг). IPO – традиционный способ привлечения инвестиций путем продажи акций предприятия. Эта сфера хорошо отрегулирована законодательством. В случае с ICO речь идет о привлечении инвестиций путем продажи коинов – виртуальных денег или токенов – виртуальных акций.

Финансовым регуляторам уже нет возможности просто отмахиваться, и наступил период имплементации – включения криптовалют в сферу правового обеспечения. Хронологически сначала был определен механизм оборота криптовалют законом 259-ФЗ (2019), а только потом легализация –

259-ФЗ (2020). Российское законодательство не использует термины «блокчейн», «криптовалюта», «криптовбиржа», «коины», «токены», а вводит термины на русском языке. Термины получаются более громоздкие, из нескольких слов и их значение не абсолютно совпадает с англоязычными аналогами. Это нормально. Разночтения возникают всегда при вводе явления в новое для него правовое окружение.

При легализации криптовалют возникает необходимость преодолеть особенности, которые оцениваются регулятором как негативные.

Первое – сила воздействия на финансовую систему государства. Быстрый и неконтролируемый приток или отток больших финансовых ресурсов способен привести к дестабилизации денежной системы государства, дает возможность для нерыночных воздействий на экономику или отдельные отрасли, а также финансовых спекуляций глобального масштаба.

Поэтому запрещено использовать криптовалюту как средство платежа на товары и услуги предприятий и организаций Российской Федерации. Это соответствует норме Конституции, где указано, что рубль является единственным средством платежа на территории Российской Федерации. То есть вначале следует конвертировать криптовалюту в рубли, которые и использовать для расчета. Обратная операция – расплата за полученные товары и услуги с зарубежными предприятиями и организациями, нерезидентами – разрешена.

*Резидент* – это гражданин другого государства, который проживает легально длительное время (в сумме не менее 183 дней за последний год) в данном государстве. Для резидентов и нерезидентов водится различный правовой режим, комплекс прав и обязанностей. Например, резидент должен платить налоги в стране пребывания. В обмен он обладает преимуществом в других сферах. Нерезидент может принимать оплату в криптовалюте, а резидент – нет.

С 1 января 2021 года вступили в силу большинство норм закона 259-ФЗ (2020), который содержит правила выпуска цифровых финансовых активов и оборота цифровой валюты. Закон определяет цифровые финансовые активы как цифровые права, включающие, среди прочего:

- денежные требования;
- возможность осуществлять права по эмиссионным ценным бумагам;
- права участия в капитале непубличного АО.

Таким образом, термин «цифровые финансовые активы» (ЦФА) объединяет в себе и коины (единицы учета стоимости, напоминающие деньги) и токены (единицы учета прав, напоминающие акции). Аналог термина «блокчейн» - распределенный реестр.

В российском праве и акции, и цифровые финансовые активы существуют только в форме записей. Это позволяет избежать многих криминальных явлений в этой сфере. В законе указывается, что «выпуск, учет и обращение ЦФА возможны только путем добавления записей в информационную систему на основе распределенного реестра, а также в другие системы».

Если права собственности на обычные акции регистрируются в обычном реестре (книге учета), который ведет специализированная организация – реестродержатель, за счет акционерного общества, то в случае с ЦФА только путем добавления записей в информационную систему на основе распределенного реестра. Это основное требование. Возможно ведение учета в других информационных системах, но только как дополнение, а не в качестве замены распределенного реестра (технологии блокчейна).

Особо выделяется первый обладатель ЦФА. Права, удостоверенные ЦФА, будут возникать у их первого обладателя с момента внесения в систему записи о зачислении ему таких активов. Эти записи смогут вносить индивидуальный предприниматель и юридические лица.

Вид и объем прав, которые удостоверяются ЦФА, нужно назвать в решении об их выпуске. ЦФА учитываются в системе их выпуска. По общему правилу записи о ЦФА можно вносить или изменять по указанию эмитента этих активов и их обладателя.

Банк России уже определил, в частности, признаки ЦФА, которые вправе покупать только квалифицированные инвесторы.

В законе нет закрытого списка сделок, которые можно будет совершать с ЦФА. Однако упоминаются, в частности, купля-продажа ЦФА, а также обмен ЦФА одного вида на такие же активы другого вида.

Сделки потребуются заключать через оператора обмена ЦФА. Им могут стать банки, организаторы торговли и другие юрлица. Они должны быть в реестре таких операторов.

Закон вместо термина «криптовалюта» содержит другой - «цифровая валюта». Его определение довольно громоздкое, поэтому следует выделить основные детали:

- цифровая валюта - это совокупность электронных данных (цифрового кода или обозначения) в системе;

- их можно принять как инвестиции или средство платежа, который не является денежной единицей;

- в отношении цифровой валюты по общему правилу нет лица, обязанного перед каждым обладателем таких электронных данных.

Цифровая валюта является имуществом. Об этом говорится в Законе о банкротстве и в Законе об исполнительном производстве.

Второй момент – а н о н и м н о с т ь . Это качество криптовалют, схожее с наличными деньгами, вызывает критику как возможность ухода от налогов, отмывания средств, полученных преступным путем, финансирования терроризма. Закон устанавливает меры по преодолению этого качества.

Лица смогут предъявлять свои требования, связанные с обладанием цифровой валютой, смогут защитить свои права в суде, только если они

сообщили о том, что у них есть такая валюта и они совершали с ней сделки, операции. Анонимные обладатели цифровой валютой не смогут воспользоваться судебной защитой.

В Законе о рекламе прописан запрет распространять сведения о предложении и приеме цифровой валюты как способе оплаты товаров, работ и услуг.

Новое явление современности – стартапы (StartUp). Стартап – это возникающее или только возникшее предприятие, часто создаваемое одним или небольшой группой людей. Большинство разоряется, но некоторых сопровождает быстрый успех. Все современные гиганты информационной индустрии возникли как стартапы: «Apple», «Google», «Facebook», «Amazon», «Twitter». Флагманы софтверной индустрии калибром поменьше также начинали с малого.

Стартапы создаются молодыми людьми при практически полном отсутствии финансирования. Первое время существуют на чистом энтузиазме создателей. Такие предприятия остро нуждаются в финансовых ресурсах для своего развития. Банки неохотно дают кредиты, по причине высокой рискованности.

Кроме того, кредиты сопровождаются большим количеством условий, но самое главное – их надо возвращать. Альтернативный вариант – это инвестиции, когда инвестор разделяет с создателями риски неудачи проекта. В этом случае оптимальным, менее рискованным является финансирование нескольких проектов, чем вкладывать все деньги в один.

Сформировался альтернативный вариант привлечения средств, который получил название «краудфайдинг» (crowdfunding). Это повторение исторического института сбора пожертвований, но при использовании цифровых технологий и возможности получения выгоды, что объединило процедуры пожертвований и инвестирование.

Подобная форма финансирования в цифровой среде быстро приобрело организованный характер. Возникли виртуальные посредники, получившие название «криптовбиржи» (инвестиционные платформы), где, с одной стороны, размещаются описания идей и проектов, а другой стороны, потенциальные инвесторы имеют возможность выбрать и профинансировать идею, которая вызвала интерес.

Привлечение инвесторов для финансирования стартапов с использованием инвестиционных платформ в настоящее время приобретает массовый характер, но нуждается в правовом обеспечении. Для правовой системы – это новое явление, однако напоминает создание акционерного общества, которое хорошо проработано, обеспечено нормативной базой.

В данной теме будет рассматриваться правовое обеспечение цифровых технологий по привлечению инвестиций, прежде всего Федеральный закон от 02.08.2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее - 259-ФЗ (2019)).

Следует отметить, что Гражданским кодексом РФ введены и легализованы цифровые права - обязательственные и иные права, отвечающие установленным законом признакам, для которых содержание и условия осуществления определяются в соответствии с правилами информационной системы. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу.

Если иное не предусмотрено законом, обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность распоряжаться этим правом. В случаях и по основаниям, которые предусмотрены законом, обладателем цифрового права признается иное лицо. Переход цифрового права на основании сделки не требует согласия лица, обязанного по такому цифровому праву.



Закон направлен на поддержание правопорядка, защиту прав как инвесторов, так и получателей инвестиций, стремится найти баланс между объемом дозволенного и запрещенного, поддержать прогресс, развитие экономики, но при этом снизить риски.

Любое новое явление в сфере экономики сопровождается проблемами, сопрягающимся со статьей 159 УК РФ «Мошенничество». Так как инвестор и получатель лично не встречаются, никакие бумаги не подписываются, удостоверение личности происходит дистанционно и в электронной форме, возникает очень большой соблазн получить деньги и исчезнуть. Чтобы урегулировать этот процесс, обеспечить правопорядок, стимулировать привлечение инвестиций, развивать экономику, но при этом не допускать мошенничества, направлен указанный закон.

Основной метод реализации – сделать процесс привлечения средств открытым, публичным, честным, надежным, но под присмотром государства и его правоохранительных органов и финансовых регуляторов. Основное внимание направлено на запреты, не на получение разрешений у чиновников, а на то, чтобы в случае возникновения проблем или споров быстро и точно определить участников, определить виновного. Чтобы судебный процесс по разрешению спора проходил быстро, точно и справедливо.

259-ФЗ (2019) регулирует только цифровой способ привлечения инвестиций, то есть при использовании инвестиционных платформ. Для остальных случаев существуют другие законы, например 39-ФЗ «О рынке ценных бумаг». Для начала необходимо разобраться с новой терминологией для обозначения субъектов, объекта и содержания правоотношений в этой области. Понятия «информационная система» используется в значении, указанном в 149-ФЗ.

Следует рассмотреть основные понятия, которые введены 259-ФЗ (2019).

*Инвестиционная платформа* - информационная система в информационно-телекоммуникационной сети Интернет, используемая для заключения с помощью информационных технологий и технических средств этой информационной системы договоров инвестирования, доступ к которой предоставляется оператором инвестиционной платформы. Внешне это выглядит как интернет-сайт, напоминающий электронный магазин, через который совершаются сделки по приобретению токенов, то есть по осуществлению инвестиций.

*Инвестиции* - денежные средства, используемые в целях получения прибыли или достижения иного полезного эффекта путем приобретения ценных бумаг или цифровых прав либо путем предоставления займа. Происходит конвертация денег в цифровые финансовые активы, которые предусмотрены 259-ФЗ (2019). Также необходимо обратить внимание, что это не кредитование. Займ и кредит в Гражданском кодексе имеют разное значение. Займ имеет более широкое содержание. Кредит – частный случай займа.

Сам сайт не может быть бесхозным, то есть не безответственный. Вводится субъект, который отвечает за функционирование информационной системы по привлечению инвестиций. Это - оператор инвестиционной платформы - хозяйственное общество, осуществляющее деятельность по организации привлечения инвестиций. То есть это организация, хозяйственное общество (не товарищество, не кооператив, а только общество с ограниченной ответственностью или акционерное общество). Все операторы должны быть включены в реестр операторов инвестиционных платформ, который ведет Банк России, что перекрывает возможность возникновения мошеннических сервисов.

Оператор инвестиционной платформы оказывает услуги по содействию в инвестировании двум категориям клиентов: инвесторам и лицам, получающим инвестиции. Инвестором может быть гражданин (физическое лицо) или организация (юридическое лицо). В качестве лица, привлекаю-

щего инвестиции, обычный гражданин выступать не может. Только в статусе индивидуального предпринимателя.

В качестве объекта правоотношения выступают цифровые права, которые могут приобретаться, отчуждаться и осуществляться в инвестиционной платформе, или утилитарные цифровые права. Утилитарное – значит полезное. Цифровые права могут существовать только в цифровом пространстве. Утилитарные цифровые права – это перемещение цифровых прав в реальный мир, в сферу, где действует институт собственности.

К утилитарным цифровым правам относятся:

- 1) право требовать передачи вещи (вещей);
- 2) право требовать передачи исключительных прав на результаты интеллектуальной деятельности и (или) прав использования результатов интеллектуальной деятельности;
- 3) право требовать выполнения работ и (или) оказания услуг.

В первом пункте имеются в виду, прежде всего, изделия, на создание которых собираются деньги (особый гаджет), или деньги, другие материальные объекты, ценные бумаги и много другое, которые по гражданскому праву являются разновидностями вещей (ст. 128 ГК РФ).

Деятельность платформы понимается как оказание услуг с использованием инвестиционной платформы двух видов: по содействию в инвестировании и по привлечению инвестиций.

Содействие в инвестировании – клиентом выступает инвестор. В случае привлечения инвестиций – заказчиком выступает соискатель финансирования. Например, стартап. Лицо, привлекающее инвестиции, формулирует оферту - предложение заключить с ним договор инвестирования или инвестиционное предложение. Это предложение должно сопровождаться развернутым описанием проекта и обязательств перед инвестором.

Целью и результатом работы инвестиционной платформы является заключение договора инвестирования - договора между инвестором и лицом,

привлекающим инвестиции, по которому осуществляется инвестирование. Обязательно способами, предусмотренными Федеральным законом.

Закон предусматривает, что в работе инвестиционной платформы можно участвовать дистанционно, через устройства, на которых установлено соответствующее программное обеспечение или мобильное приложение. В формулировке закона, мобильное приложение – это программное обеспечение, применяемое физическими лицами с использованием технического устройства (мобильного телефона, смартфона или компьютера, включая планшетный компьютер), подключенного к информационно-телекоммуникационной сети Интернет, для доступа к инвестиционной платформе.

Закон достаточно подробно определяет ответственность, подконтрольность, прозрачность инвестиционной платформы. Здесь необходимо вспомнить о положении 149-ФЗ о распространении и предоставлении информации. Распространение – это предоставление информации неопределенному кругу лиц, что соответствует рекламе. 259-ФЗ (2019) использует более узкий термин из закона «О рынке ценных бумаг». Раскрытие информации - это предоставление информации все тем, кто проявил интерес. В отличие от рекламы, такая информация не навязывается.

Оператор инвестиционной платформы обязан осуществлять раскрытие информации о работе платформы, то есть обеспечение доступности информации неопределенному кругу лиц путем размещения информации в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте, владельцем которого является оператор инвестиционной платформы. Познакомиться с общими сведениями по деятельности инвестиционной платформы должны иметь возможность все желающие.

Оператор инвестиционной платформы отчитывается по своей деятельности перед Центральным банком Российской Федерации (Банк России). Он обязан представлять отчеты об осуществлении деятельности по органи-

зации привлечения инвестиций в порядке, форме и сроки, которые установлены нормативными актами Банка России. За нарушение при исполнении этой обязанности оператор может быть исключен из реестра операторов инвестиционных платформ.

Вносить инвестиционные предложения, заключать договоры, участвовать в работе инвестиционной платформы могут только зарегистрированные (идентифицированные) участники. Для них определен другой режим – предоставление информации. Предоставление информации оператором инвестиционной платформы - действия оператора инвестиционной платформы, направленные на получение информации участниками инвестиционной платформы и (или) передачу информации участникам инвестиционной платформы. Здесь уже не упоминается неопределенный круг лиц, информация предоставляется определенному кругу лиц.

Деятельность по организации привлечения инвестиций осуществляется на основании заключения трех видов договоров:

- договоров об оказании услуг по привлечению инвестиций;
- договоров об оказании услуг по содействию в инвестировании;
- договор инвестирования.

Договор об оказании услуг по привлечению инвестиций заключается оператором с лицом, привлекающим инвестиции (получателем средств), о предоставлении доступа к инвестиционной платформе, а договор об оказании услуг по содействию в инвестировании уже с инвестором о предоставлении доступа. Между собой инвестор и получатель инвестиций заключают договор инвестирования с помощью информационных технологий и технических средств инвестиционной платформы, которой управляет оператор. То есть путем манипуляций кнопками на мобильном устройстве. Быстро, надежно, без необходимости в личной встрече и бумажного оформления.

Закон допускает многообразные формы оплаты услуг оператора инвестиционной платформы. Можно предусмотреть, что:

- платят только соискатели инвестиций при получении доступа;
- платят только соискатели инвестиций при заключении каждого договора инвестирования;
- платят только соискатели инвестиций при достижении запланированного объема инвестирования;
- платят все (и соискатели, и инвесторы) при каждом действии;
- не платит никто, услуги оператора оплачиваются из других источников;
- другие варианты.

Но выбранные варианты оплат услуг оператора инвестиционной платформы должны быть прописаны в правилах инвестиционной платформы и быть едиными для всех участников.

Договор об оказании услуг по привлечению инвестиций и договор об оказании услуг по содействию в инвестировании являются договорами присоединения, условия которых определяются оператором инвестиционной платформы. Для всей участников должны быть единые правила, привилегированных быть не должно.

Очень важным требованием к инвестиционной платформе является недопущение анонимности и, как следствие, неправомерных действий, в том числе и уклонение от налогов. Оператор инвестиционной платформы обязан установить каждое лицо (инвесторов и соискателей инвестиций), с которым заключаются договоры об оказании услуг. При этом оператор инвестиционной платформы вправе пользоваться единой системой идентификации и аутентификации.

Инвестирование, финансирование проектов с использованием инвестиционной платформы обычным гражданином (неквалифицированным инвестором) может осуществляться следующими способами:

- путем предоставления займов;
- путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы (с исключениями);
- путем приобретения утилитарных цифровых прав;
- путем приобретения цифровых финансовых активов.

Исключением является приобретение ценных бумаг кредитных организаций, некредитных финансовых организаций, а также структурных облигаций и ценных бумаг, предназначенных для квалифицированных инвесторов.

Исходя из опыта финансовых пирамид, закон предусматривает ряд мер с целью не допустить существенных финансовых потерь для обычных граждан. Это удостоверение в понимании рисков и ограничение по сумме инвестиций. Оператор до заключения договора с инвестором - физическим лицом предоставляет подтверждение того, что он ознакомился с рисками, связанными с инвестированием, осознает, что инвестирование с использованием инвестиционной платформы является высокорискованным и может привести к потере инвестиций в полном объеме, и принимает такие риски.

Ограничение по сумме инвестиций состоит в том, что оператор инвестиционной платформы может предоставить возможность физическому лицу инвестировать в течение одного календарного года денежные средства в сумме не более 600 тысяч рублей.

Указанное ограничение не распространяется на индивидуальных предпринимателей и квалифицированных инвесторов, на сделки с публичным акционерным обществом. Признание физического лица квалифицированным инвестором осуществляется оператором инвестиционной платформы по заявлению гражданина.

Введены ограничения и для получателей инвестиций. Одно лицо в течение одного календарного года не может привлечь инвестиций на сумму,

превышающую один миллиард рублей. Для очень крупных проектов предназначен Закон «Об акционерных обществах».

Предполагается, что основным способом инвестирования с использованием инвестиционных платформ будет приобретение утилитарных цифровых прав. Это новое явление для правовой системы, которое следует рассмотреть подробнее.

Утилитарные цифровые права – аналог токена. Утилитарные цифровые права функционируют только в рамках инвестиционной платформы. Возникновение утилитарного цифрового права, его осуществление, распоряжение им, в том числе передача, залог, обременение утилитарного цифрового права другими способами, или ограничение распоряжения утилитарным цифровым правом возможны только в инвестиционной платформе.

В инвестиционной платформе могут приобретаться, отчуждаться и осуществляться следующие цифровые права (утилитарные цифровые права):

- право требовать передачи вещи (вещей);
- право требовать передачи исключительных прав на результаты интеллектуальной деятельности и (или) прав использования результатов интеллектуальной деятельности;
- право требовать выполнения работ и (или) оказания услуг.

Утилитарное цифровое право возникает у первого приобретателя, переходит от одного лица к другому лицу и (или) прекращается. Время совершения сделки - момент внесения информации об этом в инвестиционной платформе.

Оператор инвестиционной платформы обеспечивает всем участникам инвестиционной платформы техническую возможность приобретать утилитарные цифровые права при их обращении, знакомиться с их содержанием, осуществлять утилитарные цифровые права, а также распоряжаться ими.



Цифровые финансовые активы могут документироваться в форме цифровых свидетельств. *Цифровое свидетельство* - неэмиссионная бездокументарная ценная бумага, не имеющая номинальной стоимости, удостоверяющая принадлежность ее владельцу утилитарного цифрового права. Учет цифровых свидетельств осуществляет депозитарий, который также оказывает услуги по осуществлению утилитарного цифрового права и (или) распоряжения им определенным образом.

### ***Контрольные вопросы:***

1. В чем состоят цифровые права?
2. Каковы основные признаки цифровой валюты?
3. Является ли цифровая валюта имуществом?
4. Допускается ли оплата цифровой валютой товаров и услуг в РФ?
5. Каковы последствия анонимного обладания цифровой валютой?
6. Как определяется и характеризуется инвестиционная платформа?
7. Кто отвечает за функционирование инвестиционной платформы и каковы его обязанности?
8. Какие услуги оказывает инвестиционная платформа?
9. Какие виды договоров предусмотрены для инвестиционной платформы?
10. Каково назначение и признаки утилитарных цифровых прав?

## **Тема 6. ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ**

Глобализация способствует перемещению производства в страны с более дешевой рабочей силой. Старые центры стремятся сохранить свое доминирующее положение, ставя в центр отношений интеллектуальную собственность. Рушатся устоявшиеся правовые институты, основанные на частной собственности на средства производства, на их место приходят новые, основанные на авторском праве и интеллектуальной собственности.

Результаты творческой деятельности в области программирования, конструирования новых устройств (гаджетов), нуждаются в правовой защите, прежде всего на международном уровне, чтобы сохранить блага, вытекающие из авторства изобретений и разработок новых технологий.

Создание новых знаний, идей, решений, патентов в условиях хозяйственного уклада индустриального общества было построено по образцу промышленного производства. Основными продуцентами выступали крупные специализированные организации: научно-исследовательские институты, конструкторские бюро, которые по своей организационной структуре повторяют промышленные предприятия.

Промышленные предприятия обладают характерными признаками. Это иерархия в управлении, разделение функций, наличие организационных структур (цеха, участки, бригады), планирование, определение заданий и сроков, отчетность, а также разработанная система измерения усилий и результатов, определения вознаграждения и мер стимулирования.

Постиндустриальный уклад не сильно изменил организацию интеллектуальной сферы. В значительной степени сохранились черты индустриальной организации. Несмотря на то, что возникли новые процессы в области производства знаний, связанные со сферой обслуживания, они не имели определяющего значения. Система закрепления прав на объекты интеллектуальной собственности в форме патентования и способы оборота таких прав не претерпели существенных изменений.

Становление информационного общества, основанного на развитии компьютерной техники, создании прорывных информационных технологий, показывает не соответствие индустриальных и постиндустриальных подходов к новым условиям.

Новации последних десятилетий связывают с очень небольшими коллективами, созданными на неформальной основе, а иногда одиночками. Инициаторами возникновения «Apple» было трое молодых людей, «Micro-

soft» и «Google» – двое. Создание «Facebook» и HTML (основы web-технологий) связывают с именем и идеями одного человека. Примеры «Instagram», «Twitter», «WhatsApp», «Uber» демонстрируют как результаты усилий небольшой группы людей, без использования тяжелого промышленного оборудования, только применяя универсальные компьютеры, позволяют создавать нечто, что впоследствии было оценено весьма значительными суммами. Об этом говорят суммы по приобретению прав на успешные программные продукты.

Для современной интеллектуальной деятельности характерно следующее: нет управляющей надстройки, иерархии и планирования, не привлекаются значительные финансовые и материальные ресурсы. Проект возникает и реализуется в значительной степени на энтузиазме инициаторов, а основным ресурсом являются специальные знания.

Более того, что удивительно для образа мыслей индустриальной эпохи, полученный продукт предоставляется потребителям бесплатно, но это оказывается выгодным. Пользование мощнейшими информационными системами «Google», «Facebook», «Instagram», «YouTube» для обычного человека представляется совершенно бесплатным. Однако доходы извлекаются. Причем очень большие, о чем свидетельствует размер капитализации компаний, которые этими информационными ресурсами владеют.

Для сохранения доминирующего положения в условиях существующих правовых систем таким компаниям необходимы два компонента. Первый - закрепление за собой интеллектуальных прав на созданные информационные продукты, что связано с институтом интеллектуальной собственности. Второй - постоянно совершенствовать, развивать продукты и закреплять за собой права на новые продукты, на результаты интеллектуальной деятельности. Это также связано с институтом интеллектуальной собственности. Быстрая фиксация приоритета путем получения патентов или другими способами обозначения принадлежности интеллектуальных

прав позволяет активно привлекать дополнительные финансовые средства и ресурсы для развития компаний.

Нормы правового обеспечения интеллектуальной собственности содержатся в четвертой части Гражданского кодекса Российской Федерации. Вводится понятие «интеллектуальные права», которое включает права авторства, исключительные права и патентные права. Права авторства принадлежат автору результата интеллектуальной деятельности. Права авторства неотчуждаемы и непередаваемы. Отказ от этих прав ничтожен. Авторство и имя автора охраняются бессрочно.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произведения, публичного исполнения и иной подобной форме), в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 ГК РФ.

Для результатов интеллектуальной деятельности, претендующих на статус изобретения, предусмотрена процедура регистрации или патентование, целью которой является признание патентных прав. В случае успешного патентования изобретению предоставляется правовая охрана, если определено, что заявленное техническое решение является новым, имеет изобретательский уровень и промышленно применимо.

В качестве изобретения признается техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу

(процессу осуществления действий над материальным объектом с помощью материальных средств).

Не могут быть объектами патентных прав: 1) способы клонирования человека и его клон; 2) способы модификации генетической целостности клеток зародышевой линии человека; 3) использование человеческих эмбрионов в промышленных и коммерческих целях; 4) результаты интеллектуальной деятельности, если они противоречат общественным интересам, принципам гуманности и морали.

Коммерческий интерес вызывают исключительные права, которые в отличие от прав авторства отчуждаемы и с ними можно совершать сделки, заключать договоры. Исключительное право на результат интеллектуальной деятельности первоначально возникает у его автора. Лицо, которому автор передал исключительное право, именуется как правообладатель. Правообладатель может по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности.

Правообладатель может распорядиться принадлежащим ему исключительным правом, в том числе путем его отчуждения по договору другому лицу (договор об отчуждении исключительного права) или предоставления другому лицу права использования соответствующих результатов интеллектуальной деятельности в установленных договором пределах (лицензионный договор). Стороны лицензионного договора - лицензиар (правообладатель) и лицензиат (получатель лицензии). Заключение лицензионного договора не влечет за собой переход исключительного права к лицензиату.

Существующая система патентования, регистрации авторских и исключительных прав на результаты творческой деятельности соответствует индустриальному укладу, не соответствует условиям информационного общества. Однако отказываться от сложившихся механизмов правового обеспечения интеллектуальной деятельности преждевременно.

Следует отметить, что область охраняемых правом результатов интеллектуальной деятельности ограничена. В рамках российской правовой системы авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты и другое (п. 5 ст. 1259 ГК РФ). Однако это не означает, что подобные результаты интеллектуальной, творческой деятельности не нуждаются в правовой защите.

Всемирная организация интеллектуальной собственности (ВОИС) признает в качестве охраняемых результатов творческой деятельности также научные открытия, научные теории, математические методы, открытия природных веществ, методы медицинского лечения. Список является открытым. Добавлена оговорка, что в него включаются все другие права, относящиеся к интеллектуальной деятельности в производственной, научной, литературной и художественной областях. Подобное положение не имплементировано в российское законодательство. Однако оно нуждается, по крайней мере, в общественной поддержке.

Существующие другие способы фиксации прав на результаты интеллектуальной деятельности, такие как нотариальная надпись или депозитарий по примеру Библиотеки Конгресса США, не справляются с все возрастающей нагрузкой как по объему, так и по многообразию объектов интеллектуальной собственности, а также по скорости и надежности регистрации.

Быстрое развитие социальных сетей и легкость создания контента в форме изображений, коротких сообщений, видеороликов, можно охарактеризовать как появление огромного количества объектов интеллектуальной собственности, которые могут быть быстро распространены через сеть Интернет, в том числе с нарушением норм права. Регистрация прав на объекты интеллектуальной собственности проводится в разных странах по бюрократической схеме, в то время как институт интеллектуальной собственности должен развиваться вместе с научно-техническим прогрессом.

Существующие, предусмотренные правом, процедуры в области авторского и патентного права имеют недостатки. Во-первых, не покрывают все многообразие объектов интеллектуальной собственности, особенно имеющих цифровую форму. Во-вторых, имеют высокую стоимость регистрации, чрезмерную для современных условий продолжительность регистрации технических решений (патентное право) и сложности защиты интеллектуальных прав. В-третьих, существует проблема быстрого и надежного определения достоверности факта обладания при оформлении сделок по реализации интеллектуальной собственности (отчуждение исключительных прав, лицензирование).

Многообразие сделок с интеллектуальной собственностью приближается к многообразию сделок в материально-вещественной сфере. Патентное ведомство и система нотариата явно нуждаются в поддержке современными информационными технологиями.

Интересы авторов, инвесторов, а также организаторов интеллектуальной деятельности остро нуждаются в механизмах фиксации прав интеллектуальной собственности, учета и согласования интересов. Использование информационных технологий позволяет делать это быстро.

Если законодательство не всегда успевает с формированием правового обеспечения новых форм отношений в сфере интеллектуальной деятельности, то это не может служить препятствием для создания других средств информационной и организационной поддержки, создания новых систем учета, стимулирования сделок, оформления реализации прав на результаты интеллектуальной деятельности, распределения вознаграждения.

Необходимо искать новые формы сопровождения интеллектуальной деятельности, определения и обеспечения баланса интересов сторон: автора (правообладателя), инвестора (приобретателя) и организатора (посредника), обеспечивая при этом их права в полной мере.

Требуется технология, способная если не вытеснить, то существенно дополнить бюрократический подход. Технология должна обладать компактностью, экономичностью и надежностью, действовать автоматически, без посредников, децентрализовано, проверяемо, надежно, без возможности внесения последующих исправлений. При этом имела бы высокую достоверность, юридическую значимость. Также необходимо реализовать такие качества, как доступность и экономичность при создании и функционировании.

Технология, которая обладает необходимыми достоинствами и возможностями, существует. Это технология распределенного реестра или блокчейн. Указанная технология широко применяется и уже в достаточной степени проявила свои возможности, достоинства и недостатки. С одной стороны, она обладает такими качествами, как децентрализация, неизменность, отсутствие посредника, достоверность, проверяемость, имеет глобальный характер, но с другой стороны, с трудом поддается масштабированию.

Алгоритм, лежащий в основе технологии распределенного реестра, не сложный и основан на применении функции хеширования, расчета хеш суммы файла. Но, главное, этот алгоритм сочетается с существующим порядком, с таким понятием, как «документ».

«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» (Федеральный закон «Об обязательном экземпляре документов» от 29.12.1994 г. № 77-ФЗ 3, ст. 2).

Практически любой результат интеллектуальной деятельности подлежит документированию. В цифровом пространстве эквивалентом документа является файл. Файл может содержать все, что подлежит оцифровке,



превращению в последовательность битов. Но в отличие от бумажного документа, содержимое файла легко можно изменить. Поэтому существует проблема определения достоверности файла. Решением данной проблемы и является использование технологии распределенного реестра.

Распределенный реестр - это новая технология, способная вытеснить бюрократический подход. Несмотря на то, что впервые широкое распространение и использование данной технологии осуществлялось для регистрации транзакций первой криптовалюты – биткойна, в настоящее время раскрываются более широкие возможности для применения, в том числе и в сфере интеллектуальной собственности.

Разработку приложений на основе технологии распределенного реестра можно разделить на три основных этапа: версии 1.0, 2.0 и 3.0. Версия 1.0 использовалась для криптовалют, и его целью было облегчить простые транзакции денежных средств. Версия 2.0 поддерживала «умные» (smart) контракты, контролируемые особые условия и критерии, которые должны быть выполнены прежде, чем транзакция будет зарегистрирована в реестре, то есть пройдет платеж. Регистрация в распределенном реестре происходит без вмешательства третьей стороны. В версии 3.0 реализуются многочисленные возможности применения технологии распределенного реестра в других сферах, таких как государственное управление, здравоохранение, наука и образование, в том числе и в сфере управления интеллектуальной собственностью.

Примером для создания подобной системы могут выступить положения 259-ФЗ (2019), рассмотренные в предыдущей теме учебного пособия. Этот закон создает правовое окружение для применения технологии распределенного реестра для целей финансирования. Если адаптировать некоторые положения закона и дополнить новым объектом правоотношений, а именно интеллектуальные цифровые права, то вполне возможно создать систему правовой охраны и управления интеллектуальной собственностью.

стью, не противоречащую существующему законодательству и соответствующую тем требованиям, которые указаны выше.

Эффективное управление правами интеллектуальной собственности является важным аспектом обеспечения экономической безопасности предприятий, регионов, государства и объединений государств. Помимо общеизвестных макроэкономических и микроэкономических функций, регистрация прав на объекты интеллектуальной собственности создает новый экономический фактор - систему управления, стимулирования и применения интеллектуального капитала общества.

### ***Контрольные вопросы:***

1. В каком законе содержатся нормы правового обеспечения интеллектуальной собственности?
2. Что включается в понятие «интеллектуальные права»?
3. Что признается в качестве изобретения?
4. Что не может быть объектом патентных прав?
5. Как именуется стороны лицензионного договора?

## **Тема 7. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ**

Основопологающим документом, определяющим позиции в вопросах построения кибербезопасности, была принятая в сентябре 2000 года «Доктрина информационной безопасности Российской Федерации». Обновленная версия документа датирована 5 декабря 2016 года.

Доктрина является документом стратегического планирования, основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Среди основных интересов Российской Федерации в киберпространстве выделяют положения о стремлении государства обеспечить возможность гражданам, организациям и органам государственной власти беспрепятственно взаимодействовать в электронном пространстве, обеспечить гарантии стабильности информационной среды, а также способствовать развитию национальной технологической базы.

Наиболее значимой характеристикой информации в Доктрине выделяется ее достоверность, которая может быть нарушена из-за угроз исходящих из информационной сферы.

*Информационная сфера* - совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

В Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Обеспечение информационной безопасности – это осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Важнейшим защищаемым объектом в Доктрине признается информационная инфраструктура. Информационная инфраструктура Российской Федерации - совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

С целью обеспечения информационной безопасности требуется, чтобы информационные системы, связанные с государственной или служебной тайной, не могут быть подключены к сети Интернет. Если же существует необходимость такого подключения, то обязательно применение сертифицированных средств защиты информации, в том числе шифровальных (криптографических). Сертификацию проводит Федеральная служба безопасности Российской Федерации, подтверждение соответствия - Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Особое место при обеспечении информационной безопасности занимает защищенность персональных данных. Как обеспечение из достоверности, так и обеспечение ограничения доступа.

К персональным данным относится как любая информация о конкретном лице, так и информация, с помощью которой лицо можно идентифицировать, то есть установить.

К таким данным относятся:

– фамилия, имя, отчество;

- пол, возраст;
- образование, квалификация, профессиональная подготовка и сведения о повышении квалификации;
- место жительства;
- семейное положение, наличие детей, родственные связи;
- факты биографии и предыдущая трудовая деятельность (место работы, размер заработка, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.);
- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

В соответствии со ст. 9 ФЗ № 152 обработку персональных данных осуществляет оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора.

### ***Контрольные вопросы:***

1. В каком документе определяется и характеризуется информационная безопасность Российской Федерации?
2. Что входит в состав информационной инфраструктуры Российской Федерации?
3. Как обеспечивается безопасность информационных систем, связанных с государственной или служебной тайной?
4. Что является персональными данными?
5. Как осуществляется обработка и защищенность персональных данных?

### **Тема 8. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ**

Юридическая ответственность понимается как обязанность лица претерпевать определенные лишения государственно-властного характера, предусмотренные законом, за совершенное противоправное деяние.

Юридическая ответственность всегда связана с государственным принуждением, которое выступает ее содержанием. *Государственное принуждение* – это воздействие на поведение людей, основанное на его организованной силе.

Характерная особенность такого принуждения – это принуждение к исполнению конкретных правовых норм. Кроме того, такая деятельность строго регламентирована. Субъектами этой деятельности являются государство в лице правоохранительных органов, суд, прокуратура, а также администрации различных государственных учреждений, которые занимаются рассмотрением правонарушений.

В российской правовой системе существуют следующие виды юридической ответственности: дисциплинарная, гражданско-правовая, административная и уголовная. Ответственность в случае плагиата не является

юридической, а носит социальный, общественный характер и выражается в репутационных, в том числе статусных потерях для автора.

Дисциплинарная ответственность информационных работников не отличается от дисциплинарной ответственности других сотрудников, регулируется нормами трудового права с учетом специфики труда в информационной сфере. К дисциплинарной ответственности примыкает материальная ответственность информационных работников, где действуют те же правовые нормы, как и в трудовом праве.

Гражданско-правовая ответственность в сфере информационных отношений – наиболее активно разрабатываемое направление правового регулирования в настоящее время. В то время, как общие основания гражданско-правовой ответственности – денежное возмещение вреда, убытков и ущерба остаются неизменными, то методы определения потерь, вины и меры ответственности совершенствуются с учетом возможностей информационно-коммуникационных технологий. Одним из вопросов является признание за виртуальными валютами реальной ценности.

Указанная ответственность заключается в применении установленных законом или договором мер воздействия, влекущих для виновного неблагоприятные последствия имущественного характера — возмещение убытков, уплату неустойки (штрафа, пени), возмещение вреда.

Административная ответственность в области связи и информации – наиболее разработанная область государственного принуждения, целью которого является обеспечение гарантий конституционных прав граждан на неприкосновенность связи, переписки и других форм обмена информацией. Основная область административного регулирования, сфера действия административных норм – это техническая составляющая информационных систем и технологий, методы, средства и процедуры обеспечения защиты информации, информационная безопасность.

К административным правонарушениям относятся: нарушение сбора, использования, хранения и распространения персональных данных, правил защиты информации; незаконная деятельность в сфере защиты информации; разглашение информации, относящейся к данным ограниченного доступа; злоупотребление информацией, свободной и массовой; воспрепятствование распространению, нарушение порядка изготовления продукции СМИ; нарушение правил распространения сообщений, предоставления статистической информации; нарушение правил комплектования, хранения, использования и учета цифровых архивных документов, порядка объявления выходных данных и др.

За административные правонарушения в информационной сфере предусмотрены следующие виды наказаний: предупреждение, административный штраф, изъятие или конфискация предмета и орудия совершения административного правонарушения, административный арест, выдворение за пределы РФ, дисквалификация.

Уголовная ответственность в сфере компьютерной информации включает в себя несколько составов преступлений. Это неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Особо выделяется и защищается уголовным законом критическая информационная инфраструктура Российской Федерации.

К уголовно наказуемым действиям в информационной сфере относятся: неправомерный доступ к цифровой информации (ст. 272 УК РФ); использование и распространение, создание вредоносных (вирусных) программ (ст. 273 УК РФ); нарушение правил эксплуатации компьютерного оборудования и сетей (ст. 274 УК РФ).



Правоохранительные и специальные органы в сфере связи и информации включают в себя прокуратуру, федеральную службу безопасности, следственный комитет, полицию, а также Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Прокуратура - единая федеральная централизованная система органов, осуществляющих от имени Российской Федерации надзор за соблюдением Конституции Российской Федерации и исполнением законов, действующих на территории Российской Федерации.

Следственный комитет - федеральный государственный орган, осуществляющий в соответствии с законодательством Российской Федерации полномочия в сфере уголовного судопроизводства.

Федеральная служба безопасности – единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности Российской Федерации.

Органы внутренних дел (полиция) предназначены для защиты жизни, здоровья, прав и свобод граждан, для противодействия преступности, охраны общественного порядка, собственности и для обеспечения общественной безопасности. Полиция в пределах своих полномочий оказывает содействие федеральным органам государственной власти, органам государственной власти субъектов Российской Федерации, иным государственным органам, органам местного самоуправления, иным муниципальным органам, общественным объединениям, а также организациям независимо от форм собственности, должностным лицам этих органов и организаций в защите их прав.

Роскомнадзор осуществляет функции по контролю и надзору в сфере средств массовой информации и массовых коммуникаций, использования информационных технологий и некоторые другие функции.

### ***Контрольные вопросы:***

1. Как понимается юридическая ответственность?
2. В чем состоит характерная особенность юридической ответственности?
3. Какие существуют виды юридической ответственности?
4. В чем заключается и как реализуется гражданско-правовая ответственность в сфере информационных отношений?
5. Что относится к административным правонарушениями в области связи и информации?
6. Какие действия в информационной сфере являются уголовно наказуемыми?
7. Какие правоохранительные органы обладают полномочиями и осуществляют деятельность в информационной сфере?

## Раздел 2 ПОДГОТОВКА К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Самостоятельная работа состоит из двух частей: подготовки к практическим занятиям в форме семинара и создания контрольной работы в форме реферата. Реализовав указанные виды деятельности, магистрант должен усвоить знания, сформировать способность определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки, а также приобрести навыки по фиксации результатов творческой деятельности как своей, так и коллектива сотрудников, что позволит в будущем руководить отделом технического документирования.

Реформа системы высшего образования, вытекающая из необходимости усвоения все большего и большего объема информации при ограниченности аудиторных занятий, вызывает необходимость перемещения значительной части учебной работы в виртуальное пространство. Коммуникационные технологии позволяют это сделать с высокой эффективностью.

Аудиторные занятия дополняются использованием электронной информационной образовательной среды (ЭИОС), где развернута электронная версия дисциплины. Использование ЭИОС позволяет быстро актуализировать информацию, вносить коррективы в содержание дисциплины, подключать новые нормативно-правовые акты и их проекты, давать ссылки на обсуждение инициатив. Также ЭИОС позволяет организовать обратную связь, выдавать и получать индивидуальные задания, размещать тесты и программировать оценивание тестов, организовывать обсуждение интересных вопросов и проблем за пределами места и времени аудиторных занятий, что для магистрантов является весьма актуальным.

Для тех, кто стремится получить более глубокие знания, сопоставимые со знаниями элитных университетов, не запрещается записываться и проходить аналогичные массовые открытые онлайн-курсы, размещенные сер-

тифицированными учебными заведениями, получать сертификаты и удостоверения. Другим продвинутым средством повышения качества обучения и приобретения дополнительных навыков является разработка и использование собственной самостоятельно созданной образовательной среды, аналога научной сети, индивидуальной или коллективной.

Информационные ресурсы, накопленные в подобной среде, могут стать существенным конкурентным преимуществом при трудоустройстве, использоваться в профессиональной или предпринимательской деятельности, стать залогом жизненного успеха. Ценностью подобной системы является не столько накопленные сведения, которые достаточно быстро устаревают, сколько навыки по созданию и использованию подобной сети, классификации и упорядочиванию информации, определения достоверности и приоритетов, что существенно повышает способность к самоорганизации и самообразованию.

В качестве основы рекомендуется использовать существующие некоммерческие библиоменеджеры, интегрированные с облачными технологиями, на базе которых сформировались академические и профессиональные социальные сети. На настоящее время это наиболее доступное и функциональное средство для коллективного творчества в интеллектуальной сфере, на примере которых также можно рассматривать возможности правового обеспечения творческой деятельности и ее технологической поддержки.

В результате изучения дисциплины «Киберправо» студент должен продемонстрировать освоение указанных знаний умений и навыков по трем формам: 1) устные или письменные доклады на практических занятиях; 2) результирующая письменная работа; 3) тест и/или устный ответ на зачете. Факультативными средствами контроля знаний являются призовые места в студенческих смотрах конкурса, участие в научных конференциях, публикации в научных журналах, другие формы признания приоритета и закрепления результатов творческой деятельности.

Необходимо помнить, что помимо образовательных компетенций, существуют еще компетенции, проверяемые и удостоверяемые при профессиональной сертификации. Более подробно с требованиями можно познакомиться в профессиональных стандартах получаемой профессии.

Целью практических занятий, помимо направленных на усвоение универсальных и профессиональных компетенций, является формирование навыков в сфере использования информационных технологий.

- 1) поиск и селекция информации;
- 2) определение достоверности и значимости сведений, возможности их дальнейшего использования;
- 3) анализ (выделение отдельных сторон, частей, разделение);
- 4) синтез (агрегирование, структурирование, систематизация, классификация, логическое связывание, изложение и др.);
- 5) фиксация, документирование, в том числе приоритета и прав, изложение, публикация, апробация.
- 6) критика в форме публичного обсуждения или письменного рецензирования.

Результатом успешного выполнения практических занятий по дисциплине в учебном плане на хорошую или отличную оценку является: как минимум – выступление (доклад) на практическом занятии, как максимум – научная публикация. Идеальным является использование в профессиональной деятельности, но это происходит за пределами учебного процесса. Таким образом, смысл и назначение практических занятий – не только изложить результаты, но обменяться опытом по поиску, систематизации информации на примере изучения правовой системы информационного права. Само практическое занятие должно стать источником знаний.

Особое внимание при изучении информационного права уделяется привитию таких ценностей, которые противостоят незаконному использованию информации, а именно: прямому заимствованию, без необходимых

ссылок и отсылок к автору. Следует предостеречь и всячески противодействовать такой форме коррупции, как интеллектуальное пиратство или интеллектуальный паразитизм. Для этого необходимо усвоить навыки правильного цитирования, создания ссылок на первоисточник информации – своеобразной валюты научного мира.

### **Раздел 3 ПОДГОТОВКА КОНТРОЛЬНОЙ РАБОТЫ**

Письменная работа (семестровая работа, контрольная работа и реферат) является основным доказательством успешного изучения материалов учебной дисциплины, самостоятельной работы студента. В письменной форме закрепляются и демонстрируются полученные знания, степень усвоения учебного материала, правильность использования специальных терминов и понятий, умение находить и использовать сведения, найденные в дополнительной литературе, правильно, кратко, логично и последовательно оформлять результаты самостоятельной работы.

Письменная работа, прежде всего, представляет собой обзор устоявшихся, а также обсуждаемых, но признанных в научном сообществе гипотез, теорий, концептов, положений, выводов и определений в конкретной области знаний, по выбранной теме. Обзор должен быть изложен систематически, кратко и последовательно, обязательно содержать вывод.

Смысл письменной работы состоит в том, чтобы выделить только те сведения, которые относятся к теме письменной работы, систематизировать их, найти общее (результат), выразить все это в словесной форме и зафиксировать, то есть изложить в письменном виде и правильно оформить, продемонстрировать интеллектуальную культуру. Культуру научного творчества.

Письменная работа состоит из титульного листа, плана, введения, основной части не менее чем из трех пунктов, заключения и списка исполь-

зованной литературы. Введение пишется в последнюю очередь и является кратким изложением положений всей работы. Введение лучше начинать с оценки актуальности, разработанности темы. Резюме по исследуемой области знания в рамках учебной дисциплины. Допускается упоминание полученных выводов (результатов).

В заключении формулируется итоговый вывод, указывается на возможность и направление дальнейших исследований. Развитие результатов письменной работы происходит уже за пределами учебного процесса, в рамках НИРС (научно-исследовательской деятельности студентов), результаты представляются на студенческих научных конференциях и публикуются в сборниках научных трудов. В последнее время количество публикаций – более значимый критерий, чем успеваемость, средний балл оценок.

Информационные технологии уже достигли такого уровня, когда все учебные работы могут размещаться в файловых хранилищах и, возможно, смогут выступать в роли уже формального приложения к диплому, характеризующая уровень подготовки выпускников, наряду с вкладом к диплому, где перечисляются изученные дисциплины и полученные оценки.

## ПРИМЕРНЫЕ ТЕМЫ КОНТРОЛЬНЫХ РАБОТ

1. Киберправо как подотрасль информационного права.
2. Информация как объект правоотношений.
3. Хартия информационного общества.
4. Субъекты информационных правоотношений.
5. Объекты информационных правоотношений.
6. Содержание информационных правоотношений.
7. Институт права на информацию.
8. Источники информационного права.
9. Правовое содержание понятий «информационные технологии» и «информационные системы».
10. Правовые информационные системы.
11. Владелец информации и его правовая характеристика.
12. Права и обязанности организатора распространения информации в сети Интернет.
13. Права и обязанности оператора информационной системы.
14. Права и обязанности владельца сайта и (или) страницы сайта в сети Интернет.
15. Права и обязанности оператора поисковой системы .
16. Права и обязанности владельца новостного агрегатора.
17. Права и обязанности владельца аудиовизуального сервиса.
18. Права и обязанности владельца социальной сети.
19. Права и обязанности провайдера хостинга.
20. Информационные технологии: правовой аспект.
21. Информационная система: правовой аспект.
22. Информационно-телекоммуникационная сеть как объект правового регулирования.
23. Единая система идентификации и аутентификации.
24. Правовое обеспечение доступа в сеть Интернет.



25. Правовое обеспечение деятельности в сети Интернет.
26. Правовое обеспечение предпринимательской деятельности в сети Интернет.
27. Правовое обеспечение образовательной деятельности в сети Интернет.
28. Государственное регулирование в сфере применения информационных технологий.
29. Правовое обеспечение информационной безопасности детей.
30. Единый реестр российских программ для электронных вычислительных машин и баз данных.
31. Документированная информация и ее виды.
32. Конфиденциальность информации.
33. Идентификация и аутентификация.
34. Правовое обеспечение цифровой экономики.
35. Правовое обеспечение предпринимательства в сети Интернет.
36. Цифровой бизнес и его правовое обеспечение.
37. Цифровые права.
38. Цифровая валюта.
39. Цифровые финансовые активы.
40. Утилитарные цифровые права.
41. Инвестиционные платформы.
42. Права и обязанности оператора инвестиционной платформы.
43. Права и ответственность участников инвестиционной платформы.
44. Услуги инвестиционной платформы: виды и содержание.
45. Договоры, заключаемые на инвестиционной платформе: правовое обеспечение.
46. Ответственность и подконтрольность инвестиционной платформы.
47. Кибербезопасность.
48. Киберпреступность и средства противодействия.

49. Кибертерроризм и средства противодействия.
50. Информационная безопасность Российской Федерации.
51. Информационная инфраструктура Российской Федерации.
52. Персональные данные и обеспечение их сохранности и защищенности.
53. Правовые аспекты защиты тайн (государственной, банковской, коммерческой, медицинской, личной, семейной).
54. Виды юридической ответственности в информационной сфере.
55. Уголовная ответственность в сфере компьютерной информации.
56. Административная ответственность в области связи и информации.
57. Гражданско-правовая ответственность в цифровой сфере.
58. Дисциплинарная ответственность информационных работников.
59. Правоохранительные и специальные органы в сфере связи и информации.
60. Международное сотрудничество по противодействию преступлениям в сфере информационных технологий.

## СПИСОК СОКРАЩЕНИЙ

ГК РФ – Гражданский кодекс Российской Федерации.

УК РФ – Уголовный кодекс Российской Федерации.

КоАП – Кодекс об административных правонарушениях.

ООН – Организация объединенных наций.

ШОС – Шанхайская организация сотрудничества.

ЦФА – Цифровые финансовые активы.

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ИТ – Информационные технологии.

ИРО – Первичное размещение бумаг, форма получения инвестиций на фондовом рынке.

ИСО–Первичное размещение коинов (токенов), форма получения финансирования на цифровых инвестиционных платформах.

149-ФЗ – Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г. № 149-ФЗ.

152-ФЗ – Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

259-ФЗ (2019) – Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» от 02.08.2019 г. № 259-ФЗ.

259-ФЗ (2020) – Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. № 259-ФЗ.

## СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.).
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11. 1994 г. № 51-ФЗ.
3. Гражданский кодекс Российской Федерации (часть вторая) от 26.01 1996 г. № 14-ФЗ.
4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 г. № 230-ФЗ.
5. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 г. № 195-ФЗ.
6. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
7. Закон РФ от 21.07.1993 г. № 5485-1 «О государственной тайне».
8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
9. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
10. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» от 02.08.2019 г. № 259-ФЗ.
12. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. № 259-ФЗ.
13. Федеральный закон от 26.12.1995 г. № 208-ФЗ (ред. от 31.07.2020 г., с изм. от 24.02.2021 г.) «Об акционерных обществах» (с изм. и доп., вступ. в силу с 01.01.2021 г.).
14. Федеральный закон от 25.02.1999 г. № 39-ФЗ (ред. от 08.12.2020 г.) «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений».
15. Федеральный закон от 22 апреля 1996 года г. № 39-ФЗ «О рынке ценных бумаг».
16. Федеральный закон «О защите прав и законных интересов инвесторов на рынке ценных бумаг» от 5 марта 1999 г. № 46-ФЗ.
17. Федеральный закон «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22.12.2008 г. № 262-ФЗ.
18. Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02.2009 г. № 8-ФЗ.
19. Федеральный закон «О рекламе» от 13.03.2006 г. № 38-ФЗ.
20. Федеральный закон «О несостоятельности (банкротстве)» от 26.10.2002 г. № 127-ФЗ.
21. Федеральный закон «Об исполнительном производстве» от 02.10.2007 г. № 229-ФЗ.
22. Федерального закона от 5 марта 1999 года г. № 46-ФЗ «О защите прав и законных интересов инвесторов на рынке ценных бумаг».
23. Федеральный закон от 26.12.1995 г. № 208-ФЗ «Об акционерных обществах».
24. Федеральный закон от 25.02.1999 г. № 39-ФЗ «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений».
25. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг».
26. «Всеобщая декларация прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948 г.).

27. «Окинавская хартия глобального информационного общества» (подписана 22 июля 2000 г. лидерами стран «Большой восьмерки»).
28. *Архипов, В. В.* Интернет-право: учебник и практикум для бакалавриата и магистратуры/ В. В. Архипов. — М.: Юрайт, 2018. — 249 с.
29. *Бачило, И. Л.* Информационное право: учебник для академического бакалавриата/ И. Л. Бачило. — 5-е изд., перераб. и доп. — М.: Юрайт, 2018. — 419 с.
30. *Рассолов, И. М.* Информационное право: учебник и практикум для академического бакалавриата / И. М. Рассолов. — 5-е изд., перераб. и доп. — М.: Юрайт, 2018. — 347 с.
31. *Леонтьев, А. Н.* Государственное и общественное регулирование рекламно-информационной деятельности [Текст]: учеб. пособие/ А. Н. Леонтьев; ВолгГТУ. - Волгоград, 2013. - 31, [2] с.
32. *Леонтьев, А. Н.* Информационное право [Текст]: учеб. пособие/ А. Н. Леонтьев; ВолгГТУ. - Волгоград, 2019. - 74, [2] с.
33. *Леонтьев, А. Н.* Основы правовых знаний [Электронный ресурс]: учеб. пособие/ А. Н. Леонтьев; ВолгГТУ. - Волгоград, 2016. - 64 с.
34. *Леонтьев, А. Н.* Правовое обеспечение инженерной деятельности [Текст]: учеб. пособие/ А. Н. Леонтьев; ВолгГТУ. - Волгоград, 2015. - 64 с.
35. *Леонтьев, А. Н.* Правовые аспекты научного творчества: учеб. пособие/ А. Н. Леонтьев; ВолгГТУ. - Волгоград, 2015. - 64 с.
36. *Леонтьев, А. Н.* Теоретические основания создания информационного общества: учеб. пособие/ А. Н. Леонтьев, П. В. Терелянский; ВолгГТУ. - Волгоград, 2013. - 31 с.
37. *Леонтьев, А. Н.* Хозяйственное право [Текст]: учеб. пособие/ А. Н. Леонтьев [и др.]; ВолгГТУ. - Волгоград, 2014. - 57, [2] с.
38. Справочная правовая система «Гарант». – Режим доступа: <https://www.garant.ru>
39. Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>
40. Справочно-правовая система «Право.ру». – Режим доступа: <https://pravo.ru/>
41. Информационно-правовая система «Законодательство России». – Режим доступа: <http://pravo.gov.ru/>
42. Справочно-правовая система «Кодекс». – Режим доступа: <http://kodeks.ru/>
43. Электронный фонд правовых и нормативно-технических документов. – Режим доступа: <http://docs.cntd.ru/>
44. Электронно-библиотечная система издательства «Лань». – Режим доступа: <https://e.lanbook.com>
45. Электронно-библиотечная система издательства «Юрайт». – Режим доступа: <https://urait.ru>
46. Научная электронная библиотека. – Режим доступа: <https://www.elibrary.ru/>
47. Научная электронная библиотека «КиберЛенинка». – Режим доступа: <https://cyberleninka.ru/>
48. Национальная электронная библиотека. – Режим доступа: <https://rusneb.ru>
49. Электронная библиотека Российской Национальной библиотеки. – Режим доступа: <http://nlr.ru/elibrary>
50. Университетская информационная система (УИС Россия). – Режим доступа: <https://www.uisrussia.msu.ru>
51. Электронно-библиотечная система «Университетская библиотека онлайн». – Режим доступа: <https://biblioclub.ru/>
52. Информационно-библиотечный центр ВолгГТУ. – Режим доступа: <http://library.vstu.ru/>

## ОГЛАВЛЕНИЕ

Введение.....	3
Раздел 1. Теоретические материалы.....	6
Тема 1. Киберправо – подотрасль информационного права.....	6
Контрольные вопросы.....	12
Тема 2. Конституционные гарантии информационных прав.....	12
Контрольные вопросы.....	18
Тема 3. Объекты, субъекты и содержание правоотношений в цифровой сфере....	19
Контрольные вопросы.....	26
Тема 4. Государственное регулирование в сфере применения информационных технологий.....	27
Контрольные вопросы.....	32
Тема 5. Правовое обеспечение цифровой экономики.....	33
Контрольные вопросы.....	48
Тема 6. Интеллектуальная собственность в цифровом пространстве.....	48
Контрольные вопросы.....	57
Тема 7. Правовое обеспечение кибербезопасности.....	57
Контрольные вопросы.....	61
Тема 8. Юридическая ответственность в информационной сфере.....	61
Контрольные вопросы.....	65
Раздел 2. Подготовка к практическим занятиям.....	66
Раздел 3. Подготовка контрольной работы.....	69
Примерные темы контрольных работ.....	71
Список сокращений.....	74
Список рекомендуемой литературы.....	75

Учебное издание

Александр Николаевич **Леонтьев**

## **КИБЕРПРАВО**

*Учебное пособие*

Редактор *Е. В. Кравцова*

Темплан 2021 г. (учебники и учебные пособия). Поз. № 29.  
Подписано в печать 9.07.2021 г. Формат 60×84 1/16. Бумага газетная.  
Гарнитура Times. Печать офсетная. Усл. печ. л. 4,65. Уч.-изд. л. 3,93.  
Тираж 100 экз. Заказ .

Волгоградский государственный технический университет  
400005, г. Волгоград, пр. Ленина, 28, корп. 1.

Отпечатано в типографии Издательства ВолгГТУ  
400005, г. Волгоград, пр. Ленина, 28, корп. 7.